

MEGA Administration-Supervisor

Web Administrator Guide



Information in this document is subject to change and does not represent a commitment on the part of MEGA International.

No part of this document is to be reproduced, transmitted, stored in a retrieval system, or translated into any language in any form by any means, without the prior written permission of MEGA International.

© MEGA International, Paris, 1996 - 2019

All rights reserved.

HOPEX is a registered trademark of MEGA International.

Windows is a registered trademark of Microsoft Corporation.

The other trademarks mentioned in this document belong to their respective owners.

CONTENTS



Contents	1
-----------------------	----------

About HOPEX Administration	9
Presentation of this Guide	10
HOPEX Structure.	11

Web Administration Desktop	13
Connecting to the Administration Desktop.	14
Administration Desktop Description.	17
<i>Toolbar.</i>	<i>17</i>
<i>Navigation panes and trees.</i>	<i>19</i>
<i>Edit area.</i>	<i>21</i>

Managing Users	23
Actions to be Performed to Define a User	24
Before Defining a User: Profile and Person Group Concepts.	24
Compulsory Actions to be Performed to Define a User	25
Compulsory Actions to be Performed to Define a User Group.	26
Optional Actions to be Performed to Define a User	26
Other Actions to Set or Manage a User	27
Checking the Configuration of Persons	27
Introduction to Profile Management	28
Description of a Profile	28
<i>Definition of the profile.</i>	<i>28</i>

Profile assignment	29
Connection Diagrams	29
Connection diagram (with WET)	29
Connection diagram (without WET).	31
The Administration Profiles Provided	32
HOPEX Administrator profile	33
HOPEX Administrator - Production profile	34
User Management Web Administrator profile	35
Functional Administrator profile of a Solution.	35
Profile Properties	36
Name	36
Products accessible on the license (Command Line)	36
Assignable.	37
Administrator profile.	37
Set of UI access rights	37
Tiles Homepage (WET)	38
Profile display	38
Profile status	38
_GUIName.	38
MetaPicture	38
Persons and Person Groups	38
Working Environment Template (WET)	38
Available applications	39
Available desktops	39
Assignable profiles	39
Terminology.	39
Available types.	39
Introduction to User Management	40
Users Delivered	41
User: Definition	41
Person Properties	42
Name	42
Image.	42
E-mail.	42
Phone number and initials	42
Data language	43
Default library	43
Person reading access area and reading access area at creation	43
Person writing access area and writing access area at creation	43
Login	43
Belongs to a Person Group.	44
Assignments - Profile Assignments	44
Object assignments	44
Person Login Properties	45
User code	45
Login Holder	45
Status (Login)	45
Products accessible on the license (Command Line)	45
Authentication mode (case of authentication managed within HOPEX)	45
LDAP server.	46
Introduction to Person Group Management	47
Managing Person Groups Rather than Persons	48

Belonging to a Person Group	49
User Groups Delivered	49
Person Group Properties	49
Name	50
Person group writing access area and writing access area at creation	50
Person group reading access area and reading access area at creation.	50
Login	50
Default connection group	50
Person group types	51
Persons	52
Data language.	52
Assignments - Profile	52
Properties of a Person Group Login.	52
User code	52
Login Holder	53
Inactive person group (Status)	53
Command line.	53
Authentication mode (case of authentication managed within HOPEX)	53
LDAP server	54
Managing Profiles.	55
Viewing Profile Characteristics	55
Customizing the UI Access (Permissions) of an Existing Profile	56
Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile	57
Creating a Profile	57
Configuring a Profile	59
Configuring profile characteristics	60
Assigning a WET to a profile	60
Defining the applications accessible to the users of a profile (non WET-based configuration)	62
Defining the application desktops accessible to the users of a profile (non WET-based configuration)	62
Associating a terminology with a profile	63
Defining the object types available for a profile	64
Checking a Profile Compliancy with Connection Regulation	65
Assigning a profile to a person.	65
Assigning a profile to a person	66
Performing a Mass Profile Assignment to Persons	66
Mass assignment of profiles to persons.	67
Assigning a profile to a person group	67
Assigning a profile to a person group	68
Performing a mass profile assignment to person groups	68
Performing a mass assignment of profiles to a person group.	69
Deleting a Profile	69
Access to User Management.	70
Accessing the User Management Pages.	70
Managing persons who have an identical characteristic	71
Managing a group of persons who have a specific characteristic	71
Actions performed from the Persons management page	72
Actions performed from the Person Group page.	73
Accessing the list of persons who have the same profile assigned	73
Accessing the list of person who belong to the same group.	73

<i>Accessing the list of persons connected to a specific writing access area</i>	74
<i>Accessing the list of persons connected to a specific reading access area</i>	74
<i>Accessing the list of persons who have or do not have a login</i>	74
<i>Accessing a person using his/her name</i>	75
<i>Accessing a group of persons connected to a specific profile</i>	75
<i>Accessing the list of person groups connected to a specific writing access area</i>	75
<i>Accessing the list of person groups connected to a specific reading access area</i>	75
Viewing the Person Characteristics	76
Viewing the Person Group Characteristics	78
Viewing the Login Characteristics	79
Creating and Managing Users	81
Creating Users	81
Defining a Person	83
Creating the Login of a Person	85
Defining the Login of a Person	86
Modifying User Properties	88
Connecting a Person to a Writing Access Area	88
Connecting a Person to a Reading Access Area	89
Preventing User Connection	89
Deleting a User	90
Creating and Managing a Person Group	91
Creating a Person Group	91
Defining a Person Group	92
<i>Adding one or more persons to a person group</i>	93
<i>Defining a dynamic person group (LDAP or SSO type)</i>	93
<i>Defining a dynamic person group with a Macro</i>	94
<i>Defining a default connection group</i>	94
Connecting a Person Group to a Writing Access Area	95
Connecting a Person Group to a Reading Access Area	95
Modifying the Login of a Person Group	96
Modifying User Group Properties	97
Preventing User Group Connection	97
Deleting a Person Group	97
Managing User Options	99
Configuring the Metamodel Access	99
Prohibiting the Administrator from Modifying User Options	100
Authorizing Deletion of a Dispatched Object	100
Authorizing HOPEX Data Modification	100
Making a Comment Mandatory on Dispatch	100
Managing User Inactivity	101
<i>Activating/Deactivating user inactivity management</i>	101
<i>Managing user inactivity</i>	101
Authentication in HOPEX (Web Front-End)	102
Authentication and Mapping Principle	103
Introduction to Authentication in HOPEX (Web Front-End)	103
<i>Choosing an authentication mode</i>	104
<i>Defining an external authentication mode</i>	104
Defining Default HOPEX Authentication Mode	105
<i>Viewing default authentication mode</i>	105
<i>Defining default authentication mode to LDAP</i>	105
<i>Modifying a user authentication mode</i>	106
Authentication Group	107

Authentication groups	107
Defining an authentication group	108
Configuring LDAP Authentication	108
Accessing LDAP server management	109
Creating an LDAP server	109
Configuring the LDAP server	109
Configuring an LDAP parameter	111
Modifying LDAP directory import content	113
Checking the configuration of an LDAP server	114
Importing persons from an LDAP server	114
Authentication and a user created on the fly	115
Configuring SSO Authentication	115
The claims	115
Configuring SSO Authentication	116
Modifying the claim used for mapping authentication groups	117
Mapping	118
Mapping Diagram	118
Principle	120
Connection request and user created on the fly	120
Associating a HOPEX user group with an authenticated user group	121
Defining an Authentication Parameter	122
Managing the Password of a Web User	125
Initializing a User Web Account	125
Modifying the Lifetime of the First Connection Link	126
Modifying Password Management Configuration	126
Reinitializing a User Password	127
Defining a Temporary Password to a User	127
Specifying the Data Language	129
Managing Business Roles	130
Business Role Properties	130
Name	130
MetaPicture	130
_GUIName	130
Multiplicity	131
Creating Business Roles	131
Configuring a Business Role	131
Defining a Business Role	132
Assigning a Business Role to a Person	134
Assigning an object to a person	134
Mass assignment of objects to persons	135
Transferring Responsibilities to a Person	135
Duplicate the Responsibilities of a Person	136
Deleting a Business Role	137
 Managing workspaces	 139
Private Workspace Principle	140
Private workspace	140
Collaborative Workspace	141

Using Your Private Workspace	142
Connecting to a HOPEX Desktop	142
Saving Sessions	144
HOPEX Repository State Changes	145
Dispatching Your Work	145
Dispatch Conflicts	146
<i>Creation of duplicated objects</i>	146
<i>Deletion of already deleted objects or links</i>	147
<i>Modifying or linking a renamed object.</i>	147
Rejects When Dispatching	147
<i>Change in writing access values between opening and dispatching a private workspace</i>	147
<i>Rename/create collisions.</i>	147
<i>Verifying link uniqueness.</i>	147
<i>Attribute uniqueness (other than name)</i>	148
<i>Updating a deleted object</i>	148
Refreshing Data	148
Conflicts When Refreshing	150
Discarding Work	150
<i>Discarding work from a private workspace.</i>	151
<i>Discarding work performed in a collaborative workspace.</i>	151
Exiting a Session	151
<i>Exiting a session from a private workspace</i>	152
<i>Exiting a session from a collaborative workspace</i>	153
Workspace Administration	154
Accessing the Management Page for Workspaces	154
Deleting a Workspace	155
Private Workspace Life: Example	157
<i>Private workspace 1</i>	157
<i>Private workspace 2</i>	157
<i>Private workspace 3</i>	158
<i>Private workspace 4</i>	158
<i>Private workspace 5</i>	159
<i>Private workspace 6</i>	159
Performance and Health Tests	160
Test Description	160
<i>Infrastructure performance test description</i>	160
<i>Repository health test description.</i>	160
Viewing the HOPEX Health Report	161
<i>Accessing HOPEX daily health reports</i>	161
<i>HOPEX Health report description</i>	164
Managing Updates.	165
Displaying Updates Made in the Repository	165
Private Workspaces and Repository Size	166
<i>Private workspace life</i>	166
<i>Private workspace monitoring</i>	166
<i>Modifying the maximum duration of a private workspace</i>	167
Exporting a Private Workspace Log	167
Managing locks	169
Principle.	169
<i>Preventing conflicts.</i>	169
<i>Deleting a lock or unlocking an object.</i>	169
<i>Details on the operating method of the locks</i>	169

Managing Locks on Objects	170
<i>Viewing locks on objects.</i>	171
<i>Managing immutable locks on objects</i>	172

Managing objects 173

Importing - exporting a command file 174

Importing a command file in HOPEX	174
Exporting Objects	176

Comparing and Aligning Objects Between Repositories 178

Compare and Align Principle	178
Compare and Align Warnings	178
<i>Repository log</i>	179
<i>Users</i>	179
<i>Reading (confidentiality) and writing access levels.</i>	179
Compare and Align	179

Managing UI Access (Permissions) 183

Introduction to UI Access Management (Permissions)	183
<i>Prerequisites and definitions</i>	183
<i>Accessing the UI Access Management Pages (Permission)</i>	183
Object UI Access Values	184
<i>MetaClass occurrence access permissions</i>	184
<i>MetaAssociationEnd access permissions</i>	184
<i>MetaAttribute access permissions</i>	185
<i>Permissions on a tool</i>	185
Managing UI Access	185
<i>Modifying access permissions on occurrences of a MetaClass</i>	188
<i>Modifying access permissions on MetaAttributes of a MetaClass</i>	191
<i>Modifying access permissions on tools of a MetaClass</i>	191
<i>Modifying access permissions of a link around a MetaClass</i>	192
<i>Modifying access permissions on links around a MetaClass</i>	193
<i>Rules on permissions while aggregating Sets of UI access rights</i>	194
Generating a Report on Permissions by Profile	194
<i>Generating a report on permissions</i>	194
<i>Report content</i>	195
Managing General UI Access	195

Managing Options. 199

Options Overview 200

Accessing Options. 202

Options Level	202
<i>Modifying options at environment level.</i>	202
<i>Modifying options at profile level</i>	202
<i>Modifying options at user level</i>	202
Option Inheritance	203

Modifying an option value	203
Reinitializing the value of an option	203
Controlling modification of the Options	203
Option Groups (User Level)	204
Installation	204
Data Exchange	204
Documentation	204
Repository	204
Queries	204
Languages	204
Text Editing	204
Diagrams/Edit Shapes	204
Status indicators	204
Collaborative Environment	204
Mapping Editor	205
Modeling and Methods Regulations	205
Business Process and Architecture Modeling	205
Simulation	205
Compatibility	205
Technical Support	205
Monitoring	205
Web Application-Linked Options	206
Installation Options	206
Specifying the Web application access path	206
Specifying SMTP configuration	206
Network Quality Test Option (Browser and Connection)	208
Displaying the network quality test report	208
Removing access to the network quality test report	208
Managing Languages in Web Applications	210
Modifying the interface language in Web applications at environment level	210
Modifying the data language in Web applications at environment level	210
Managing Date Format	211
Glossary	215

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** or **HOPEX Power Supervisor**). 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).

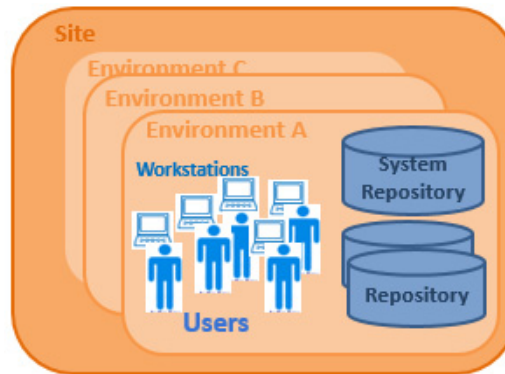
 To perform **HOPEX** administration tasks from the **HOPEX Administration** application (Windows Front-End), see the *HOPEX Administration - Supervisor* guide.

The following points are covered here:

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

HOPEX STRUCTURE

Some basic knowledge is required to understand the architecture and operation of **HOPEX**.



HOPEX (Web Front-End) is organized on the following levels:

- **site**
A site groups together everything that is shared by all **HOPEX** users on the same local network: the programs, standard configuration files, online help files, standard shapes, workstation installation programs, and version upgrade programs.
- **environment**
An environment groups a set of users, the repositories on which they can work, and the system repository. It is where user private workspaces, users, system data, etc. are managed.
- **user**
A user is a person (or person group) with a login. 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](#)
- ✓ [Administration Desktop Description](#)

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](#).

☛ 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.

3. In the **Password** field, enter your password.

☛ If you have lost your password, click **Forgot Password**, see [Resetting Your Password](#).

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 drop-down menu for groups, select the group with which you want to connect or "My assignments" to connect with one of your own assignments.
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](#)
 - ☛ 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 with the profile selected, you can only access the **Administration (Web Front-End)** application, 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.

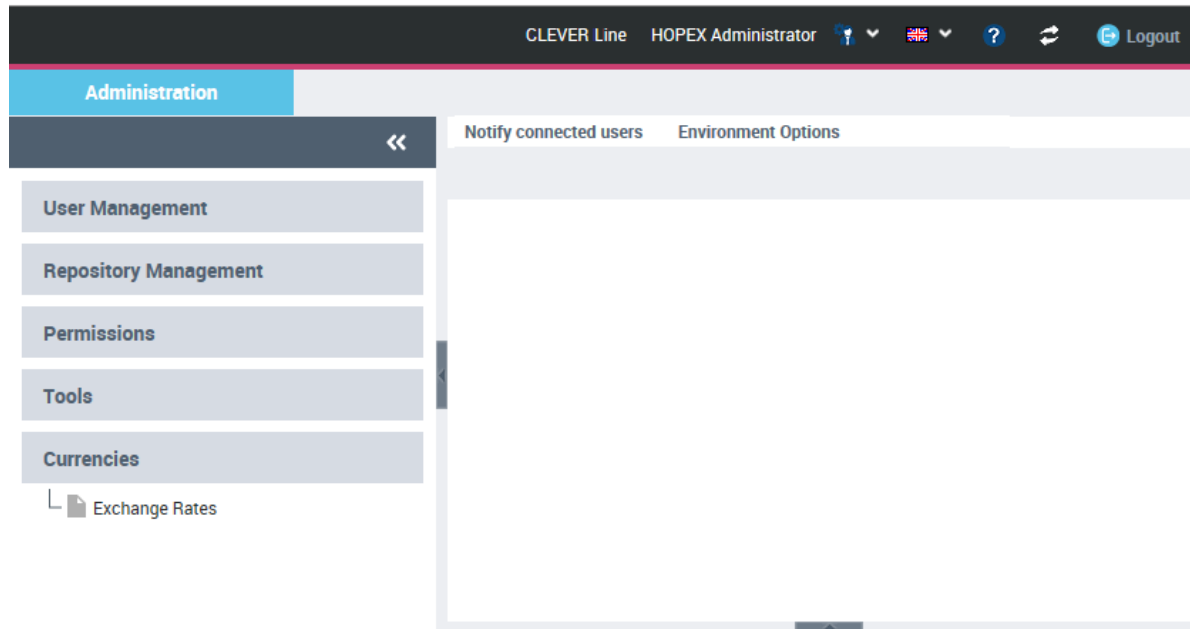
The screenshot shows a login interface with the following elements:

- A dropdown menu for groups with "SOHO" selected.
- A dropdown menu for profiles with "HOPEX Administrator" selected.
- A checkbox labeled "I have read and accept the privacy policy" which is checked.
- A large blue button labeled "LOGIN »".
- Two buttons at the bottom: "<< BACK" and "PRIVACY POLICY".

11. Click **LOGIN**.

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

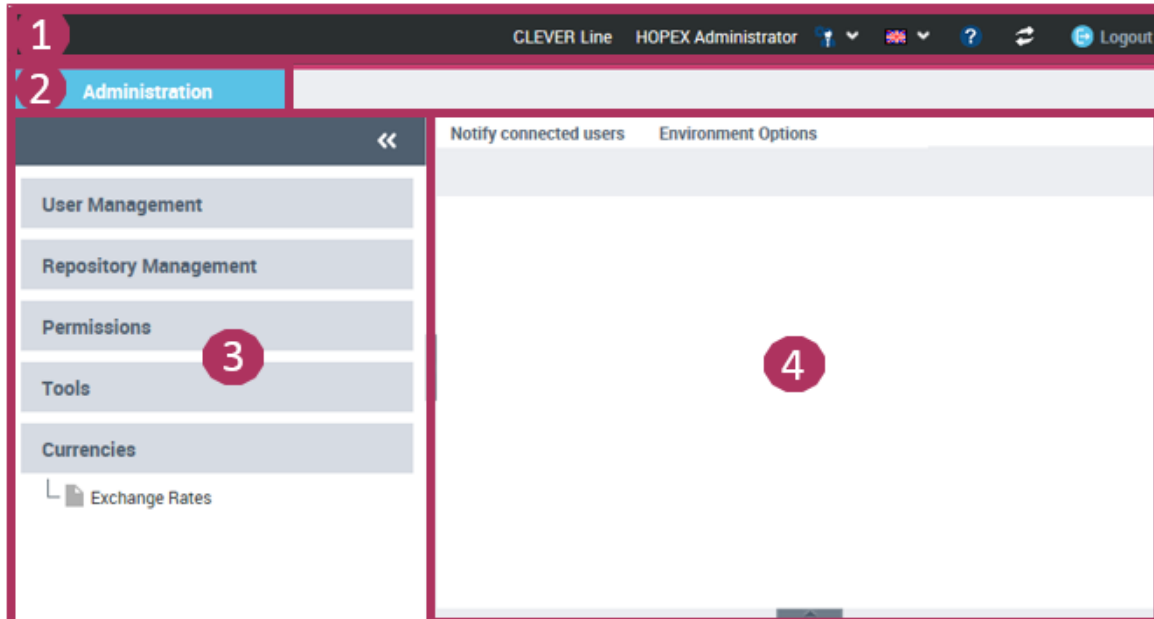
The **Administration** desktop appears and the session is opened.



➡ See [Administration Desktop Description](#).

ADMINISTRATION DESKTOP DESCRIPTION

To access the **Administration** desktop, see [Connecting to the Administration Desktop](#).



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

The **Administration** desktop includes:

- a toolbar.
➤ See [Toolbar](#).
- an **Administration** tab that contains panes and trees to select the objects to manage.
➤ See [Navigation panes and trees](#).
- an edit area to manage objects.
➤ See [Edit area](#).

Toolbar



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

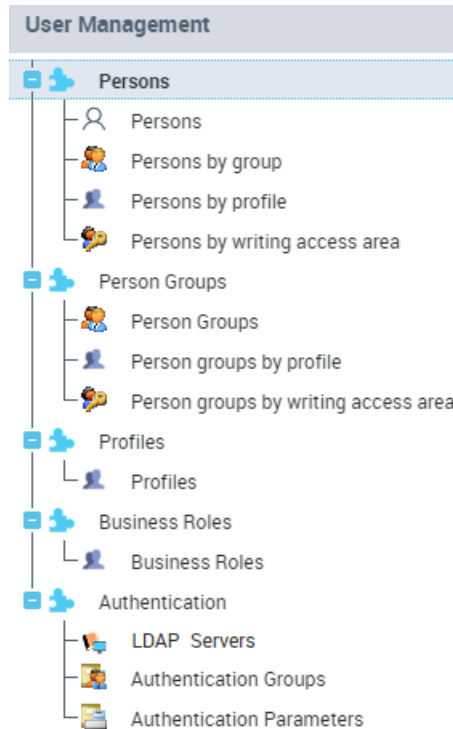
From the **Administration** desktop toolbar, you can:

- 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 [Option Groups \(User Level\)](#).*
 - 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
 - display the test report regarding your browser performance and network connexion
 - ☛ *See [Network Quality Test Option \(Browser and Connection\)](#).*
 - reinitialize your personal parameters
 - ☛ *See the **HOPEX Common Features** guide - Resetting Customizing to Your Desktop section.*
- access the documentation
- modify the interface data language 
 - ☛ *To manage languages, see [Managing Languages in Web Applications](#).*
- access online documentation 
- update your desktop 
- disconnect from the **Administration** desktop .

Navigation panes and trees

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

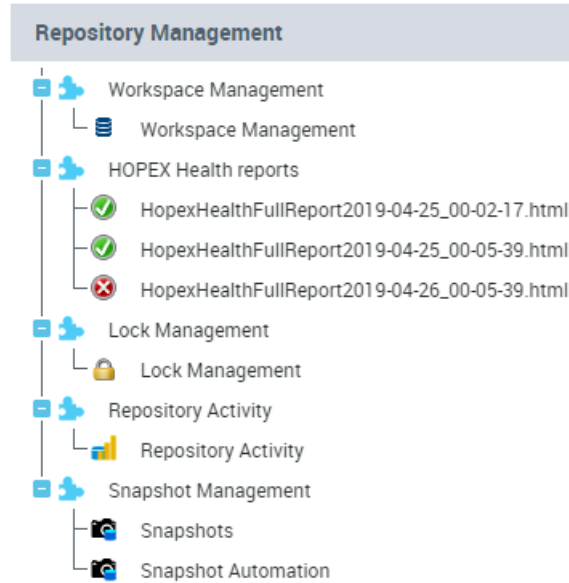
- **User Management** to manage *users*:



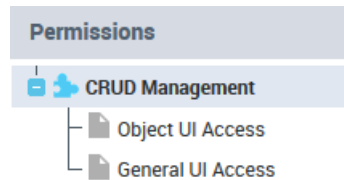
- *persons*
 - ☞ The **Persons by reading access area** sub-folder is available if reading access management is activated.
- *person groups*
 - ☞ The **Person groups by reading access area** sub-folder is available if management of reading access is activated.
- *profiles*
- *business roles*
- *authentication*
 - ☞ The **LDAP servers** folder is available only if LDAP authentication is the user default authentication mode, see [Defining default](#)

authentication mode to LDAP.

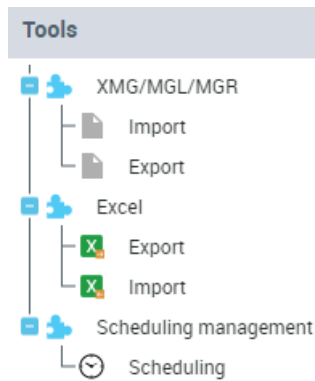
- **Repository management** to:
 - manage the *workspaces*, the *locks*, the *repository* and the *snapshots*
 - access the repository health reports



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



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



- **Currency** to manage exchange rates.

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

Edit area

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

You can:

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

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:

The big picture

- ✓ [Actions to be Performed to Define a User](#)

Introduction

- ✓ [Introduction to Profile Management](#)
- ✓ [Introduction to User Management](#)
- ✓ [Introduction to Person Group Management](#)

Management

- ✓ [Managing Profiles](#) (available with HOPEX Power Supervisor)
- ✓ [Access to User Management](#)
- ✓ [Creating and Managing Users](#)
- ✓ [Creating and Managing a Person Group](#)
- ✓ [Managing User Options](#)
- ✓ [Authentication in HOPEX \(Web Front-End\)](#)
- ✓ [Mapping](#)
- ✓ [Managing the Password of a Web User](#)
- ✓ [Specifying the Data Language](#)
- ✓ [Managing Business Roles](#)

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](#)
- [Compulsory Actions to be Performed to Define a User](#)
- [Compulsory Actions to be Performed to Define a User Group](#)
- [Optional Actions to be Performed to Define a User](#)
- [Other Actions to Set or Manage a User](#)
- [Checking the Configuration of Persons](#)

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](#).



See [Creating a Person Group](#).

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

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

This profile defines:

- the products accessible



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



See [Products accessible on the license \(Command Line\)](#).

- the desktops to which the user can access.



See [Connection Diagrams](#).

- the UI access rights (permissions) of the user

Assigning a profile to a person defines:

- ☛ See [Assigning a profile to a person](#).
- the repository concerned by the assignment
- the person's access rights to repositories with this profile assignment
- (optional) the validity period of the assignment

Compulsory Actions to 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](#).
- 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](#).
 - The login of the user is created automatically on creation of the person, see [Creating Users](#) (If necessary, see [Creating the Login of a Person](#)).*
 - The login status must be active so the person can connect, see [Status \(Login\)](#).*
- (highly recommended for a Web user) define 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.
 - ☛ See [Creating Users](#).
 - ☛ See [Defining a Person](#).
 - ☛ See also [Specifying SMTP configuration](#).
- (mandatory for a Web user) initialize the user Web account, so that the user can create his/her password.
 - ☛ See [Initializing a User Web Account](#).
 - With Unified Authentication System (UAS), the **HOPEX authentication**, system, a user needs a password for the Web connection.*
 - If the user does not have an email address, see [Defining a Temporary Password to a User](#).*
- 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](#).

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](#).
- 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](#).*
 - ☛ See [Modifying the Login of a Person Group](#).
- 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](#).
 - ☛ See [Performing a mass assignment of profiles to a person group](#).

See [Defining a Person Group](#).

See also the authentication in the case of a person group, [Authentication Group](#).

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
 - ☛ *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](#).
- (where writing access management is activated) define the writing access area of the user
 - ☛ See [Defining a Person](#).
 - ☛ See [Connecting a Person to a Writing Access Area](#).
- (where reading access management is activated) define the reading access area of the user
 - ☛ See [Defining a Person](#).
 - ☛ See [Connecting a Person to a Reading Access Area](#).
- define if the person belongs to a person group.
 - ☛ See [Defining a Person](#).

Other Actions to Set or Manage a User

You can:

- define the telephone number and initials of the person
✎ See [Defining a Person](#).
- define the data language of the Web user
✎ See [Defining a Person](#).
- restrict user access to certain products
✎ The products accessible to this user are at the intersection of the values of the **Command Line** attribute of the user login and profile.
✎ See [Defining the Login of a Person](#).
✎ See [Configuring a Profile](#).
- modify user authentication mode
✎ See [Defining the Login of a Person](#).
- make the user inactive.
✎ See [Defining the Login of a Person](#).
✎ See [Preventing User Connection](#).

Checking the Configuration of 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](#).
2. Select the **Persons** or **Person Group** sub-folder.
3. In the list of persons, select the persons whose configuration you want to check.
✎ If you do not select a person, the check takes place on all the persons listed in all the pages.
4. In the edit area, click **Check** .
✎ If the button is hidden, click  to access it.

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

INTRODUCTION TO PROFILE MANAGEMENT

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

See:

- [Description of a Profile](#)
- [Connection Diagrams](#)
- [The Administration Profiles Provided](#)
- [Profile Properties](#)

Description of a Profile

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

➡ See [Viewing Profile Characteristics](#).

The description of a profile includes:

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

➡ See [Profile Properties](#).

Definition of the profile

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

Example: Application Portfolio Manager, Enterprise Architect).

The profile defines:

- the products accessible

➡ See [Products accessible on the license \(Command Line\)](#).

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

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

- the desktops to which the user can access.

➡ See [Connection Diagrams](#).

➡ See [Assigning a WET to a profile](#) or [Defining the applications accessible to the users of a profile \(non WET-based configuration\)](#).

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

➡ See [Managing UI Access](#).

Profile assignment

You must assign each person at least one profile so that this person can connect to **HOPEX**.

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

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

- the repository concerned by the assignment
- the person's data access rights (reading, writing) with this profile assignment
- (optional) the validity period of the assignment

☛ See [Assigning a profile to a person](#).

☛ See [Assigning a profile to a person group](#).

Connection Diagrams

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

Connection diagram (with WET)

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

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

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

- a login

☛ See [Creating Users](#).

☛ The login status must be active so the person can connect, see [Status \(Login\)](#).

- at least one profile

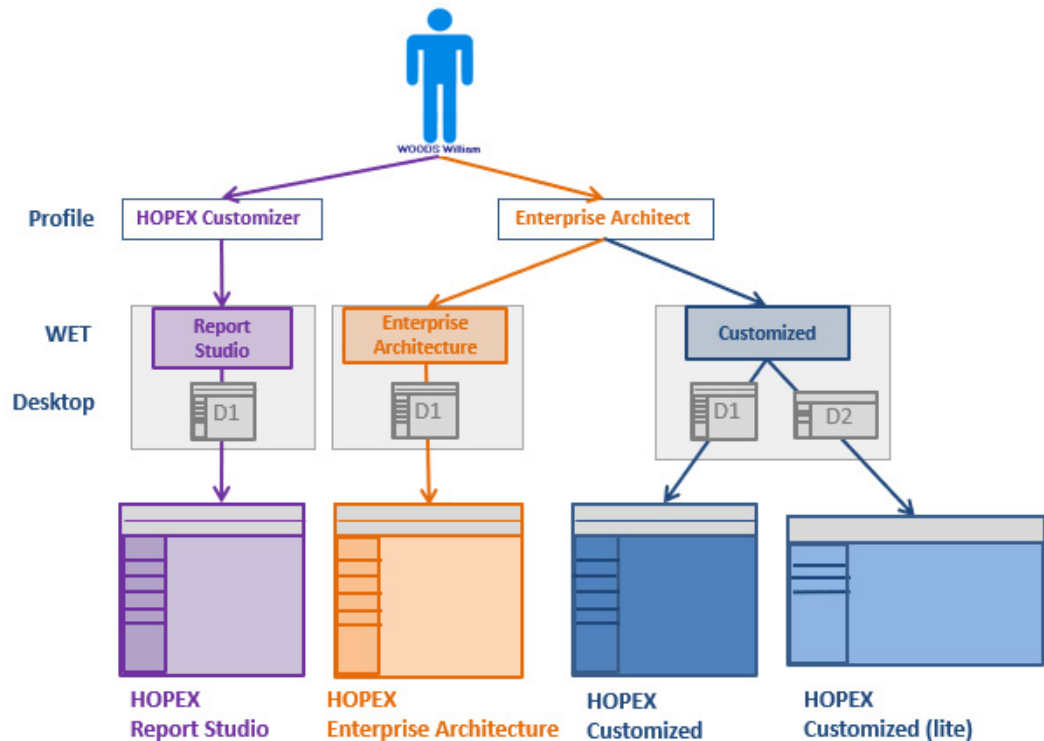
The profile gives access to one or several WET-based desktops.

☛ See [Assigning a profile to a person](#).

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

☛ See [Assigning a WET to a profile](#).

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



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

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

Connection diagram (without WET)

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

- a login
 - ☛ See [Creating Users](#).
 - ☛ The login status must be active so the person can connect, see [Status \(Login\)](#).
- at least one profile.
 - ☛ See [Assigning a profile to a person](#).

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

All desktops connected to the application are then accessible.

☛ To modify a profile supplied by **MEGA**, **MEGA** recommends you create a new profile, see [Customizing the UI Access \(Permissions\) of an](#)

Existing Profile.

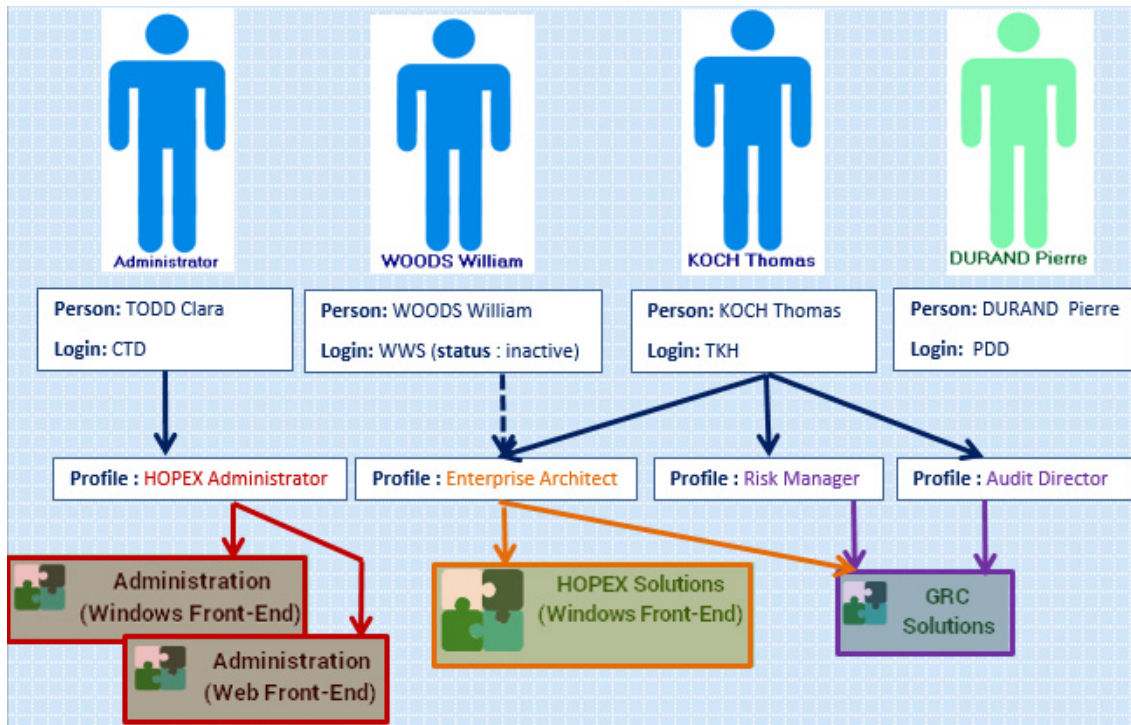
☛ To enable access to only certain desktops of the application, see [Restricting access to the desktops of an application](#).

Example:

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

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

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



In the previous example:

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

Restricting access to the desktops of an application

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

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

☛ To modify a profile provided by **MEGA**, you must have rights to modify **HOPEX** data. Alternatively, you can create a new profile, see [Customizing the UI Access \(Permissions\) of an Existing Profile](#).

- the application containing the desktops.

☛ See [Defining the applications accessible to the users of a profile \(non WET-based configuration\)](#).

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

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

Example:

P1 profile is connected to:

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

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

The Administration Profiles Provided

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

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

These profiles are dedicated to:

- global Administration, with exclusive access to **Administration** applications (Windows Front-End and Web Front-End):
HOPEX Administrator
 See [HOPEX Administrator profile](#).
- Administration (Web Front-End), with exclusive access to the **Web Administration** desktop:
 - **HOPEX Administrator - Production**
 See [HOPEX Administrator - Production profile](#).
 - **User Management Web Administrator**
 See [User Management Web Administrator profile](#).
- 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](#).

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

 See [Customizing the UI Access \(Permissions\) of an Existing Profile and Configuring a Profile](#).

HOPEX Administrator profile

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

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

- **Profiles**
 See [Managing Profiles](#).
- **users (Persons and Logins)**
 See [Creating and Managing Users](#).
- **User groups (Person groups and Logins)**
 (Web Front-End specific) A person group groups persons in a group. These persons share the same connection characteristics.
 See [Creating and Managing a Person Group](#).
- **Business Roles**
 See [Managing Business Roles](#).
- **Permissions**
 See [Managing UI Access \(Permissions\)](#).
- **Authentication**
 See [Authentication in HOPEX \(Web Front-End\)](#).

It also allows to perform tasks linked to:

- **Repository management:**
 - workspace management
 - ☞ See [Managing workspaces](#).
 - repository activity management
 - ☞ See [Managing Updates](#).
 - lock management
 - ☞ See [Managing locks](#).
 - snapshot management
 - ☞ To create a repository snapshot, see the **HOPEX Common Features - Repository Snapshots** guide.
- **Tools** such as:
 - XMG/MGL/MGR file import/export
 - ☞ See [Importing a command file in HOPEX](#).
 - ☞ See [Exporting Objects](#).
 - 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 in the **Web Administration** Desktop, without permission management rights.

User Management Web Administrator profile

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

- **users (Persons and Logins)**
 - 📖 A user is a person with a login.
 - ☞ See [Creating and Managing Users](#).
- **User groups (Person groups and Logins)**
 - 📖 (Web Front-End specific) A person group groups persons in a group. These persons share the same connection characteristics.
 - ☞ See [Creating and Managing a Person Group](#).
- **Business Roles**
 - ☞ See [Managing Business Roles](#).

It also gives access to management of:

- **Authentication**
 - ☞ See [Authentication in HOPEX \(Web Front-End\)](#).
- **Locks.**
 - ☞ See [Managing locks](#).

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](#).
 - users (**Persons** and **Logins**)
 - 📖 A user is a person with a login.
 - ☞ See [Creating and Managing Users](#).
 - **User groups** (**Person groups** and **Logins**)
 - 📖 (Web Front-End specific) A person group groups persons in a group. These persons share the same connection characteristics.
 - ☞ See [Creating and Managing a Person Group](#).
 - **Business Roles**
 - ☞ See [Managing Business Roles](#).
- It also gives access to:
- scheduler use
 - ☞ See [HOPEX Power Studio - Scheduler guide](#).
 - **Authentication** management.
 - ☞ See [Authentication in HOPEX \(Web Front-End\)](#).

Profile Properties

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

- ☞ See [Introduction to Profile Management](#).
- ☞ To assign a profile to a person or a person group, see [Assigning a profile to a person](#) and [Assigning a profile to a person group](#).
- ☞ To manage profiles, see [Managing Profiles](#).

Name

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

Products accessible on the license (Command Line)

😊 The command line of each profile is also described in the online documentation: [Concepts > Profiles](#).

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

Format of the command is:

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

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

HOPEX products. To authorize only HOPEX Business Process Analysis and HOPEX IT Portfolio Management modules to users that have this profile, enter:

/RW'HBPA;APM'

🔑 To determine the product code, see the online documentation: **Concepts > Products**.

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

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

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

Assignable

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

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

🔑 The default value is "No".

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".

Set of UI access rights

The **Set of UI Access Rights** attribute enables to define permissions associated with one or several profiles.

Tiles Homepage (WET)

The **Tiles Homepage** attribute enables to define the profile homepage, that is:

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

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

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

Profile display

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

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

- "always": the profile is provided at connection even if it is included in the definition of another profile,
 See [Customizing the UI Access \(Permissions\) of an Existing Profile](#).
- "If not included in another profile" (default value): the profile is provided at connection only if it is not included in another profile.

Profile status

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

_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.

Persons and Person Groups

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

Working Environment Template (WET)

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

➤ See [Assigning a WET to a profile](#).

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

Available applications

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

➤ See [Defining the applications accessible to the users of a profile \(non WET-based configuration\)](#).

Available desktops

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

➤ To restrict the desktops accessible, see [Defining the application desktops accessible to the users of a profile \(non WET-based configuration\)](#).

Assignable profiles

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

➤ To assign a profile, see [Assigning a profile to a person](#).

Terminology

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

➤ See [Associating a terminology with a profile](#).

Available types

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

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

➤ See [Defining the object types available for a profile](#).

INTRODUCTION TO USER MANAGEMENT

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

User management involves the following concepts:

- **users** :
 A user is a person with a login.
- **persons**
 A person is defined by his/her name and e-mail.
- **logins**
 A Login uniquely defines a user or user group. It can be assigned to only one Person or Person Group.
- **profiles**
 A profile defines what a person can see or not see and do or not do in the tools, and how the person sees the tools and can use them. The profile defines options, access rights to repositories and products, read/write and read-only rights on objects.
- **permissions**:
 - **object UI access**
 Object UI access defines user rights on creation, reading, update, and deletion on these objects and their tools. By default, object UI accesses have value *CRUD (C: create, R: read, U: update, D: delete, *: default value).
 - **general UI access**
 General UI access defines if tools are available or not. By default, general UI accesses have value *A (A: Available, *: default value)

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

☛ See [Introduction to Person Group Management](#).

The following points are detailed here:

- introduction:
 - [Users Delivered](#)
 - [User: Definition](#)
- properties:
 - [Person Properties](#)
 - [Person Login Properties](#)
- access:
 - [Accessing the User Management Pages](#)
- characteristics:
 - [Viewing the Person Characteristics](#)
 - [Viewing the Login Characteristics](#)

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 "Mega" user at installation.

To connect to a HOPEX (Web Front-End) desktop, a user must have a password. To initialize Mega user's Web account, see [Initializing a User Web Account](#) or to define a temporary password to Mega user, see [Defining a Temporary Password to a User](#).
-

User: Definition

For each environment, a user has:

- personal characteristics defined by his/her **Person**.
 - ☛ see [Viewing the Person Characteristics](#).
- a **login** which defines his/her connection identifier, his/her status and his/her authentication **HOPEX** mode. The login can also restrict the accessible products.
 - ☛ see [Person Login Properties](#).
- a **user code** which enables naming of user associated files, for example the work repository.
 - ☛ see [Person Login Properties](#).
- at least one **profile** assigned that determines the products (restricted by the products defined for the user login), applications, desktops, and

repositories to which the user has access as well the access rights to UIs (permissions).

By default the user does not have an assigned profile.

- ☛ see [Profile Properties](#).
- ☛ see [Managing Profiles](#).
- ☛ see [Assigning a profile to a person](#).

- **options**

- ☛ see [Managing Options](#).

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

- ☛ see [Assigning a Business Role to a Person](#).

Only a user with 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](#).

Person Properties

- ☛ To consult properties of a person, see [Viewing the Person Characteristics](#).

- ☛ To define the properties of a person, see [Defining a Person](#).

Name

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

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

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

Phone number and initials

The phone 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](#).

Belongs to a Person Group

A person can:

- belong to a group
 - See [Creating a Person Group](#).
- have the **Belongs to a person group** attribute selected

When the "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 \(LDAP or SSO type\)](#).

➤ See [Defining a dynamic person group with a Macro](#).

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](#).

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.

Assignments - Profile Assignments

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

The profile determines:

- the objects and tools to which the person has access
 - See [Managing UI Access \(Permissions\)](#).
- the Web applications to which the person can connect.
- repository access
- access to products

➤ See [Description of a Profile](#).

➤ See [Assigning a profile to a person](#).

Object assignments

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

➤ See [Managing Business Roles](#).

➤ See [Assigning a Business Role to a Person](#).

Person Login Properties

To:

- create the login of a person, see [Creating Users](#) or [Creating the Login of a Person](#).
- view login characteristics, see [Viewing the Login Characteristics](#).
- configure the login of a person, see or [Defining the Login of a Person](#).

User code

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

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

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 \(Command Line\)](#).

 **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 (case of authentication managed within HOPEX)

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

 See [Defining Default HOPEX Authentication Mode](#).

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

- **MEGA**
The HOPEX authentication service checks that the password entered matches the password stored (hashed and encrypted) in HOPEX repository.
This is the user's default authentication mode when the Authentication mode defined at environment option level is "Standard".
 For more details, see [Authentication in HOPEX \(Web Front-End\)](#).
- **LDAP**
Passwords are managed and stored in the LDAP server of the enterprise. The directory configuration is stored in HOPEX options.
The **HOPEX** user is authenticated at the LDAP server level.
This is the user's default authentication mode when the Authentication mode defined at environment option level is "LDAP".
 For more details, see [Configuring LDAP Authentication](#).
- **Custom**
Password management is delegated to an SSO or external module.
- **Windows**
Passwords are managed by Windows.

LDAP server

 This field only appears when the **Authentication Mode** is "LDAP", see [Authentication mode \(case of authentication managed within HOPEX\)](#).

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](#)
 - [Belonging to a Person Group](#)
 - [User Groups Delivered](#)
- properties:
 - [Person Group Properties](#)
 - [Properties of a Person Group Login](#)
- access:
 - [Accessing the User Management Pages](#)
- characteristics:
 - [Viewing the Person Group Characteristics](#)
 - [Viewing the Login Characteristics](#)

Managing Person Groups Rather than Persons

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

Example: the group of auditors.

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

Persons belonging to a group:

- depend on the same environment.
 - share the same connection characteristics defined by the **profile** of the group and its assignment.
 - ☞ see [Before Defining a User: Profile and Person Group Concepts](#).
 - ☞ see [Description of a Profile](#).
 - connect to the application with their **login**.
 - share the assignments defined for the group.
 - ☞ See [Assigning a profile to a person group](#).
 - share the characteristics defined for the group.
 - ☞ see [Person Group Properties](#).
- 💡 **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](#).
- connect more than one person to a person group simultaneously:
 - ☞ See [Adding one or more persons to a person group](#).

Belonging to a Person Group

A person can:

- belong to a group
 - ☛ See [Creating Users](#).
 - ☛ See [Creating a Person Group](#).
 - ☛ See [Adding one or more persons to a person group](#).
- have the **Belongs to a person group** attribute selected
 - ☛ See [Belongs to a Person Group](#).

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 \(LDAP or SSO type\)](#).
- ☛ See [Defining a dynamic person group with a Macro](#).

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](#).

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](#)).

Person Group Properties

- ☛ For information on a person group, see: [Managing Person Groups Rather than Persons](#), [User Groups Delivered](#), [Viewing the Person Group Characteristics](#), and [Modifying the Login of a Person Group](#).

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. It enables to make the group inactive.

✎ For more details, see [Properties of a Person Group Login](#).

🔑 **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 [Defining a default connection group](#).

Person group types

A person can belong to:

- a static group
Persons are explicitly connected to the group.
☛ See [Defining a Person Group](#).
- a dynamic group
The group computes group persons on the fly.
☛ See [Connection request and user created on the fly](#).

Examples of dynamic groups:

- LDAP groups (case of LDAP authentication)
☛ See [Defining a dynamic person group \(LDAP or SSO type\)](#).
- SSO type groups (SSO authentication case)
☛ See [Defining a dynamic person group \(LDAP or SSO type\)](#).
- 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](#).

LDAP dynamic group

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

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.

SSO type dynamic group

An SSO type group is characterized by claims.

Dynamic group connected to a macro

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

The macro should implement the following function:

```
Function IsUserExists (oPersonGroup, sUserName as String)
as Boolean
sUserName: authentication login of the person.
oPersonGroup: person group object executing the query.
```

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

Persons

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

Data language

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

☛ By default, the data language is defined in the environment options for all users at installation (Options/Installation/Web application) via the **Data language** option.

Assignments - Profile

🔒 **To be able to connect to HOPEX the user must have at least one profile.**

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

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

The profile determines the following for the person group:

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

☛ See [Description of a Profile](#).

- the objects and tools accessible

☛ See [Managing UI Access \(Permissions\)](#).

The profile assignment defines:

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

☛ See [Assigning a profile to a person group](#).

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](#).
- view login characteristics, see [Viewing the Login Characteristics](#).
- define the login of a person group, see [Modifying the Login of a Person Group](#).

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.

Command line

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

Authentication mode (case of authentication managed within HOPEX)

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

➡ See [Defining Default HOPEX Authentication Mode](#).

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

- **MEGA**

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

➡ For more details, see [Authentication in HOPEX \(Web Front-End\)](#).

- **Windows**

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

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

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

➡ For more details, see [Configuring LDAP Authentication](#).

- **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 [Configuring LDAP Authentication](#).

LDAP server

 This field only appears when the **Authentication Mode** is "LDAP", see [Authentication mode \(case of authentication managed within HOPEX\)](#).

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](#).



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

The following points are detailed here:

- [Viewing Profile Characteristics](#)
- [Customizing the UI Access \(Permissions\) of an Existing Profile](#)
- [Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile](#)
- [Creating a Profile](#)
- [Configuring a Profile](#)
- [Checking a Profile Compliancy with Connection Regulation](#)
- [Assigning a profile to a person](#)
- [Assigning a profile to a person group](#)
- [Deleting a Profile](#)

You can also:

- modify profile options
 - ☛ See [Managing Options](#).
- manage metamodel filters at profile level
 - ☛ See [Managing UI Access](#).
- implement data access rules
 - ☛ See [Managing Data Access Dynamically](#) (HOPEX Administration documentation).

Viewing Profile Characteristics

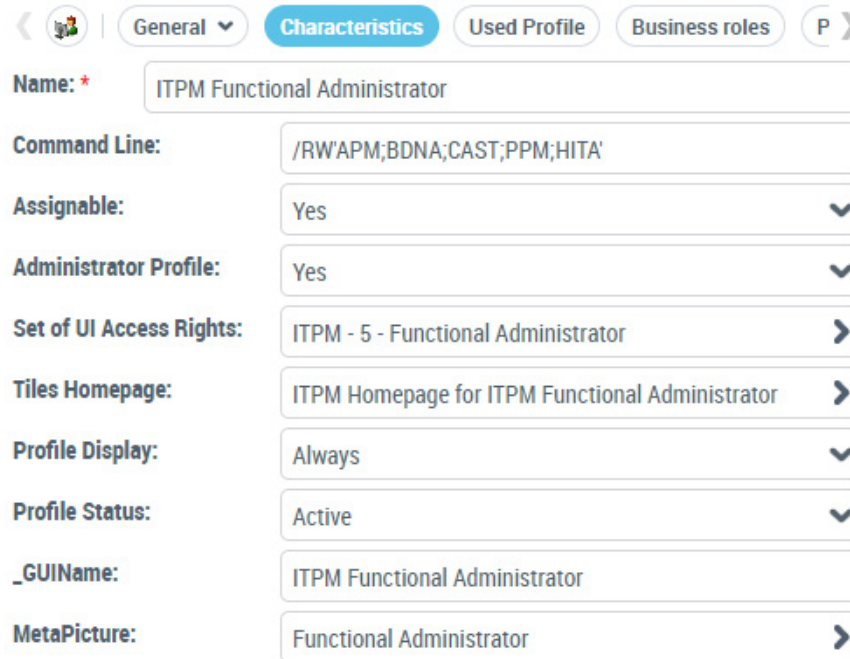
To view profile characteristics:

1. Access the user management pages.
 - ☛ See [Accessing the User Management Pages](#).
2. Select the **Profiles** sub-folder.
3. In the edit page, select the profile.

- In the toolbar, click **Properties** .

The profile **Properties** dialog box opens.

 For detailed information on characteristics of a profile, see [Profile Properties](#).



The screenshot shows the 'Characteristics' tab of the 'Properties' dialog box for a profile named 'ITPM Functional Administrator'. The tabs at the top are 'General', 'Characteristics' (selected), 'Used Profile', and 'Business roles'. The fields are as follows:

Name: *	ITPM Functional Administrator
Command Line:	/RWAPM;BDNA;CAST;PPM;HITA'
Assignable:	Yes
Administrator Profile:	Yes
Set of UI Access Rights:	ITPM - 5 - Functional Administrator
Tiles Homepage:	ITPM Homepage for ITPM Functional Administrator
Profile Display:	Always
Profile Status:	Active
_GUIName:	ITPM Functional Administrator
MetaPicture:	Functional Administrator

 See [Configuring a Profile](#).

Customizing the UI Access (Permissions) of an Existing Profile

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

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

- Access the properties of the profile.
 See [Viewing Profile Characteristics](#).
- In the **Set of UI Access Rights** field, click the arrow and access its **Properties**.
- In the **Characteristics** page, click the arrow of the **Customizing Set of UI Access Rights** and select **Create Set of UI Access Rights**.

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

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

- (If needed) Modify its **Name**.

5. Click **OK**.
The set of UI access rights you created is predefined with the same UI access rights as those defined for the profile concerned.
6. Customize the UI Access of the set of UI Access rights you just created.
☛ See [Managing UI Access \(Permissions\)](#) and in the **Access Rights** field select the Set of UI access rights you just created.

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

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

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

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

1. Create a profile and configure its **Set of UI Access Rights** by aggregating the set of UI access rights of the profile on which is based your profile.
☛ See [Creating a Profile](#).
2. Configure the profile.
☛ See [Configuring a Profile](#).

Creating a Profile

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

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

To create a profile you must define:

- its name
- its set of UI access rights

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

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

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

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

To create a profile:

1. Access the Profiles management pages.
 ➤ See [Accessing the User Management Pages](#).
2. In the **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. In the **Set of UI Access Rights** field, click the arrow and select **Create Set of UI Access Rights**.
5. In the **Name** field, enter a name for the Set of UI access rights of the profile.
6. (Optional, to use one or several Sets of UI access rights already defined)
 Click **Connect** :
 - (Optional) In the search field, enter the character string to be searched for.
 - Click **Find** .
 - In the list, select the Set of UI access rights on which you want to base the Set of UI access rights of your profile.
 ➤ You can select several Sets of UI access rights.
 The set of UI access rights you are creating inherits from the permissions defined on all the sets of UI access rights you connected to it.
- Click **OK**.
7. Click **OK**.
 The new profile appears in the list of profiles.
8. Configure the profile characteristics.
 ➤ See [Configuring profile characteristics](#).
 Example: In the **Characteristics** page, set the **Assignable** parameter to "Yes", connect a **Tiles Homepage**.
9. (WET-based desktop) Assign a WET to the profile.
 ➤ See [Assigning a WET to a profile](#).
10. (Non WET-based desktop) Define:
 - the accessible desktop(s)
 ➤ See [Defining the application desktops accessible to the users of a profile \(non WET-based configuration\)](#).
 - the available applications
 ➤ See [Defining the applications accessible to the users of a profile \(non WET-based configuration\)](#).
 Example: "The Web Front-End for a Web application."
11. (If needed) Define the Set of UI access rights of the profile.
 ➤ See [Managing UI Access \(Permissions\)](#).

Configuring a Profile

From the profile properties window you can define:

- ✎ See [Profile Properties](#).
 - products accessible to users with the current profile.
 - ✎ See [step 2](#).
 - if the profile is assignable or not.
 - ✎ See [step 3](#).
 - if the profile is an administrator profile or not.
 - ✎ See [step 4](#).
 - if the profile is provided at connection.
 - ✎ See [step 5](#).
 - if the profile is active or not.
 - ✎ See [step 6](#).
 - the profile display name in the interface.
 - ✎ See [step 7](#).
 - the profile icon in the interface.
 - ✎ See [step 8](#).
 - the Working Environment template (WET), which defines the desktops to which the users of the profile have access.
 - ✎ See [Assigning a WET to a profile](#).
- Or in a non WET-based configuration:
- applications accessible to the users of the profile.
 - ✎ See [Defining the applications accessible to the users of a profile \(non WET-based configuration\)](#).
 - (If needed) desktops accessible to the users of the profile.
 - ✎ See [Defining the application desktops accessible to the users of a profile \(non WET-based configuration\)](#).
 - the terminology associated with the profile.
 - ✎ See [Associating a terminology with a profile](#).
 - object types available.
 - ✎ See [Defining the object types available for a profile](#).

To:

- customize the UI access rights of the profile, see:
 - [Customizing the UI Access \(Permissions\) of an Existing Profile](#).
- perform a mass profile assignment to persons, see:
 - [Performing a Mass Profile Assignment to Persons](#).
 - [Performing a mass assignment of profiles to a person group](#).
- check that the profile complies with the connection regulation, see:
 - [Checking a Profile Compliancy with Connection Regulation](#).

Configuring profile characteristics

To configure profile characteristics:

1. Access the properties of the profile.
 - ☛ See [Viewing Profile Characteristics](#).
2. (Optional) In the **Command Line** field, enter the command defining products that can be accessed by users with the current profile.
 - ☛ See [Products accessible on the license \(Command Line\)](#).
3. (Optional) In the **Assignable** field, modify the attribute value via the drop-down menu.
 - ☛ By default, the profile is not assignable.
 - ☛ See [Assignable](#).
4. (Optional) In the **Administrator Profile** field, modify the attribute value.
 - ☛ By default, the profile is not an administrator profile.
 - ☛ See [Administrator profile](#).
5. (Optional) In the **Profile Display** field, modify the default behavior of the profile display at connection.
 - ☛ A profile is provided by default at connection when it is not included in another profile.
 - ☛ See [Profile display](#).
6. (Optional) In the **Profile Status** field, modify the attribute value.
 - ☛ By default, the profile is active.
7. (Optional) In the **_GUIName** field, enter the profile name displayed in the interface.
8. (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 **Connect**.

Assigning a WET to a profile

☛ To see the connection diagram, see [Connection diagram \(with WET\)](#).

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

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

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

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

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

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

Assigning a WET to a profile (standard version)

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

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

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

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

1. Access the properties of the profile.
☛ See [Viewing Profile Characteristics](#).
2. Select the **Working Environment Template Assignments** page.
3. Click **New** .
4. In the **Assigned Working Environment Template** field, select the Working Environment Template you want to assign to the profile.
5. Select the **Desktop selected via Desktop Manager** mode.
6. Select **Create a Desktop Manager**.
☛ To reuse a Desktop Manager, keep **Reuse existing Desktop Manager** and in the drop-down list select the Desktop Manager.
7. Click **Next**.
8. (Optional) In the **Name** field, modify the default desktop manager name.
☛ The default name is **<Profile name> / <Assigned WET name> / Desktop Manager**.
😊 This can be useful if you need to reuse this desktop manager for another WET assignment.
9. Click **Connect**  and connect the desktops adapted to the devices you want to define for the profile.
10. Click **OK**.
The desktops associated with the **Desktop Manager** are specified. You must define each desktop use context.
11. In the desktop list, for each desktop, in the **Device** column, select the device type adapted to the desktop.

Example: Tablet, Computer.

12. Click **OK**.

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

Example:

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

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

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

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

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

☛ See [Connection diagram \(without WET\)](#).

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

To define applications available for a profile:

1. Access the properties pages of the profile.

☛ See [Viewing Profile Characteristics](#).

2. Select **Available Applications**.

3. In the toolbar, click **Connect** .

The applications query tool appears.

4. (Optional) In the second field, enter the characters to search for.

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

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

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

☛ See [Restricting access to the desktops of an application](#).

To do this, you must connect to the profile:

- the application containing the desktops.
 - ☛ See [Defining the applications accessible to the users of a profile \(non WET-based configuration\)](#).
- the desktops you want the users of the profile can connect to.
 - ☛ The application desktops that are not connected to the profile are not accessible to users of the profile.
 - ☛ To modify a profile supplied by **MEGA**, **MEGA** recommends you create a new profile, see [Creating a Profile](#).

To define application desktops available for a profile:

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

☛ See [Defining the applications accessible to the users of a profile \(non WET-based configuration\)](#).

1. Access the properties pages of the profile.
 - ☛ See [Viewing Profile Characteristics](#).
2. Select **Available Desktops**.
3. In the toolbar, click **Connect** .

The desktop query tool appears.
4. (Optional) In the second field, enter the characters to search for.
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](#).
2. Select **Terminology**.
3. In the toolbar, click **Connect** .

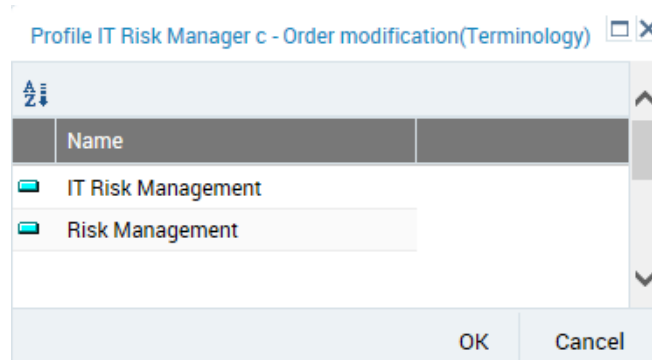
The business roles query tool appears.
4. (Optional) In the second field, enter the characters to search for.
5. Click **Find** .
6. In the query results, select the terminology you want to connect.
 - ☛ You can select several terminologies.
7. Click **Connect**.

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](#).
2. Select **Terminology**.
3. In the toolbar, click **Reorganize** .
4. Drag and drop to place the priority terminology at the top.



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

Defining the object types available for a profile

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

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

To define the object types available for a profile:

1. Access the properties of the profile.
See [Viewing Profile Characteristics](#).
2. 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 search for.
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](#).
2. In the **Profiles** page, right-click the profile concerned and select **Manage > Check > Regulation with propagation**.
3. Select **Connection regulation**.
4. Click **OK**.
 The connection regulation report for the selected profile is displayed.

Assigning a profile to a person

 A person may have several profiles.

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

Assigning a profile to a person defines:

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

Repository Snapshot:

 A repository snapshot defines repository state at a given moment.

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

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

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

Restrictions:

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

 See [Administrator profile](#).

Only administration dedicated profiles (HOPEX Administrator, HOPEX Administrator - Production, User Management Web Administrator) allow

to assign any profile (including administration dedicated profiles) to persons.

- A functional administrator of a Solution can only assign this Solution dedicated profiles.

E.g.: The **Application Design Functional Administrator** profile allows to assign the **Application Design Viewer**, the **Application Designer**, and the **UML Designer** profiles.

☛ In the profile property pages, **Assignable Profiles** lists the profiles it allows to assign, see [Assignable profiles](#).

See:

- [Assigning a profile to a person](#)
- [Performing a Mass Profile Assignment to Persons](#)
- [Mass assignment of profiles to persons](#)

Assigning a profile to a person

☛ To assign one or more profiles to one or more persons at a time, see [Mass assignment of profiles to persons](#)

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

To assign a profile to a person:

1. Access the properties of the person.
 - ☛ See [Viewing the Person Characteristics](#).
2. In **Assignments**, click **Profile Assignments**.
3. Click **New** .
4. In the **Profile assigned** field, click the drop-down menu and select the profile you want to assign to the person.
 - ☛ To execute a filtered query on a profile, click the arrow and select **Query**.
5. (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, with read-only data access) In the **Connection Snapshot** field, select a connection repository snapshot.
7. (optional, to define a validity date) Click **Valid for a limited period**.
 - (optional) In the **Validity start date** field, use the calendar to define the start date of profile assignment validity.
 - (optional) In the **Validity end date** field, use the calendar to define the end date of profile assignment validity.
8. Click **OK**.
The profile is assigned to the person on the selected repository for the specified duration.

Performing a Mass Profile Assignment to Persons

☛ To perform a mass profile assignment with a validity date to persons, see [Mass assignment of profiles to persons](#).

To perform a mass profile assignment to persons:

1. Access the user management pages and select the **Persons by Profile** sub-folder.
 See [Accessing the User Management Pages](#).
2. In the edit area, select the profile you want to connect to persons.
3. In the edit area, click **Connect** .
4. In the **Repository** field, select the repository concerned by the assignment.
5. (optional, to define a validity date) Click **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.
6. Select the persons to whom you want to assign the profile.
7. Click **OK**.
 The selected profile is assigned to the selected persons, on the selected repository, for the defined period.

Mass assignment of profiles to persons

To perform a mass assignment of profiles to persons:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select the **Persons** sub-folder.
 The list of persons appears.
3. Select the persons to whom you want to assign one or more profiles.
4. Click **Assign Profiles**.
 The list of profiles appears.
5. In the **Repository** field, select the repository concerned by the assignment.
6. By default, assignments do not have a validity limit. If you must define a validity period for assignments, select **Define validity dates**.
 - In the **Validity start date** field, click the calendar and select a validity start date.
 - In the **Validity end date** field, click the calendar and select a validity end date.
7. Select the profiles that you want to assign to the selected persons.
8. Click **OK**.
 The selected profiles are assigned to the selected persons, on the selected repository, for the defined period.

Assigning a profile to a person group

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

The profile assignment is specific to a repository.

☞ *A person group can have several profiles.*

See:

- [Assigning a profile to a person group](#)
- [Performing a mass profile assignment to person groups](#)
- [Performing a mass assignment of profiles to a person group](#)

Assigning a profile to a person group

To assign a profile to a person group:

1. Access the properties of the person group.
☞ See [Viewing the Person Group Characteristics](#).
2. In **Assignments**, click **New** .
3. In the **Assigned profile** field, click the drop-down menu and select the profile you want to assign to the person group.
4. 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](#).
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 search for.
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](#).
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](#).
2. In the **Profiles** tab, select the profile you want to delete.
 You can select more than one.
3. Click **Remove** .
The delete objects dialog box opens.
4. Click **Delete**.
The profile is deleted from the environment

ACCESS TO USER MANAGEMENT

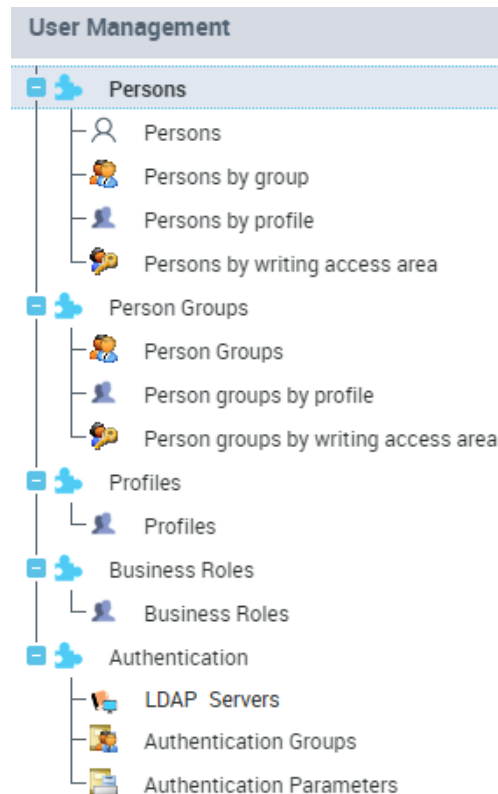
See:

- [Accessing the User Management Pages.](#)
- [Viewing the Person Characteristics.](#)
- [Viewing the Person Group Characteristics.](#)
- [Viewing the Login Characteristics.](#)

Accessing the User Management Pages

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

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



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

The management page selected appears.

See:

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

Managing persons who have an identical characteristic

To manage persons who have an identical characteristic, see:

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

Managing a group of persons who have a specific characteristic

To manage persons who have a specific characteristic, see:

- [Accessing a group of persons connected to a specific profile](#)
- [Accessing the list of person groups connected to a specific writing access area](#)
- [Accessing the list of person groups connected to a specific reading access area](#)

Actions performed from the Persons management page

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

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

Actions performed from the Person Group page

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

- create user groups
➤ See [Creating a Person Group](#).
- define the properties of a person group
➤ See [Defining a Person Group](#).
- configure the characteristics of a login
➤ See [Modifying the Login of a Person Group](#).
- assign a profile to a person group
➤ See [Assigning a profile to a person group](#).
- connect a person group with a writing access area
➤ See [Connecting a Person Group to a Writing Access Area](#).
- connect a person group with a reading area access
➤ See [Connecting a Person Group to a Reading Access Area](#).
- define a person group
➤ See [Deleting a Person Group](#).
- modify user group properties
➤ See [Modifying User Group Properties](#).

Accessing the list of persons who have the same profile assigned

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

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

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

Accessing the list of person who belong to the same group

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

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

1. Access the user management page.
➤ See [Accessing the User Management Pages](#).
2. Select the **Persons by group** sub-folder.
3. In the edit area, in the **Persons by group** tab, select a person group.
The **Persons** tab lists all the persons who belong to the selected group.
In the case of 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](#).

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

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

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

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

 See [Actions performed from the Persons management page](#).

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

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

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

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

 See [Actions performed from the Persons management page](#).

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

You can filter persons according to their login.

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

1. Access the user management page.
 See [Accessing the User Management Pages](#).
2. Select a **Persons** sub-folder.
3. In the edit area, click **Display filters** .
Fields appear under the header of each column.
4. In the **Login** column field, click the filtering operator and select:
 - **Shows non empty values only** 
The persons who have a login are listed.
 - **Shows empty values only** 
The persons who do not have a login are listed.

Accessing a person using his/her name

You can filter persons according to their name.

To find a person using his/her name:

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

Accessing a group of persons connected to a specific profile

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

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

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

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

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

1. Access the user management page.
 See [Accessing the User Management Pages](#).
2. Select the **Person groups by writing access area** sub-folder.
3. In the edit area, in the **Person groups by writing access area** tab, select a writing access area.
4. In the edit area, in the **Person groups and objects** tab, click:
 - **Person Groups** to list all the person groups connected to the selected writing access area.
 - **Objects** to list all the objects that are connected to the selected writing access area. See [Actions performed from the Person Group page](#).

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

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

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

1. Access the user management page.
➤ See [Accessing the User Management Pages](#).
2. Select the **Person groups by reading access area** sub-folder.
3. In the edit area, in the **Person groups by reading access area** tab, select a reading access area.
4. In the edit area, in the **Person groups and objects** tab, click:
 - **Person Groups** to list all the person groups connected to the selected reading access area.
 - **Objects** to list all the objects connected to the selected reading access area.➤ See [Actions performed from the Person Group page](#).

Viewing the Person Characteristics

 |
General ▾ **Characteristics** Widgets Assignments Skills Comment

Name: *



E-mail:

Phone Number:

Initials:

Data Language: ▾

Default Library: ▸

CAST Highlight ID: ▴ ▾

Writing access area: * ▾ ▸

Writing access area at creation: ▾ ▸

Login: ▸

☐ **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](#), [Creating Users](#) and [Assigning a profile to a person](#) (or [Performing a Mass Profile Assignment to Persons](#)).

To view the person characteristics:

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

➤ See [Accessing the User Management Pages](#).

2. Select:

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

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

➤ You can sort or filter the display according to columns. See [Accessing the list of persons who have or do not have a login](#) and [Accessing a person using his/her name](#).

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

3. In the Persons list, select the person.

4. In the toolbar, click **Properties** .

The **Properties** dialog box of the person opens.

5. Click:

- the **Characteristics** tab to define or modify the person properties.
➤ See [Person Properties](#).
➤ See [Defining a Person](#).
- **General > History** to display the actions performed on the person.
- **Assignments** to display and assign profiles to the person.

Viewing the Person Group Characteristics


General
Characteristics
Assignments
Comment

Writing access area: Administrator

Writing access area at creation:

Login: Trainees

☐ Default connexion group

Authentication Group:

Persons Computation:

Persons:

New
Connect
Reorganize
Properties
Disconnect

	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 4

Data Language:

To view the person group characteristics:

- Access the **User Management** pages.
See [Accessing the User Management Pages](#).

2. Select:

- the **Person Groups** sub-folder for direct access, or
- a classification sub-folder (**Person groups by profile**, **Person groups by writing access area**, or **Person groups by reading access area**), then in the edit area select the **Profile**, the **Writing access area** or the **Reading access area** concerned.

The list of person groups appears with for each group, where necessary, its associated LDAP group or associated macro and its 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 person group list, select a person group.

4. In the toolbar, click **Properties** .

The **Properties** dialog box of the person group opens.

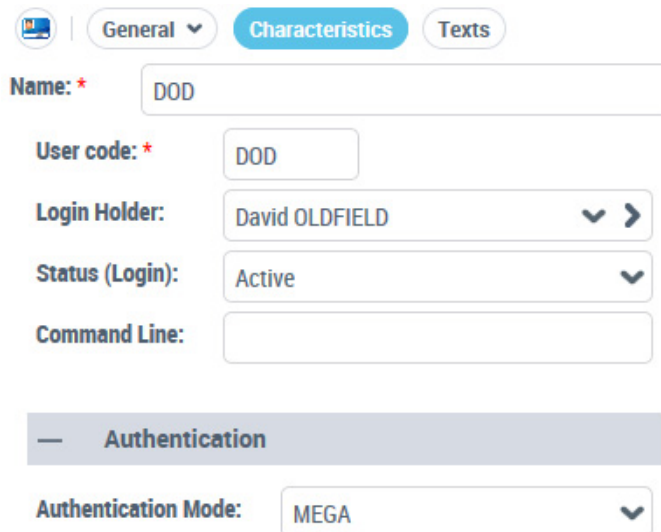
5. Click:

- **Characteristics** to define or modify the person group properties.
 - ☞ See [Person Group Properties](#).
 - ☞ See [Defining a Person Group](#), [Defining a dynamic person group \(LDAP or SSO type\)](#), [Defining a dynamic person group with a Macro](#).
- **General > History** to display the actions performed on the person group.
- **Assignments** to display the profiles assigned to the person group.

Viewing the Login Characteristics

☞ For detailed information on characteristics of a login, see [Person Login Properties](#).

☞ To configure a login, see [Defining the Login of a Person](#).



The screenshot shows the 'Person Group Properties' dialog box with the 'Characteristics' tab selected. The 'General' tab is also visible. The 'Name' field is labeled 'Name: *' and contains 'DOD'. The 'User code' field is labeled 'User code: *' and contains 'DOD'. The 'Login Holder' field is labeled 'Login Holder:' and contains 'David OLDFIELD'. The 'Status (Login)' field is labeled 'Status (Login):' and contains 'Active'. The 'Command Line' field is labeled 'Command Line:' and is empty. Below these fields is a section titled 'Authentication' with a sub-section 'Authentication Mode:' containing 'MEGA'.

To view the login characteristics:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select the **Persons** or **Person Groups** sub-folder.
3. In the Persons list, select the person concerned and click **Login Properties** .

CREATING AND MANAGING USERS

For an overview of actions to be performed to create and define a user see [Actions to be Performed to Define a User](#).

 To manage person groups, see [Managing Person Groups Rather than Persons](#) and [Creating and Managing a Person Group](#).

The following points are covered here:

- configuration:
 - [Creating Users](#)
 - [Defining a Person](#)
 - [Creating the Login of a Person](#)
 - [Defining the Login of a Person](#)
 - [Modifying User Properties](#)
 - [Connecting a Person to a Writing Access Area](#)
- management:
 - [Checking the Configuration of Persons](#)
 - [Connecting a Person to a Writing Access Area](#)
 - [Connecting a Person to a Reading Access Area](#)
 - [Preventing User Connection](#)
 - [Deleting a User](#)
 - [Creating and Managing a Person Group](#)
 - [Managing User Options](#)

For information on managing business roles for persons, see:

- [Assigning a Business Role to a Person](#)
- [Transferring Responsibilities to a Person](#)
- [Duplicate the Responsibilities of a Person](#)

Creating 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 [Importing persons from an LDAP server](#)).

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](#).

 For detailed information on characteristics of a login, see [Person Login Properties](#).

 To import users from an LDAP directory, see [Configuring LDAP Authentication](#).

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](#).

To create a user:

1. Access the **User Management** pages.
 - ☛ See [Accessing the User Management Pages](#).
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](#)). 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 enable the user to connect to **HOPEX** (Web Front-End) initialize the user Web account, see [Initializing a User Web Account](#).

 To define the characteristics of the user, see [Defining a Person](#).

 You must configure the login of the user, see [Defining the Login of a Person](#).

 To check the configuration of the user, see [Checking the Configuration of Persons](#).

Defining a Person



Person represents a physical person or a system.

 For more information on properties of a person, see [Person Properties](#).

 To check the configuration of a person, see [Checking the Configuration of Persons](#).

 To assign:

a profile to a person (mandatory), see [Assigning a profile to a person](#).
an object to a person (if needed), see [Assigning a Business Role to a Person](#).

From the 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 the Person Characteristics](#).
2. (Optional) To add or update the image of the person, click **Update Image**, select the image and click **OK**.
☞ The image is stored in binary on an attribute of the person. To delete the image, click **Reinitialize Image**.
3. (Recommended) In the **E-mail** field, enter the e-mail address of the person.
☞ The e-mail address is required, for example, 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](#).
6. (Optional) In the **Default Library** field, click the arrow and select the default library in which objects created by the user are stored if the creation context does not define one.

7. (Optional, with the **HOPEX Power Supervisor** technical module) You can modify the values at the following levels:
 - user writing access via the drop-down menu in the **Writing Access Area** field.
 - ☛ By default, all users are connected to the only writing access area that exists: "Administrator".
 - ☛ See also [Connecting a Person to a Writing Access Area](#).
 - user writing access at creation via the drop-down menu in the **Writing Access Area** field.
 - reading access via the drop-down menu in the **Reading Access Area** field.
 - ☛ This field only appears if reading access management has been activated.
 - ☛ See also [Connecting a Person to a Reading Access Area](#).
 - reading access at creation via the drop-down menu in the **Writing Access Area** field.
 - ☛ This field only appears if reading access management has been activated.
8. So that the person can connect to **HOPEX**, the person must have a **Login**.
 - ☛ See [Creating the Login of a Person](#).
9. (optional) If necessary select **Belongs to a Person Group**
The person is configured.
 - ☛ To notify the users connected of your changes, click **Notify Connected Users**.

Creating the Login of a Person

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

When you create a person from:

- 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 the Person Characteristics](#).
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](#).
- 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 3](#).
- (Case of authentication managed within HOPEX) modify user authentication mode
The value of this parameter is inherited, at user creation, from the value of the **Authentication Mode** option defined in the environment options (**Installation > User Management > Authentication Mode**). If you change the option value at environment level after the user creation, the user is not impacted.
 - ☞ See [step 4](#).

To define the login of a person:

1. In the login properties pages, display **Characteristics**.
 - ☞ See [Viewing the Login Characteristics](#).
 - The login **Name** and **User Code** attributes are already created, but you can modify these if necessary.
 - 📖 *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 \(Login\)](#).

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 the HOPEX Business Process Analysis and HOPEX IT Portfolio Management modules to a user, enter:

/RW' HBPA;APM'

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

 **If a user is connected to a profile and 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. (If needed) In the **Authentication Mode** field, click the arrow and modify the authentication mode.

The default value is

- "MEGA" (if in the environment options, the Authentication mode is "Standard").
- "LDAP" (if in the environment options, the Authentication mode is "LDAP").

 See [Authentication mode \(case of authentication managed within HOPEX\)](#).

Modifying User Properties

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

- person:
 - its name
 - image
 - e-mail address
 - telephone number
 - initials
 - data language
 - default library
 - writing access area
 - reading access area
 - group
 - profile assignments (connection)
 - object assignments (business roles)
 - skills
 - ☞ See [Person Properties](#).
 - ☞ See [Viewing the Person Characteristics](#).
 - ☞ See [Defining a Person](#).
- login:
 - its name
 - user code

 **To assure consistent actions history, the user code should not be modified.**

 - status
 - accessible products (Command Line)
 - authentication mode
 - ☞ See [Person Login Properties](#).
 - ☞ See [Viewing the Login Characteristics](#).
 - ☞ See [Defining the Login of a Person](#).

Connecting a Person to a Writing Access Area

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

☞ To connect a person to a writing access area, see also [Defining a Person](#).

To connect a person to a writing access area:

1. Access the **User Management** pages.
 - ☞ See [Accessing the User Management Pages](#).
2. Select the **Persons by reading access area** sub-folder.
3. In the edit area, select a writing access area.

4. Click **Connect** .

 To add a person not yet created, click **New** , see [Creating Users](#).

5. (Optional) In the query field, enter the characters to search for.

6. Click **Find** .

7. In the result list, select the person you want to connect.

8. Click **Connect**.

The selected person is connected to the selected writing access area.

Connecting a Person to a Reading Access Area

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

 To connect a person to a reading access area, see also [Defining a Person](#).

To connect a person to a reading access area:

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

 See [Accessing the User Management Pages](#).

2. Select the **Persons by reading access area** sub-folder.

3. In the edit area, select a reading access area.

4. Click **Connect** .

 To add a person not yet created, click **New** , see [Creating Users](#).

5. (Optional) In the query field, enter the characters to search for.

6. Click **Find** .

7. In the result list, select the person you want to connect.

8. Click **Connect**.

The selected person is connected to the selected reading access area.

Preventing User Connection

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

To render a user inactive:

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

 See [Viewing the Login Characteristics](#).

2. In the **Status (Login)** field, select "Inactive".

The user can no longer connect to **HOPEX**.

Deleting a User

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

To delete a user:

1. Access the user management page.
 See [Accessing the User Management Pages](#).
2. In **Persons**, select the person to be deleted and click **Delete** .
-  *You can select more than one.*

The **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](#).

The following points are covered here:

- configuration:
 - [Creating a Person Group](#)
 - [Defining a Person Group](#)
 - [Defining a default connection group](#)
 - [Connecting a Person Group to a Writing Access Area](#)
 - [Connecting a Person Group to a Reading Access Area](#)
 - [Modifying the Login of a Person Group](#)
- management:
 - [Preventing User Group Connection](#)
 - [Deleting a Person Group](#)

Creating a Person Group

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

For detailed information on:

- connecting persons belonging to a group, see [Managing Person Groups Rather than Persons](#):
- the types of person groups, see [Person group types](#).
- the characteristics of a person group, see [Person Group Properties](#).
- the characteristics of the login of a person group, see [Properties of a Person Group Login](#).

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

To create a person group:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. You can create:
 - either a non-predefined person group:
Select the **Person Groups** sub-folder and go to step 4.
 - or a predefined person group:
Select the sub-folder:

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

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

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

3. In the edit area, select the profile, the writing access area or the reading access area that you want to connect to the group.
4. Click **New** .
The **Creation of Person Group - Characteristics** 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](#).

Defining a Person Group

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

-  See [Managing Person Groups Rather than Persons](#).
-  For detailed information on:
 - the characteristics of a person, see [Person Properties](#).
 - the characteristics of a person group, see [Person Group Properties](#).
 - the characteristics of a login, see [Properties of a Person Group Login](#).
 - the types of person groups, see [Person group types](#).

A person group can be created:

- statically
 -  See [Adding one or more persons to a person group](#).
- dynamically
 -  See [Defining a dynamic person group \(LDAP or SSO type\)](#).
 -  see [Defining a dynamic person group with a Macro](#).

To configure a person group, you must:

- assign a profile to the person group
 -  See [Assigning a profile to a person group](#).

You can also:

- define a default connection group.
☛ See [Defining a default connection group](#).
- connect the person group with access to a reading area
☛ See [Connecting a Person Group to a Reading Access Area](#).
- connect the person group with access to a writing area
☛ See [Connecting a Person Group to a Writing Access Area](#).
- define the data language of the person group
☛ [Specifying the Data Language](#).
- modify the properties of the person group
☛ See [Modifying User Group Properties](#).

Adding one or more persons to a person group

Case of a person group created statically.

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

1. Access the property pages of the person group you want to configure.
☛ See [Viewing the Person Group Characteristics](#).
2. Select **Characteristics**.
3. In the **Persons** pane, click **Connect** .

☛ To add a person not yet created, click **New** , see [Creating Users](#).

4. (Optional) In the query field, enter the characters to search for.
5. Click **Find** .
6. In the result list, select the persons you want to connect.
These persons must have a login.

 **A person belonging to a group connects to the application with its login. A person without a login cannot connect to an application.**

☛ Use the [Ctrl] key to select more than one person at the same time.

7. Click **Connect**.
The person(s) are connected to the person group.

Defining a dynamic person group (LDAP or SSO type)

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

 A dynamic group is a group that computes group users on the fly (see [Connection request and user created on the fly](#)).

☛ For information on person group types, see [Person group types](#).

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

Prerequisite: the (LDAP or SSO type) group is already created.

➤ See [Defining an authentication group](#).

To define a dynamic **Person Group** (LDAP or SSO type):

1. Access the properties pages of the person group.
➤ See [Viewing the Person Group Characteristics](#).
 2. Select **Characteristics**.
 3. In the **Authentication Group** field, click the arrow and connect the required authentication group.
 4. Click **OK**.
- The dynamic person group is configured with LDAP or SSO.

Defining a dynamic person group with a Macro

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

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

➤ For information on person group types, see [Person group types](#).

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

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

1. Access the properties pages of the person group.
➤ See [Viewing the Person Group Characteristics](#).
2. Select **Characteristics**.
3. In the **Computed Persons** field, click the arrow and connect the required macro.

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

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

omPersonGroup represents the person group object executing the query.

sLogin represents the authentication login of the person.

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

Defining a default connection group

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

➤ For information on person group types, see [Person group types](#).

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

To define a default connection group:

1. Access the properties pages of the person group.
 See [Viewing the Person Group Characteristics](#).
2. Select **Characteristics**.
3. Select **Default connection group** option.

Connecting a Person Group to a Writing Access Area

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

To connect a person group to a writing access area:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select the **Person groups by writing access area** sub-folder.
3. In the edit area, select a writing access area.
4. Click **Connect** .
 To add a person group not yet created, click **New** , see [Creating a Person Group](#).
5. (Optional) In the query field, enter the characters to search for.
6. Click **Find** .
7. In the result list, select the person group you want to connect.
 You can connect several person groups.
8. Click **OK**.
 The person groups selected are connected to the writing access area selected.

Connecting a Person Group to a Reading Access Area

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

To connect a person group to a reading access area:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select the **Person groups by reading access area** sub-folder.
3. In the edit area, select a reading access area.
4. Click **Connect** .
 To add a person group not yet created, click **New** , see [Creating a Person Group](#).
5. (Optional) In the query field, enter the characters to search for.

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

Modifying the Login of a Person Group

When you create a person group, the login of the group is automatically created.
From the Login properties window, you can:

-  See [Properties of a Person Group Login](#).
- modify the name of the login and the user code associated with the login
- modify the status of the person group (inactive)

- modify authentication mode

To modify the login of a person group:

1. Access the property pages of the login.
 See [Properties of a Person Group Login](#).
2. Select **Characteristics**:
 - The login **Name** and **User Code** attributes are already created, but you can modify these if necessary.
 *A **login** is unique and defined for a person or person group.*
 *The **User code** is the short identifier (upper case) of the user. It is of no use in case of a person group.*
 - The **Login Holder** represents the person group associated with this login.
 - The value of the **Status (Login)** field defines if the person group is active or not.

Modifying 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 the default connection group
 - group type (LDAP/SSO type group, person group computed by macro, or persons directly connected to group)
 - persons owned in the group
 - ☛ See [Person Group Properties](#).
 - ☛ See [Viewing the Person Group Characteristics](#).
 - ☛ See [Defining a Person Group](#).
 - ☛ See [Defining a dynamic person group \(LDAP or SSO type\)](#).
 - ☛ See [Defining a dynamic person group with a Macro](#).
- login:
 - name and user code
 - status
 - authentication mode
 - ☛ See [Properties of a Person Group Login](#).
 - ☛ See [Viewing the Login Characteristics](#).
 - ☛ See [Modifying the Login of a Person Group](#).

Preventing User Group Connection

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

To deactivate a person group:

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

Deleting a Person Group

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

To delete a person group:

1. Access the user management page.
 See [Accessing the User Management Pages](#).
2. In **Person Groups**, select the person group to be deleted and click **Delete** .
 You can select more than one.
The **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](#)).

See:

- [Configuring the Metamodel Access](#)
- [Authorizing Deletion of a Dispatched Object](#)
- [Authorizing HOPEX Data Modification](#)
- [Making a Comment Mandatory on Dispatch](#)
- [Managing User Inactivity](#)

Configuring the Metamodel Access

With the **Metamodel Access** option (**Options > Repository** field), 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](#)).
- **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).**

Prohibiting the Administrator from Modifying User Options

By default the **HOPEX** (Web Front-End) administrator can modify the options at environment, profile, and user level. The option levels are governed by an inheritance mechanism (Site > Environment > Profile > user).

➡ See [Options Overview](#).

The **Enables modification of user option by the administrator** option (**Options > Installation > User Management** folder) enables to prohibit the administrator from modifying options at user level.

Authorizing Deletion of a Dispatched Object

Users working in a public workspace can delete objects.

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

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

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

Authorizing HOPEX Data Modification

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

The **Authorizing HOPEX Data Modification** (**Options > Repository** folder) allows modifying 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.

Making a Comment Mandatory on Dispatch

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

Managing User Inactivity

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

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

By default, user inactivity management is not activated.

Activating/Deactivating user inactivity management

To activate/deactivate user inactivity management:

1. Access **Options** at the environment level.
 See [Accessing Options](#).
2. In the **Options** tree, select **Workspace**.
3. In the right pane:
 - to activate user inactivity management, select **Automatic Session Timeout**.
 - to deactivate user inactivity management, clear **Automatic Session Timeout**.

Managing user inactivity

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

☞ *The **Period of inactivity requiring authentication** is **HOPEX** (Windows Front-End) specific.*

To manage user inactivity:

1. Access **Options** at the environment level.
 See [Accessing Options](#).
2. In the **Options** tree, select **Workspace**.
3. In the right pane, enter a value for the **Duration of inactivity before closing HOPEX** option.
 **If the **Period of inactivity requiring authentication** option is lower than the **Duration of inactivity before closing HOPEX** value, thus the value taken into account for user disconnection is this latter.**

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

AUTHENTICATION IN HOPEX (WEB FRONT-END)

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

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

➤ See **Installation and Deployment > HOPEX Unified Authentication Service** documentation.

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

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

This solution offers several advantages, including:

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

The Single Sign On system used in **HOPEX** is based on standard security protocols natively integrated in Windows: Kerberos, 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 "Single Sign-On in Windows 2000 networks" document at the following Web address:
<http://technet.microsoft.com/fr-fr/library/bb742456.aspx>

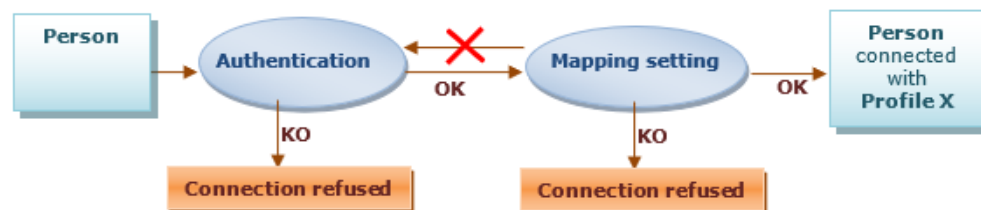
See:

- [Authentication and Mapping Principle](#)
- [Introduction to Authentication in HOPEX \(Web Front-End\)](#)
- [Defining Default HOPEX Authentication Mode](#)
- [Authentication Group](#)
- [Configuring LDAP Authentication](#)
- [Configuring SSO Authentication](#)

Authentication and Mapping Principle

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

- **Phase 1: Authentication**
The authentication phase consists in checking that the person connecting to HOPEX exists and that his/her identification is valid. This authentication can be independent of the HOPEX repository.
Once validated, this authentication phase is not called later at the mapping phase.
- **Phase 2: Mapping**
The mapping phase consists in defining the profile with which the authenticated person will connect to the application.
Without a profile assigned the connection is refused to the user, even authenticated.
- **Phase 3: Connection and access to the repository**
Once authentication and mapping phases are validated, the person can connect to the application and access the repository.
The person selects the repository and the profile with which he/she wants to connect.



Introduction to Authentication in HOPEX (Web Front-End)

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

☛ For a detailed description, see **Installation et déploiement > HOPEX Unified Authentication Service > UAS Configuration** documentation.

Choosing an authentication mode

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

- **by an external module**
If your enterprise has an external authentication or SSO module, it is preferable to use the delegated authentication system.
Example: SAML2, OpenId.
☛ See [Defining an external authentication mode](#).
- **within the HOPEX platform** (by default)
 - **LDAP**
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](#).
 - **Standard** (by default)
If you have no standard authentication system in your enterprise, you can use the authentication system managed within HOPEX.
☛ See [Viewing default authentication mode](#).

Defining an external authentication mode

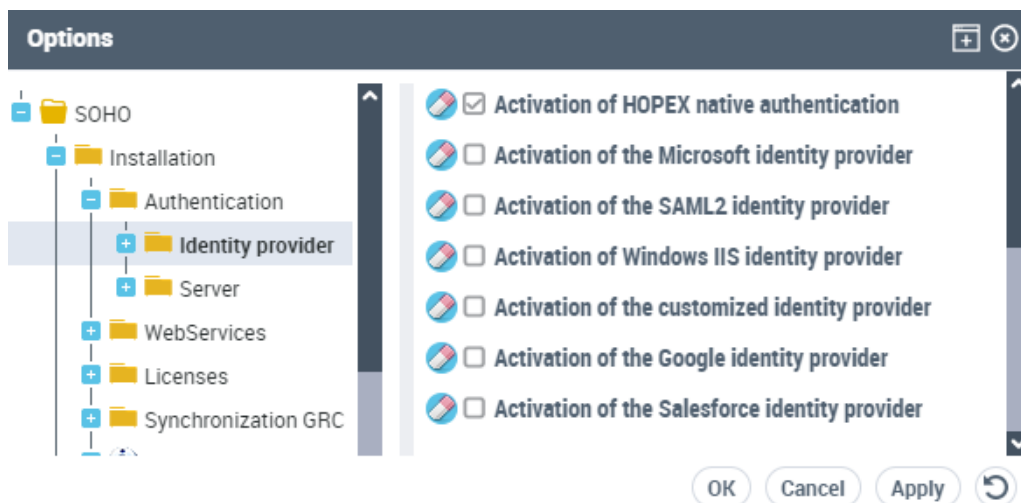
By default, authentication is managed within **HOPEX** platform.
You can choose to define an external authentication:

- SAML2
- openId

To choose an external authentication mode:

1. Access environment options.
☛ See [Modifying options at environment level](#).
2. Right-click **Options** and select "Extended".
3. Expand **Installation > Authentication** and select **Identity provider**.
By default "Activation of HOPEX native authentication" is selected.

4. Select your external authentication mode.



5. To configure your authentication, see **Installation and Deployment > HOPEX Unified Authentication Service** documentation.

Defining Default HOPEX Authentication Mode

By default, authentication is managed within **HOPEX** platform.

➤ Configuration of authentication delegated to a third party service is described in **Installation and Deployment > HOPEX Unified Authentication Service** documentation.

In the environment options, you can view and modify the **Authentication Mode**. This **Authentication Mode** enables to define the default **Authentication Mode** value (on the Login) of the user at creation.

Viewing default authentication mode

In the environment options, the default **Authentication Mode** values are:

- Standard (by default at installation)
- LDAP

To view default authentication mode:

1. Access environment options.
➤ See [Modifying options at environment level](#).
2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, view the value of the **Authentication Mode** option.

Defining default authentication mode to LDAP

When you define the default authentication mode to LDAP, users are managed in an LDAP directory and authentication is managed by the LDAP directory.

When you change the default authentication mode while users are already created, these users keep their defined authentication mode.

☛ To change the authentication mode of a user, see [Modifying a user authentication mode](#).

However, if you define the default authentication mode to LDAP, at authentication, whatever the person, the authentication service checks if the person belongs to LDAP. If the answer is:

- yes, the person is authenticated via LDAP.
- no, the authentication service checks on the login of the person if another authentication mode is defined.

☛ See also the full authentication diagram (including person groups): [Mapping Diagram](#).

To define default LDAP authentication mode:

1. Access environment options.

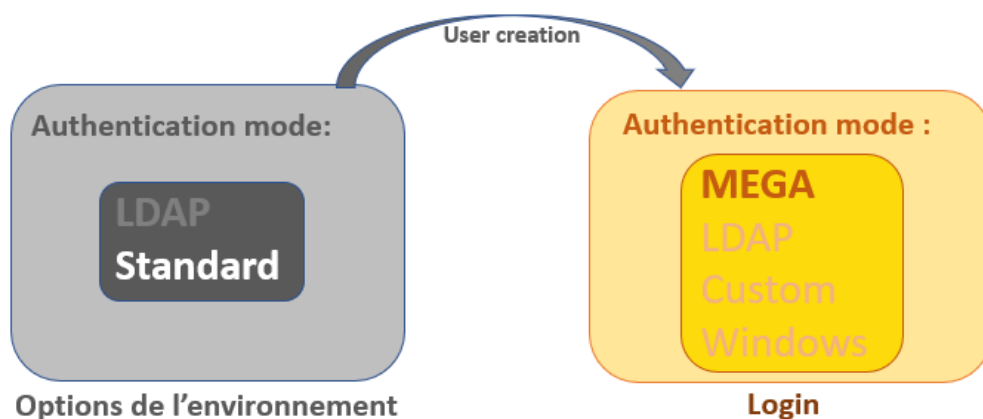
☛ See [Modifying options at environment level](#).
2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, for:
 - the **Authentication Mode** option, select "LDAP" value.
 - the **Default writing access area for LDAP import**, select the writing access area you want to define to the persons at LDAP import.

Modifying a user authentication mode

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

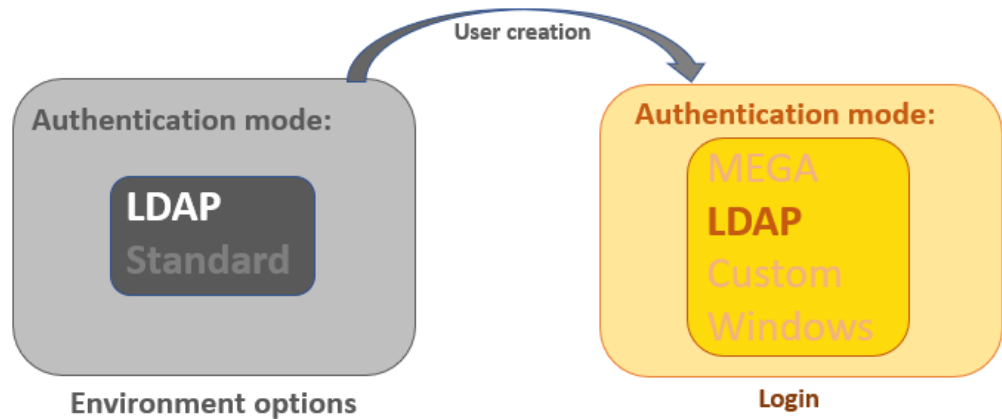
☛ See [Authentication mode \(case of authentication managed within HOPEX\)](#).

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](#)).



In "Standard" authentication mode, HOPEX (Web Front-End) provides the **MEGA** authentication mode (by default): the

HOPEX authentication service checks that the password entered matches the password stored in HOPEX repository.



In "LDAP" authentication mode, HOPEX (Web Front-End) provides the **LDAP** authentication mode (by default).
To modify the authentication mode of a user, see [Defining the Login of a Person](#).

Authentication Group

Authentication groups

LDAP authentication group

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

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 profiles

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.

SSO type authentication group

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

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

Defining an authentication group

Prerequisite: in case of LDAP authentication, the LDAP Server must be configured, see [Configuring LDAP Authentication](#).

To define an authentication group:

1. Access the authentication group management pages.
 See [Accessing the User Management Pages](#).
2. In the edit area, in the **Authentication groups** tab, right-click **Authentication groups** folder and select **New > Authentication group**.
 The authentication group creation window appears.
3. In the **Name** field, enter a name for the authentication group.
4. (LDAP authentication) In the **LDAP server** field, select your LDAP server.
5. In the **Authentication identifier** field:
 - (LDAP authentication) enter the identifier of the group within the LDAP directory or Active Directory.
 Example: OU=ResearchandDevelopment, OU=UNIVERSITE, OU=FRANCE, DC=fr, DC=mega, DC=com
 - (SSO authentication) enter the identifier of the claim with which you want to map the authentication group.
 Example: the claim role "rCmp-WebAXDevRemoteRdpTier2@MEGA"
6. Associate an HOPEX person group with the authentication group.
 See [Associating a HOPEX user group with an authenticated user group](#).

Configuring LDAP Authentication

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

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](#).

To configure LDAP authentication:

1. Create an LDAP server in **HOPEX Administration**.
 See [Creating an LDAP server](#).
2. Specify parameters of your LDAP server.
 See [Configuring the LDAP server](#).
3. (Optional) You can:
 - configure LDAP parameters
 See [Configuring an LDAP parameter](#).
 - modify LDAP import parameters
 See [Modifying LDAP directory import content](#).

4. Check the configuration of the LDAP server.
 - See [Checking the configuration of an LDAP server](#).
5. Once LDAP authentication is configured, you must:
 - import persons from the LDAP directory.
 - ⚠ **Do not overload HOPEX repository with user who are not intending to connect to HOPEX.**
 - See [Importing persons from an LDAP server](#).
 - or if you manage person groups:
 - define authentication groups and map them to person groups in **HOPEX**.
 - See [Defining an authentication group](#) and [Associating a HOPEX user group with an authenticated user group](#).

When connecting to **HOPEX**, the authentication service uses the HOPEX login and password entered by the user to authenticate the user with the list of available LDAP servers.

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](#) and that LDAP authentication is the user default authentication mode, see [Defining default authentication mode to LDAP](#).

To access LDAP server management:

1. From the **Administration** desktop, select the **LDAP Servers** sub-folder.
 - See [Accessing the User Management Pages](#).

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](#).
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](#).

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](#).

1. Access the LDAP server management pages.
➡ See [Accessing LDAP server management](#).
2. Select the new LDAP server and click **Properties** .

General	Characteristics	LDAP Parameters	Persons	LDAP Groups	Texts
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 the 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.
- (If needed) Select **Synchronize with LDAP directory** to synchronize LDAP parameters defined on the LDAP server (HOPEX) with the updates of the LDAP directory parameters.

☛ See [Configuring an LDAP parameter](#).

4. Click **Save**.

The LDAP server is configured.

You can also:

- configure an LDAP parameter, see [Configuring an LDAP parameter](#).
- modify content of LDAP directory import, see [Modifying LDAP directory import content](#).

Configuring an LDAP parameter

An LDAP parameter is an authentication parameter that exists in the LDAP directory and that 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" 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](#).
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 the person's characteristics corresponding to the LDAP parameters.
4. Enter a **Name** for the authentication parameter then click **Properties** .
Examples: E-mail, Name (person).
5. (Optional, "expert" metamodel access) Select **Index on Persons**, so that the parameter value enables unique identification of a person. If a person in **HOPEX** has the same e-mail as a person defined in the LDAP directory, this person is reused (instead of creating a new person and risking duplicating the same person).
6. (Optional, "expert" metamodel access) Select **Is available for search** so that an e-mail can be entered in the import entry area.
Example: if you enter ctodd@mega.com, you should find Clara TODD.
7. In the **Authentication Identifier** field enter the name of the attribute corresponding to the parameter within the LDAP directory or Active Directory.
Examples : mail, DN
8. In the **Mapped MetaAttribute** field, click the arrow and select **Connect MetaAttribute**.

9. Perform the search and select the MetaAttribute corresponding to the parameter within HOPEX.

Example: E-mail, Name (person).

Name	LDAP Server Name	LDAP Port
LDAP Server Paris	Paris	389

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

To define content of LDAP directory import:

1. Access environment options.
See [Modifying options at environment level](#).
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](#).
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](#).

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).

 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](#).
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](#).
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**.

Authentication and a user created on the fly

When a user has been created on the fly (see [Connection request and user created on the fly](#)), the LDAP parameters can be used as indexing identifier (**Index on Person** attribute, see [Configuring an LDAP parameter](#)) 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: the authentication service creates the login associated with the person.
 - Answer no: the authentication service creates the person and the login associated with the e-mail.

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

Configuring SSO Authentication

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

The claims

The claims are included in the SSO service.

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

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

To identify a person, you can for example map:

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

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

➡ See [Modifying the claim used for mapping authentication groups](#).

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

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

Example of information included in an SSO service:

```
{
  "ValidateLifetime": true,
  "AccessTokenType": "Reference",
  "TokenHandle": "52c900bcfe54f2ef081b3fa704e19e11",
  "Claims":{
    "aud": "https://hopex/UAS/resources",
    "iss": "https://hopex/UAS",
    ....
    "displayname": "Lou,Watts",
    "name": "lws",
    "email": "lwatts@mega.com",
    "given_name": "",
    "family_name": "Watts",
    "groupsid": [
      "S-1-5-21-0123456789-0123456789-513",
      "S-1-1-0",
      "S-1-5-32-544",
      "S-1-5-32-545",
    ],
    "role":[
      "Domain Users@MEGA",
      "Everyone",
      "Administrators@BUILTIN",
      "Users@BUILTIN",
      "NETWORK@NT AUTHORITY",
      "Authenticated Users@NT AUTHORITY",
      "This Organization@NT AUTHORITY",
      "rCmp-WebAXDevRemoteRdpTier2@MEGA",
      "tNtfs-USTLVUCSD651DImagesRecorderModify@MEGA",
      "tSvc-WebAX8AppXtenderRetentionFilingServiceFull@MEGA"
    ],
    "lws": "1ae8ad551970e66e071536655b9542ad"
  }
}
```

Configuring SSO Authentication

To configure SSO authentication:

1. Define the authentication parameters.

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

➡ See [Defining an Authentication Parameter](#).

2. If you manage person groups:
 - Define the authentication groups.
 - See [Defining an authentication group](#).
 - Map the authentication groups with the person groups defined in HOPEX.
 - See [Associating a HOPEX user group with an authenticated user group](#).

Modifying the claim used for mapping authentication groups

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

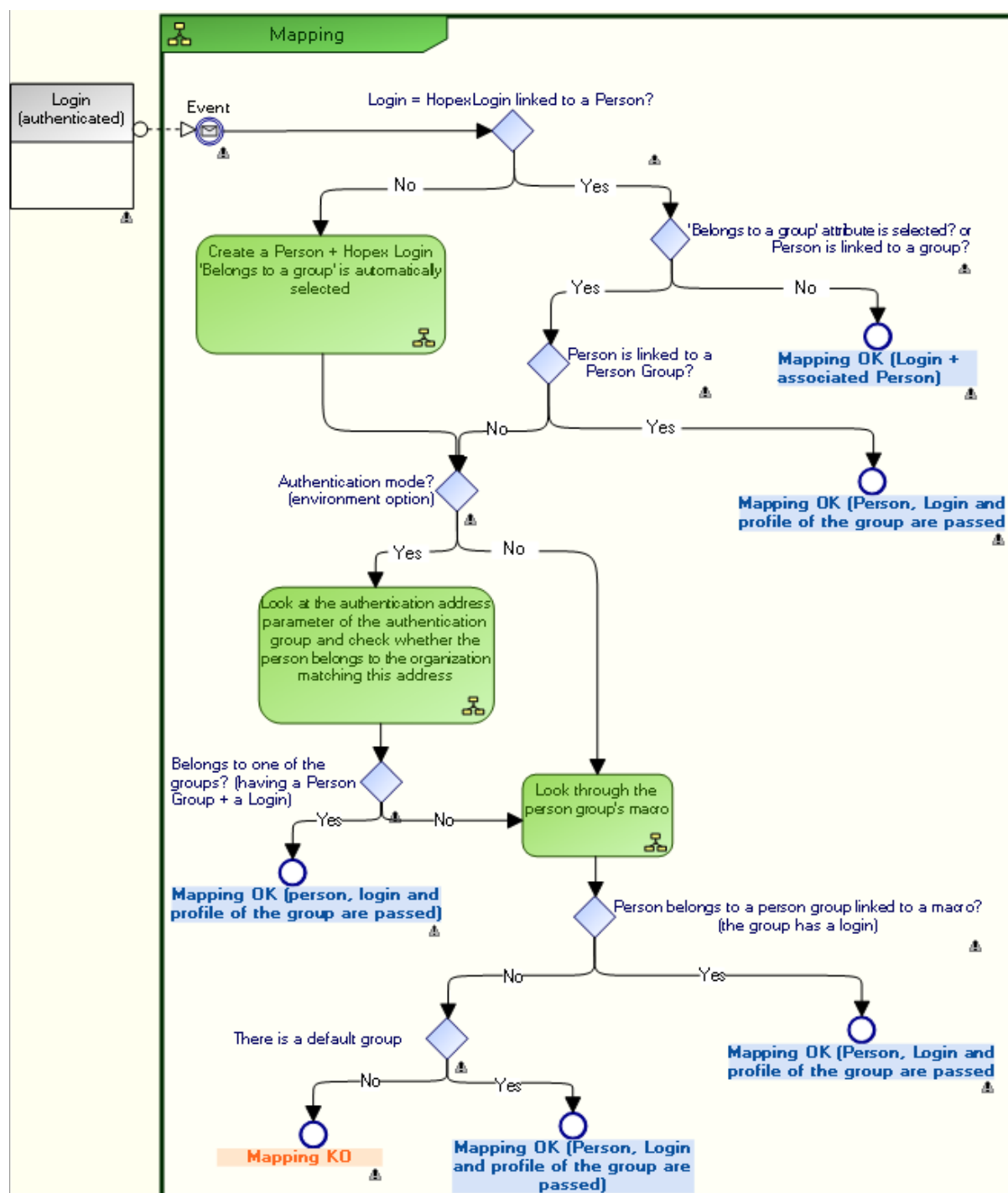
To modify the claim used for mapping authentication groups:

1. Access environment options.
 - See [Modifying options at environment level](#).
2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, modify the **Claim to be used for mapping to authentication groups** option.
Default value: role.

MAPPING

Mapping Diagram

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



Principle

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

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

See [Defining an Authentication Parameter](#).

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

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

☛ See [Creating and Managing a Person Group](#).

Connection request and user created on the fly

In the case of LDAP/SSO authentication, when an authenticated user requests connection to **HOPEX**:

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

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

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

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

So if the person:

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

Example: Alexandre DUBOIS belongs to the Marketing group whose login is Marketing,

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

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

- The person created on the fly (Assignable Element) from the LDAP/SSO server
The aim of creating a person on the fly is to keep a record of actions. The user acts in his/her name and not in the name of the group.
- The list of the person groups he/she belongs to (and his/her assignments, if he/she has profiles assigned).
A profile is associated with the group. This indicates with which profile the person created on the fly will connect to the application.

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

☛

Associating a HOPEX user group with an authenticated user group

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

So that when a person of the HOPEX person group connects to HOPEX, he/she is authenticated thanks to the user group authenticated in the LDAP directory or SSO service.

☛ *If a default person group is defined (example "Guests") any person in HOPEX with the **Belongs to a person group** attribute selected (see [Person Properties](#)) automatically belongs to the group defined by default (example: "Guests").*

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

☛ See:

[Creating a Person Group](#)

[Defining an authentication group](#)

[Defining a dynamic person group \(LDAP or SSO type\).](#)

To associate a HOPEX person group with an authenticated user group:

1. Access the properties of:
 - the authentication group
 - or
 - the person group.
- ☛ See [Accessing the User Management Pages](#).
2. Display the **Characteristics** page.
 3. Click the arrow of:
 - the **Person group** field and connect the HOPEX person group to be associated with the authenticated user group.
 - or
 - the **Authentication group** field and connect the authenticated user group to be associated with the person group.

The authentication Group query wizard appears.

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

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

Defining an Authentication Parameter

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

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

Authentication parameters enable to:

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

Example (LDAP): the "E-mail" 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).

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

To configure an authentication parameter:

1. Access the authentication management pages.

☛ See [Accessing the User Management Pages](#).

2. Select **Authentication parameters**.

3. Click **New** .

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

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



Examples: E-mail, Name (person).

5. (Optional, "expert" metamodel access) Select **Index on Persons**, so that the parameter value enables unique identification of a person. If a person in **HOPEX** has the same e-mail as a person defined in the LDAP directory or SSO service, this person is reused (instead of creating a new person and risk duplicating the same person).
6. (Optional, "expert" metamodel access) Select **Is available for search** so that an e-mail can be entered in the import entry area.

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

7. In the **Authentication identifier** field, enter:
 - (LDAP) the name of the attribute corresponding to the parameter within the LDAP directory or Active Directory.

Examples : mail, DN

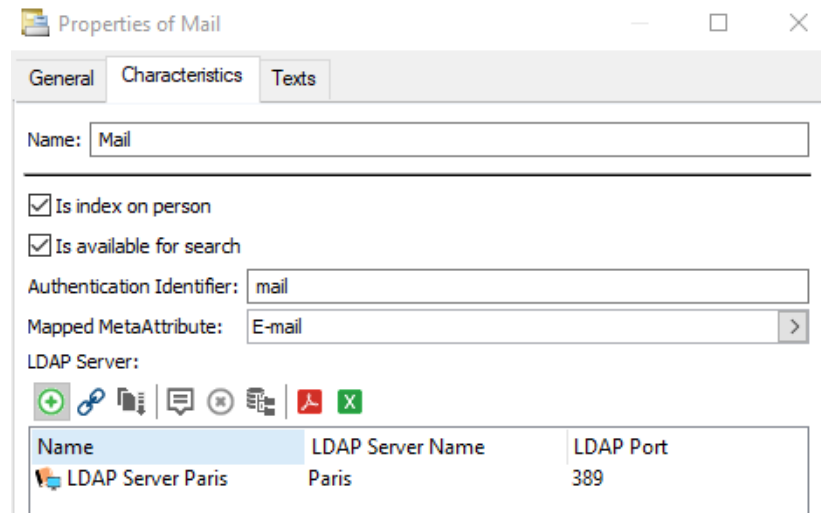
- (SSO) the claim associated with the SSO service.

Example: email

8. In the **Mapped MetaAttribute** field, click the arrow and select **Connect MetaAttribute**.
9. Perform the search and select the HOPEX MetaAttribute you want to associate with the authentication identifier (LDAP or SSP) defined step 7.

Examples: E-mail, Name (person).

10. (LDAP) In the **LDAP Server** pane, click **Connect** and connect the LDAP server.



Properties of Mail

General Characteristics Texts

Name: Mail

☒ Is index on person

☒ Is available for search

Authentication Identifier: mail

Mapped MetaAttribute: E-mail

LDAP Server:

Name	LDAP Server Name	LDAP Port
LDAP Server Paris	Paris	389

MANAGING THE PASSWORD OF A WEB USER

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

The following points are detailed here:

- [Initializing a User Web Account](#)
- [Modifying the Lifetime of the First Connection Link](#)
- [Modifying Password Management Configuration](#)
- [Reinitializing a User Password](#)
- [Defining a Temporary Password to a User](#)

Initializing a User Web Account

Prerequisite:

Before initializing the Web account of a user:

- ensure the e-mail of the person is specified.
 See [Viewing the Person Characteristics](#).
- check that the following options relating to Web applications are specified:
 - [Specifying the Web application access path](#)
 - [Specifying SMTP configuration](#)

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

To initialize the Web account of a user:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select the **Persons** sub-folder.
3. In the Persons list, select the person concerned.
4. Click **Initialize 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 lifetime of the first connection link, see [Modifying the Lifetime of the First Connection Link](#).

Modifying the Lifetime of the First Connection Link

To modify the lifetime of the first connection link:

1. Access environment options.
 See [Modifying options at environment level](#).
2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, modify the value of the **Life of first connection link** option.

Modifying Password Management Configuration

You can modify:

- the number of attempts to enter the correct password
 Default value: 3
- the password change frequency
 Default value: 40 days
- the number of non-reusable passwords, among the last passwords defined by the user
 Default value: 5
- the password security level
 Security levels are presented as colors as the user enter his password (Low : red, Medium : yellow, High : green)
 Default value: High

To modify configuration linked to password management:

1. Access environment options.
 See [Modifying options at environment level](#).
2. In the options tree, expand the **Installation** folder and select **User Management**.
3. In the right pane, you can modify the default configuration of options:
 - **Number of tries before password invalidation**
 Default value: 3
 - **Password expiry**
 Default value: 40 days
 - **Number of last non-reusable passwords**
 Default value: 5
 - **Password strength**
 Default value: High

Reinitializing a User Password

Prerequisite:

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

- [Specifying the Web application access path](#)
- [Specifying SMTP configuration](#)

☛ *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](#).
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.

Defining a Temporary Password to a User

☛ *This action is only available to **HOPEX Administrator** and **HOPEX Administrator production profiles**.*

This feature is useful for a user whose e-mail is not set. Without email, a user cannot define his/her password via the e-mail sent at account initialization.

☛ See [Initializing a User Web Account](#).

You must define this user a temporary password. At first connection to **HOPEX**, the user must change this password.

To define a temporary password to a user:

1. Access the user management page.
☛ See [Accessing the User Management Pages](#).
2. Select a **Persons** sub-folder.
3. In the edit area, select the person for whom you want to set a temporary password.
☛ *You can select several users. They will all have the same temporary password.*
4. Click **Set Password** .
5. In the **Password** field, enter the temporary password you want to set for the user.

6. Click **OK**.
The user's temporary password is saved.
At first connection to **HOPEX**, the user must enter this temporary password. Once connected he/she is prompted to define his/her password.

SPECIFYING THE DATA LANGUAGE

The data language is the language with which the user connects by default the first time. If the user changes his/her data language (see [Modifying the Data Language](#)) in the interface, this is kept for the next connection.

By default, the data language is defined in the environment options. If 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](#).
- the data language at environment level, see [Modifying the data language in Web applications at environment level](#).

To specify for a user or user group a data language different from that inherited and defined in environment options:

- 1 Modify the **Data Language** parameter in the user or user group properties.

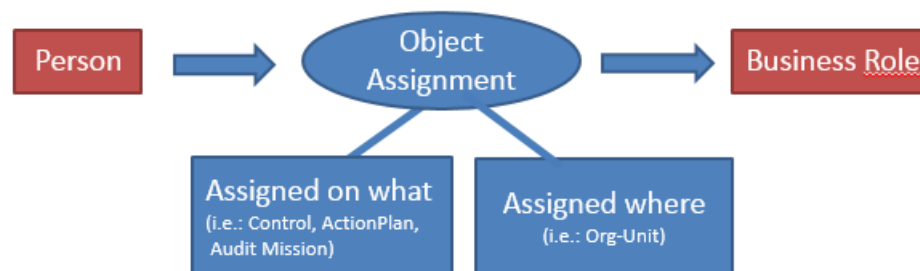
 See [Defining a Person](#).

 See [Viewing the Person Group Characteristics](#).

MANAGING BUSINESS ROLES

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

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



See:

- [Business Role Properties](#)
- [Creating Business Roles](#)
- [Defining a Business Role](#)
- [Assigning a Business Role to a Person](#)
- [Transferring Responsibilities to a Person](#)
- [Duplicate the Responsibilities of a Person](#)
- [Deleting a Business Role](#)

Business Role Properties

Name

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

MetaPicture

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

_GUIName

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

Multiplicity

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

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

Creating Business Roles

Specific business roles are supplied with each Solution.

☛ *See the guides specific to the Solutions.*

To create a business role:

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

☛ *See [Accessing the User Management Pages](#).*

2. Click **New** .

The business role creation 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](#).*

☛ *To define the business role, see [Defining a Business Role](#).*

Configuring a Business Role

Specific business roles are supplied with each Solution.

To configure a business role:

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

☛ *See [Accessing the User Management Pages](#).*

2. Select the business role concerned and click **Properties** .

3. Click **Characteristics**.

4. (Optional) In the **Business Role Status** field, modify the attribute value.

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

5. (Optional) In the **MetaPicture** field, click the arrow and select **Connect MetaPicture**.

- In the query field, enter the characters you want to find and click **Find**.

- In the results list, select the icon and click **OK**.

6. (Optional) In the **_GUIName** field, enter the business role name you want to be displayed in the interface.

Defining a Business Role

Defining a business role consists of defining:

- objects assigned to define a task to a person
E.g.: control, audit mission, action plan.
- localizing objects to define a specific location (in the organization of the company)
E.g. : USA agency.
For example, for risk management specific to the country where it is applied.
- optional parameters:
 - multiplicity to define the number of assignments of business roles possible for a person.
 ➤ A multiplicity business role 1 or 0..1 cannot be assigned to more than one person at the same time.
 - candidate queries, to filter persons to whom the business role can be assigned.
 ➤ See [Assigning a Business Role to a Person](#).

To define a business role:

1. Access the user management pages and select the **Business Roles** sub-folder.
 ➤ See [Accessing the User Management Pages](#).
 2. Select the business role concerned and click **Properties** .
 3. Click **Business Role Definition**.
 4. In the **Business Role Multiplicity** field, select the multiplicity for the business role.
 5. (optional) In the **Assigned MetaClass** section, click **Connect** .
- 🔔 **You must specify at least one of the two sections, see step 6.**

The MetaClasses query tool appears.

- (Optional) In the second field, enter the characters to search for.
 - 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 search for.
- 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 search for.
- Click **Find** .
- In the query results, select the query you want to connect.
- Click **Connect**.

The filtering query is connected to the business role.

E.g.: for the "Auditor of an audit mission" business role, the "Auditors and lead auditors (profile)" query is used to filter the persons who have the "Auditor" or "Lead Auditor" profile assigned.

- By default, filtering is not offered when assigning the business role to a person; in the **_FavoriteRequest** field of the query, select "Yes" to offer the filtering.
- Select **Propose all users** to, in addition to the query filtering, assign other persons who are not part of the filtering.

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

 See [Assigning a Business Role to a Person](#).

Assigning a Business Role to a Person

A business role can be assigned to a person:

- for a specific object

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

☛ See [Assigning an object to a person step 5](#).

- to a given geographical location

Example: David Oldfield is Risk Manager at London Branch.

☛ See [Assigning an object to a person step 6](#).

- to a given geographical location for a specific object

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

☛ See [Assigning an object to a person steps 5 and 6](#).

See:

- [Assigning an object to a person](#)
- [Mass assignment of objects to persons](#)

Assigning an object to a person

☛ To assign one or more objects to one or more persons at a time, see [Mass assignment of objects to persons](#)

☛ To assign an object to a person from the user management page, see [Mass assignment of objects to persons](#).

To assign an object to a person:

1. Access the properties of the person.

☛ See [Viewing the Person Characteristics](#).

2. In **Assignments**, click **Object Assignments**.

3. Click **New** .

4. In the **Business Role** field, click the drop-down menu and select the business role concerned.

5. (If necessary) In the **Assigned Object** field, click the arrow and select **Search**.

☛ This field appears only if the selected business role has at least one assigned object, see [Defining a Business Role](#).

In the 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 search for.
- Click **Find** .
- Select the object and click **OK**.

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

 This field appears only if the selected business role has at least one Localizing MetaClass, see [Defining a Business Role](#).

In the query dialog box,

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

Mass assignment of objects to persons

To perform a mass assignment of objects to persons:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select a **Persons** sub-folder.
The list of persons appears.
3. Select the persons concerned.
4. Click **Assign Objects**.
5. In the list of business roles, select the business role in question.
 Only the business roles that can be assigned to more than one person at the same time (cardinality >1) are displayed.
6. In the **Assigned Object** frame, click **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 search for.
 - Click **Find** .
8. Select the object and click **Connect**.
 You can select more than one.
9. Click **Connect**.

Transferring Responsibilities to a Person

From the **Administration** desktop, you can transfer all or part of user responsibilities to one or more users.

The responsibilities transferred are deleted from the source user. To keep the responsibilities you can duplicate the responsibilities of the source user.

 See [Duplicate the Responsibilities of a Person](#).

To transfer the responsibilities from one person to another:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select a **Persons** sub-folder.

3. In the list of persons, select the person for whom you want to transfer the responsibilities and click **Transfer responsibilities**.
 You can select more than one person.
 The responsibilities transfer wizard opens.
4. (If required) Select the person then click **Properties**  to view or modify the assignments of the source person.
5. Click **Next**.
6. Click **Connect** .
7. (Optional) In the query wizard, in the second field, enter the character string you want to search for.
8. Click **Find** .
9. Select the person to whom you want to transfer the responsibilities.
 You can select more than one person.
 If you select more than one target user, only the object assignments that can be assigned to more than one person are available.
10. Click **Connect**.
11. Click **Next**.
12. Select the responsibilities you want to transfer.
 - In the **Profile Assignment** frame, select the profiles that you want to transfer to the target user (or to the selected persons).
 - In the **Object Assignments** frame, select the object assignments that you want to transfer.
13. (optional) In the **Validity date of profile assignments** part, you can modify the validity dates defined for the source person. Select:
 - **Assignments always valid** to avoid restricting the validity of assignments.
 - **Define validity dates** (and select the validity start and end dates).
14. Click **OK**.
 The assignments selected are deleted from the source user (or source users) and transferred to the target user (or target users).

Duplicate the Responsibilities of a Person

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

To duplicate the responsibilities from one person to another:

1. Access the **User Management** pages.
 See [Accessing the User Management Pages](#).
2. Select a **Persons** sub-folder.

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

 You can select more than one person.

 If the button is hidden, click  to access it.

The responsibilities duplication wizard opens.

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

 You can select more than one person.

 **Only object assignments that can be assigned to more than one person are available (see the definition of the multiplicity of a business role: [Defining a Business Role](#)).**
10. Click **Connect**.
11. Click **Next**.
12. In the **Profile Assignments** frame, select the profiles that you want to assign (duplicate) to the target user (or to the selected persons).
13. In the **Object Assignments** frame, select the assignments that you want to assign (duplicate) to the target user (or to the selected persons).
14. Click **OK**.
The selected assignments are assigned (duplicated) to the target user (or target users).

Deleting a Business Role

To delete a business role:

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

 See [Accessing the User Management Pages](#).
2. Select the business role you want to delete.

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

MANAGING WORKSPACES



Workspaces are managed by the administrator.

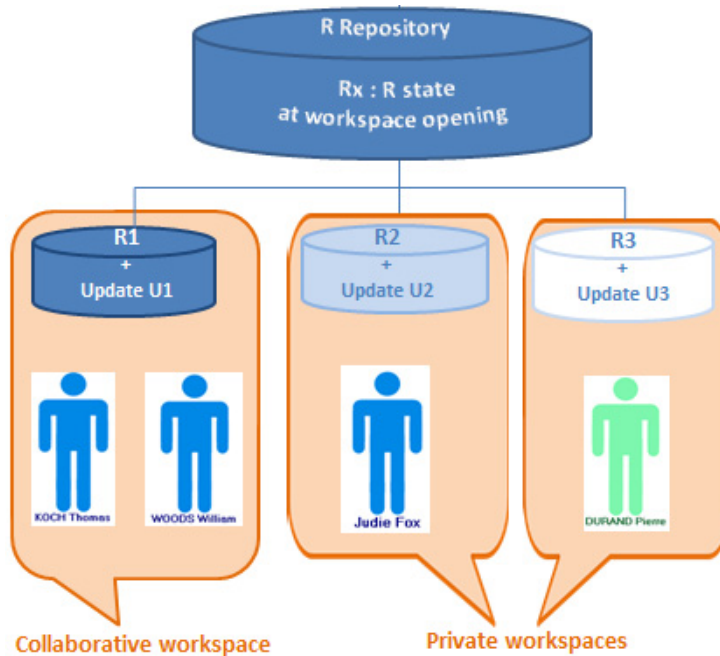
The following points are covered here:

- ✓ [Private Workspace Principle](#)
- ✓ [Using Your Private Workspace](#)
- ✓ [Workspace Administration](#)
- ✓ [Private Workspace Life: Example](#)
- ✓ [Performance and Health Tests](#)
- ✓ [Managing Updates](#)
- ✓ [Managing locks](#)

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](#).

The user controls opening duration of his/her private workspace.

➡ *The private workspace is open for each user on both his/her repository and on the system repository. A private workspace always*

exists on system repository even if the user is not using any of the system repository objects.

Several users can have private workspaces open in parallel. In his/her private workspace, the user is independent of updates carried out simultaneously by other users in their respective private workspaces.

☛ *Locks* inform the user of objects modified by others. See [Managing locks](#).

The user can also update his/her private workspace with the updates of other users. To do this, the user refreshes his/her private workspace.

☛ See [Refreshing Data](#).

HOPEX allows several users to work at the same time.

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](#)
- [Saving Sessions](#)
- [HOPEX Repository State Changes](#)
- [Dispatching Your Work](#)
- [Dispatch Conflicts](#)
- [Rejects When Dispatching](#)
- [Refreshing Data](#)
- [Conflicts When Refreshing](#)
- [Discarding Work](#)
- [Exiting a Session](#)
- [Workspace Administration](#)
- [Displaying Updates Made in the Repository](#)
- [Exporting a Private Workspace Log](#)

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

To connect to a **HOPEX** desktop:

1. Start the **HOPEX** application from its HTTP address.
 - ☛ *If you do not know this address, contact your administrator.*
 The connection page appears.
2. In the **Login** field, enter your identifier.
3. In the **Password** field, enter your password.
 - ☛ *If you have lost your password, click **Forgot Password**, see [Resetting Your Password](#).*

4. 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 drop-down menu for groups, select the group with which you want to connect or "My assignments" to connect with one of your own assignments.
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.
9. 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.

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 modifications you have made in your *session* since the last save:

1. In your **HOPEX** desktop, click **Main Menu** .
2. Click **Save**.

☛ These modifications are not saved in the repository. To save your modifications in the repository, you must dispatch these modifications, see [Dispatching Your Work](#).

HOPEX Repository State Changes

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

➤ See example [Private Workspace Life: Example](#).

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

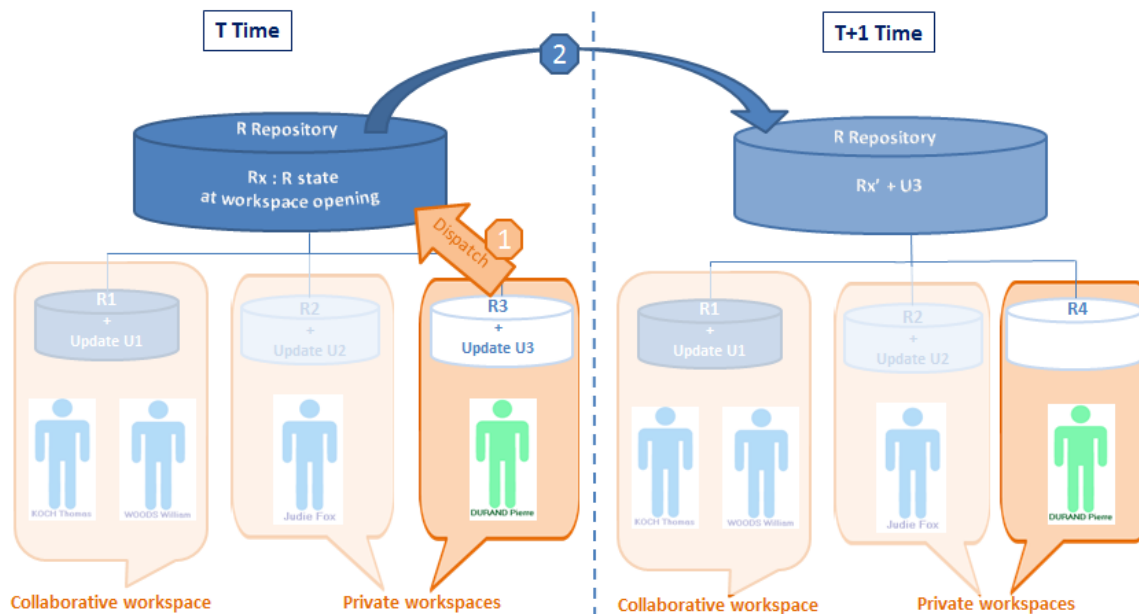
The repository changes from state N to state N+1 with memorization of new data related to the previous situation (state N).

If the user does not save updates, the changes made since the last valid state are forgotten. The repository remains in state N. Note that **HOPEX** repository state changes are managed automatically.

A workspace opens on the latest states of the repository and system repository.

Dispatching Your Work

Dispatch consists of making public the work carried out in a private workspace, 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](#).

From your Web desktop, to dispatch your work in the repository:

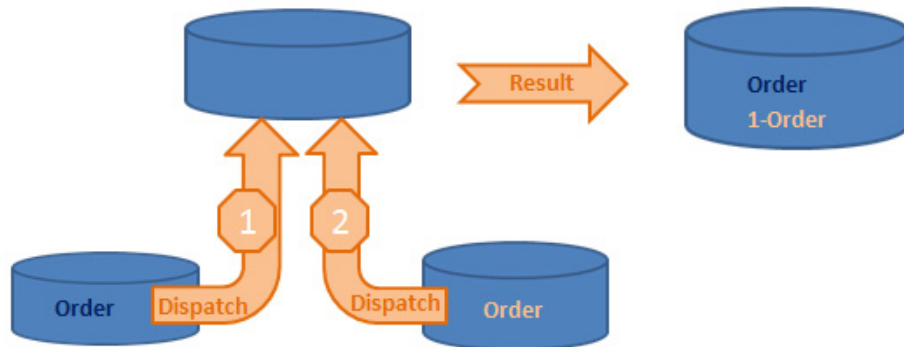
1. In your **HOPEX** desktop, click **Main Menu** .
2. Click **Dispatch**.
Your modifications are saved in the repository.

Dispatch Conflicts

The dispatch process automatically manages most conflicts that may arise when several users make updates.

Creation of duplicated objects

When duplicate objects are created, a prefix is added before the name of the second object.



Two users create an object with the same name. The first to dispatch his/her work actually creates the object. The second user to dispatch his/her work creates an object with a prefixed name.

This is indicated in the dispatch report.

The administrator or the users can then decide to rename one of these objects if they are actually different, or combine them into one object if they are in fact the same object.

Deletion of already deleted objects or links

As the deletion has already been performed, nothing happens. There is no mention of this in the dispatch report.

Modifying or linking a renamed object

This happens when a user modifies an object that in the interim has been renamed by another user, or tries to link something to this object. The new one is kept and the changes are executed normally. The object can be found using its *absolute identifier*. Note that this does not create a reject, but the dispatch report indicates that the object was renamed.

 *An absolute identifier is a string of characters associated with each object in the repository. This string is computed using the date and time the session was opened, the number of objects created since the session started, and the object creation date (in milliseconds). An absolute identifier provides a unique way to identify an object in the repository, so that even if the object is renamed, all the links to it are retained.*

Rejects When Dispatching

There are normally no rejects when dispatching work carried out in a private workspace. Most conflicts are managed automatically.

Rare cases of rejects are listed in the *rejects file*.

 *When updating a repository (importing, restoring, dispatching), a reject file is created in order to store rejected commands. Rejected commands are stored with the reason for which they were rejected. These are found in the "MegaCrd.txt" file located in the environment folder.*

Change in writing access values between opening and dispatching a private workspace

If you have access to the writing access management function, you can, for example, protect an object in the repository while a user is deleting it in his/her private workspace. When the user dispatches his/her work, he/she is no longer allowed to delete the object and the deletion is rejected.

Rename/create collisions

A user renames an object in his/her private workspace, for example, from "Customer" to "Customers". Then another user dispatches his/her private workspace in which he/she created an object having the same name "Customers". When the first user dispatches his/her private workspace, since the "Customers" object already exists, the object "Customer" cannot be renamed "Customers". The rename command will therefore be rejected.

Verifying link uniqueness

A user creates a link for which there is a uniqueness check. For example, he/she indicates that the "Order" message is sent by the "Customer" org-unit. In the meantime, another user indicates in his/her private workspace that the "Order"

message is sent by the "Customers" org-unit. When the second user dispatches his/her private workspace, the link is rejected if the uniqueness control imposes that a message can be sent by only one object.

☛ See the **HOPEX Power Studio - Imposing MetaAssociation Uniqueness** Technical Article for information on MetaAssociation uniqueness check.

Attribute uniqueness (other than name)

Other attributes besides name may also be checked for uniqueness. If two users give two different objects the same value for this attribute, the second update will be rejected.

Updating a deleted object

If a user has made changes to an object in his/her private workspace and the object has been deleted by another user, the updates are rejected. The **Connect** and **Change** commands concerning this object are also rejected. All these rejects are listed in the private workspace report file.

Refreshing Data

A user can see modifications dispatched by other users of this repository without dispatching his/her own modifications. To do this, the user refreshes his/her data.

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.

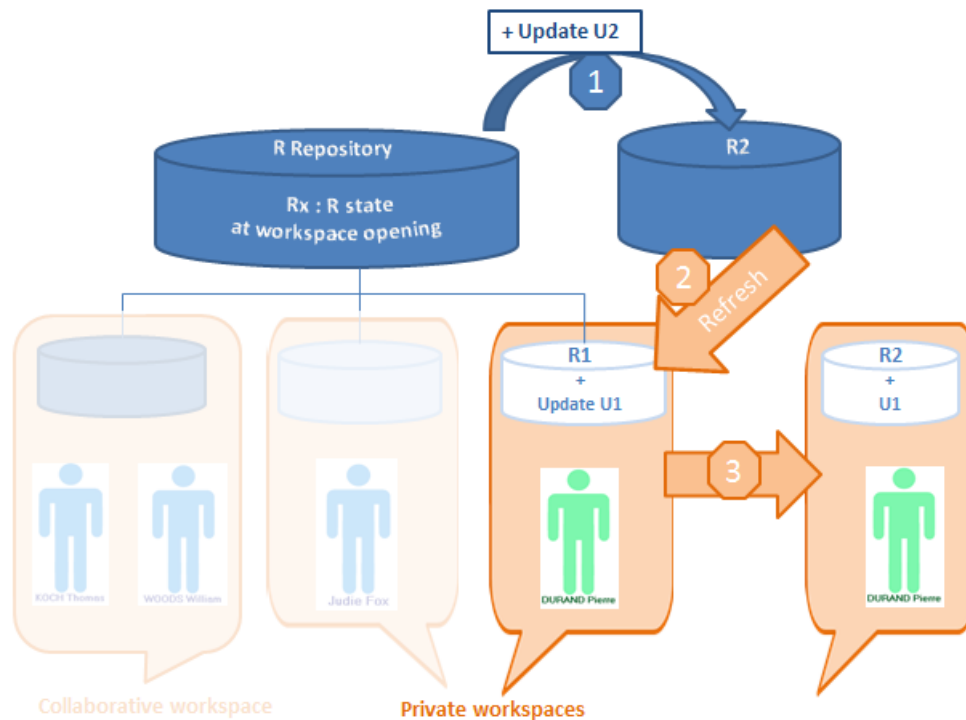
Refreshing allows a user to incorporate repository and system repository changes made by other users, without dispatching current work.

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](#).

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



In your Web desktop, to update your workspace with data dispatched in the repository by the other users:

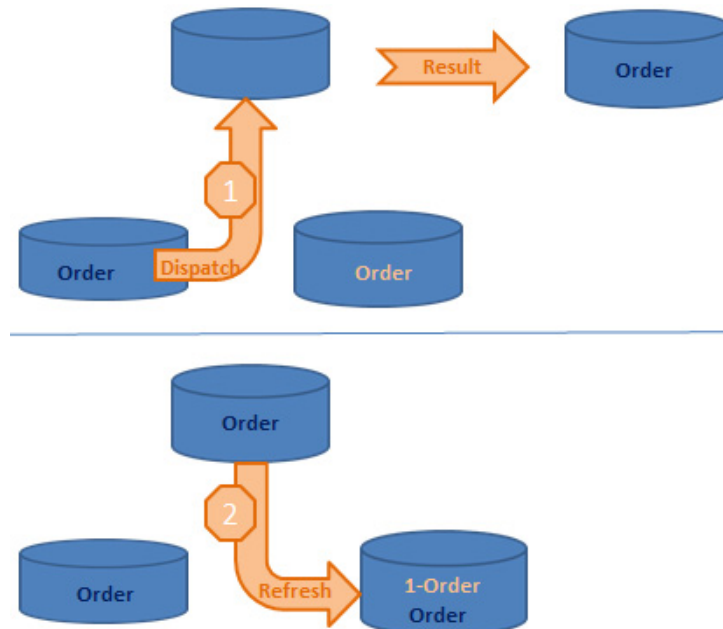
1. In your **HOPEX** desktop, click **Main Menu** .
2. Click **Refresh**.

 Your workspace is updated.

Conflicts When Refreshing

Conflicts when refreshing are the same as when dispatching, but they apply to the private workspace only.

☛ For more details on the main causes of rejects, see [Dispatch Conflicts](#) and [Rejects When Dispatching](#).



As is true in dispatching, if two objects are created with the same name, the second object name is prefixed:

The second "Order" object is renamed "1-Order".

Discarding Work

Discarding a workspace (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 **Main Menu** , select **Export**.

2. In the **Main Menu** , select **Discard**.

☛ You can also discard your private workspace at disconnection, see [Exiting a Session](#) (choose not to dispatch modifications).

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 **Main**

Menu , select **Export**.

2. In the **Main Menu** , select **Collaborative workspace > Discard**.

☛ Your 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

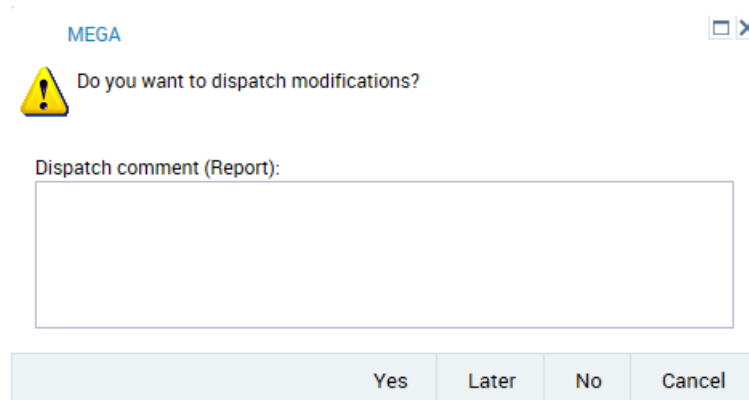
☛ These modifications will remain awaiting validation, subsequent modification, or deletion.
 - cancel modifications you have made.
- a collaborative workspace you can:
 - keep modifications you have made

☛ 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.



2. (Optional) In the **Dispatch comment (Report)** frame, enter a comment to remind you of modifications made in your private workspace.
3. Select your **HOPEX** exit mode.
 - ☛ Click **Cancel** to not exit your private workspace.
 - **Yes**
Modifications you have made in your private workspace are saved in the repository.
 ☺ *In order to work effectively as a team, it is recommended that you dispatch frequently and regularly. Other users can update their own private workspace without dispatching their work (menu **File > Refresh**).*
 ☛ *This exit mode also allows the user to select a different repository the next time he/she logs in.*
 - **No**
All modifications you made since your last dispatch will be lost. 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.
 ☛ **You can have only one current private workspace. When you select the "Later" exit mode, any next session open in a private workspace re-opens the pending private workspace (the profile being the same or not). The private workspace exit mode is**

applied to all of the modifications you have made in this private workspace (desktops being the same or not).

☛ *When you switch the desktop (in private workspaces), if you want to keep your modifications in a desktop, it is recommended that you dispatch them.*

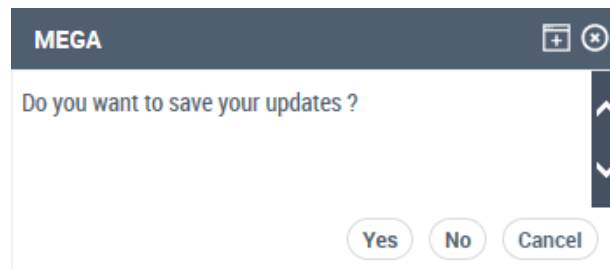
Exiting a session from a collaborative workspace

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.



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](#)
- [Deleting a Workspace](#)

Accessing the Management Page for Workspaces

To access the list of current workspaces in an environment:

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

Workspace Management

Discard and Delete

Publish and Delete

Export logs and Delete

Excel

Instant Report

	Name ↑	User	Type	Access Mode	Creation Date	Status
☐	de BELLEG...	de BELL...	Private workspace	Read/Write	6/13/2019 4:38:48 ...	Inactive
☐	GARNIER ...	GARNIE...	Private workspace	Read/Write	6/13/2019 7:15:58 ...	Inactive
☒	GLEVER He...	GLEVER...	Public workspace (Micro)	Read/Write	6/14/2019 9:16:15...	Active
☐	IMPERIALI...	IMPERI...	Private workspace	Read/Write	6/13/2019 11:35:1...	Inactive
☐	KOTBI Saad	KOTBI S...	Public workspace (Micro)	Read/Write	6/14/2019 11:07:4...	Active
☐	LE GUELLE...	LE GUEL...	Private workspace	Read/Write	6/13/2019 2:11:06 ...	Inactive
☐	MA.IID Mar	MA.IID	Private workspace	Read/Write	6/13/2019 4:40:03	Inactive

« < | Page 1 of 1 | > »

Show

50

elements

Displaying 1 - 24 of 24

Persons who have accessed the workspace

	Name ↑	User	Access Mode	Duration (Days)	Session Start	Session End	Code	Status
☒	GLEVER H...	GLEVER...	Read/Write	0	6/14/2019 9:16:...		HGR	Active

The management page for workspaces currently in progress details the following for each workspace:

☛ To sort workspaces according to a column, click the header of the corresponding column.

😊 You can also arrange columns in the order you want. To do this, click the header of the column to be moved and, holding down the mouse button, move it to the required position.

- the **User** of the workspace
- the **Type** of workspace:
 - "Private Workspace":
The user can modify data. His/her updates are kept in his/her private workspace until dispatched.
 - "Public Workspace (micro)":
The user can modify data. As soon as he/she saves his/her updates, they are visible to other users.
The user sees the updates of other users, as their updates progress.
- the **Access Mode** of the workspace, for example:
 - "Read/Write" when a session is open.
 - "Read-only" when the user is in consultation only.
 - no value, if the private workspace is passive (the user has saved his/her session but is not currently connected to **HOPEX**).
 - no value if the user is in offline mode
- its **Creation** date and time
- the **Status** of the workspace
 - 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](#).

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: deletion 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

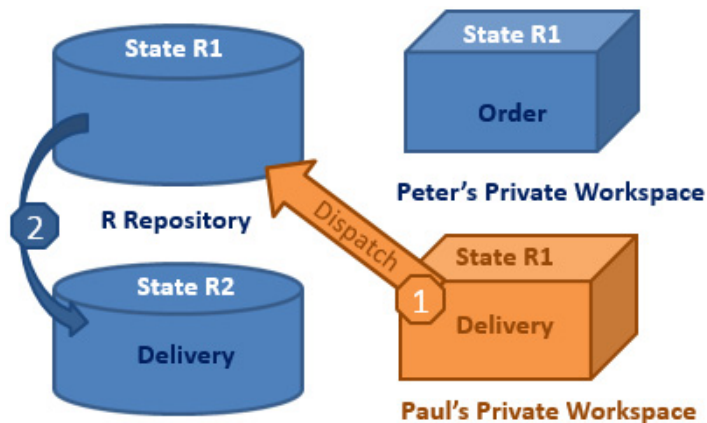
To illustrate how private workspaces work, the following is an example of some steps in the work of several users:

Private workspace 1



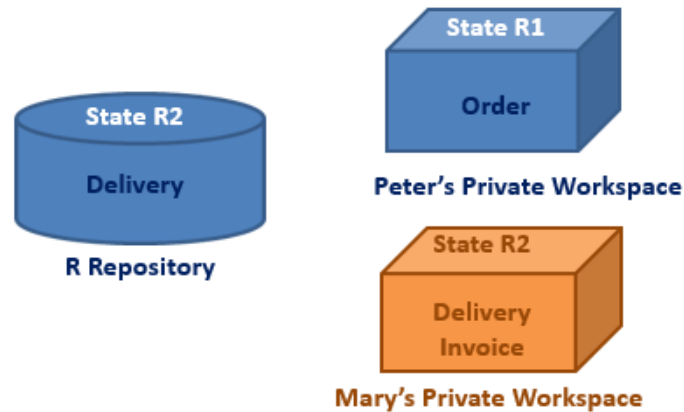
- Peter opens a private workspace, his repository view is state "n" (R1).
- He creates the "Order" message, which he links to the "Customer" org-unit.
- In parallel, Paul dispatches his private workspace...

Private workspace 2



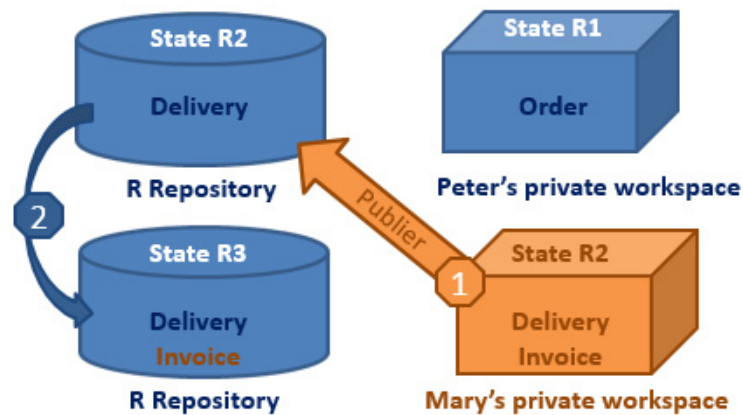
- The private workspace that Paul dispatched created the "Delivery" message, linked to the "Customer" org-unit.
- Paul's dispatch changes the repository to state "n+1" (R2).
- This new message is not seen from Peter's private workspace...

Private workspace 3



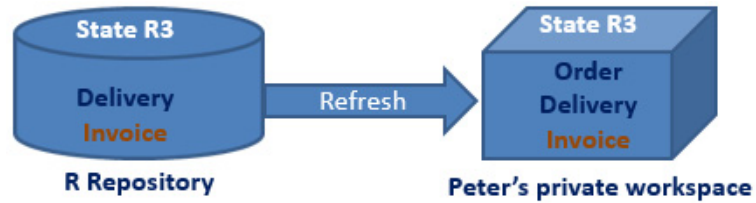
- Mary opens a new private workspace, her repository view is state "n+1" (R2).
- Mary creates the message "Invoice" connected to the "Customer" org-unit...

Private workspace 4



- Mary dispatches her private workspace.
- The repository moves to state "n+2" (R3).
- Peter's view is still in state "n" (R1).
- Peter refreshes his private workspace...

Private workspace 5



- Peter has refreshed his private workspace.
- His view now corresponds to state "n+2" (R3).
- He can now see the "Customer" org-unit with the additions made by Paul and Mary.
- Peter dispatches his private workspace...

Private workspace 6



- When Peter, Paul, and Mary have dispatched their work, all the modifications they have made are visible in state "n+3" (R4) of the repository.

PERFORMANCE AND HEALTH TESTS

With **HOPEX** you can daily generate a repository health report. This report enables to detect:

- performance or usage anomalies that users can face daily.
- any significant change.

For this purpose, performance and health tests are run daily. Events are generated when anomalies are detected

➡ See [Events: Infrastructure Performance and Repository Health](#).

Test Description

Infrastructure performance test description

HOPEX standard use scenarios are carried out every afternoon ("RepositoryHealth Daily Afternoon Trigger" job, 04:00 pm GMT):

- Reading of 1000 existing large objects (BLOB).
- Exploring an existing graph (1000 objects and 500 MetaAssociations).
- ERQL query on an existing graph (1000 objects and 500 MetaAssociations).
- Reading of 1000 large texts (BLOB).
- Creation of a graph including 1000 objects and 500 MetaAssociations.
- Deletion of a graph including 1000 objects and 500 MetaAssociations.
- ERQL query on a recently created graph (1000 objects and 500 MetaAssociations).

➡ *In a cluster-type configuration, performances are measured on all of the machines.*

Each scenario generates a result, which is stored in the repository. These results are analyzed daily in the evening ("RepositoryHealth Daily Evening Post Trigger" job, 11:05 pm GMT)

An history of 30 results are needed before generating an alert.

Repository health test description

It is essential to analyze certain usages to identify anything that might compromise data integrity, whether in the daily work or following a **HOPEX** update.

For all of the repositories of all of the environments, the following checks are performed every evening ("RepositoryHealth Daily Evening Trigger" job, 11:00 pm):

- Administration
 - Compatibility checks between the SQL structure of the data and the server version.
 - table fragmentation
 - index fragmentation
 - SQL maintenance plan execution
- Customization
 - HOPEX data modification
 - HOPEX data volume
- Usage
 - workspace volume

 In a cluster-type configuration, usage tests are performed randomly on a single machine only.

Viewing the HOPEX Health Report

Accessing HOPEX daily health reports

The **Administration** desktop gives access to HOPEX daily health reports. Each report includes the anomalies detected on all the machines, in all the repositories. Reports are listed chronologically (the oldest first) in the following format:

HopexHealthFullReportYYYY-MM-DD_hh-mm-ss.html

with: YYYY: year, MM: month, DD: day, hh: hours, mm: minutes, and ss : seconds.

The report icon is represented by:

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

To view HOPEX daily health reports:

 To access the content of the **Repository Management** pane, you must have **Expert** metamodel access (see [Configuring the Metamodel Access](#)).

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

 See [Connecting to the Administration Desktop](#).

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



The report is displayed in a new browser tab.

HOPEX Health Report Details

Infrastructure Alerts (-)

Host: WIN-5FI7NVKBR16 (-)

No performance fall detected on this host.

Host: 787-500-TST5233 (-)

No performance fall detected on this host.

Host: W-HGR-NEW (-)

No performance fall detected on this host.

Data Alerts (-)

Environment: EnvTestsLab_SQLSERVER_787_500tst_5233 (-)

Repository: EA (-)

Query Execution Alert (+)

Full scans may be normal for some requests. If possible, try to make your queries on the smallest possible set of elements.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

Data Volume Alert (+)

Exceeding the maximum number of recommended objects may rise usage/ergonomic problems.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

Repository: SOHO (-)

Query Execution Alert (+)

Full scans may be normal for some requests. If possible, try to make your queries on the smallest possible set of elements.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

Macro Execution Alert (+)

It may be normal for a macro to exceed the execution time limit and you can disable, on an individual basis, the monitoring of those macros.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

Data Volume Alert (+)

Exceeding the maximum number of recommended objects may rise usage/ergonomic problems.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

Repository: SystemDb (-)

SQL Maintenance Alert (+)

Mitigation: With your DBA, schedule the SQL maintenance plan - at least - every week. If the problem persists, reduce the time frame between two maintenance plan executions.

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

HOPEX Health report description

The HOPEX health report includes a short description of the anomalies detected at performance or usage level. It shows alerts detected at:

- infrastructure level (**Infrastructure Alerts**)
- data level (**Data Alerts**) for each repository of each environment

Example : detection of three alerts ("Query Execution Alert", "Macro Execution Alert" and "Data Volume Alert") at data level, on "Soho" repository.

Data Alerts (-)

 **Environment: EnvTestsLab_SQLSERVER_787_500tst_5233 (-)**

 **Repository: EA (+)**

 **Repository: SOHO (-)**

 **Query Execution Alert (+)**

Full scans may be normal for some requests. If possible, try to make your queries on the smallest possible set of elements.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

 **Macro Execution Alert (+)**

It may be normal for a macro to exceed the execution time limit and you can disable, on an individual basis, the monitoring of those macros.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

 **Data Volume Alert (+)**

Exceeding the maximum number of recommended objects may rise usage/ergonomic problems.

Mitigation: Please call or email your MEGA contact to confirm users might not face issues using HOPEX.

 **Repository: SystemDb (+)**

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](#)
- [Private Workspaces and Repository Size](#)
- [Exporting a Private Workspace Log](#)

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 the Metamodel Access](#)).

1. Connect to the **Administration** desktop.
☛ See [Connecting to the Administration Desktop](#).
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 listed by day, week and month.
3. Expand the folders to access the dispatch you are interested in.
4. Click the dispatch.
The dispatch property pages are displayed in the edit area.
5. Click **Updates**.
The **Updates** page details the content of the dispatch in the form of a list of actions displayed in chronological order.

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

➡ See [Exporting a Private Workspace Log](#).

The screenshot displays the 'Repository Activity' window. On the left, a tree view shows 'Repository Dispatch' for 'SOHO' with a list of actions from 2019/06/04. The right pane is titled 'General' and shows details for a selected action: 'Create' on a 'Folder of Favorites' object. Below the table, a log shows the command and its output.

Action	Target	Object	Object	Responsible
Create	Folder of Favorites	Favorites	LAZAF	LAZAF
Connect	Owned Folder of F...	LAZARE ...	Favor...	LAZAF
Update	Folder of Favorites	Favorites	LAZAF	LAZAF
Create	GraphSet	[Duplicate...	LAZAF	LAZAF

```

- "~zWq)l4GD5n40[Folder of Favorites]" ""
.Create "~zWq)l4GD5n40[Folder of Favorites]" "" -
.CHK "JpXczffzSfZUC30000mCpCpCV0heYCQAEzbC" -
"--52000000L40[Create Version]" "30837" -
"--51000000L00[Creation Date]" "2019/06/04 16:21:17" -
"--(10000000v30[Creator]" "V0heYCQAEzbC" -
"--61000000P00[Modification Date]" "2019/06/04 16:21:17" -
"--b1000000L20[Modifier]" "V0heYCQAEzbC" -
"--210000000900[Name]" "9A1C9A7D5CF67A3A" -
"--(20000000z70[Reading access area identifier]" "sTIVwxH3100" -
"--62000000P40[Update Version]" "30837"

```

Private Workspaces and Repository Size

Private workspace life

A private workspace gives a user a frozen view of a repository.

When the repository is modified by other dispatched private workspaces, this private workspace keeps the view it had when created.

Since the data corresponding to these views is kept in the repository, its size grows, and may become disproportionate to the actual repository contents.

➡ See [Dispatching Your Work](#) and [Refreshing Data](#).

Private workspace monitoring

More than one user can connect to a single repository via network share. The first time a user connects to the repository, he/she opens a private workspace. This private workspace ends only when the user dispatches, discards, or refreshes his/her modifications, and not when simply disconnecting from the **HOPEX** repository.

➡ See [Refreshing Data](#) and [Discarding Work](#).

Modifications made by the user are saved in a temporary space (data) in his/her private workspace dedicated to the data of his/her private workspace. The repository is updated only when the user dispatches these changes.

➡ See [Dispatching Your Work](#).

All data accessed by a user is "frozen" for the duration of the private workspace.

Example:

If an object is renamed in the reference repository after the private workspace is opened, the user sees the previous name unless the private workspace is refreshed. However, users connecting after the modification has been dispatched will have a view reflecting the most recent state of the repository.

If other users connected before you dispatch your updates, and are accessing the same data as you, they will have an obsolete view of the data until they refresh their private workspace. Note that when you dispatch your updates, your view is refreshed automatically.

This means that data being accessed by user A and modified at the same time by user B is duplicated. It is stored in its initial state for each user private workspace; if a user makes a change, the previous state is stored along with the new one.

When the updates are dispatched and all users accessing the updated data have refreshed their private workspaces, the previous state is no longer required.

Modifying the maximum duration of a private workspace

By default the maximum duration of a private workspace is 6 days

Once this duration has elapsed, at connection, a message prompts the user to dispatch or refresh his/her private workspace.

To modify the maximum duration of a private workspace:

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

Exporting a Private Workspace Log

You can create an export file (*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](#).
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](#)
- [Managing Locks on Objects](#)

Principle

With the network version, concurrent accesses to objects can be checked using *locks*.

Preventing conflicts

As soon as a user modifies an object, a lock is placed on this object. Another user can thus only view this object. This user cannot access a new update until the first user dispatches his/her private workspace, and he/she refreshes his/her private workspace. This prevents conflicts between the state of the object in the repository and the obsolete view of the second user.

Deleting a lock or unlocking an object

Lock management is automatic. You do not normally need to delete locks or unlock objects.

The few exceptions are due to abnormal operations, for example when a private workspace has been deleted from the private Workspace management window, or at desynchronization of clocks.

When a lock is deleted, another user can modify the object without dispatching or refreshing his/her private workspace.

 *A user can delete locks placed on his/her private workspace since its creation.*

When a user dispatches his/her work, the lock (his/she had placed on an object) is unlocked but not deleted. The lock is deleted only when all other private workspaces, which were created before the lock was unlocked, are closed. A private workspace is closed when it is dispatched, discarded, or refreshed.

Details on the operating method of the locks

HOPEX only indicates that objects are locked when their attributes are modified (unlike links for example).

Warning on unlocking

If you attempted to use an object that was locked, a message alerts you as soon as the object is freed for you to use again.

Diagrams

There are two types of locking applied to diagrams

- **The diagram has simply been viewed and not modified:** as soon as the first user closes the diagram it can be opened by a second user.
- **The diagram has been modified:** as for classical locking, the second user must wait until the diagram has been dispatched by the first user and therefore unlocked.

Managing Locks on Objects

The lock management page of the **Administration** desktop provides access to:

- the **Locks** page, which details for each lock:
 - the **Name** of the object concerned
 - the **Type** of object concerned
 - the **User** who owns the lock
 - the date and time (GMT0) of the **Lock**, and, if applicable, **Unlock**.
 - the **Status** of the lock (locked or otherwise)

➡ See [Viewing locks on objects](#).

- the **Immutable Locks** page, which details the following for each immutable lock:
 - the **Name** of the object concerned
 - the **Type** of object concerned
 - the **User** who owns the lock
 - its **Lock** date and time (GMT0).
 - the **Status** of the lock (locked or otherwise)

➡ See [Managing immutable locks on objects](#).

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.

Lock Management						
 Properties  Locks  Immutable Locks  Unlock  Unlock and propagate						
	Name ↑	Type	User	Lock Date	Status	
☐	1. AS-IS::6. APM:...	Application	Administra...	2016/07/21 1...	Protected	
☐	1. AS-IS::6. APM:...	Request P...	Administra...	2016/07/21 1...	Protected	
☐	1. AS-IS::6. APM:...	Service Poi...	Administra...	2016/07/21 1...	Protected	
☒	1. AS-IS::6. APM:...	Request P...	Administra...	2016/07/21 1...	Protected	
☐	1. AS-IS::6. APM:...	Applicatio...	Administra...	2016/07/21 1...	Protected	
☐	1. AS-IS::6. APM:...	Applicatio...	Administra...	2016/07/21 1...	Protected	
☐	1. AS-IS::6. APM:...	Applicatio...	Administra...	2016/07/21 1...	Protected	
☐	1. AS-IS::6. APM:...	Software T...	Administra...	2016/07/21 1...	Protected	
☐	1. AS-IS::6. APM:...	Software T...	Administra...	2016/07/21 1...	Protected	

Viewing locks on objects

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

1. Connect to the **Administration** desktop.
 See [Connecting to the Administration Desktop](#).
2. In the **Repository Management** pane, click the **Lock Management** sub-folder.
The **Lock Management** page appears and displays by default the **Locks** list.
3. (Optional) To sort locks according to column, click the column header.
 You can also arrange columns in the order you want. To do this, click the header of the column to be moved and, holding down the mouse button, move it to the required position.
4. 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](#).
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](#)
- ✓ [Comparing and Aligning Objects Between Repositories](#)
- ✓ [Managing UI Access \(Permissions\)](#) (function available with **HOPEX Power Supervisor**)

IMPORTING - EXPORTING A COMMAND FILE

Export of an object with propagation enables creation of a consistent set allowing transfer of part of the repository to another repository. For example, export of **HOPEX** objects from a library includes objects present in the library and their dependent objects.

From your **Administration** Web desktop, you can import command files to a **HOPEX** repository:

-  See [Importing a command file in HOPEX](#).
 - in **text format** (.MG*).
 -  For more details on .MG* file syntax, see [Command File Syntax](#).
 - In **MEGA XML format**. These files have .XMG extension and contain commands or data (objects and links).
 -  For more details on MEGA XML data exchange format, see technical article [MEGA Data Exchange XML Format EN](#).

The following points are detailed here:

- [Importing a command file in HOPEX](#)
- [Exporting Objects](#)

Importing a command file in HOPEX

You can update a repository by importing a command file produced by the repository backup tool, an export file of an object, or any other means of command file production.

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

1. Connect to the **Administration** desktop.
 -  See [Connecting to the Administration Desktop](#).
2. In the **Administration** tab, click the **Tools** pane.
The management tree for tools appears.
3. In the tree, select the **XMG/MGL/MGR > Import** sub-folder.
The **Hopex File Import - Parameterization** page appears.
4. In the **Command File** field, click **Browse**  to browse the folders and select the backup file.
 -  The command file must not exceed 30 MB.
5. 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 if no reject encountered** saves the changes only if no rejects were encountered.
 - **Never** is used to carry out tests before the effective update, for example for syntax checking.
8. In the **Checks** pane, the checks to be carried out are selected automatically, based on the file extension:
 - **Check Absolute Identifiers** is not selected in the case of a command file that does not come from a **HOPEX** repository.
 - **Control writing access areas** is selected when the **HOPEX Power Supervisor** technical module is available on the site, ensuring that the user who executed the update has the corresponding writing access in the repository.
 - ☛ *For command files with the MGR extension (repository backup), absolute identifiers are included in the imported objects and writing access levels are maintained.*
 - ☛ *For command files with the MGL extension (log extraction 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** pane, select the import behavior to be applied:
 - **Standard Reprocessing** changes creation of an already existing object into a modification, or into creation of an object of the same name preceded by a number if their absolute identifiers are different.
 - **Reassign User** ignores the writing accesses contained in the imported file. All elements in the imported file are given the same writing access level as the user executing the import. This is useful when you have the **HOPEX Power Supervisor** technical module. The creator and modifier names are replaced with the name of the user executing the import.
 - ☛ *It is recommended that you enable this option when the import file comes from an environment where the writing access diagram is not the same as the one for the environment where this file is being imported.*

The options you select are controlled by the software, based on the file extension and the standard processing to be applied. If your choices are not consistent with the file extension, a message box informs you of this fact and its possible consequences.

 - ☛ *For more details on the main causes of rejects, see [Dispatch Conflicts](#) and [Rejects When Dispatching](#).*
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](#).

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\DiagrammeAuthentication.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\DiagrammeAuthentication.mgr
- Environment : C:\Users\Public\Documents\MEGA 2009 SP5\Demonstration
- DataBase : Adventure
- User : User
- *****

- Root objects:
- Authentication_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:

- **plain text**

The exported file is in the form of an .MGR file.

☛ For more details on .MGR file syntax, see [Command File Syntax](#).

- **XML MEGA**

The exported file is in the form of an *.XMG file containing commands or data (objects and links).

☛ For more details on MEGA XML data exchange format, see technical article "MEGA Data Exchange XML Format 70".

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

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

☛ See [Connecting to the Administration Desktop](#).

2. In the **Administration** 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](#).

COMPARING AND ALIGNING OBJECTS BETWEEN REPOSITORIES

HOPEX enables comparison and alignment of:

- two complete repositories
- objects in different repositories
- objects of the public repository with those of the current private workspace.
- 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](#)
- [Compare and Align Warnings](#)
- [Compare and Align](#)

Compare and Align Principle

The principle of comparing and aligning objects between repositories is as follows:

1. **Extraction**

The selected objects and any linked objects are extracted from the two repositories, browsing links according to **HOPEX** principles of object extraction.

Comparison

The two sets of data are compared on the basis of *absolute identifiers* of the objects they contain.

2. **Comparison result**

A window displays the results of the comparison. You can also generate a report and a command file in this window.

☛ *The page showing differences displays a maximum of 1000 lines. If the list of differences is greater than 1000 lines, a message prompts you to either ignore this limit and display all the lines (in this case, the list may take some time to load) or not.*

3. **Alignment**

The upgrade command file is imported in the target repository.

Compare and Align Warnings

You must be aware of the following points before alignment and selection of the user executing alignment.

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](#).*

To compare and align:

1. Connect to the **Administration** desktop.
 - ☛ See [Connecting to the Administration Desktop](#).
 - ☛ 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 and go to step 10.

⚠ **Warning:** processing of this option can be time-consuming.

7. Click **Next**.
The dialog box for selection of objects to be compared opens.
8. In the **Perimeter** field, select the perimeter type (by default **Standard for Comparison**)

⚠ For detailed information on perimeters, see the **HOPEX Power Studio - Perimeters** technical article.

9. In the **Elements to compare** pane, select:

- **Add from source**  to add objects from the source repository, or
- **Add from target**  to add objects from the target repository.

⚠ If you have opened the comparison wizard from an object, this object is automatically added in the list of objects to be compared.

10. Click **Next**.

The **Comparison Progress** window opens. It presents the differences between compared objects and their modifications.

Comparison - Comparison Progress

Difference list:

	Order...	Difference	Kind	Target	Object 1	Object 2
	23	Connected	Link	(Time Period/Lifecycle Status)	Accounting Link [Production]	Pro
	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

Generate a difference file

Generate a report

Previous Next OK Cancel

The **Difference** column presents differences by update category:

- **Created**: objects not existing in the target repository.
- **Deleted**: objects existing in the target repository but not in the source repository.
*Deletion commands of compare and align can be generated in a separate file. 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)

Introduction to UI Access Management (Permissions)

Prerequisites and definitions

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

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

You can manage:

- **object UI access**

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



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

- **general UI access**

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

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

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

Accessing the UI Access Management Pages (Permission)

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

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

 See [Object UI Access Values](#).

 See [Managing UI Access](#).

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

 See [Object UI Access Values](#).

 See [Managing General UI Access](#).

To access the UI access management pages:

1. Connect to the **HOPEX Administration** desktop with the **HOPEX Administrator** profile
 -  See [Connecting to the Administration Desktop](#).
2. In the **Administration** tab, click the **Permissions** pane.

3. In the **CRUD Management** tree, select the sub-folder:
 - **Object UI access**
 - **General UI access**

Object UI Access Values

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

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

When a MetaClass is hidden to a user, it is not available in the repository.

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

MetaClass occurrence access permissions

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

- C: Create
- R: Read
- U: Update
- D: Delete

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

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

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

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

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

☛ See:

[Customizing the UI Access \(Permissions\) of an Existing Profile and Customizing the Characteristics of an Existing Profile / Creating a Profile from an Existing Profile.](#)

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

For example the "Auditor/Controller" Set of UI access rights (of the **Auditor/Controller** profile) inherits from

the permissions defined on the "Auditor" and "Internal Controller" Sets of UI access rights.

Properties of Auditor/Controller

General

Characteristics

Texts

Name: *

Auditor/Controller

Used Set of UI Access Rights

New

Connect

Reorganize

Name ↑	Customizing Set of UI Access Rights
Auditor	
Internal Controller	

- Inherited from the permissions defined by default (<HOPEX default>), if it does not use any Set of UI access rights.
 See [Creating a Profile](#).

Object UIs

Access Rights: *

Auditor/Controller

Perspective: *

<Default>

MetaModel: *

HOPEX Internal Audit

MetaAttributes / MetaAssociationEnds / Tools

Name ↑

Permission

Account

-R

Application

-R

Audit

*CRUD

Audit Activity

*CRUD

Audit Theme

*CRUD

Business Line

-R

Business Process

-R

Control

-CRUD

Control System

*CRUD

Expense (Mission)

*CRUD

Expense Sheet

*CRUD

External reference

*CRUD

Finding

*CRUD

General Task

*CRUD

Name ↑

SlaveMetaClass

Link Permis...

Attached Document

Business Doc...

*CRUD

Attached Document ...

Business Doc...

*CRUD

Audit Activity

Audit Activity

*CRUD

Audit Plan

Plan

*CRUD

Audit Theme

Audit Theme

*CRUD

Business Process

Business Pro...

*CRUD

Context Of

Assessment ...

*CRUD

MetaAssociationEnd's MetaAttributes / Slave MetaClasses / MetaAssociations

Name ↑

Permission

Associative Object

*RU

Link Comment

*RU

Link creation date

*R

Link Creator

*R

Workflow Definition

In the **Object UIs** tab:

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

To define access permissions on objects, see:

- [Modifying access permissions on occurrences of a MetaClass.](#)
- [Modifying access permissions on MetaAttributes of a MetaClass.](#)
- [Modifying access permissions on tools of a MetaClass.](#)
- [Modifying access permissions of a link around a MetaClass.](#)
- [Modifying access permissions on links around a MetaClass.](#)

Modifying access permissions on occurrences of a MetaClass

To modify access permissions on occurrences of a MetaClass:

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

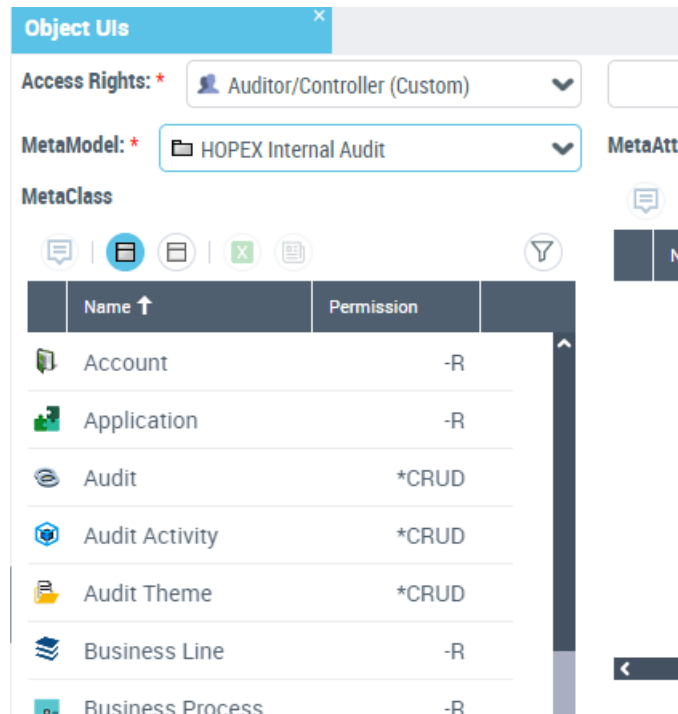
➤ See [Accessing the UI Access Management Pages \(Permission\)](#).

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

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

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

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



Name ↑	Permission
Account	-R
Application	-R
Audit	*CRUD
Audit Activity	*CRUD
Audit Theme	*CRUD
Business Line	-R
Business Process	-R

4. In the **MetaClass** frame, select the MetaClass for which you want to modify configuration of access permissions.
 By default, its configuration is that inherited from <HOPEX Default>.
5. In the **Permission** field, enter the new value.
 See [MetaClass occurrence access permissions](#).

MetaClass








Name ↑	Permission
 Account	-R
 Application	-R
 Audit	CRU
 Audit Activity	+CRUD

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
Account	-R
Application	-R
Audit	*

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

MetaClass

Name ↑	Permission
Account	-R
Application	-R
Audit	?

Help

i Meta permission for 'Audit' : CRUD
Licence and CommandLine permission for 'Audit' : CRUD

OK

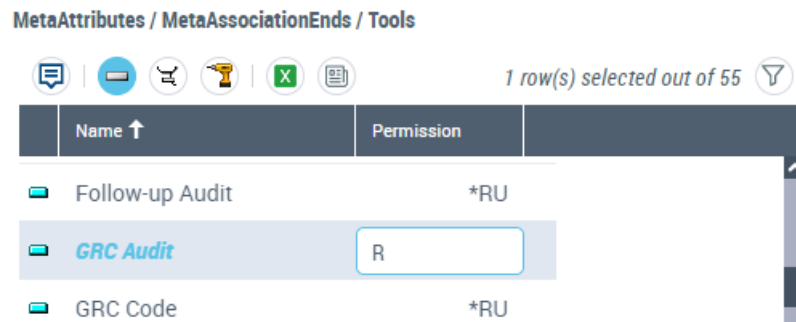
You can also modify the MetaAttributes/MetaAssociationEnds/Tools of a MetaClass, see:

- [Modifying access permissions on MetaAttributes of a MetaClass.](#)
- [Modifying access permissions on tools of a MetaClass.](#)
- [Modifying access permissions of a link around a MetaClass.](#)
- [Modifying access permissions on links around a MetaClass.](#)

Modifying access permissions on MetaAttributes of a MetaClass

To modify access permissions of MetaAttributes of a MetaClass:

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



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

Modifying access permissions on tools of a MetaClass

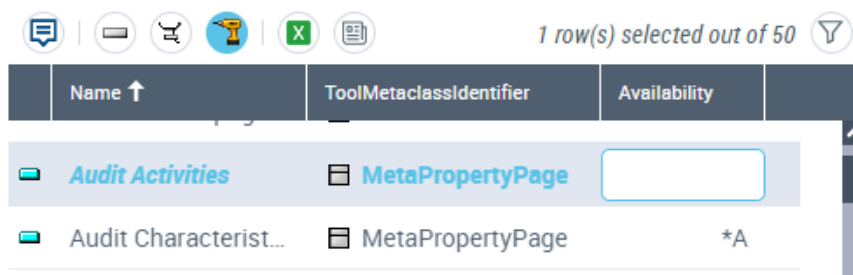
A tool can be available or not.

To modify access permissions on tools of a MetaClass:

1. Access the UI access management pages and select the **Object UI Access**.
See [Accessing the UI Access Management Pages \(Permission\)](#).

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

MetaAttributes / MetaAssociationEnds / Tools



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

Modifying access permissions of a link around a MetaClass

To modify access permissions of a link around a MetaClass:

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

7. In the **Permission** field, enter the new value.
 See [MetaAssociationEnd access permissions](#).

MetaAttributes / MetaAssociationEnds / Tools

1 row(s) selected out of 26

	Name ↑	SlaveMetaClass	Link Permis...
	Attached Document ...	 Business Doc...	*CRUD
	Audit Activity	 Audit Activity	*CRUD
	Audit Plan	 Plan	*RUD
	Audit Theme	 Audit Theme	*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](#).

Modifying access permissions on links around a MetaClass

You can modify access permissions on:

- the link according to the MetaClass accessed via the link
- one of the MetaAttributes of the link
- one of the MetaClasses accessed via the link

Example: You can grant rights to connect (but not to create) an IT Service to an Application via this same link.

To modify access permissions on links around a MetaClass:

1. Select the MetaAssociationEnd.
 See [Modifying access permissions of a link around a MetaClass, steps 1 to 6](#).
2. In the menu bar of the **MetaAttributes of MetaAssociationEnds/ Slave MetaClasses/MetaAssociations**, click **MetaAttribute** , **MetaClass** , or **MetaAssociation** .
3. In the list, select the MetaAttribute, MetaClass or MetaAssociation concerned.
4. In the **Permission** field, modify the permission value.
 See [MetaAttribute access permissions](#).
 See [MetaClass occurrence access permissions](#).

5. Press "Enter".

The value of the access permission is modified.

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

☛ To obtain information on origin of an inherited value, enter the character ?.

Rules on permissions while aggregating Sets of UI access rights

When a **Set of UI access rights** uses one or several Sets of UI access rights, its permissions are defined by addition of permissions defined on the Sets of UI access rights it uses.

Example:

The Sets of UI access rights S1 and S2 are connected to the Set of UI access rights S3 of the profile P3.

If the permission value on an object A of the Set of UI access rights S1 is CR and the one of the Set of UI access rights S2 is RUD, then this permission value on object A for the Set of UI access rights S3 is CRUD.

Attention to default values

A permission value with * means that this value is the default permission value and that it has not been specifically defined. Only those values specifically defined are taken into account in aggregation.

Example:

The Sets of UI access rights S1 and S2 are connected to the Set of UI access rights S3 of the profile P3.

If the permission value on an object A of the Set of UI access rights S1 is *CRUD and the one of the Set of UI access rights S2 is R, then this permission value on object A for the Set of UI access rights S3 is R.

Generating a Report on Permissions by Profile

The following report templates enable to generate permission related reports:

- **Profile Permission report** enables to generate the detail of permissions for a given profile.
- **Profile Permissions comparison Report** enables to compare permissions of several profiles.
- **Workflow Permissions** enables to generate the detail of permissions for a given workflow.

Generating a report on permissions

To generate a report on permissions:

1. In your **HOPEX** desktop, access your reports.
 - ☛ See [Accessing your reports in a HOPEX solution..](#)
2. Click **New** .

3. (Optional) In the **Local Name** field, modify the default report name.
4. In the **Report Template** pane, select the report template concerned.
 *Use the table filtering tool to easily access the report type.*
5. Click **Next**.
6. Select the report parameters:
 - in the **MetaModel** pane, click **Connect** and select the metamodel concerned.
 *For the **Workflow Permissions** report template, in the **Workflow** field, click the arrow and select **Connect Workflow Definition**.*
 - in the **Profile** field, click the arrow and select **Connect Profile**.
 *For a faster result, do not select a large number of profiles.*
7. Click **OK**.
 The report is generated as a matrix.
 *Generation can take some time, depending on the parameters you have selected.*
8. (If needed) Filter the report according to permission values.

Report content

All MetaClasses of the selected metamodel appear in the report.

For each MetaClass, the report displays:

- (in rows) all MetaAttributes, Tools, MetaAssociations (and MetaAttributes of MetaAssociations) of the MetaClass.
- (in columns) permissions for all selected profiles.
 *For improved readability, missing permissions are replaced by _.*
*For example: *RU is replaced by *_RU_.*

Managing General UI Access

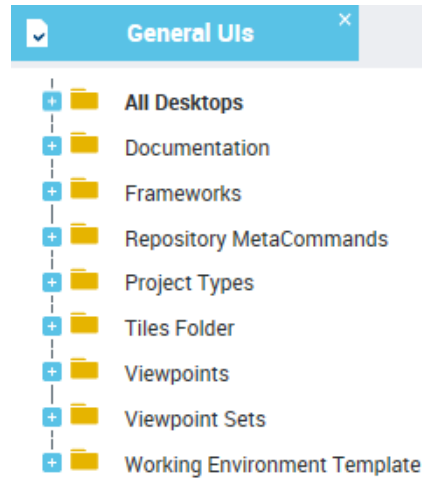
You can manage general UI access for a profile. General UIs are classified by category:

- desktop
- command category
- command group
- general command
- properties page
- tree

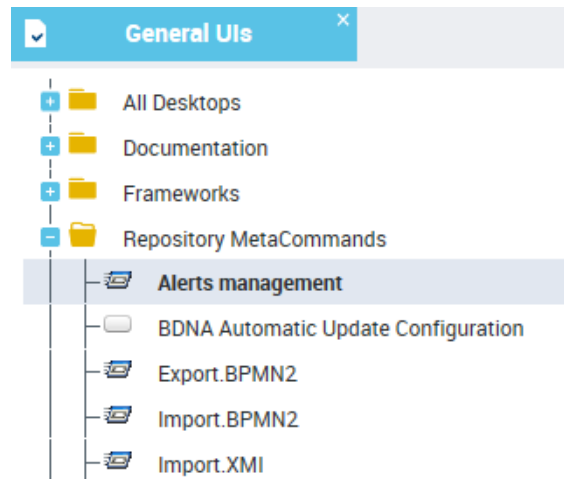
To manage general UI access:

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

➡ See [Accessing the UI Access Management Pages \(Permission\)](#).



2. Expand the folder of the category concerned.
3. In the list, select the tool concerned.



4. In the **Access rights and Availability** pane, select the Set of UI access rights for which you want to modify access on the tool.

5. In the **Tool Availability** field, enter the availability value.

Access rights and Availability

X Excel

Instant Report

	Name ↑	Perspective	Tool Availability
	Application Design Funct...	<Default>	*A
	Application Design Viewer	<Default>	*A
	Application Designer	<Default>	*A
	ArchiMate Application Ar...	<Default>	*A
	ArchiMate Business Arch...	<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](#)
- ✓ [Accessing Options](#)
- ✓ [Option Groups \(User Level\)](#)
- ✓ [Web Application-Linked Options](#)
- ✓ [Managing Languages in Web Applications](#)
- ✓ [Managing Date Format](#)

OPTIONS OVERVIEW

In the **Administration** desktop, **HOPEX** options can be configured at the following levels:

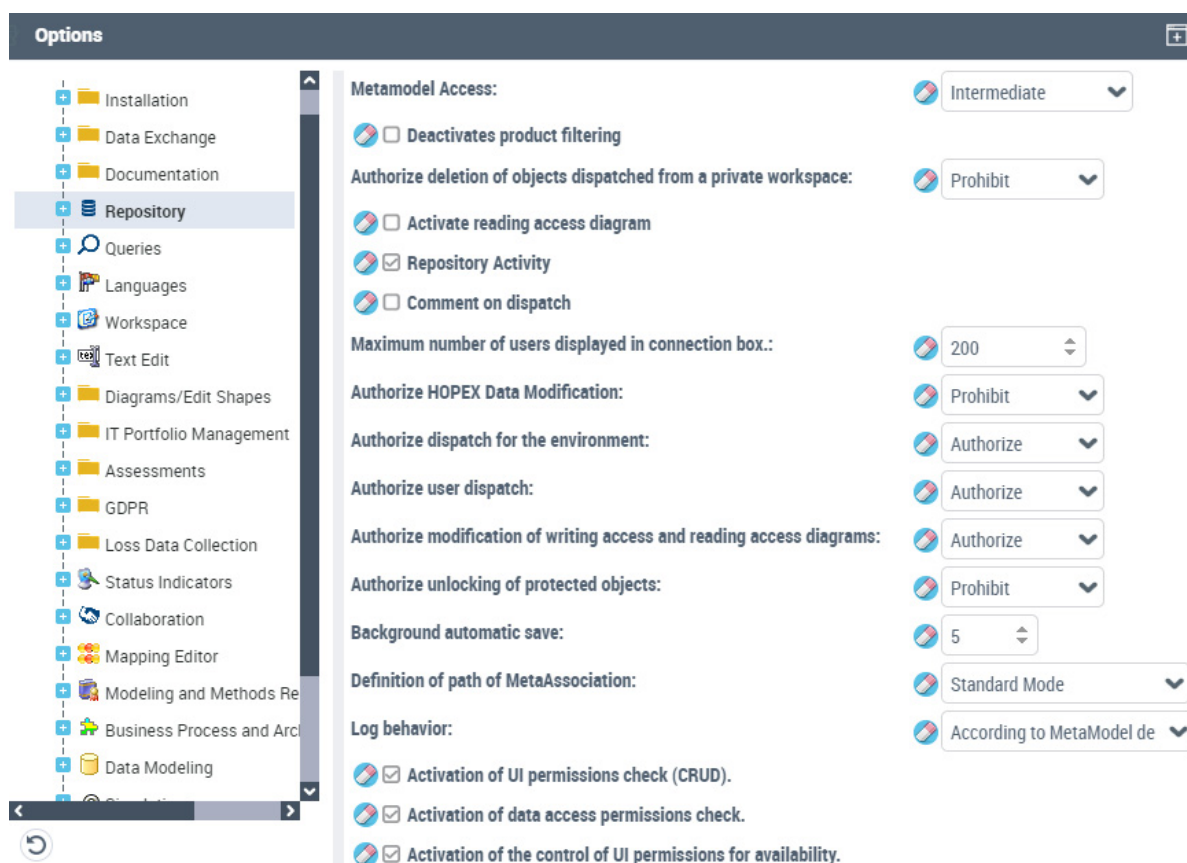
- environment
- profile (which groups a configuration common to several users)
- user

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.**



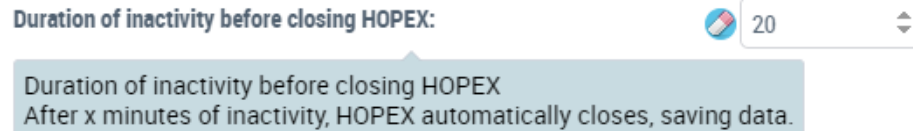
The left pane contains the option tree classified by group.

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:

- Hold the mouse over the option to display context-sensitive help.



When the user has a private workspace in progress, you cannot modify his/her options from **HOPEX Administration**.

ACCESSING OPTIONS

Options Level

You can modify the options at the following levels:

- environment
- profile
- user

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](#).
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](#).
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](#).

To modify the options of a user from the **Administration** desktop:

1. Access the user management page.
 See [Connecting to the Administration Desktop](#).
2. Select a **Persons** sub-folder.
3. In the edit area, select the person concerned.
4. Click **Options**.
 The person's options window opens.

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:

-  indicates the inheritance from the higher level.
-  indicates that the inherited option value has been modified. The value is no longer inherited from the higher level.

Modifying an option value

To modify the value of an option inheriting from a higher level:

1. Access the Options page.
 See [Options Level](#).
2. Modify the value of the option concerned.

The icon  indicates that the option value is modified.

Reinitializing the value of an option

To reinitialize the value of an option:

1. Access the options.
 See [Options Level](#).
2. Click .

The value of the option is reinitialized and the icon changes to .

Controlling modification of the Options

With **HOPEX Administration** (Windows Front-End) you can prohibit modification of any option at a level lower than your current level.

Example: if you open the options of the environment, you can prohibit modification of all options at user level.

 See [Controlling the Modification of the Options](#).

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 concerning collaborative work in **HOPEX**.

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](#).

You cannot access installation options from your **HOPEX Administration** desktop. They are defined at **HOPEX** site level in **HOPEX Administration** application.

Specifying the Web application access path

The Web application access path is defined at **HOPEX** site level and cannot be performed from your **HOPEX Administration** desktop.

To specify the Web applications access path:

1. Launch **HOPEX Administration**.
2. In the **Options** tree, right-click the site name and select **Options > Modify**.
3. In the **Options** tree, expand the **Installation** folder and select **Web Application**.
4. In the right pane, specify the **Web Application Path** option.

Example: `http://<Server Name>/HOPEX`

Specifying SMTP configuration

The SMTP configuration is defined at **HOPEX** site level and cannot be performed in your **HOPEX Administration** desktop.

You must define the **Electronic Mail** options:

- **Default address of author via SMTP (FROM)**

Default address, used when no email address is defined.

For example at Web account initialization, if the administrator does not have an email address, this default

address is used as the sender address of the email sent to the user to define his password.

- **Default address of sender via SMTP (SENDER)**
Address used for security authentication purpose, in addition to the known address or the default address (**Default address of author via SMTP (FROM)**).
It enables to **HOPEX** automatic emails to be validated by your enterprise security checks.

For example: at Web account initialization, this address is also used in the email sent to the user to define his password. If the administrator:
 - has an email address:
SENDER@company.com on behalf of AdminName@company.com
 - does not have an email address:
SENDER@company.com on behalf of FROM@company.com
- **SMTP Server**
SMTP address of your server

To specify SMTP configuration:

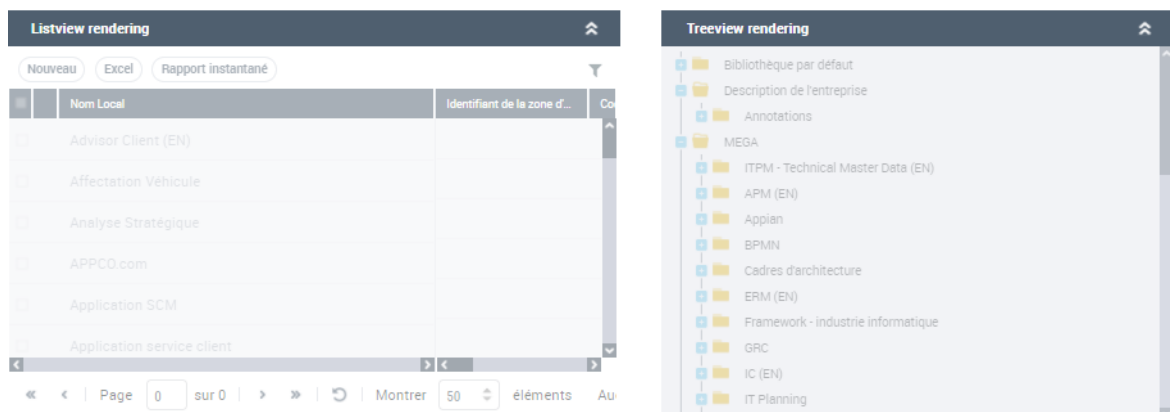
1. Launch **HOPEX Administration**.
 See *HOPEX Administration > Accessing HOPEX Administration documentation*.
2. Right-click the site name and select **Options > Modify**.
The Site level **Options** window is displayed.
3. In the **Options** tree, expand the **Installation** folder and select **Electronic Mail**.
4. In the right pane, specify the following options:
 - **Default address of author via SMTP (FROM)**
Example: sender@company.com, AdminName@company.com
 - **Default address of sender via SMTP (SENDER)**
Example: server@company.com, AdminName@company.com
 - **SMTP Server**
Example: exa.fr.company.com
5. Restart the SSP to take this configuration into account.

Network Quality Test Option (Browser and Connection)

The Web administrator can measure his browser performance in terms of capability to display pages showing lists or trees. These tests enable highlighting the source of slowness issue.

The report displays the following graphics (html format):

- Client-Server connection
 - **Network latency**
 - **Bandwith**
- **Rendering behavior measures** with the current browser and their corresponding graphics:
 - **Listview rendering behavior**
 - **Teeview rendering behavior**



Depending on the result quality, you can for example switch to another browser or change the client machine.

Displaying the network quality test report

To display the network quality test report:

1. In the tool group of your Web Administration desktop, click **My account**.
 ➡ See [Toolbar](#).
2. Select **HOPEX System Web Report**.
 The test page is displayed.

Removing access to the network quality test report

By default the Web administrator can access the test report (html format). You can remove access to this report.

To remove access to the network quality test report:

1. In your Web Administration desktop, access environment options.
 ➡ See [Modifying options at environment level](#).

2. In the options tree, expand the **Installation** folder and select **Web Application**.
3. In the right pane, clear **Availablility 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

In Web applications, you can modify:

- the interface language.
- the data language.

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 Language of Your Desktop](#).

To define the interface language in Web applications:

1. Access the environment options management window.
 See [Modifying options at environment level](#).
2. In the options tree, 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 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 ([Modifying the Data Language](#)), 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](#).

 **The data language defined at user level takes priority over the language defined in the environment options.**

To modify the data language at environment level:

1. Access the environment options management window.
 See [Modifying options at environment level](#).
2. In the 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.

MANAGING DATE FORMAT

In **HOPEX**, the date format depends on the data language.

This format is defined for each language in the Windows parameters of **HOPEX** installation server.

If needed you can change this format in **HOPEX**.

☛ This customization might be lost at HOPEX update.

To change the date format for a language:

1. Connect to **HOPEX**.
☛ Check that you are in "Expert" metamodel access and that you are allowed to modify HOPEX data (**Options > Repository**).
2. Access the advanced search (**Main menu > Advanced search**).
3. In the search wizard toolbar, click **Display** .
4. Select **View all the object types**.
5. In the search by object type tool, in the first field, select **Languages**.
6. Click **Find** .
7. In the result list, roll the mouse over the **Name** column of the language concerned and click **Properties**.
8. Display the **Characteristics - Characteristics** tab,.
9. In the **_LanguageCharacteristics** pane, add the date format you want to be customized:

```
[DateFormat]
date=<date format>
```

You can use separating characters like: "/", ",", "-", or " ".

Examples:

date=yyyy/MM/dd displays 2018/04/24

date=d-MM-yy displays 4-03-18

date=dd MMMM yy displays 04 july 18

date= dddd, MMMM d, yyyy displays Tuesday, June 5, 2018

English

 | Characteristics - Characteristics ▾

Name: *

_LanguageCharacteristics:

[System]
 PrimaryLanguage = 9
 SubLanguage = 1
 SortID = 0
 [Mega]
 InitalSubsidy=1

 [DateFormat]
 date=yyyy-MM-dd

The date format is automatically taken into account.



This modification uncompile the technical data.

10. Compile the technical data.



See *HOPEX Administration > Compiling an environment documentation*.

Date Format	Description
d	The day of the month with one or two digits 1...9, 10, 11,..31
dd	The day of the month with two digits 01...09, 10, 11,..31.
ddd	The abbreviated name of the day of the week
dddd	The full name of the day of the month
M	The numeric format month with one or two digits 1...9, 10, 11, 12
MM	The numeric format month with two digits 01...09, 10, 11, 12
MMM	The abbreviated name of the month
MMMM	The full name of the month

Date Format	Description
y	The year with one or two digits 9,18
yy	The year with two digits 09, 18
yyyy	The year with four digits 2018

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 <i>Characteristic</i> .
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 <i>users</i> , the <i>repositories</i> on which they can work, and the <i>system repository</i> . It is where user private workspaces, users, system data, etc. are managed.
external reference	An external reference enables association of an object with a document from a source outside HOPEX . This can relate to regulations concerning safety or the environment, legal text, etc. Location of this document can be indicated as a file path or Web page address via its URL (Universal Resource Locator).
functionality	A functionality is a means proposed by the software to execute certain actions (for example: the shapes editor and the descriptor editor are functionalities proposed as standard).
general UI access	General UI access defines if tools are available or not. By default, general UI accesses have value *A (A: Available, *: default value)
identifier	An absolute identifier is a string of characters associated with each object in the repository. This string is computed using the date and time the session was opened, the number of objects created since the session started, and the object creation date (in milliseconds). An absolute identifier provides a unique way to identify an object in the repository, so that even if the object is renamed, all the links to it are retained.
importing	Importing a command file, a backup file, or a logfile consists of applying the commands in the file to this new repository.
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 (SQL Server). The remainder is in a directory tree (content of Business Document versions, backup logfiles, locks).

The different users in the environment can access the repositories connected to it.

repository log

The repository log stores all the updates of users working in a repository. It is reinitialized during the repository reorganization procedure.

**repository
snapshot**

A repository snapshot identifies an archived state of the repository.

Creating a repository snapshot allows you to label important states in the repository life cycle.

The repository archived states for which a snapshot exists are not deleted by repository cleanup mechanisms (Repository history data deletion).

restore

A physical restore consists of copying previously saved repository files.

saving	The work done in a session is saved when you request it, or when you exit. By default, the software executes an automatic save (the time interval between two saves is specified in the options: Options > Repository > 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 <i>repository snapshot</i>
style	A style is a particular format applied to a paragraph of text in a word processor. Styles allow you to systematically apply formats such as fonts, margins, indents, etc. Several styles are available for report (MS Word) configuration. These styles have the M- prefix and are based on the M-Normal style that is similar to the Word Normal style. Note that the M-Normal style text is in blue. All these styles are contained in the Megastyl.dot style sheet.
Terminology	A Terminology defines a set of terms used in a specific context instead of the standard term.
text	You can associate text with each object found when browsing object descriptors (HOPEX Power Studio technical module). This text is formatted for MS Word. It presents what will be displayed for each of the objects in the generated report (MS Word). In the text you can insert the object name, its characteristics, and its comment. You can also insert the characteristics of other objects linked to it.

user	A user is a person with a login. The code associated with the user is used to generate file names as well as a specific work folder for the user. By default at installation, Administrator (Login: System) and Mega (Login: Mega) persons enable administration of repositories and creation of new users.
variable	A setting is a parameter of which value is only determined when the function with which it is associated is executed. You can use variables to condition a query (HOPEX Power Studio technical module). When you execute this query, a dialog box asks you to enter these settings, with a box for each setting defined in the query.
writing access	see "writing access area".
Writing access area	A writing access area is a tag attached to an object to protect it from unwanted modifications. Each user is assigned a writing access area. There is a hierarchical link between writing access areas. A user can therefore only modify objects with the same or lower authorization level. The structure of writing access areas is defined in the writing access diagram. By default there is only one writing access area, "Administrator", to which all objects and users are connected. Writing access management is available with the HOPEX Power Supervisor technical module.
writing access diagram	The writing access diagram is available if you have the HOPEX Power Supervisor technical module. With this diagram, you can create users and manage their writing access rights for repositories and product functions. By default only one writing access area is defined, named "Administrator". Attached to it are the "Administrator" and "Mega" persons. This is the highest writing access level and it should normally be reserved for repository management. You cannot delete this writing access area.