Administrator Guide

ABOUT MEGA ADMINISTRATION

MEGA products can be used on a stand-alone workstation or in a configuration including dozens of users.

This guide is for the person responsible for repository and user administration. When there are only a few users, administration is usually done by one of the users. In such cases, it mainly consists of carrying out regular backups and reorganizing repositories when required.

Chapters ("Managing Users", page 33 and "Managing Repositories", page 163) cover most administration requirements of a structure with only a few users. In a structure with many users, the administrator must respond to more specific requirements, which are detailed in the following chapters.

Most of the functions described here can be used by the repository and user administrator, whatever the products enabled through his/her security key. However, certain functions are only available with specific technical modules (**HOPEX Studio**, **MEGA Supervisor**, or **HOPEX Collaboration Manager**). These are indicated by a note in the text.

MEGA administration is managed from the **MEGA Administration** application (Windows Front-End), "Administration.exe", or from the MEGA **Administration** desktop (Web Front-End). Some actions can also be performed from the main **MEGA** application (Windows Front-End), "Mega.exe", or from certain **MEGA** desktops (Web Front-End).

The **MEGA** administration applications (Windows Front-End and Web Front-End) are designed for administrators **MEGA**: they are used to administer environments, repositories, users, etc.

A **MEGA** installation can contain a large number of environments, repositories and users. To facilitate their management, **MEGA Administration** provides all the key concepts and tools required for their administration in a unified hierarchical structure.

☛ *Remark on the preceding points.*

📖 *Definition of terms used.*

☺ *A tip that may simplify things.*

Compatibility with previous versions.

Things you must not do.

Very important remark to avoid errors during an operation.

Commands are presented as seen here: **File > Open**.

Names of products and technical modules are presented in bold as seen here: **MEGA**.

PRESENTATION OF THIS GUIDE

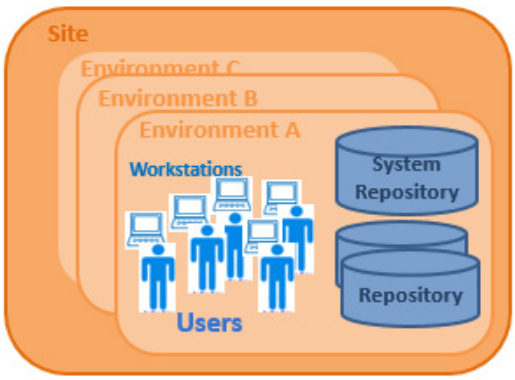
The following points are covered here:

- "Accessing MEGA Administration", page 19: how to access **MEGA Administration**.
- "Managing Users", page 33: to create users, user profiles and business roles.
- "Managing Repositories", page 163: to create, save, restore, check, reorganize, copy and move repositories.
- "Managing Private Workspaces", page 219: principle of private workspaces, dispatch and refresh private workspaces, and lock management.
- "Managing Environments", page 257: to create, back up, restore, check, copy and move an environment.
- "Managing Events", page 277: to supervise events with the **MEGA Server Supervisor tool**.
- "Managing objects", page 297: Advanced administration functions available with:
  - the **HOPEX Studio technical module** to extract objects
  - the **MEGA Supervisor technical module** to manage user interface (UI) access, query isolated objects, compare objects in two repositories.
- "Managing Data Writing Access", page 345: to set up management of organized projects in the form of data writing access, using the **MEGA Supervisor** technical module.
- "Managing Data Reading Access", page 371: to install a confidentiality strategy using a reading access diagram and access areas.
- "Command File Syntax", page 403: description of the syntax used in command files.
- "Frequently Asked Questions (FAQ)", page 435: answers to frequently asked questions and some administration tips.
- "Glossary", page 441: definition of the main terms used in this guide.
- "Index", page 453

MEGA ADMINISTRATION CONCEPTS

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

MEGA is organized in four tiers: the *site*, the *environment*, the *workstation* and the *user*.



📖 *A site groups together everything that is shared by all MEGA users on the same local network: the programs, standard configuration files, online help files, standard shapes, workstation installation programs, and version upgrade programs. The site is installed on a local network resource or on each workstation if you are working without a network connection.*

📖 *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.*

📖 *A workstation is defined for each computer connected to the environment. A workstation contains programs and a configuration file that allow you to use MEGA on that machine.*

📖 *A user is a person (or person group) with a login.*

A user:

- has a specific workspace in each repository.
- can connect to a repository from all workstations connected to the environment in which this repository is referenced.
- has a specific configuration and is authorized to access specific product functions and repositories in the environment.

At installation, two users are created by default. They can manage repositories, users and create new users:

- the **Mega** user, with login "mega"
- the **Administrator** user, with login "system".

ACCESSING MEGA ADMINISTRATION

The **Administration** application (Windows Front-End) is the **MEGA** administration application accessible from the Windows desktop. This application contains the tools required to manage users, repositories, environments and private workspaces. It is used to manage users (individuals, business roles and profiles, access to GUIs, writing access as well confidentiality using reading access management, servers, LDAP servers) and repositories (workspaces, locks, repository snapshots, Scheduler).

The **Administration** desktop (Web Front-End) is the **MEGA** administration application available 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 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:

THE MEGA ADMINISTRATION APPLICATION (WINDOWS FRONT-END)

The **Administration** application **(Windows Front-End)** is the **MEGA** *administration* application accessible from the Windows desktop.

Connecting to MEGA Administration (Windows Front-End)

To access the **MEGA Administration** application **(Windows Front-End)**:

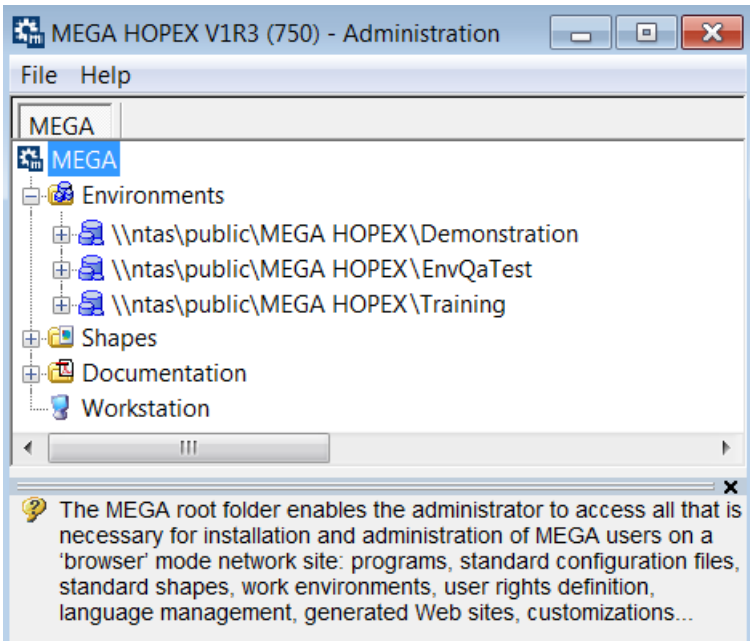
- Double-click the "Administration.exe" file 

.

  ☛ *The administration icon is created during setup of an administrator workstation.*

The **MEGA Administration** main window opens.

☛ *Environments preceded by a red icon are not accessible.*



MEGA Administration is presented in the form of a navigation tree:

- containing the elements you can manage:
  - *site*
  - *environments*
  - *repositories*
- enabling access to:
  - the list of shapes used in **MEGA**
  - user guides and technical articles on products **MEGA**

    ☛ *The most recent versions of these documents are delivered to this address: http://community.mega.com/t5/Documentation-Downloads/ct-p/Docs-Downloads.*
  - technical characteristics of the **MEGA** installation on your workstation.

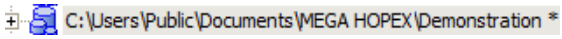
Connecting to an Environment

To connect to an environment:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*
2. Expand the **Environments** folder.
   The list of referenced environments appears.

   ☛ *The asterisk that may appear after the environment name means that you must compile the metamodel and/or the technical data, see "Compiling an Environment", page 231.*

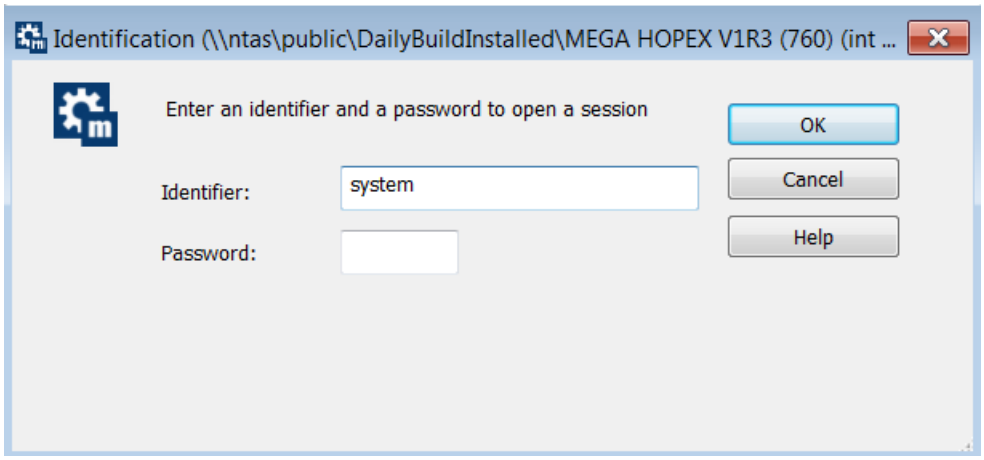
   

3. Right-click the environment you want to connect to and select **Open**.
   The environment connection dialog box appears.
4. In the **Identifier** field, enter the identifier of an *Administrator*.

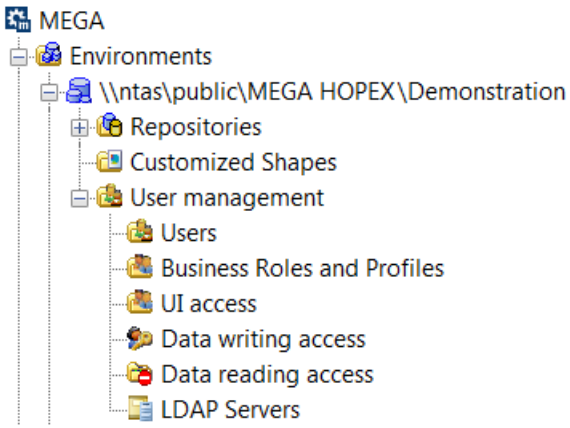
   ☛ *Administrator and Mega users own administration rights. The Administrator user identifier is System. The Mega user identifier is Mega.*

5. (optional) Type the user **Password**.

☛ *By default, Administrator and Mega users do not have a password.*



6. Click **OK**.
The content of the environment folder is available.



This environment folder contains the folders:

- **Repositories** containing repositories referenced in the environment
- **Customized Shapes** containing **MEGA** shapes customized by the user. They are stored in the Mega_Usr folder of the environment.
- **User Management** to manage:
  - *users*
  - the *business roles* and the *profiles* of each user

    ☛ *Business roles do not appear when the "Assignment of business roles to persons" option (Options/Installation/User Management) is not selected.*
  - the *UI Access* of each user
  - the *Data Writing Access areas*
  - the *Data Reading Access areas*
  - the *LDAP Servers*.

THE MEGA ADMINISTRATION DESKTOP (WEB FRONT-END)

The **Administration** desktop (Web Front-End) is the **MEGA** Administration application accessible via an internet browser.

Connecting to the Administration Desktop (Web Front-End)

From the **Administration** desktop (Web Front-End), 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 for example with the **MEGA Administrator** profile or business role.

☛ *See "Business Roles Supplied", page 89 or "Profiles Supplied", page 86.*

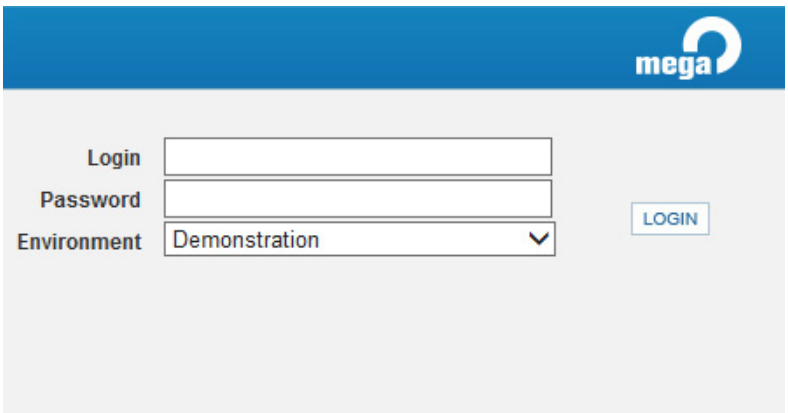
☛ *At installation, only the Mega user can connect to the Web Administration desktop.*

To connect to the **Administration** desktop (Web Front-End):

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

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

   The connection page appears.



2. From the connection page and in the **Login** field, enter your identifier.

   `Example: Mega is the MEGA administrator login.`

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

   ☛ *If you have lost your password, click Lost password (under the connection dialog box), see "Reinitializing Your Password", page 10.*

4. In the **Environment** field, click the arrow and 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 LOGIN.
   When you have been authenticated, a new dialog box appears.
6. In the **Repository** field, click the arrow and select your work repository.

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

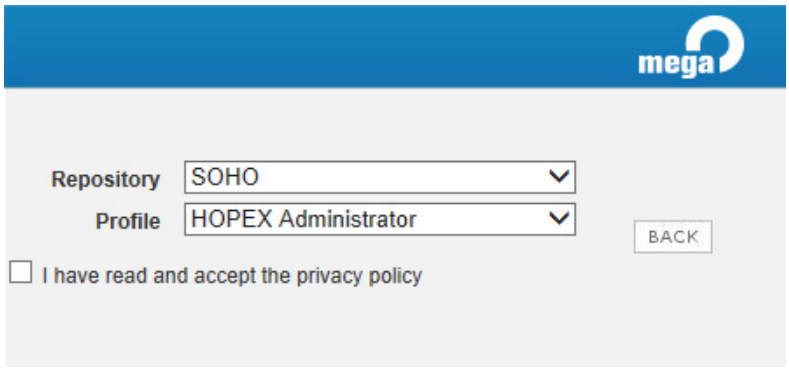
7. In the **Profile** or **Business Role** field, click the arrow and select the MEGA Administrator profile or business role.

   ☛ *In the environment options (Options/Installation/User Management), when the "Management of assignment of business roles to persons" option is cleared, the **Profile** field appears instead of **Business Role**.*

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

8. In the **Application** field, click the arrow and select the **Administration (Web Front-End)** application.

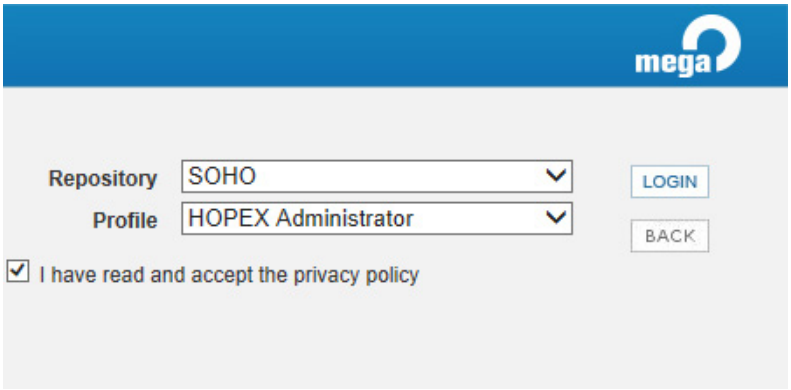
   ☛ *If you can access only the **Administration (Web Front-End)** application with the profile or business role selected, this is automatically taken into account and the application selection field does not appear.*



9. Click Privacy Policy (under the connection dialog box), read the confidentiality policy, then select **I have read and accept the privacy policy**.

   The LOGIN button appears.

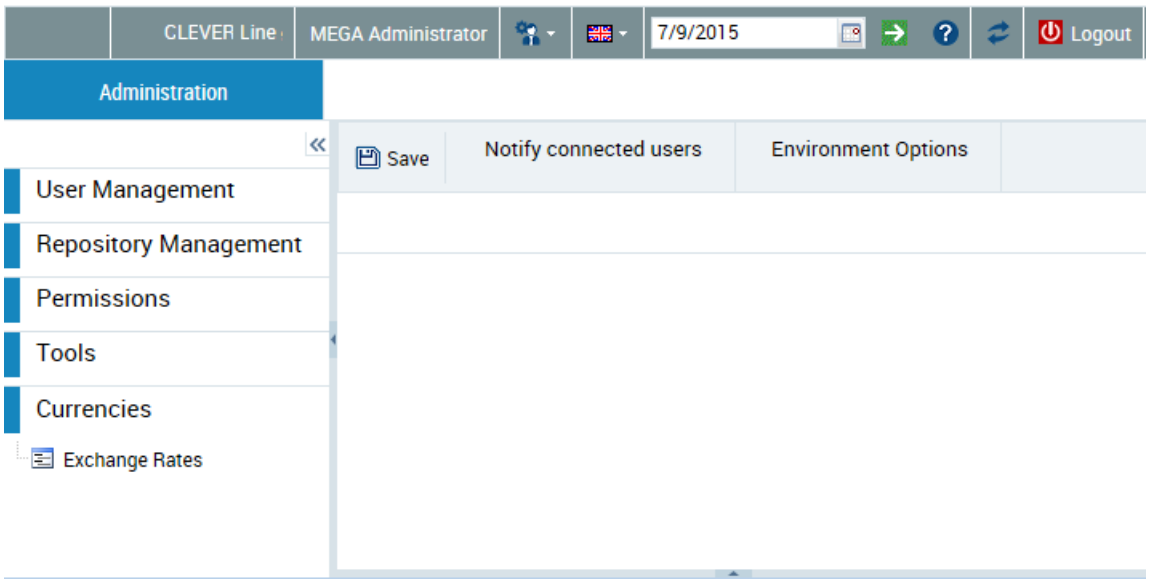
   ☛ *This step is requested only once, at your first connection to a **MEGA** Web desktop. A certificate is automatically linked to your person.*



10. Click **LOGIN**.

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

    The **Administration** desktop (Web Front-End) appears and the session is opened.



☛ *See "Administration Desktop Description (Web Front-End)", page 11.*

Reinitializing Your Password

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

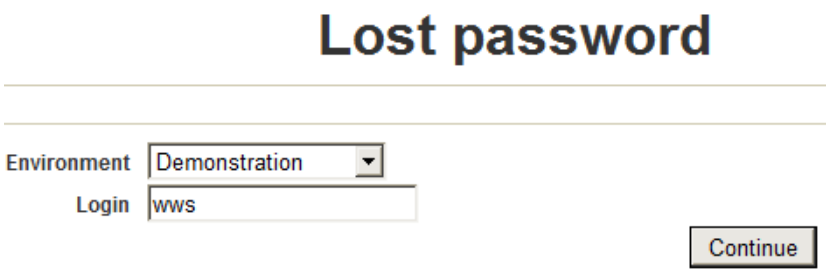
☛ *See "Authentication in MEGA", page 120.*

To reinitialize your password:

1. Open the connection page.

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

2. Under the connection dialog box, click Lost password.
   The **Lost password** page appears.



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

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

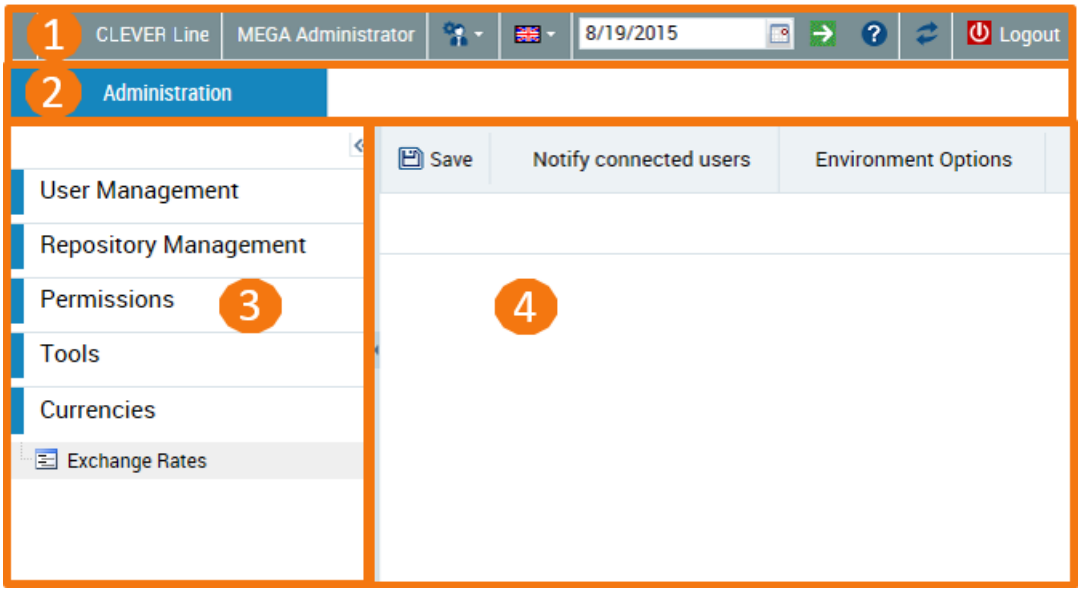
4. In the **Login** field, enter your login.
5. Click **Continue**.
6. Answer the security question.
7. Click **Reinitialize**.
   An e-mail containing a link with limited validity period is sent to you.
8. Click this link.
   The **Modify Password** page appears.
9. Enter your password and answer the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

   ☛ *By default, a password must contain between 8 and 16 characters, with at least one letter, at least one figure and at least one special character, see "Modifying password definition rules", page 133.*

10. Click **Apply**.

Administration Desktop Description (Web Front-End)

To access the **Administration** desktop (Web Front-End), see "Connecting to the Administration Desktop (Web Front-End)", page 7.



The **Administration** desktop (**Web Front-End**) includes:

- a toolbar (1).
  - ☛ *See "Toolbar", page 11.*
- an **Administration** (2) tab that contains panes and trees to select the objects to manage (3).
  - ☛ *See "Navigation panes and trees", page 13.*
- an edit area to manage objects (4).
  - ☛ *See "Edit Area", page 15.*

Toolbar

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

From the **Administration desktop** (**Web Front-End**) toolbar, you can:

- access your 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 "User options", page 375.*
  - modify the theme of your desktop

    ☛ *The theme used in the Web applications also define the theme used in the reports. To customize reports, see the **MEGA Common Features** guide.*
  - manage your alerts

    ☛ *see **MEGA Common Features**guide.*
  - obtain information on your licenses
  - diagnose the installation

    ☛ *This information simplifies error diagnostics. It can help explain application slow response time.*
  - reinitialize your personal parameters
- modify the interface data language 
- display data as it was at a prior date, with the **Time Machine**

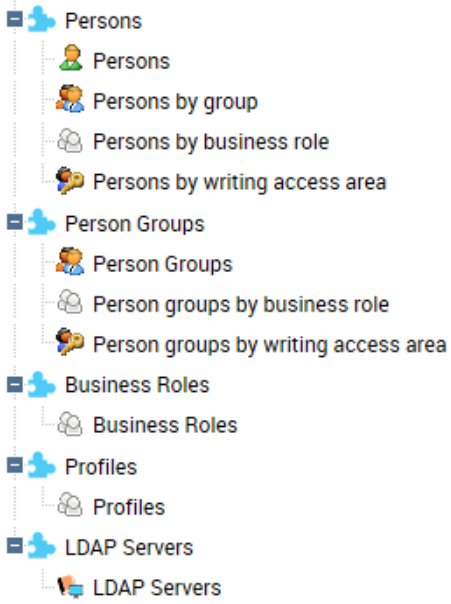
  

- access online help 
- update your desktop 
- disconnect from the **Administration** desktop (**Web Front-End**)  .

Navigation panes and trees

In the **Administration** desktop (**Web Front-End**), the **Administration** tab contains the following panes:

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



  - the *persons*

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

    ☛ *The **Persons by business role** sub-folder is replaced by **Persons by profile** when, at the level of the environment options (Options/ Installation/User Management), the "Management of assignment of business roles to persons" option is cleared.*

  - the *person groups*

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

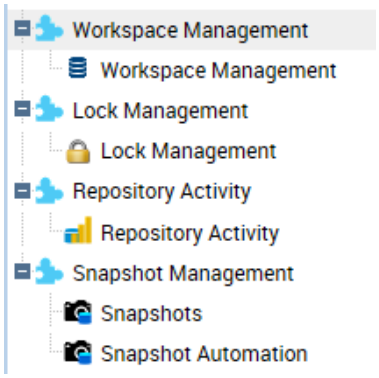
    ☛ *The **Person groups by business role** sub-folder is replaced by **Person groups by profile** when, at the level of the environment options (Options/Installation/User Management), the "Management of assignment of business roles to persons" option is cleared.*

  - the *profiles* and the *business roles* of each user

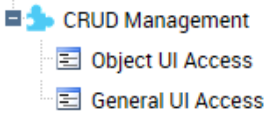
    ☛ ***Business Roles** is not visible when, at the level of the environment options (Options/Installation/User Management), the "Management of assignment of business roles to persons" option is cleared.*

  - the *LDAP servers*

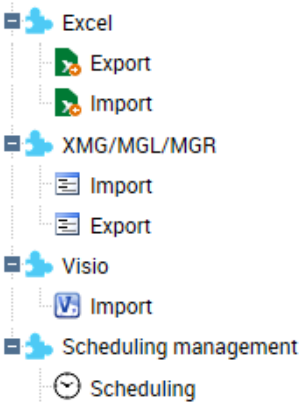
- the **Repository Management** pane to manage the *workspaces*, the *locks*, the *repository* and the *snapshots*



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



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



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

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

Edit Area

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

You can:

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

2

MANAGING USERS

MEGA Administration is provided with tools required for user management.

This chapter explains how to create a user or a group of users and how to set and modify its characteristics.

The following points are covered here:

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. To grant administrator access rights to a user, see "Configuring a Login", page 75.*

User management involves the following concepts:

- *users*

  🕮 *A user is a person (or person group) with a login.*

  - *persons*

    🕮 *A person is defined by his/her name and electronic mail address.*

  - *person groups*

    🕮 *A Person Group groups persons in a group. These persons share the same connection characteristics.*

  - *logins*

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

- *business roles*

  🕮 *A business role defines a function of a person in a business sense. A person can have several business roles. Business roles are only considered when the "Management of assignment of business roles to persons" option is activated (default mode) A profile can be associated with a business role. Assigning a person a business role with which a profile is associated indirectly assigns this profile to this person. A business role is specific to a repository.*

- *profiles*

  🕮 *A profile defines what a person can see or not see and do or not do in tools, and how he/she sees and can do it. 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.*

- *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)*

For information on:

- managing *data writing access*, see "Managing Data Writing Access", page 297
- managing *data reading access*, see "Managing Data Reading Access", page 321

The following points are detailed here:

- introduction:
  - "Users and User Groups Supplied", page 19
  - "User: Definition", page 20
  - "User Group: Definition", page 21
- properties:
  - "Person Properties", page 21
  - "Person Group Properties", page 23
  - "Login Properties", page 26
- access:
  - "Accessing the User Management Pages (Web Front-End)", page 31
  - "Accessing User Management and UI Access Management Folders (Windows Front-End)", page 39
- characteristics:
  - "Viewing Person Characteristics", page 47
  - "Viewing Person Group Characteristics", page 49
  - "Viewing Login Characteristics", page 51

Users and User Groups Supplied

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 enables to create a first user with the "MEGA 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.*
- persons given as examples:
  - "Mega", with Login "Mega"

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

    ☛ *The "Mister Guide" user can be deleted. He/She has not administration rights. No password is assigned to "Mister Guide" at installation.*
- a person group:
  - "Guests", with Login "Guests"

    ☛ *At installation, Guests is defined as default connection group (see "Default connection group", page 25).*

User: Definition

A user is a person (or person group) with a login.

For each environment, a user has:

- personal characteristics defined by his/her **Person**.
  - ☛ *see "Viewing Person Characteristics", page 47.*
- a **login** which defines his/her connection identifier, his/her status, his/her authentication and **MEGA** access modes.
  The login can also restrict rights defined on the associated **Profile** concerning access to product functions and repositories of the environment.
  - ☛ *see "Login Properties", page 26.*
  - ☛ *see "Profile Properties", page 102.*
- a **user code** which enables naming of user associated files, for example the work repository.
  - ☛ *see "Login Properties", page 26.*
- (if "Management of assignment of business roles to persons" option is selected, default mode)
  at least one **business role**, connected to a profile, which defines the business or function of the person in the enterprise
  - ☛ *see "Without Management of Assignment of Business Roles to Persons", page 99.*
  - ☛ *see "Business Role Properties", page 119.*
  - ☛ *see "Managing Profiles and Business Roles", page 88.*
  - ☛ *see "Business Roles Supplied", page 98.*
  - ☛ *see "Configuring a Business Role (Connection)", page 122.*
  - ☛ *see "Assigning a business role to a person", page 123.*
- (if "Management of assignment of business roles to persons" is cleared, see "Without Management of Assignment of Business Roles to Persons", page 99)
  at least one **profile**, which determines products and repositories that can be accessed (restricted by products and repositories defined on his login). By default, the user is not connected to any profile.
  - ☛ *see "Profile Properties", page 102.*
  - ☛ *see "Managing Profiles and Business Roles", page 88.*
  - ☛ *see "Profiles Supplied", page 94.*
  - ☛ *see "Connecting Users to a Profile", page 115.*
- **options**
  - ☛ *see "Managing Options", page 365.*

Only a user with **MEGA Administrator** profile (or with equivalent rights) can configure and modify user properties.

- ☛ *see "MEGA Administrator profile", page 94.*

User Group: Definition

A person can belong to one or more groups. A user group is a group of persons with a login.

Persons belonging to a group:

- depend on the same environment.
- share the same connection characteristics defined on the **login** of the group.

  ☛ *see "Configuring a Login", page 75.*
- connect to the application with their **login**, but with repository access rights defined on the **login** of the group.

  ☛ *see "Login Properties", page 26.*
- share the assignments defined for the group.

  A person belonging to a group can only connect in the name of the group (the assignments defined for the persons are ignored).

  ☛ *See "Assigning a Business Role to a Person Group (Web Front-End)", page 128.*

For each environment, a user group has:

- personal characteristics defined by its **person group**.

  ☛ *see "Person Group Properties", page 23.*
- access rights to product functions and repositories of the environment, defined by its **login**.

  ☛ *see "Login Properties", page 26.*

Person Properties

☛ *For information on a user, see "User: Definition", page 20*

☛ *To consult properties of a person, see "Viewing Person Characteristics", page 47.*

Name

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

```
Example: DURAND Pierre
```

Image

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

E-mail address

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

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

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

Telephone number and initials

The telephone number and initials of the person are optional.

```
Example: +33102030405 / DP
```

Data language

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

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

☛ *To define interface language, see "Managing Languages", page 377.*

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.

User writing access area and writing access area at creation

☛ *Writing access management is available with the **MEGA 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.

☛ *See "Managing Data Writing Access", page 297.*

Reading access area

☛ *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 **MEGA** 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 or lower reading access areas.

☛ *For more details on reading access areas, see "Managing Data Reading Access", page 321.*

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 ***MEGA***.

```
Example: pdurand, pdd
```

☛ *For more details, see "Login Properties", page 26.*

Belongs to a person group

A person can:

- belong to a group

  ☛ *See "Creating a Person Group", page 68.*

  ☛ *See "Creating Users (Web Front-End)", page 65.*

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

  ☛ *See "Defining a dynamic person group with LDAP", page 72.*

  ☛ *See "Defining a dynamic person group with a Macro", page 73.*

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

  ☛ *See "Default connection group", page 25.*

A person who belongs to a person group or who has the **Belongs to a person group** attribute selected, can only connect to the application through the group, with one of the business roles/profiles defined for the group (the assignments defined for the person are ignored).

Person Group Properties

☛ *For information on a group, see "Users and User Groups Supplied", page 19, "User Group: Definition", page 21, "Viewing Person Group Characteristics", page 49 and "Creating a Person Group", page 68.*

A **Person Group** groups persons within a group. These persons share the same connection characteristics. It is the group that carries user access rights to the repository.

A person can belong to one or more groups.

Persons in a group depend on the same environment.

☛ *A group of users is created by default at creation of an environment: the "Guests" person group, with Login "Guests".*

Name

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

```
Example: HR Department
```

User group writing access area and writing access area at creation

☛ *Writing access management is available only with the **MEGA 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 user that creates it.

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.

☛ *For more details, see "Managing Data Writing Access", page 297.*

User group reading access area

☛ *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 **MEGA** 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 his/her own or lower reading access areas.

☛ *For more details on reading access areas, see "Managing Data Reading Access", page 321.*

Login

The login of a person group is a unique character string uniquely identifying the person group. It enables definition of the connection characteristics of persons belonging to the group.

☛ *For more details, see "Login Properties", page 26.*

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

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

Default connection group

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

- *Use of this attribute in read-only mode is recommended.*
- *By default, at installation "Guests" is the default connection group.*
- *See "Person Properties", page 21.*

Person group types

A person can belong to:

- a static group
  Persons are explicitly connected to the group.
  - *See "Defining a Person Group", page 70.*
- a dynamic group
  The group computes group persons on the fly.
  Examples of dynamic groups:
  - LDAP groups (case of LDAP authentication)
    - *See "Defining a dynamic person group with LDAP", page 72.*
  - groups connected to a macro (the macro checks if the person belongs to the group or not)
    - *See "Defining a dynamic person group with a Macro", page 73.*

LDAP dynamic group

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

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

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

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

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

- MEGA repository connection
- access to roles

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

Dynamic group connected to a macro

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

The macro should implement the following function:

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

sUserName: authentication login of the person.

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

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

Data language

The **Data language** attribute of a person group is specific to Web applications. It enables definition of 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.*

☛ *To define interface language, see "Managing Languages", page 377.*

Login Properties

To:

- create a login, see "Creating the Login of a Person", page 64 or "Creating Users", page 65.
- consult login characteristics, see "Viewing Login Characteristics", page 51.
- configure a login, see "Configuring a Login", page 75.

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 at creation of the user. To ensure data consistency, it should not be modified.

☛ *(Web Front-End) When a user is created from the **Web Administration** desktop, the user code is automatically defined.*

```
Example: PDD
```

Login Holder

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

```
Example: DURAND Pierre
```

Repository access definition mode

Repository access of a user is defined by the following access modes:

- ***Implicit access***:
  By default, the user has read/write access to all repositories, but access can be limited or prohibited.

  ☛ *When a repository is added in the site, by default it can be accessed by the user.*
  For more details on how to restrict user repository access rights, see "Configuring a Login", page 75 and "Configuring a Profile", page 109.

- ***Explicit access***:
  By default, the user cannot access repositories, but access can be authorized. In this case, you must at least define and authorize access to a repository.

  ☛ *When a repository is added in the site, by default it cannot be accessed by the user.*
  For more details on how to add user repository access rights, see "Configuring a Login", page 75 and "Configuring a Profile", page 109.

  ☺ *This mode is useful to install a confidentiality policy; it is preferable to first create users with explicit repository access, then progressively define their rights and the information they can access.*

At creation of a user, default access to repositories is as defined in environment and site options (**Options/Repository**) via the **Repository default access mode** option.

☛ *Repository access default mode is **Implicit Access**, to modify this value see "Managing Options", page 365.*

User repository access rights

At creation, a user can access all repositories by default.

User *access rights* to environment repositories can be restricted by the administrator. He can:

- authorize repository update (**Read/Write**)
- prohibit repository update (**Read-only**)
- prohibit repository access (**Not accessible**)

☛ *See "Restricting User Repository Access Rights", page 83.*

💣 ***If* a user already has repository access rights restricted by those defined on his/her profile, only the restricted access rights will be defined on the profile.**

☛ *For more details, see "Configuring a Profile", page 109.*

Inactive user (Status)

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

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

Products accessible on the license (Command Line)

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

☛ *For more details, see "Products accessible on the license (Command Line)", page 103.*

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

Authentication mode

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

☛ *See "Defining Default Authentication Mode", page 130.*

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

- **MEGA**
  Passwords are managed and stored in the **MEGA** repository.
  This is default authentication mode.
  ☛ *For more details, see "Authentication in MEGA", page 129.*
- **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 **MEGA** (Windows Front-End), not requiring entry of his/her password.
  ☛ ***Attention**: to connect to a **MEGA (Web Front-End)** application, the user must enter his/her password.*
  The list of users in your **MEGA** environment is automatically synchronized with the list of users defined in your Windows network.
  This authentication mode corresponds to unique authentication (SSO).
  ☛ *For more details, see "Windows Authentication", page 131.*
- **LDAP**
  Passwords are managed and stored in the LDAP server of the enterprise. The directory configuration is stored in options.
  The MEGA user is authenticated at LDAP server level.
  ☛ *For more details, see "LDAP Authentication", page 133.*
- **Custom**
  This authentication is managed by an external authentication module or SSO. This authentication mode is specific to Web applications connection: users with this authentication mode cannot connect to **MEGA (Windows Front-End)**.
  ☛ *See the technical article **Web connection overloading and configuration EN***

Windows identifier

☛ *This field only appears when the **Authentication Mode** is "Windows", see "Authentication mode", page 28.*

The **Windows Identifier** of a user enables connection of a **MEGA** user to a Windows user, see "Associating a Windows user with a MEGA user manually", page 131.

The user connected to Windows is automatically identified when connecting to **MEGA (Windows Front-End)**, without requiring a password. Windows handles user authentication and assures the security system.

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

LDAP server

☛ *This field only appears when the **Authentication Mode** is "LDAP", see "Authentication mode", page 28.*

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

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

Profile

☛ *This attribute appears in the case of definition of profiles on login of persons, see "Definition of profiles to persons mode", page 93*

In the case of assignment of business roles to persons (see "Assignment of business roles to persons mode", page 91) you do not need to connect a profile to the login. The profile is connected to the business role which is assigned to the person, see "Managing Profiles and Business Roles", page 88.

To be able to connect to MEGA the user must have at least one profile.

By default, no profile is assigned to the login of a user or user group, you must connect at least one profile to the login.

The profile determines:

- access to objects and tools

  ☛ *See "Managing UI Access (Permissions)", page 282.*
- connection to Web applications
- repository access
- access to products

If a user already has access rights restricted by the Command Line attribute on his/her Login (see "Viewing Login Characteristics", page 51), the products accessible to this user are at the intersection of values of the Command Line attribute of the user login and profile.

At installation, some profiles are already available in the environment.

☛ *See "Profiles Supplied", page 94.*

Administrator profile

☛ *This attribute appears in the case of assignment of business roles to persons mode, see "Assignment of business roles to persons mode", page 91.*

This attribute enables connection of an administrator profile to a user so that this user can connect to **Administration (Windows Front-End)** application.

☛ *See "Configuring the MEGA Administrator business role", page 123.*

ACCESS TO USER MANAGEMENT

See:

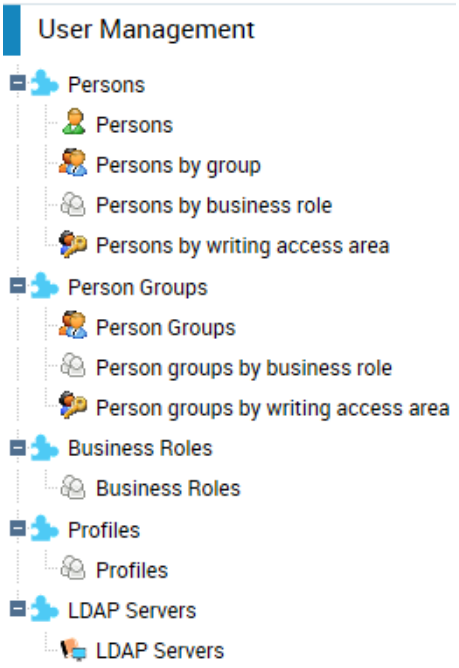
Accessing the User Management Pages (Web Front-End)

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

1. Connect to the **MEGA Administration** desktop (Web Front-End).

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

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



3. In the user management tree, click on a sub-folder for:
   - **Persons** to manage persons and logins
     ☛ *See "Actions performed in the Persons management page", page 33.*
   - **Person Groups** to manage the persons who belong to the same person group
     ☛ *See "Actions performed in the Person Groups management page", page 35.*
   - **Business Roles** to manage the business roles
     ☛ *Available if the "Management of assignment of business roles to persons" option is selected, default mode.*
     ☛ *See "Managing Profiles and Business Roles", page 88.*
     ☛ *See "Without Management of Assignment of Business Roles to Persons", page 99.*
   - **Profiles** to manage profiles
     ☛ *Not available if the "Management of assignment of business roles to persons" option is not selected.*
     ☛ *See "Managing Profiles and Business Roles", page 88.*
   - **LDAP Servers** to manage the LDAP servers.
     ☛ *See "LDAP Authentication", page 133.*

   The management page selected appears.

See:

- "Managing persons who have an identical characteristic", page 32
- "Managing a group of persons who have a specific characteristic", page 33
- "Actions performed in the Persons management page", page 33
- "Actions performed in the Person Groups management page", page 35

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 business role assigned", page 35
- "Accessing the list of person who belong to the same group", page 35
- "Accessing the list of persons connected to a specific writing access area", page 36
- "Accessing the list of persons connected to a specific reading access area", page 36
- "Accessing the list of persons who have or do not have a login", page 37

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 business role", page 37
- "Accessing the list of person groups connected to a specific writing access area", page 37
- "Accessing the list of person groups connected to a specific reading access area", page 38

Actions performed in the Persons management page

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

- create users
  - ☛ *See "Creating Users (Web Front-End)", page 65.*
- create persons
  - ☛ *See "Creating a person (Web Front-End)", page 59.*
- create logins
  - ☛ *See "Creating the Login of a Person", page 64.*
- access a person using his/her name
  - ☛ *"Accessing a person using his/her name", page 37*
- configure the characteristics of a person
  - ☛ *See "Configuring a Person", page 61.*
- check the configuration of a person
  - ☛ *See "Checking the Configuration of Persons (Web Front-End)", page 57.*
- configure the characteristics of a login
  - ☛ *See "Configuring a Login", page 75.*
- delete users
  - ☛ *See "Deleting Users", page 81.*
- modify the properties of users.
  - ☛ *See "Modifying User Properties", page 77.*
- assign Business Roles to Persons
  - ☛ *See "Assigning a business role to a person (Web Front-End)", page 123 and "Mass assignment of business roles to persons (Web Front-*

End)", page 124.

- assign an object to a person

  ☛ *See "Assigning an object to a person (Web Front-End)", page 125 and "Mass assignment of objects to persons (Web Front-End)", page 126*.

- Transferring the Responsibilities of a Person

  ☛ *See "Transferring the Responsibilities of a Person (Web Front-End)", page 78*.

- duplicate the responsibilities of a person

  ☛ *See "Duplicating the Responsibilities of a Person (Web Front-End)", page 79*.

- initialize and manage the password of a Web user

  ☛ *See "Initializing and managing the password of a Web user", page 142*.

- connect a person to a writing access area

  ☛ *See "Connecting a Person to a Writing Access Area (Web Front-End)", page 80*.

- connect a person to a reading access area

  ☛ *See "Connecting a Person to a Reading Access Area (Web Front-End)", page 81*.

- access user options

  ☛ *See "Managing Options", page 365*.

- import persons from an LDAP directory

  ☛ *See "Importing persons from an LDAP server", page 138*.

- filter persons.

  ☛ *See "Accessing the list of persons who have or do not have a login", page 37 or "Accessing a person using his/her name", page 37*.

Actions performed in the Person Groups management page

In the **Person Groups** management page you can:

- create user groups
  - ☛ *See "Creating a person group (Web Front-End)", page 68.*
- define the properties of a person group
  - ☛ *See "Defining a Person Group", page 70.*
- configure the characteristics of a login
  - ☛ *See "Configuring a Login", page 75.*
- assign business roles to a person group
  - ☛ *See "Assigning a Business Role to a Person Group (Web Front-End)", page 128.*
- connect a person group with a writing access area
  - ☛ *See "Connecting a person group with access to a writing area (Web Front-End)", page 74.*
- connect a person group with a reading area access
  - ☛ *See "Connecting a person group with access to a reading area (Web Front-End)", page 74.*
- delete users
  - ☛ *See "Deleting Users", page 81.*
- modify the properties of users.
  - ☛ *See "Modifying User Properties", page 77.*

Accessing the list of persons who have the same business role assigned

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

To access the list of persons who have the same business role assigned

1. Access the user management page.
   - ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select the **Persons by business role** sub-folder.
3. In the edit area, in the **Persons by business role** tab, select a business role.
   The **Persons** tab lists all the persons who have the selected business role assigned.
   - ☛ *See "Actions performed in the Persons management page", page 33.*

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 (Web Front-End)", page 31.*
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 in the Person Groups management page", page 35.*

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 (Web Front-End)", page 31.*
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 in the Persons management page", page 33.*

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.

☛ *See "Managing Data Reading Access", page 321.*

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 (Web Front-End)", page 31.*
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 in the Persons management page", page 33.*

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 (Web Front-End)", page 31.*
2. Select a **Persons** sub-folder.
3. In the edit area, click in the field of the **Login** column and select:
   - **Filters > Display specified values only**
     The persons who have a login are listed.
   - **Filters > Display unspecified values only**
     The persons who do not have a login are listed.

Accessing a person using his/her name

You can filter persons according to their name.

To find a person using his/her name:

1. Access the user management page.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select a **Persons** sub-folder.
3. In the edit area, click in the field of the **Name** column and in the **Filters** field, enter the name (or a part of the name) of the person queried.
   The persons with the queried name (the string) appear.

Accessing a group of persons connected to a specific business role

To access a group of persons connected to a specific business role:

1. Access the user management page.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select the **Person groups by business role** sub-folder.
3. In the edit area, in the **Person groups by business role** tab, select a business role.
   The **Person Groups** tab lists the person groups associated with the selected business role.

   ☛ *See "Actions performed in the Person Groups management page", page 35.*

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 (Web Front-End)", page 31.*
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 in the Person Groups management page", page 35.*

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.

☛ *See "Managing Data Reading Access", page 321.*

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 (Web Front-End)", page 31.*
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 in the Person Groups management page", page 35.*

Accessing User Management and UI Access Management Folders (Windows Front-End)

This section describes how to access management windows for users, profiles, and business roles.

See:

Accessing User Management and UI Access Management Folders (Windows Front-End)

The **User management** folder contains all sub-folders for management of *users*, that is:

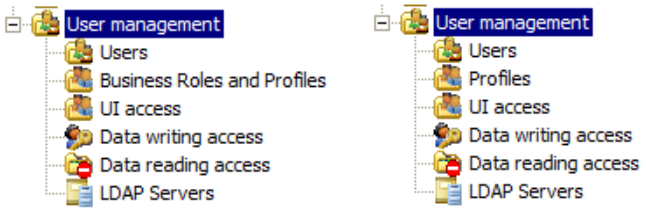
- *persons*, *person groups* and *logins*,
- *business roles* and *profiles*,
- *object UI access* and *general UI access*.

To access user management and UI access management folders:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **User management** folder of the environment.



☛ *When the "Management of assignment of business roles to persons" option is cleared, the **Business Roles and Profiles** folder becomes **Profiles**, see "Without Management of Assignment of Business Roles to Persons", page 99.*

From the **User management** folder of an environment you can access management windows:

- of **Users**
  User characteristics are defined in the following tabs:
  - **Persons**
  - **Person Groups**
  - **Logins**

    ☛ *See "Opening the user management window (Windows Front-End)", page 40.*
- of **Business Roles and Profiles**
  (case of assignment of business roles to persons)

    ☛ *See "Without Management of Assignment of Business Roles to Persons", page 99.*

    ☛ *See "Managing Profiles and Business Roles", page 88.*

    ☛ *See "Opening the business roles and profiles management window (Windows Front-End)", page 44.*
- of **Profiles**
  (case of definition of profiles on login of persons)

    ☛ *See "Managing Profiles and Business Roles", page 88.*

    ☛ *See "Opening the profile management window (Windows Front-End)", page 42.*
- of **UI access**
  Object UI access and general UI access are characteristics defined in tabs:
  - **Object UIs**
  - **General UIs**

    ☛ *See "Managing UI Access (Permissions)", page 282.*

Opening the user management window (Windows Front-End)

🕮 *A user is a person (or person group) with a login.*

Characteristics of *users* are managed in the **Users**window.

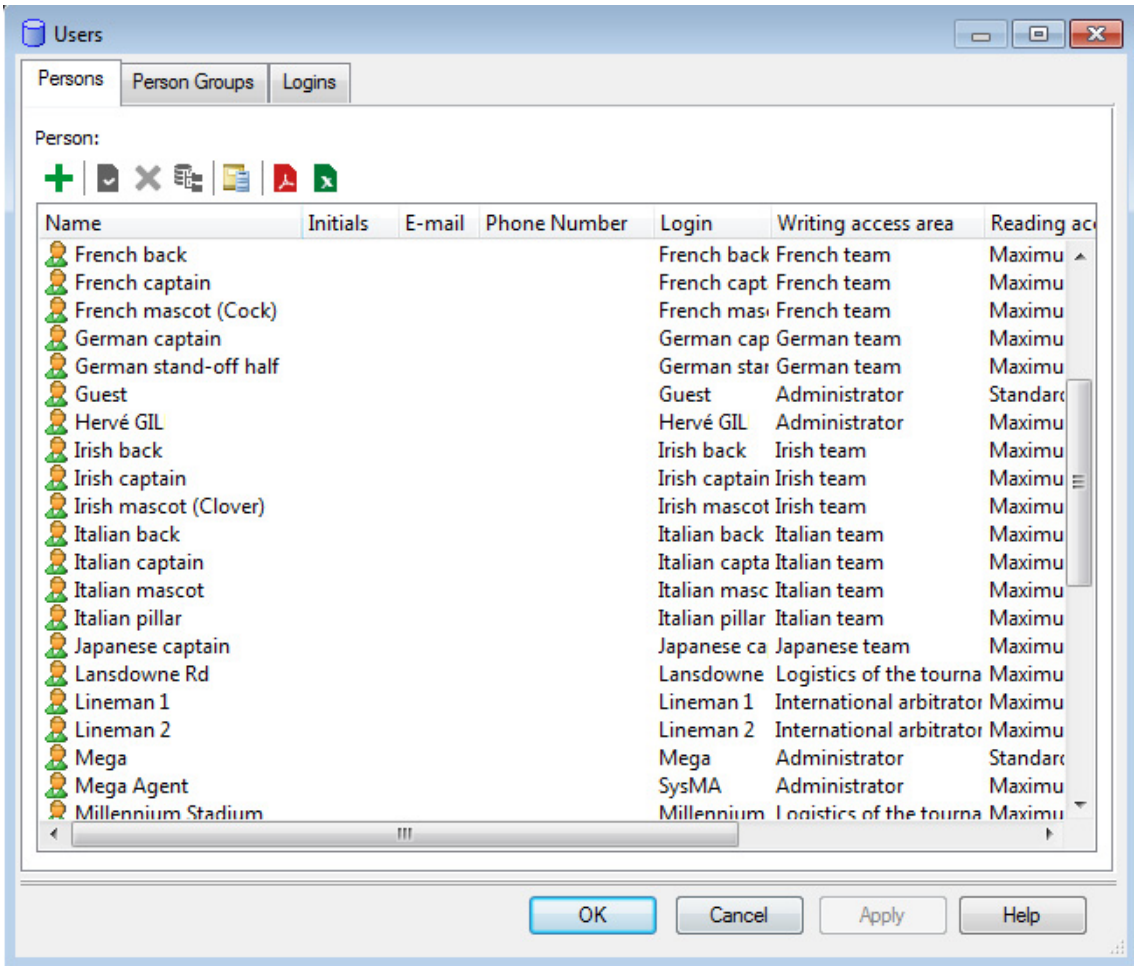
☛ *To manage user options, see "Managing Options", page 365.*

To manage users:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **User management** folder of the environment.

3. Right-click the **Users** folder and select **Manage**.
   The **Users** window opens.



The **Users** window contains tabs:

- **Persons**, listing all persons in the environment and detailing personal characteristics of each person.
- **Person Groups**, listing all person groups in the environment and detailing their characteristics.
- **Logins**, listing all users in the environment and detailing their characteristics and access rights to **MEGA** repositories.

From the **Users** management window you can:

- create:
  - persons
    - ☛ *See "Creating a Person", page 59.*
  - user management
    - ☛ *See "Creating Users", page 65.*
  - user groups
    - ☛ *See "Creating a Person Group", page 68.*
- configure characteristics:
  - of a person
    - ☛ *See "Configuring a Person", page 61.*
  - of a person group
    - ☛ *See "Defining a Person Group", page 70.*
  - of a login
    - ☛ *See "Configuring a Login", page 75.*
- delete users
  - ☛ *See "Deleting Users", page 81.*
- modify:
  - user properties
    - ☛ *See "Modifying User Properties", page 77.*
  - user passwords
    - ☛ *See "Creating or Modifying a User Password (Windows Front-End)", page 82.*
- access user options
  - ☛ *See "Managing Options", page 365.*

Opening the profile management window (Windows Front-End)

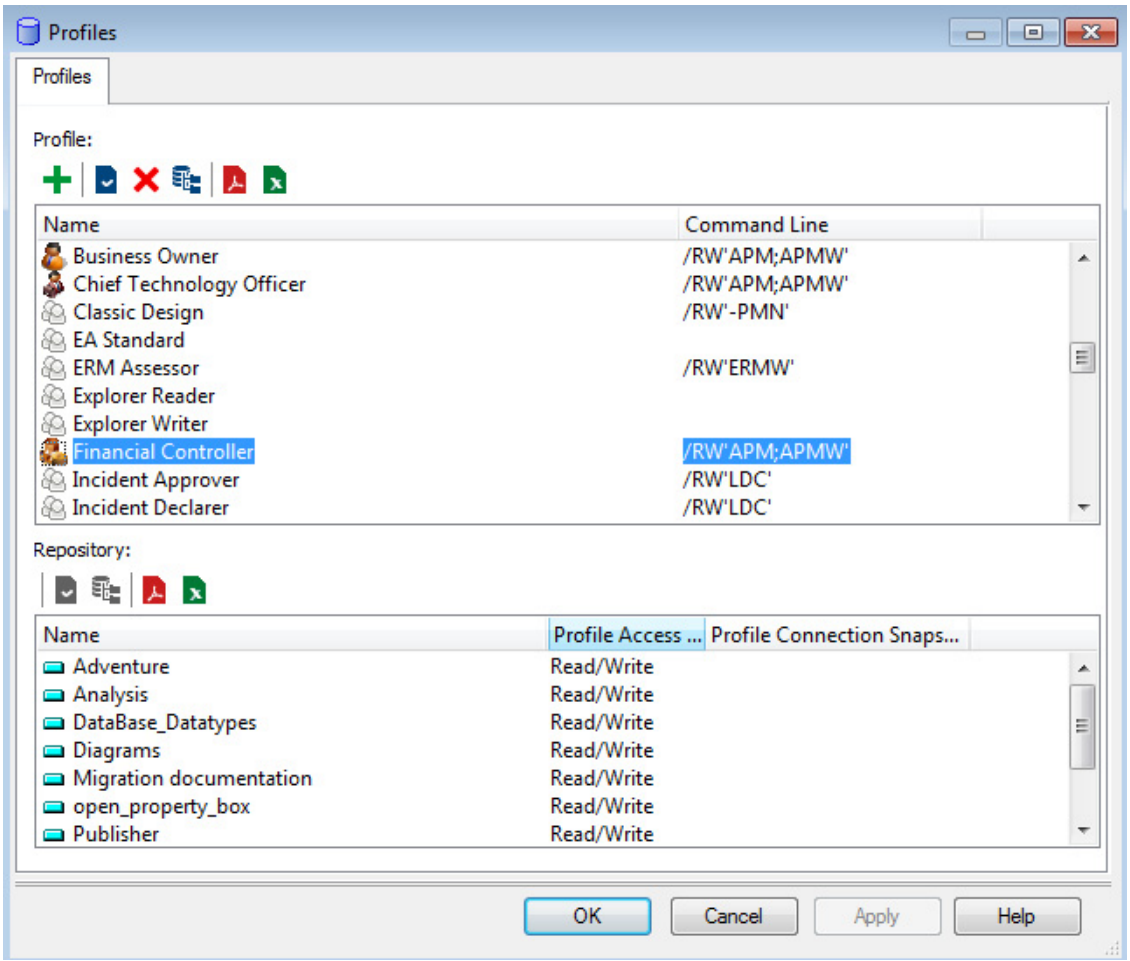
☛ *You are in the operating mode: definition of profiles to persons, see "Introduction to Business Roles and Profiles", page 89 and "Definition of profiles to persons mode", page 93.*

☛ *If you are in the operating mode: assignment of business roles to persons, see "Opening the business roles and profiles management window (Windows Front-End)", page 44.*

To manage profiles:

1. From **MEGA Administration**, connect to the environment concerned.
   - ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **User management** folder of the environment.

3. Right-click the **Profiles** folder and select **Manage**.
   The **Profiles** window opens.



The **Profiles** window of an environment enables management of user profiles. It lists all environment profiles and details for each profile the products that are accessible (optional).

☛ *See "Profiles Supplied", page 94.*

To be able to connect, a user must have at least one profile or business role depending on the selected operating mode (see "Managing Profiles and Business Roles", page 88). Users with the same profile share common characteristics (options, repository access rights, authorized products, read/write and read-only rights on objects).

☛ *See "Configuring a Profile", page 109 and "Connecting Users to a Profile", page 115.*

From the **Profiles** management window you can:

- create profiles
  - ☛ *See "Creating a Profile", page 105.*
- consult profile characteristics
  - ☛ *See "Configuring a Profile", page 109.*
- configure profiles
  - ☛ *See "Configuring a Profile", page 109.*
- connect users to profiles
  - ☛ *See "Connecting Users to a Profile", page 115.*
- delete profiles
  - ☛ *See "Deleting a Profile", page 118.*

Opening the business roles and profiles management window (Windows Front-End)

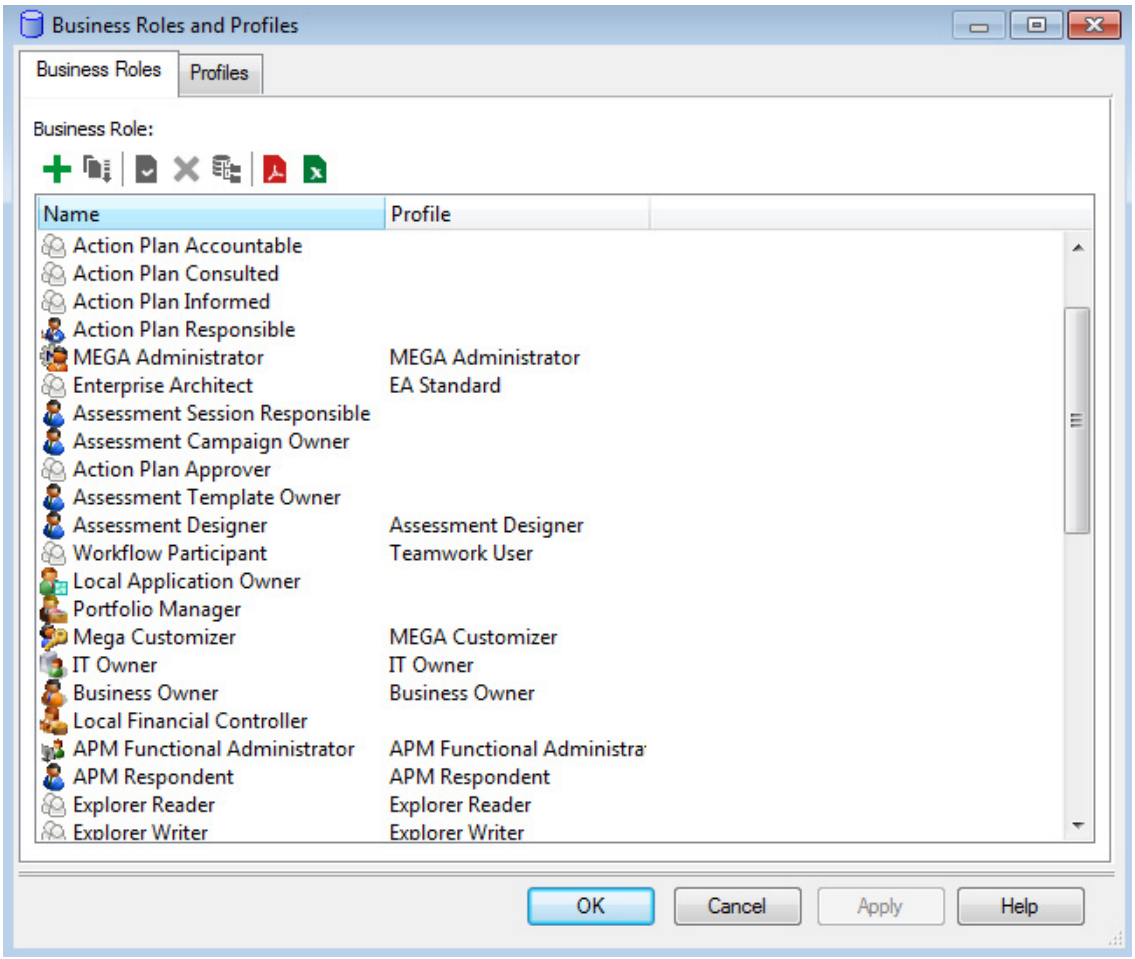
☛ *You are in operating mode: assignment of business roles to persons, see "Introduction to Business Roles and Profiles", page 89 and "Assignment of business roles to persons mode", page 91.*

☛ *If you are in operating mode: definition of profiles on login of persons, see "Opening the profile management window (Windows Front-End)", page 42.*

To manage business roles and profiles:

1. From **MEGA Administration**, connect to the environment concerned.
   - ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **User management** folder of the environment.

3. Right-click the **Business Roles and Profiles** folder and select **Manage**. The **Business Roles and Profiles** window opens.



The **Business Roles and Profiles** window enables management of user business roles and profiles.

The tab:

- **Business Roles** lists all business roles in the environment and details the associated profile for each business role used for connection.
  - ☛ *See "Business Roles Supplied", page 98.*
  - ☛ *See "Configuring a Business Role (Object Assignment)", page 122.*
- **Profiles** lists all environment profiles and specifies for each profile the products that are accessible.
  - ☛ *See "Profiles Supplied", page 94.*
  - ☛ *See "Configuring a Profile", page 109).*

Each user must have at least one business role connected to a profile. Users with the same profile share common characteristics (options, repository access rights, authorized products, read/write and read-only rights on objects).

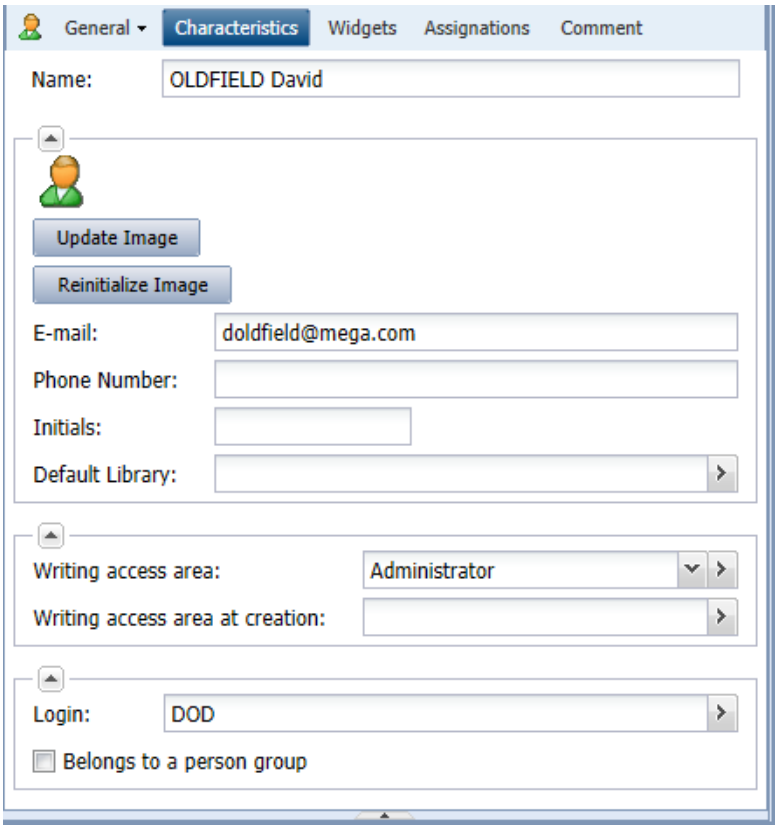
From the:

- **Business Roles** tab you can:
  - create a Business Role
    - ☛ *See "Creating Business Roles", page 120.*
  - consult Business Role characteristics
    - ☛ *See "Defining Business Role Characteristics", page 120.*
  - configure Business Roles
    - ☛ *See "Configuring a Business Role (Object Assignment)", page 122.*
  - assign Business Roles to Persons
    - ☛ *See "Assigning a business role to a person", page 123.*
  - delete Business Roles
    - ☛ *See "Deleting a Business Role", page 128.*
- **Profiles** tab you can:
  - create profiles
    - ☛ *See "Creating a Profile", page 105.*
  - consult profile characteristics
    - ☛ *See "Viewing Profile Characteristics", page 107.*
  - configure profiles
    - ☛ *See "Configuring a Profile", page 109.*
  - connect users to profiles
    - ☛ *See "Connecting Users to a Profile", page 115.*
  - delete profiles
    - ☛ *See "Deleting a Profile", page 118.*

Viewing Person Characteristics

See:

- "Viewing person characteristics (Web Front-End)", page 48
- "Viewing person characteristics (Windows Front-End)", page 48



The icon for a person is represented by:

- when the person is created (name and writing access area)
- when the person has a login (but the person's e-mail is not specified)
- when the person is configured as a **MEGA** user:
  name, writing access area, login and e-mail address are specified and a business role is assigned to the person (or a profile is connected to the person).

  ☛ *See "Configuring a Person", page 61, "Creating Users", page 65 and "Assigning a business role to a person", page 123 (or "Connecting Users to a Profile", page 115).*

Viewing person characteristics (Web Front-End)

To view person characteristics:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

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

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

   ☛ *You can sort or filter the display according to columns. See "Accessing the list of persons who have or do not have a login", page 37 and "Accessing a person using his/her name", page 37.*

   ☛ *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:
   - **Characteristics** to define or modify the person properties.

     ☛ *See "Person Properties", page 21.*

     ☛ *See "Configuring a Person", page 61.*

   - **General > History** to display the actions performed on the person.
   - **Assignments** to display and assign business roles to the person.

     ☛ *The **Assignments** tab appears in the case of management of profiles by assignment of business roles to persons, see "Without Management of Assignment of Business Roles to Persons", page 99.*

Viewing person characteristics (Windows Front-End)

To view person characteristics:

1. Open the **Users** management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*

2. Select the **Persons** tab.

   The list of persons appears with the characteristics of each person.

   ☛ *You can modify these characteristics directly in this page (with a click in the corresponding field).*

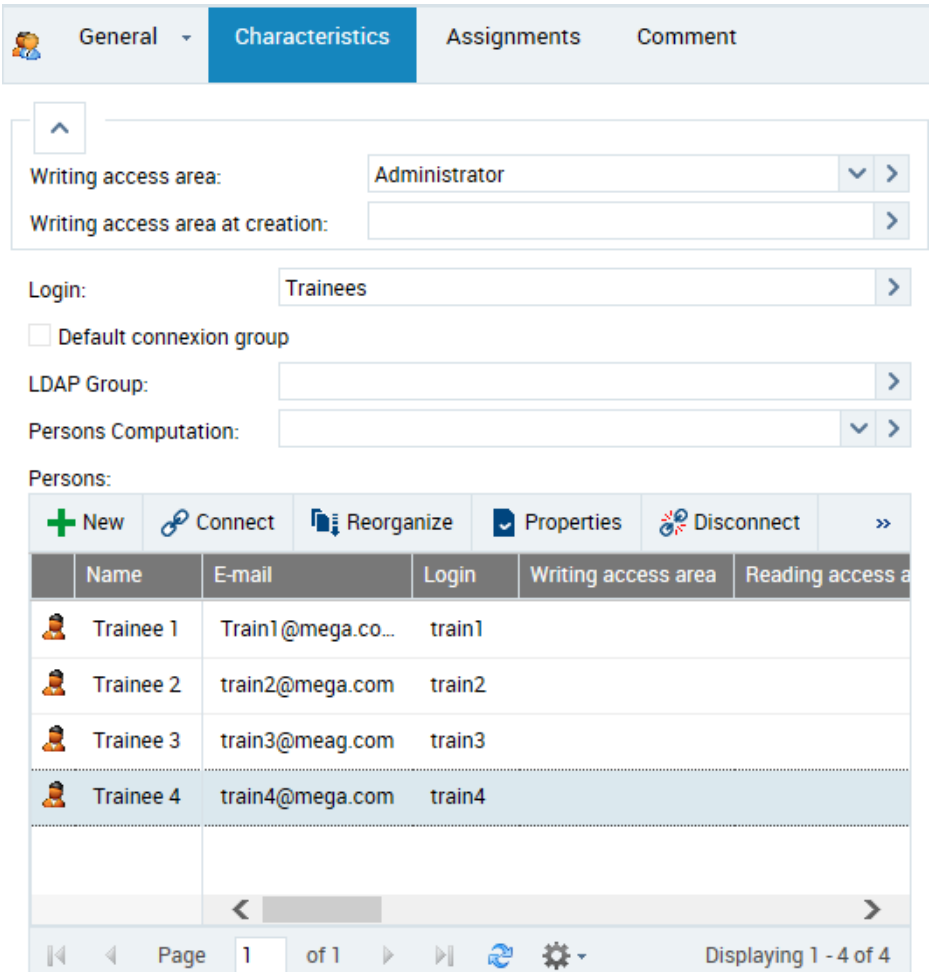
3. In the **Persons** list, select the person.
4. In the toolbar, click **Properties**  .

5. From the **Properties** dialog box for the person:
   - **Characteristics** to define or modify the person properties.
     - ☛ *See "Person Properties", page 21.*
     - ☛ *See "Configuring a Person", page 61.*
   - **General**, **History** sub-tab to display the actions performed on the person.
   - **Assignments** to display and assign business roles to the person.
     - ☛ *The **Assignments** tab appears in the case of management of profiles by assignment of business roles to persons, see "Without Management of Assignment of Business Roles to Persons", page 99.*

Viewing Person Group Characteristics

See:

- "Viewing person group characteristics (Web Front-End)", page 50
- "Viewing person group characteristics (Windows Front-End)", page 50



Viewing person group characteristics (Web Front-End)

To view person group characteristics:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

2. Select:
   - the **Person Groups** sub-folder for direct access, or
   - a classification sub-folder (**Person groups by business role**, **Person groups by writing access area**, or **Person groups by reading access area**) then in the edit area click the **Business role**, the **Writing access area** or the **Reading access area** concerned.

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

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

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

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

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

4. Click:
   - **Characteristics** to define or modify the person group properties.

     ☛ *See "Person Group Properties", page 23.*

     ☛ *See "Defining a Person Group", page 70, "Defining a dynamic person group with LDAP", page 72, "Defining a dynamic person group with a Macro", page 73.*

   - **General > History** to display the actions performed on the person group.
   - **Assignments** to display the business roles assigned to the person group.

     ☛ *The **Assignments** tab appears in the case of management of profiles by assignment of business roles to persons, see "Without Management of Assignment of Business Roles to Persons", page 99.*

Viewing person group characteristics (Windows Front-End)

To view person group characteristics:

1. Open the **Users** management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*

2. Select the **Person Groups** tab.
3. In the **Person Group** list, select the person group.
4. In the toolbar, click **Properties**  .

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

5. Select the **Characteristics** tab.

   ☛ *For detailed information on characteristics of a person group, see "Person Group Properties", page 23.*

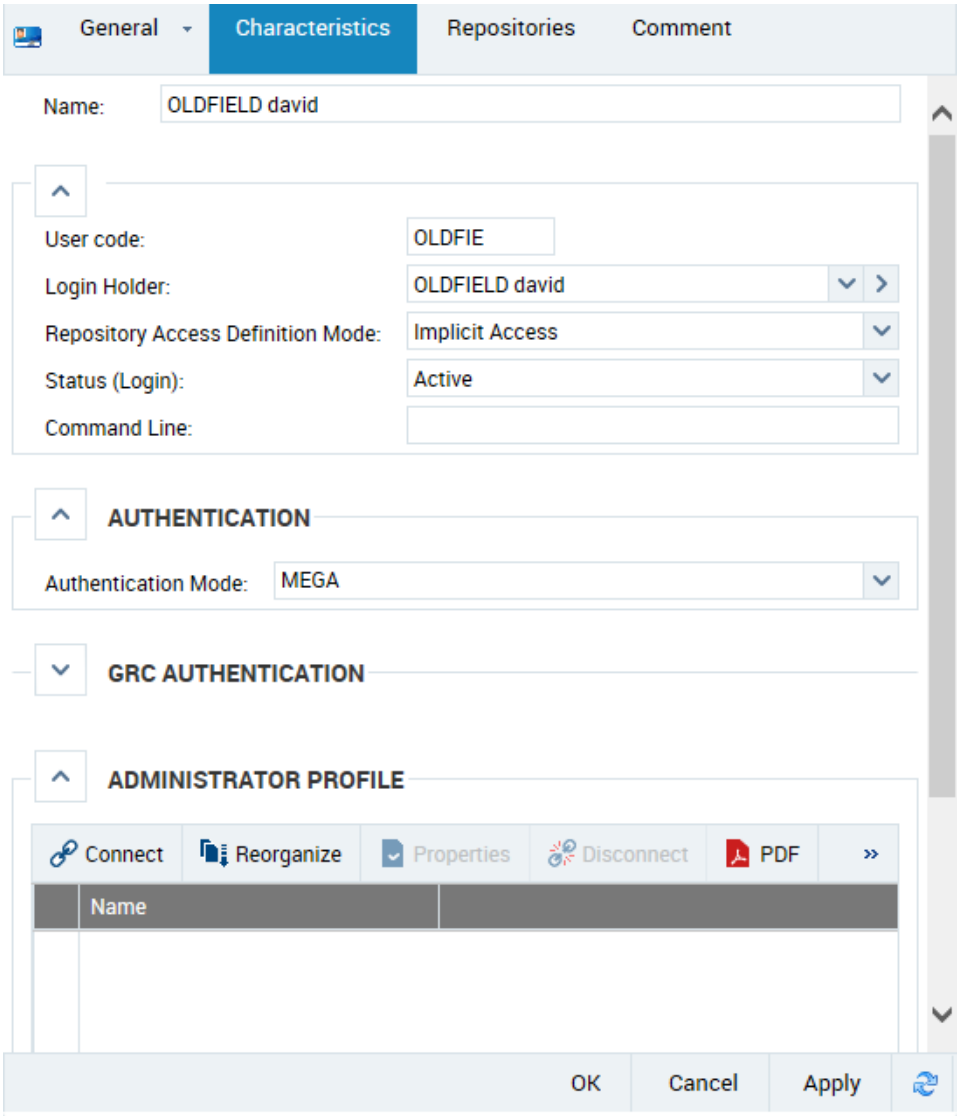
Viewing Login Characteristics

See:

- "Viewing login characteristics (Web Front-End)", page 52
- "Viewing login characteristics (Windows Front-End)", page 52

☛ *For detailed information on characteristics of a login, see "Login Properties", page 26.*

☛ *To configure a login, see "Configuring a Login", page 75.*



Viewing login characteristics (Web Front-End)

To view login characteristics:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

2. Select the **Persons** or **Person Groups** sub-folder.
3. In the Persons list, select the person concerned and click **Login Properties** .

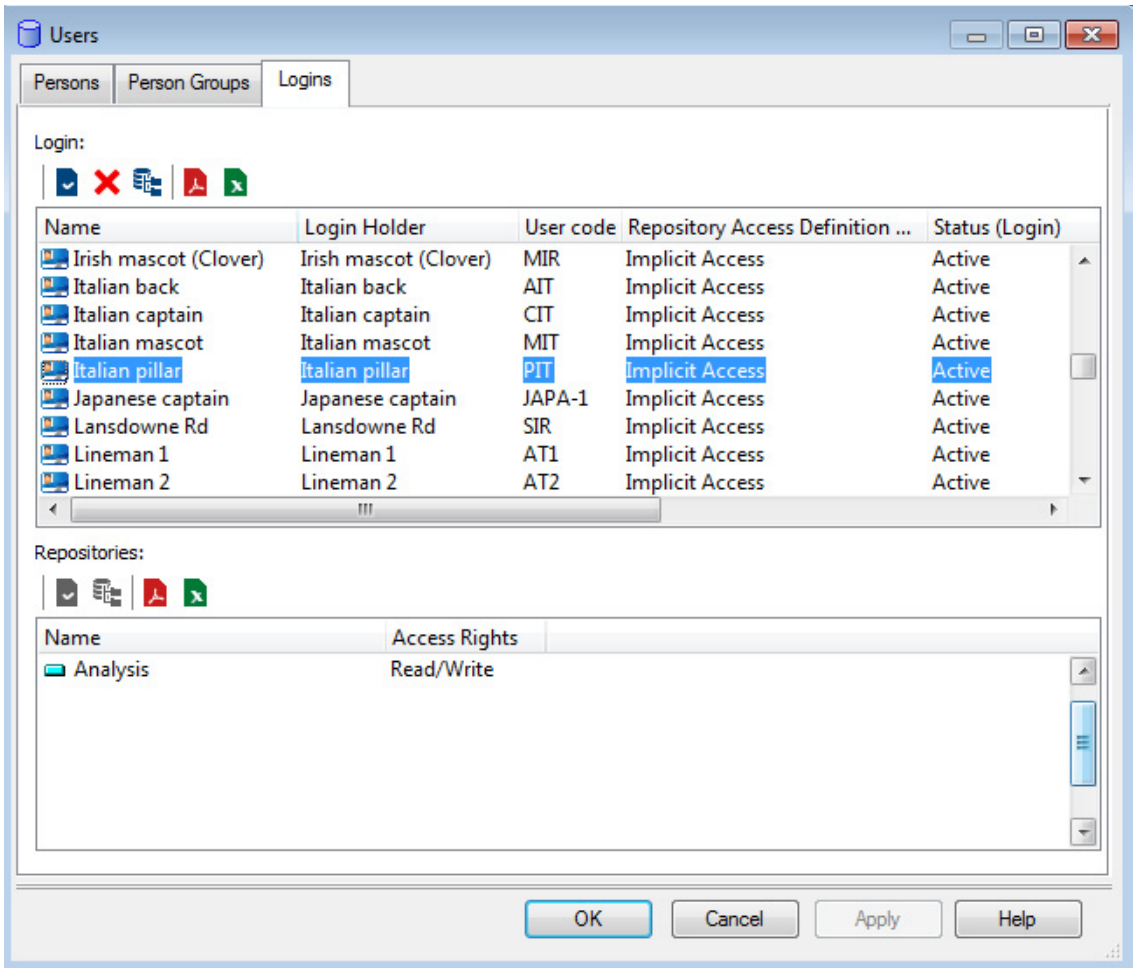
Viewing login characteristics (Windows Front-End)

To view login characteristics:

1. Open the **Users** management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*

2. Select the **Logins** tab.



3. In the **Login** frame, select the login.
   In the environment options, if the **Management of assignment of business roles to persons** option:

   ☛ *See "Without Management of Assignment of Business Roles to Persons", page 99.*

   - is selected: the **Repositories** frame displays repository access rights of the selected user.
   - is cleared: the **Repositories/Profiles** frame displays access rights to repositories of the selected user/profiles connected to the user.

4. In the toolbar, click **Properties**  .
   The **Properties** dialog box of the selected login opens.

ACTIONS TO BE PERFORMED TO DEFINE A USER

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

See:

Compulsory Actions to be Performed to Define a User

User configuration differs if the **Management of assignment of business roles to persons** option is:

☛ *See "Introduction to Business Roles and Profiles", page 89.*

- selected (by default)

☛ *See "Assignment of business roles to persons mode", page 91.*

- cleared

☛ *See "Definition of profiles to persons mode", page 93.*

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

- define the name of the person
  - ☛ *See "Creating a Person", page 59.*
  - ☛ *See "Creating Users", page 65.*
- define the login of the user
  - **A person must have a login to be able to connect to MEGA.**
  - ☛ *See "Creating the Login of a Person", page 64.*
  - ☛ *See "Creating Users", page 65.*
- (recommended) define the e-mail address of the person
  - ☛ *See "Creating Users (Web Front-End)", page 65.*
  - ☛ *See "Configuring a Person", page 61.*
  - ☛ *The e-mail address is necessary, for example, for distributing documents, receiving notifications and questionnaires, or when a Web user lost his/her password.*
- assign a business role for connection to the person ("Management of assignment of business roles to persons" option is selected, default mode)
  - **The user must have at least one business role to be able to connect to MEGA.**
  - ☛ *See "Assigning a business role to a person", page 123.*
- connect a profile to the user ("Management of assignment of business roles to persons" option is cleared)
  - **The user must have at least one profile to be able to connect to MEGA.**
  - ☛ *When the "Management of assignment of business roles to persons" option is selected, the profile is connected to the user through his/her business role. You do not have any other actions to perform.*
  - ☛ *See "Configuring a Login", page 75.*
  - ☛ *See "Connecting Users to a Profile", page 115.*

Optional Actions to be Performed to Configure 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 "Configuring a Person", page 61.*
- (where writing access management is activated) define the writing access area of the user
  - ☛ *See "Configuring a Person", page 61.*
  - ☛ *See "Connecting a Person to a Writing Access Area (Web Front-End)", page 80.*
- (where reading access management is activated) define the reading access area of the user
  - ☛ *See "Configuring a Person", page 61.*
  - ☛ *See "Connecting a Person to a Reading Access Area (Web Front-End)", page 81.*
- define if the person belongs to a person group.
  - ☛ *See "Configuring a Person", page 61.*

Other Actions to Set or Manage a User

You can:

- define the telephone number and initials of the person
  - ☛ *See "Configuring a Person", page 61.*
- (specific to Web application) define the data language of the Web user
  - ☛ *See "Configuring a Person", page 61.*
- modify user repository access definition mode
  - ☛ *See "Configuring a Login", page 75.*
- restrict user repository access rights
  - ☛ *See "Restricting User Repository Access Rights", page 83.*
- restrict user access to certain products
  - ☛ *See "Configuring a Login", page 75.*
  - ☛ *See "Configuring a Profile", page 109.*
- modify user authentication mode
  - ☛ *See "Configuring a Login", page 75.*
- make the user inactive.
  - ☛ *See "Configuring a Login", page 75.*
  - ☛ *See "Preventing User Connection", page 81.*

Checking the Configuration of Persons (Web Front-End)

From the **Administration** desktop (Web Front-End), 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 (Web Front-End)", page 31.*

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

CREATING, SETTING, AND MANAGING USERS

User configuration differs if the **Management of assignment of business roles to persons** option:

☛ *See "Introduction to Business Roles and Profiles", page 89.*

- is selected (by default): business roles must be assigned to persons

☛ *See "Assignment of business roles to persons mode", page 91.*

- is cleared: profiles must be connected to login of persons

☛ *See "Definition of profiles to persons mode", page 93.*

For an overview of actions to be performed to create and define a user see "Actions to be Performed to Define a User", page 54.

The following points are covered here:

Creating a Person

> 🕮 ***Person*** *represents a physical person or a system.*
>
> ☛ *Instead of creating persons one by one, you can import a list of persons. This list can for example come from an LDAP server (see "Synchronization with a company directory", page 131).*

If necessary, you can first create a person with a restricted configuration:

- its name
- writing access area

> ☛ *The person login is automatically created.*

To complete the configuration of the person, see "Configuring a Person", page 61.

> ☛ *To create a user directly, see "Creating Users", page 65.*

See:

- "Creating a person (Web Front-End)", page 59
- "Creating a person (Windows Front-End)", page 60

Creating a person (Web Front-End)

You can create the person as follows:

- not predefined
- predefined with one of the following criteria:
  - the group to which the person belongs
  - a business role for connection (where the "Assignment of business roles to persons" option is selected)
  - a profile (where the "Assignment of business roles to persons" option is cleared)
  - a writing access area
  - a reading access area (if reading access management is activated)

To create a **Person**:

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

   > ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

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 business role *(available if the "Management of assignment of business roles to persons" option is selected) to create a person and automatically assign to this person the business role.*

   Persons by profile *(available if the "Management of assignment of business roles to persons" option is cleared) to create a person automatically connected to 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 business role, 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. (If necessary) In the **Writing access area** field, in the drop-down menu, select the writing access area for the person.

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

   ☛ *For more details on writing access, see "Managing Data Writing Access", page 297.*
7. (If necessary) In the **Reading access area** field, in the drop-down menu, select the reading access area for the person.

   ☛ *For more details on reading access, see "Managing Data Reading Access", page 321.*
8. Click **OK**.
   The login for the person is automatically created.

   The person appears in the list of persons  .

   ☛ *To complete the configuration of the person, see "Configuring a Person", page 61.*

Creating a person (Windows Front-End)

To create a **Person**:

1. Open the user management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*
2. Select the **Person** tab.

3. Click **New**  .
   The **Creation of Person - Characteristics** dialog box opens.
4. In the **Name** field, enter the name of the person.

   ```
   Example: OLDFIELD David
   ```

   ☛ *Remember to use the same format for all persons.*
5. In the **Writing access area** field, click the arrow and select the writing access area for the user.

   ☛ *For more details on writing access, see "Managing Data Writing Access", page 297.*
6. Click **OK**.
   The login for the person is automatically created.

   The person appears in the list of persons  .

   ☛ *To complete the configuration of the person, see "Configuring a Person", page 61.*

   ☛ *By default, the new user does not have an associated password. To associate a password with the user, see "Creating or Modifying a User Password (Windows Front-End)", page 82.*

Configuring a Person

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

☛ *For more information on properties of a person, see "Person Properties", page 21.*

☛ *(Web Front-End) To check the configuration of a person, see "Checking the Configuration of Persons (Web Front-End)", page 57.*

From the properties dialog box 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.*
- login of the user
  - ☛ *See step 8.*
- if the user belongs to a person group
  - ☛ *See step 9.*

To configure a **Person**:

1. Access the properties of the person.
   - ☛ *See "Viewing Person Characteristics", page 47.*
2. (Optional) To add or update the image of the person, click **Update Image**, select the image and click **OK**.
   - ☛ *To delete the image, click **Reinitialize Image**.*
3. (Optional, but 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", page 377.*
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 **MEGA 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". For more details on writing access, see "Managing Data Writing Access", page 297.*

     ☛ *See also "Connecting a Person to a Writing Access Area (Web Front-End)", page 80.*
   - 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 "Managing Data Reading Access", page 321.*

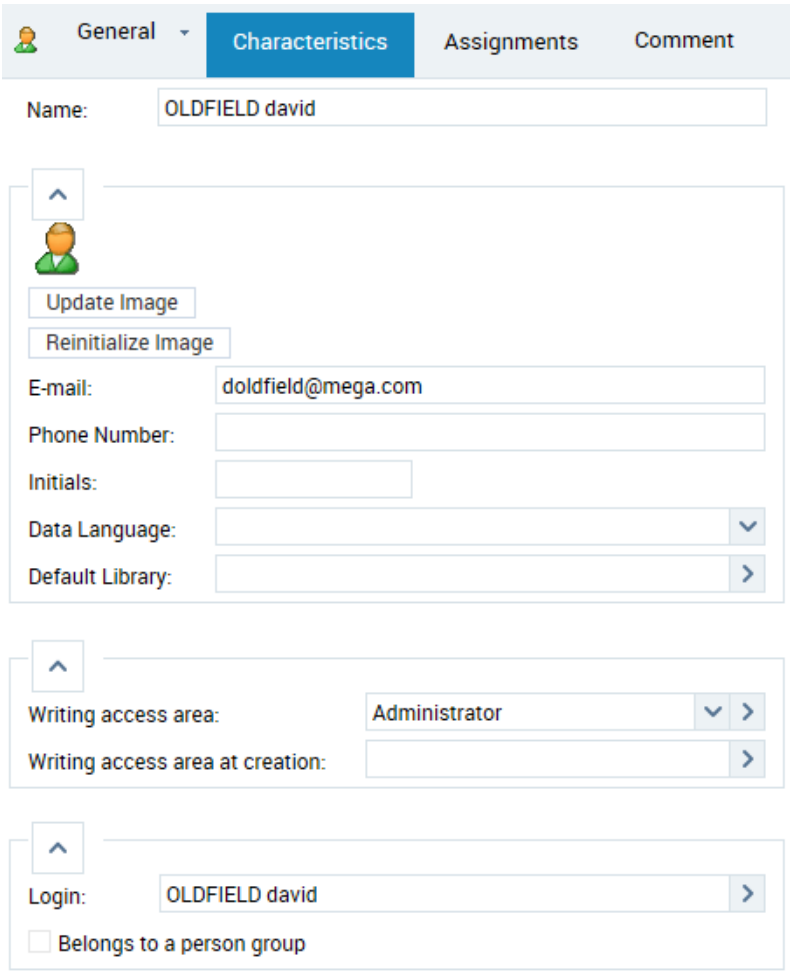
     ☛ *See also "Connecting a Person to a Reading Access Area (Web Front-End)", page 81.*
   - reading access at creation via the drop-down menu in the **Writing Access Area** field.

     ☛ *This field only appears if reading access management has been activated, see "Managing Data Reading Access", page 321.*
8. So that the person can connect to **MEGA**, the person must have a **Login**.

   ☛ *See "Creating the Login of a Person", page 64.*

   ☛ *See "Configuring a Login", page 75.*

9. (optional) If necessary select **Belongs to a Person Group**



10. (Web Front-End) Click **Save**.
    (Windows Front-End) Click **OK**.
    The person is configured.

    ☛ *(Web Front-End) To notify the users connected of your changes, click **Notify Connected Users**.*

Creating the Login of a Person

To connect to **MEGA**, a person must have a Login. When you create a person, his/her login is automatically created.

To create the login of a person:

1. Access the properties of the person.

   ☛ *See "Viewing Person Characteristics", page 47.*

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.

Creating Users

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

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

☛ *For detailed information on characteristics of a person, see "Person Properties", page 21.*

☛ *For detailed information on characteristics of a login, see "Login Properties", page 26.*

☛ *To import users from an LDAP directory, see "LDAP Authentication", page 133.*

See:

- "Creating Users (Web Front-End)", page 65
- "Creating Users (Windows Front-End)", page 67

Creating Users (Web Front-End)

To create a user:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

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 business role *(available if the "Management of assignment of business roles to persons" option is selected) to create a person and automatically assign to this person the business role.*

   Persons by profile *(available if the "Management of assignment of business roles to persons" option is cleared) to create a person automatically connected to 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 business role, 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.

   ☛ *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 **MEGA 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.*

   ☛ *For more details on writing access, see "Managing Data Writing Access", page 297.*
9. (If required, with the **MEGA 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, see "Managing Data Reading Access", page 321.*

10. Click **Next** and select:

    ☛ *If at step 2. you have selected **Person by business role** or **Person by profile**, go directly to step 11.*

    ☛ *If necessary you can assign business roles (or connect a profile) to the user at a later time, see "Assigning a business role to a person", page 123 (or "Connecting Users to a Profile", page 115). Go directly to step 11.*

    - the connection business role that you want to assign to the person (where the "Management of assignment of business roles to persons" option is selected)

      ☛ *You can assign more than one business role to the same person.*

    - the profile that you want to assign to the person (where the "Management of assignment of business roles to persons" option is cleared)

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

11. Click **OK**.

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

    ☛ *To configure characteristics of the user, see "Configuring a Person", page 61*

    ☛ *You must configure the login of the user, see "Configuring a Login", page 75.*

Creating Users (Windows Front-End)

To create a user:

1. Open the **Users** management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*

2. In the **Users** window, select the **Persons** tab.

3. Click **New** .
   The **Creation of Person - Characteristics** dialog box opens.

4. In the **Name** field, enter the name of the person.

   `Example: DUBOIS Guillaume`

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

5. (Optional, but recommended) In the **E-mail** field, enter 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.*

6. In the **Login** field, enter the login of the person.

   ☛ *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`

7. (With the **MEGA 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.

   ☛ *For more details on writing access, see "Managing Data Writing Access", page 297.*

8. (If required, with the **MEGA 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, see "Managing Data Reading Access", page 321.*

9. Click **Finish**.
   The user is created (a login is associated with the person): the person appears in the list of persons and its login appears in the list of logins.

   ☛ *You must configure the login of the user, see "Configuring a Login", page 75.*

   ☛ *By default, the new user does not have an associated password. To associate a password with the user, see "Creating or Modifying a User Password (Windows Front-End)", page 82.*

Creating a Person Group

☛ *Specific to RDBMS environments.*

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

☛ *For information on connecting persons who belong to a person group, see "User Group: Definition", page 21.*

☛ *For information on person group types, see "Person group types", page 25.*

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

☛ *For detailed information on:*

- the characteristics of a person, see "Person Properties", page 21.

- the characteristics of a person group, see ("Person Group Properties", page 23)

- the characteristics of a login, see "Login Properties", page 26.

- the types of person groups, see ("Person group types", page 25)

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

See:

- "Creating a person group (Web Front-End)", page 68.
- "Creating a person group (Windows Front-End)", page 69.

Creating a person group (Web Front-End)

To create a person group:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

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 business role *(available if the "Management of assignment of business roles to persons" option is selected) to create a person group and automatically assign to the person group the business role, that you are going to select.*

   Person groups by profile *(available if the "Management of assignment of business roles to persons" option is cleared) 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 zone, select the profile, the business role, 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 **MEGA 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.*

   ☛ *For more details on writing access, see "Managing Data Writing Access", page 297.*
7. (With the **MEGA 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. See "Managing Data Reading Access", page 321.*

   ☛ *This field only appears if reading access management has been activated, see "Managing Data Reading Access", page 321.*
8. Click **OK**.

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

   You must define this person group, see "Defining a Person Group", page 70.

Creating a person group (Windows Front-End)

To create a person group:

1. Open the **Users** management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*
2. In the **Users** window, select the **Person Groups** tab.

3. Click **New**  .
   The **Creation of Person Group - Characteristics** dialog box opens.
4. In the **Name** field, enter the name of the person group.

   ```
   Example: Marketing.
   ```
5. (With the **MEGA 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.

   ☛ *For more details on writing access, see "Managing Data Writing Access", page 297.*
6. (With the **MEGA Supervisor** technical module, if reading accesses management is activated) 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, see "Managing Data Reading Access", page 321.*
7. Click **OK**.
   The person group is created and listed in the **Person Groups** tab.
   You must define this person group, see "Defining a Person Group", page 70.

Defining a Person Group

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

☛ *See "User Group: Definition", page 21.*

☛ *For detailed information on:*

- the characteristics of a person, see "Person Properties", page 21.

- the characteristics of a person group, see "Person Group Properties", page 23.

- the characteristics of a login, see "Login Properties", page 26.

- the types of person groups, see "Person group types", page 25.

A person group can be created:

- statically

  ☛ *See "Connecting one or more persons to a person group", page 71.*
- dynamically

  ☛ *See "Defining a dynamic person group with LDAP", page 72.*

  ☛ *see "Defining a dynamic person group with a Macro", page 73.*

You can:

- define a default connection group.

  ☛ *See "Defining a default connection group", page 74.*

- connect the person group with access to a reading area

  ☛ *See "Connecting a person group with access to a reading area (Web Front-End)", page 74.*

- connect the person group with access to a writing area

  ☛ *See "Connecting a person group with access to a writing area (Web Front-End)", page 74.*

- (Web Front-End) define the data language of the person group

  ☛ *See "Specifying Data Language for a User or User Group (Web Front-End)", page 145.*

To configure a person group, you must:

- assign a business role to the person group

  ☛ *See "Assigning a Business Role to a Person Group (Web Front-End)", page 128.*

- configure its login

  ☛ *See "Configuring a Login", page 75.*

Connecting one or more persons to a person group

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

1. Access the properties of the person group you want to configure.

   ☛ *See "Viewing Person Group Characteristics", page 49.*

2. From the **Characteristics** tab, in the **Person** frame, click **Connect**  .

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

3. (Optional) In the query wizard, in the second field enter the characters to find.

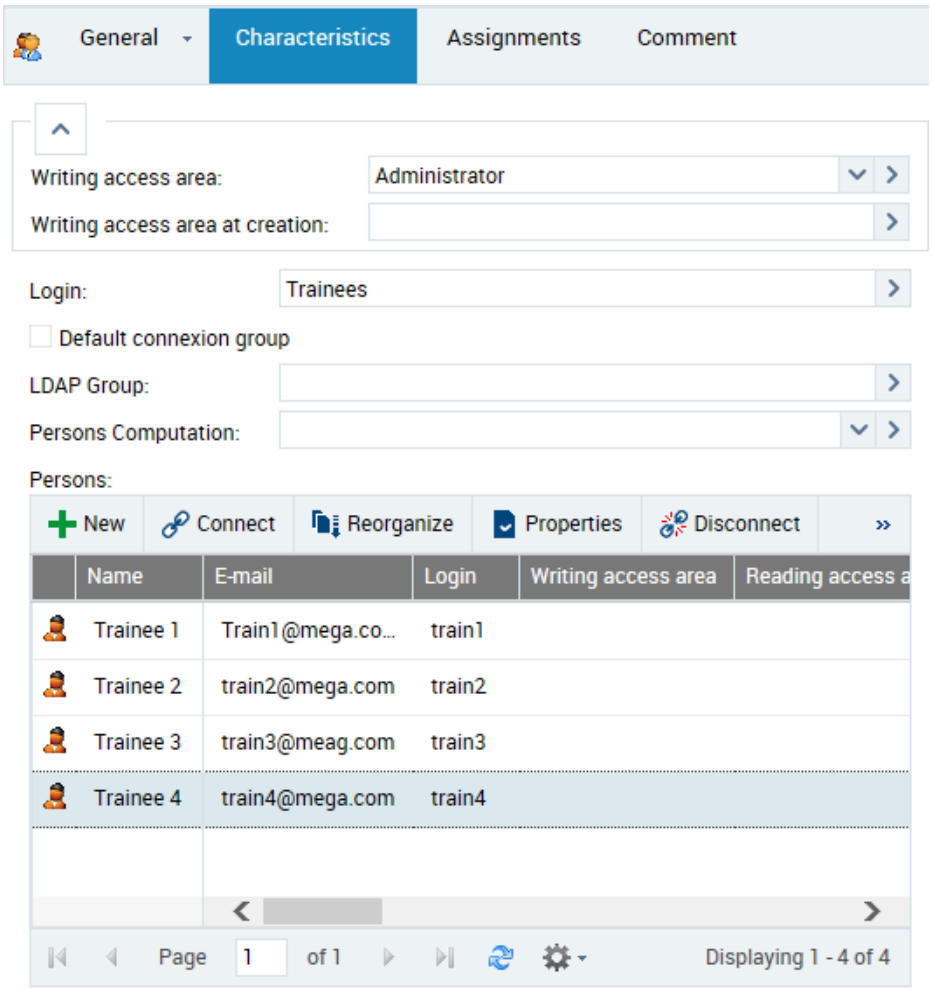
4. Click **Find**  .
   The persons queried are listed.

5. 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.*

6. Click **Add**.
   The person(s) are connected to the person group.



7. Click **OK**.

Defining a dynamic person group with LDAP

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

A dynamic group is a group that computes group users on the fly.

For information on person group types, see "Person group types", page 25.

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

Prerequisite: the LDAP group is already created.

☛ *See "LDAP Authentication", page 133.*

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

1. Open the properties dialog box of the person group.

   ☛ *See "Viewing Person Group Characteristics", page 49.*
2. Select the **Characteristics** tab.
3. In the **LDAP Group** field, click the arrow and connect the required LDAP group.
4. Click **OK**.
   The dynamic person group is configured with LDAP.

Defining a dynamic person group with a Macro

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

📖 *A dynamic group is a group that computes group users on the fly.*

☛ *For information on person group types, see "Person group types", page 25.*

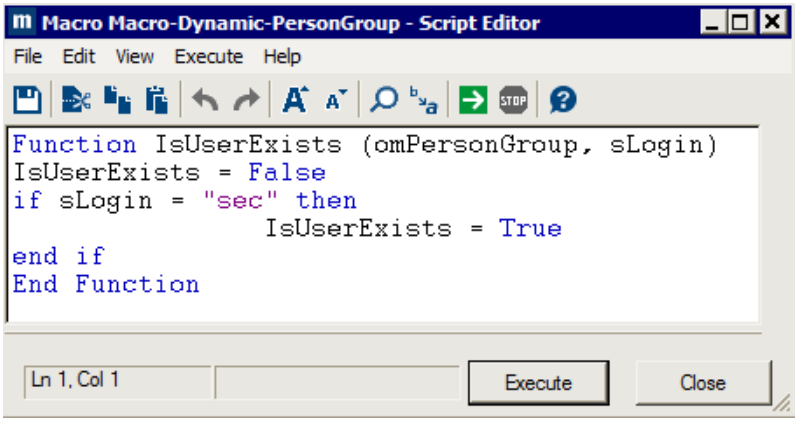
The **Computed Persons** attribute enables definition of a macro defining a list of persons connected to this person group. Persons defined by the macro use the configuration defined on the person group.

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

1. Open the properties dialog box of the person group.

   ☛ *See "Viewing Person Group Characteristics", page 49.*
2. Select the **Characteristics** tab.
3. In the **Computed Persons** field, click the arrow and connect the required macro.

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



   omPersonGroup represents the person group object executing the query.

   sLogin represents the authentication login of the person.
4. Click **OK**.
   The dynamic person group is configured with a macro.

Defining a default connection group

> *A **Person Group** is a list of persons belonging to the same group. These persons share the same connection characteristics.*
>
> ☛ *For information on person group types, see "Person group types", page 25.*

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. Open the properties dialog box of the person group.

   ☛ *See "Viewing Person Group Characteristics", page 49.*
2. Select the **Characteristics** tab.
3. Select **Default connection group** option.

Connecting a person group with access to a writing area (Web Front-End)

> ☛ *Managing writing access areas is available with the **MEGA Supervisor** technical module only. See "Managing Data Writing Access", page 297.*
>
> ☛ *To connect a person group to a writing access area, see also "Creating a Person Group", page 68.*

To connect a person to a writing access area:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select the **Persons by writing access area** sub-folder.
3. In the edit area, select a writing access area.
4. Click **Connect**  .

   ☛ *To add a person group not yet created, click **New**  .*
5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find**  .
   The person groups queried are listed.
7. In the result list, select the person group you want to connect.

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

Connecting a person group with access to a reading area (Web Front-End)

> ☛ *Managing reading access areas is only available with the **MEGA Supervisor** technical module. See "Managing Data Reading Access", page 321.*
>
> ☛ *To connect a person group to a reading access area, see also "Creating a Person Group", page 68.*

To connect a person group with a reading access area:

1. Access the **User Management** pages.
   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
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 group not yet created, click **New**  .*
5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find**  .
   The person groups queried are listed.
7. In the result list, select the person group you want to connect.
   ☛ *You can select more than one person group.*
8. Click **Add**.
   The person groups selected are connected to the reading access area selected.

Configuring a Login

From the login properties dialog box, you can:

☛ *See "Login Properties", page 26.*

- define the login name, the user code associated with login and the login holder
  ☛ *See step 1.*
- modify user repository access definition mode
  ☛ *See step 2.*
- modify user status (inactive)
  ☛ *See step 3.*
- restrict user access to certain products
  ☛ *See step 4.*
- modify user authentication mode
  ☛ *See step 5.*
- restrict user repository access rights
  ☛ *See "Restricting User Repository Access Rights", page 83.*
- (in operating mode: definition of profiles on login of persons see "Definition of profiles to persons mode", page 93) give a profile to a user, i.e. connect the user login to a profile.
  At least one profile must be connected to the login.
  ☛ *See step 6.*
  ☛ *See "Connecting Users to a Profile", page 115.*

To configure a login:

1. Display the **Characteristics** tab of the login properties.

   ☛ *See "Viewing Login Characteristics", page 51.*

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

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

     *The **User code** is the short identifier (upper case) of the user. It serves as a basis for naming user private workspaces.*

   - The **Login Holder** represents the person or person group associated with this login.

2. (Optional) Modify the value of the **Repository Access Definition Mode** field. The default value is "Implicit Access".

   ☛ *See "Repository access definition mode", page 27.*

3. (Optional) The value of the **Status** field defines if the user is active or not.

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

   For example: You have licenses for products **MEGA Process, MEGA Architecture: and other MEGA products.** To authorize only the **MEGA Process** and **MEGA Architecture:** modules to a user, enter: /RW'PRO;ARC'

   ☛ *To determine the product code, see "Product Codes", page 384.*

   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.

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

   ☛ *See "Authentication mode", page 28.*

6. (in operating mode: definition of profiles on login of persons, see "Definition of profiles to persons mode", page 93) In the **Profile** frame, click **Connect**  .

   A user without a profile cannot connect to *MEGA*. You must connect at least one profile to the login.

   A wizard lists available profiles.

7. (Optional) To restrict the query, in the second field select characters of the profile to be queried and click **Find**  .

8. In the list of profiles select the profile(s) you want to connect to the login.

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

9. Click **Add**.
   The selected profiles are connected to the user login.

10. Click **Apply**.

Modifying User Properties

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

- person:
  - its name
  - image
  - e-mail address
  - telephone number
  - initials
  - data language
  - writing access area
  - reading access area
  - login
  - group

    ☛ *See "Person Properties", page 21.*

    ☛ *See "Viewing Person Characteristics", page 47.*

    ☛ *See "Configuring a Person", page 61.*
- login:
  - its name
  - user code

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

    ☛ *See "Login Properties", page 26.*

    ☛ *See "Viewing Login Characteristics", page 51.*

    ☛ *See "Configuring a Login", page 75.*

Modifying User Group Properties

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

- person group:
  - name
  - writing access area
  - reading access area
  - login
  - if it is default connection group
  - group type (LDAP group, computed person group or persons directly connected to group)
  - persons owned in the group

    ☛ *See "Person Group Properties", page 23.*

    ☛ *See "Viewing Person Group Characteristics", page 49.*

    ☛ *See "Defining a Person Group", page 70.*

    ☛ *See "Defining a dynamic person group with LDAP", page 72.*

    ☛ *See "Defining a dynamic person group with a Macro", page 73.*
- login:
  - name
  - user code
  - repository access definition mode
  - status
  - accessible products (Command Line)
  - authentication mode
  - accessible repositories
  - profiles

    ☛ *See "Login Properties", page 26.*

    ☛ *See "Viewing Login Characteristics", page 51.*

    ☛ *See "Configuring a Login", page 75.*

Transferring the Responsibilities of a Person (Web Front-End)

From the **Administration** desktop (Web Front-End), you can transfer all or part of a 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 "Duplicating the Responsibilities of a Person (Web Front-End)", page 79.*

To transfer the responsibilities from one person to another:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
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 **Add**.
7. (Optional) In the query wizard, in the second field enter the characters to find.
8. Click **Find**.
9. Select the person to whom you want to transfer the responsibilities.

   ☛ *You can select more than one person.*

   If you select more than one target user, only the object assignments that can be assigned to more than one person and the connection business roles are offered.

10. Click **Add**.
11. Click **Next**.
12. In the **Connection Business Roles** frame, select the business roles that you want to transfer to the target user (or to the selected persons).
13. In the **Object Assignments** frame, select the object assignments that you want to transfer.
14. Click **OK**.
    The assignments selected are deleted from the source user (or source users) and transferred to the target user (or target users).

Duplicating the Responsibilities of a Person (Web Front-End)

From the **Administration** desktop (Web Front-End), 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 (Web Front-End)", page 31.*

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.*

   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 **Add**.
7. (Optional) In the query wizard, in the second field enter the characters to find.

8. Click **Find**  .
9. Select the person to whom you want to duplicate the responsibilities.

   ☛ *You can select more than one person.*

   Only the object assignments that can be assigned to more than one person and the connection business roles are offered.
10. Click **Add**.
11. Click **Next**.
12. In the **Connection Business Roles** frame, select the business roles that you want to assign to the target user (or to the selected persons).
13. In the **Object Assignments** frame, select the object assignments that you want to duplicate.
14. Click **OK**.
    The assignments are assigned to the target user (or target users).

Connecting a Person to a Writing Access Area (Web Front-End)

☛ *Managing writing access areas is available with the **MEGA Supervisor** technical module only. See "Managing Data Writing Access", page 297.*

☛ *To connect a person to a writing access area, see also "Configuring a Person", page 61.*

To connect a person to a writing access area:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select the **Persons by writing access area** sub-folder.
3. In the edit area, select a writing access area.
4. Click **Connect**  .

   ☛ *To add a person not yet created, click **New**  .*
5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find**  .
   The persons queried are listed.
7. In the result list, select the person you want to connect.

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

Connecting a Person to a Reading Access Area (Web Front-End)

☛ *Managing reading access areas is only available with the **MEGA Supervisor** technical module. See "Managing Data Reading Access", page 321.*

☛ *To connect a person to a reading access area, see also "Configuring a Person", page 61.*

To connect a person to a reading access area:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select the **Persons by writing access area** sub-folder.
3. In the edit area, select a reading access area.
4. Click **Connect**  .

   ☛ *To add a person not yet created, click **New**  .*
5. (Optional) In the query wizard, in the second field enter the characters to find.
6. Click **Find**  .
   The persons queried are listed.
7. In the result list, select the person you want to connect.

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

Preventing User Connection

When you no longer want a user to connect to **MEGA**, 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. Open the **Characteristics** tab of the login properties dialog box.

   ☛ *See "Viewing Login Characteristics", page 51.*
2. In the **Status** field, select "Inactive".
3. Click **Apply**.

Deleting Users

When you delete a user from the repository, the commands connected to this user become orphans and you lose part of the history saved in logs. To remove a user but keep its history of commands, see "Preventing User Connection", page 81.

To delete a user:

1. Access the User Management page.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*

2. In the **Persons** tab, 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 or Modifying a User Password (Windows Front-End)

☛ *To manage the password of a Web user, see "Initializing and managing the password of a Web user", page 142:*

By default, the user does not have a password.

☛ *Only a user with **Administrator** type profile has management rights. He is the only user type that can create a user password. To grant administrator access rights to a user, see "Configuring a Login", page 75.*

The password can be modified later:

- from **MEGA**, by the user, from the MEGA connection dialog box.
- from **MEGA Administration** by the Administrator, notably when the user has forgotten his/her password.

To create or modify the password of a user (Windows Front-End):

1. Open the **Users** management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*

2. Select the **Logins** tab.

3. In the logins list, right-click the login concerned and select **Password**.
The **Change User Password** dialog box opens.

4. Enter the password you want to assign to the user.
   ☛ *Do not use separation character (“!”, “$”, “@”, “:”, “;”).*
   Password confirmation entry is required.
   ☛ *If the two entries are not identical, the entry must be corrected.*
5. Click **OK**.
The user password is saved.

Restricting User Repository Access Rights

Access rights to environment repositories are defined by the profile with which the user connects to the repository.

☛ *See "Configuring a Profile", page 109.*

If repository access rights are also defined on the login of a user, these rights are added to restrictions on rights defined on the profile. Access rights defined on the login cannot extend those defined on the profile.

Restricting user repository access rights (Web Front-End)

To restrict user access rights to environment repositories:

1. Access the properties pages of the login for the person concerned.
   ☛ *See "Viewing login characteristics (Web Front-End)", page 52.*
2. Select the **Repositories** tab.
3. For each repository concerned, modify the value of the **Access Rights** field, and in the drop-down list select its value (**Not accessible** or **Read-only** if you want to restrict access to the repository concerned).
   ☛ *See "Login Properties", page 26.*
4. Click **Save** .

Restricting user repository access rights (Windows Front-End)

To restrict user access rights to environment repositories:

☛ *Alternatively, you can restrict user repository access rights from the **Login** properties dialog box in the **Repositories** tab.*

1. Display the user management window.

   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*
2. Select the **Logins** tab.
3. In the **Login** frame, select the login concerned.
4. In the menu bar of the **MEGA Repositories/Profiles** frame, click **MEGA Repositories**  .
5. For each repository concerned, modify the value of the **Access Rights** field, and in the drop-down list select its value (**Not accessible** or **Read-only** if you want to restrict access to the repository concerned).

   ☛ *See "Login Properties", page 26.*
6. Click **OK**.

Exporting and Comparing Repository Users

You can export and compare repository users. This can be useful for example to copy users and their characteristics associated with an environment into another environment.

To:

- export the log of a user:

  ☛ *See "Exporting MEGA Objects", page 260.*
- compare users of a repository with another repository:

  ☛ *See "Comparing Environments", page 234.*

MANAGING USER OPTIONS

For specific requirements, you can modify default values of certain **Options** (see "Accessing Options", page 368).

Configuring metamodel access

With the **Metamodel Access** option (accessible from **Options > Repository**) you can restrict the view of **MEGA** 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 **MEGA**. Only basic objects are visible. This level allows very simple modeling.
- **Intermediate** (default value)
  For standard use of **MEGA**. Almost all object types, links and non-technical attributes are visible.
- **Advanced**
  For advanced use of **MEGA**. 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 **MEGA** platform.
  For example, this level enables access to:
  - certain navigation windows, with a restricted view of objects (**MetaStudio**, **Utilities**)
  - the **Administration** navigation window, which gives access to reading and writing access areas.
  - the **Repository Activity** (Navigation window in **MEGA**, **Administration** desktop page (**Web Front-End**)).
- **Expert**
  This level displays all object types, links, and attributes, as well as the abstract metamodel. All MEGA platform customizations are available.

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

  This is the level for example that offers:
  - all functions of **HOPEX Studio** (**MetaStudio** navigation window)
  - report template creation (**Utilities** navigation window)
  - certain advanced commands (eg: update logfile export at particular intervals).

Authorizing Deletion of a Published Object

Users working in a public workspace can delete objects.

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

The **Authorize dispatched object deletion from private workspace** allows the user to delete dispatched objects from a private workspace, irrespective of the creator.

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

Authorizing MEGA 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.

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

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

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", page 368.

2. In the tree of **Options**, 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

User inactivity management is taken into account if the **Inactivity Management** option is selected.

☛ *See "Activating/Deactivating user inactivity management", page 86.*

To manage user inactivity:

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

☛ *See "Accessing Options", page 368.*

2. In the tree of **Options**, select **Workspace**.
3. In the right pane, select values for options:

☛ *Duration of inactivity requiring authentication must be less than that closing **MEGA.***

- **Period of inactivity requiring authentication**

When this duration has been reached, the user receives a message requesting authentication.

☛ *This duration warns the user before he/she is disconnected if the **Duration of inactivity before closing MEGA** option has been specified.*

- **Duration of inactivity before closing MEGA**

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

☛ *So that the user is warned of disconnection, the **Period of inactivity requiring authentication** must be specified and its value less than that of the **Duration of inactivity before closing MEGA**.*

MANAGING PROFILES AND BUSINESS ROLES

☛ *Management of profiles and business roles is available only with the **MEGA Supervisor** technical module.*

Profiles and *business roles* are managed in the **MEGA** administration applications: the **MEGA Administration** application (Windows-Front-End) or the **MEGA Administration** desktop (Web Front-End).

📖 *A profile defines what a person can see or not see and do or not do in tools, and how he/she sees and can do it. 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.*

📖 *A business role defines a function of a person in a business sense. A person can have several business roles. Business roles are only considered when the "Management of assignment of business roles to persons" option is activated (default mode) A profile can be associated with a business role. Assigning a person a business role with which a profile is associated indirectly assigns this profile to this person. A business role is specific to a repository.*

The following points are detailed here:

You can also:

- copy/explore a profile
- manage a profile (enables export, comparison and merge of profiles)

To:

- modify profile options

  ☛ *see "Managing Options", page 365.*
- manage metamodel filters at profile level

  ☛ *see "Managing UI Access (Permissions)", page 282.*

Introduction to Business Roles and Profiles

See:

- "Business role", page 89
- "Profile", page 90
- "Profile - Business role", page 90
- "Assignment of business roles to persons mode", page 91
- "Definition of profiles to persons mode", page 93

Business role

☛ *In the case of definition of profiles on login of persons, business roles are not taken into consideration, see "Definition of profiles to persons mode", page 93 and "Without Management of Assignment of Business Roles to Persons", page 99.*

A business role defines the function of a person or person group in the enterprise (example: Risk Manager, Enterprise Architect).

Assignment of a business role is defined at repository level. Assignment of a business role to a person can therefore be different in each repository of the environment.

Business role and connection:

To each person or person group, you must assign a business role so that this person or person group can connect to a **MEGA** application. By default, no business role is assigned to a person or person group.

Only a business role connected to a profile enables connection. Each business role serving for connection is associated with only one profile.

☛ *Several business roles can be connected to the same profile.*

☛ *See "Configuring a Business Role (Connection)", page 122.*

☛ *See "Assignment of business roles to persons mode", page 91.*

Business role and object assignment:

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

☛ *See "Configuring a Business Role (Connection)", page 122.*

☛ *See "Assigning an Object to a Person", page 125.*

Profile

A profile defines access rights to repositories, to user interfaces, and to data.

A user must have at least one profile to be able to connect to a **MEGA** application.

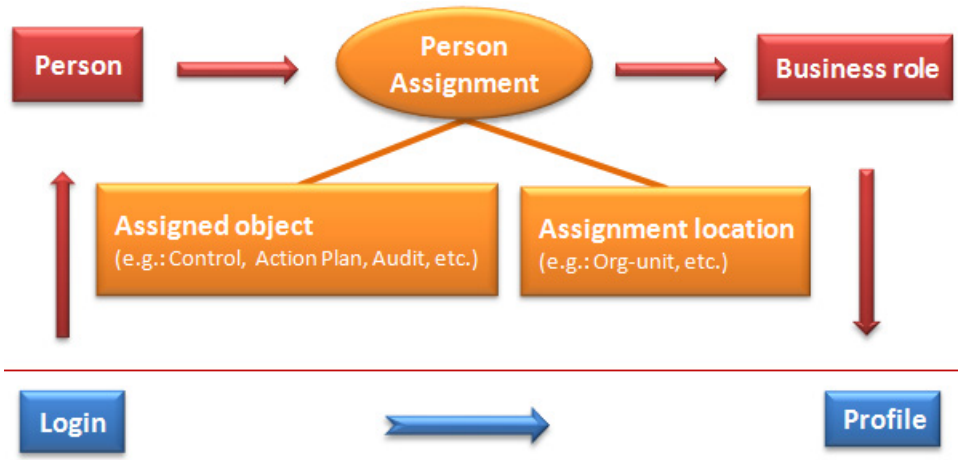
When the **Management of assignment of business roles to persons** option is:

- selected (default mode), the profile is connected to the business role, which is assigned to the person.
- cleared, the user profile is directly defined on the login of the person. By default, no profile is connected to the login of a user.

A user of administrator type must always be directly connected to the Administrator profile to be able to connect to the Administration application.

Profile - Business role

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



By default, the **Management of assignment of business roles to persons** option is selected. This option is necessary for working with **MEGA** Solutions such as risk management and audit.

Depending on business solutions implemented, localization of assignments may not be used, and the same assignments will be shared by all environment repositories. In this case, there is no need for this option and you can clear it. Profiles are then managed by direct link of profiles on login of the person or person group.

☛ *To select this profile management mode, see "Without Management of Assignment of Business Roles to Persons", page 99.*

The connection schema of a user to a **MEGA** application varies according to selection or not of the **Management of assignment of business roles to persons** (environment option):

- selected option (default value): "Assignment of business roles to persons mode", page 91
- cleared option: "Definition of profiles to persons mode", page 93

☛ *See "Without Management of Assignment of Business Roles to Persons", page 99.*

Assignment of business roles to persons mode

The **Management of assignment of business roles to persons** option is selected (default mode). In this case, you must assign a business role to the person. To connect to **MEGA**:

- the person must have a login

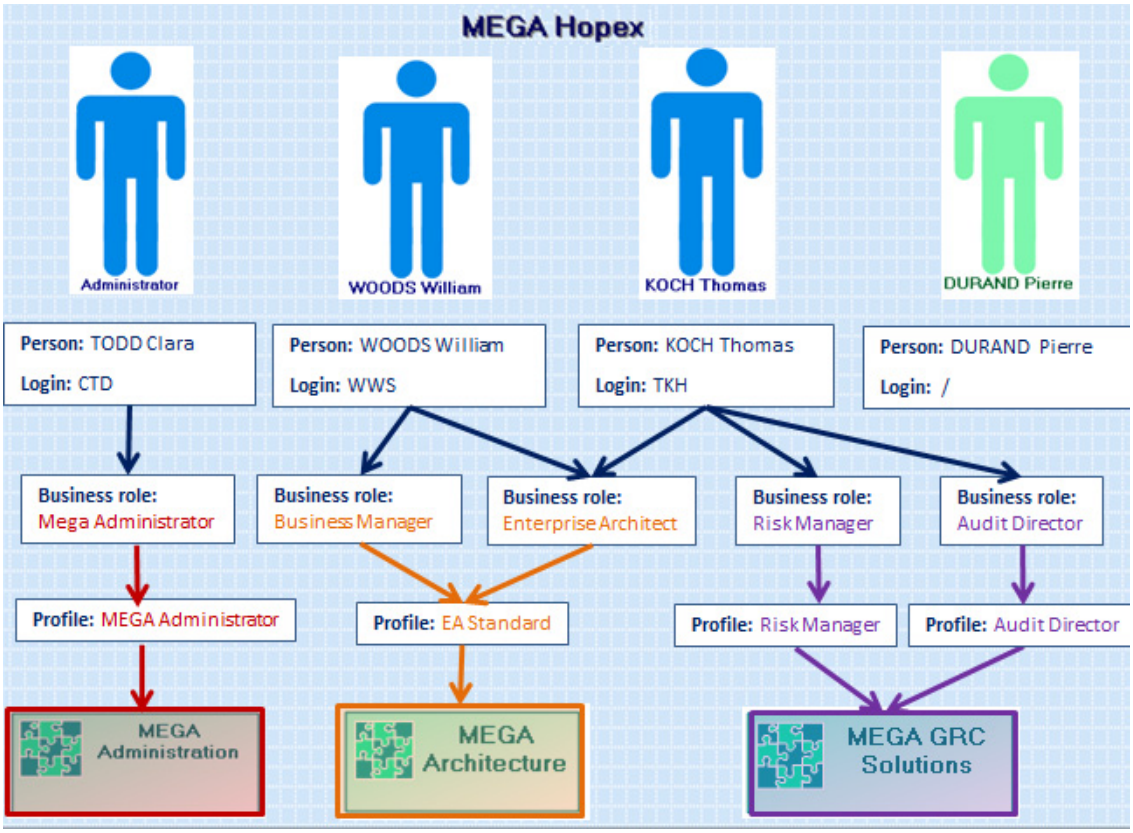
  ☛ *See "Creating Users", page 65.*
- the person must have at least one business role

  ☛ *See "Assigning a business role to a person", page 123.*

  ☛ *See "Configuring a Business Role (Object Assignment)", page 122.*
- this business role must be connected to a profile

  ☛ *See "Configuring a Business Role (Connection)", page 122.*

The profile is connected to the business role that is connected to the person by assignments.



In the above example:

- Clara TODD has a login connected to the **MEGA Administrator** business role (connected to **MEGA Administrator** profile):
  she can connect only to **Administration** applications (**Windows Front-End** and **Web-Front-End**).
- William WOODS has a login connected to **Business User** and **Enterprise Architect** business roles (connected to **EA Standard** profile):
  he can connect only to the **MEGA Architecture:** application.
- Thomas KOCH has a login connected to business roles **Enterprise Architect** (connected to **EA Standard** profile), **Risk Manager** (connected to **ERM Risk Manager** profile) and **Audit Director** (connected to **Audit Director** profile):
  he can connect to applications **MEGA Architecture:** and **MEGA GRC Solutions**.
- Pierre DURAND does not have a login:
  he cannot connect to **MEGA**.

Definition of profiles to persons mode

☛ *See "Without Management of Assignment of Business Roles to Persons", page 99.*

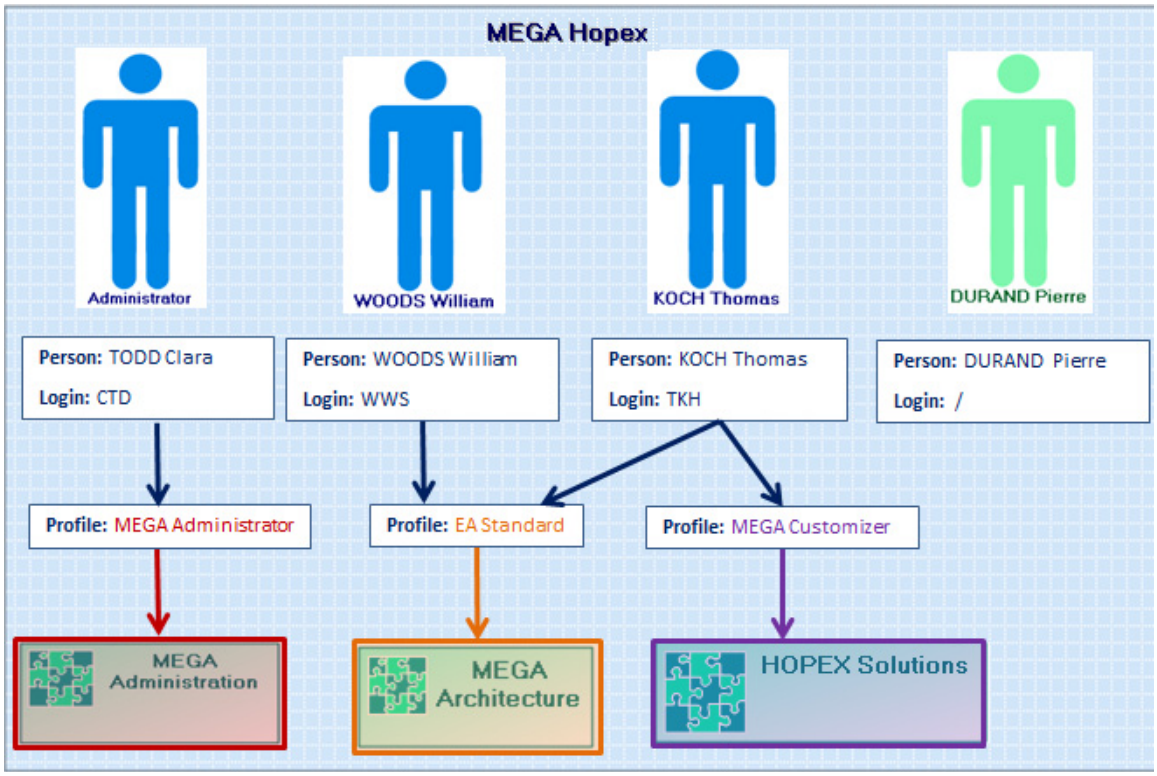
When the **Management of assignment of business roles to persons** option is cleared, profiles are directly managed on the login of the person. To connect to MEGA:

- the person must have a login

  ☛ *See "Creating Users", page 65.*

- the login of the person must be connected to at least one profile.

  ☛ *See "Configuring a Login", page 75.*



In the above example:

- Clara TODD has a login connected to the **MEGA Administrator** profile: she can connect only to **Administration** applications (**Windows Front-End** and **Web-Front-End**).
- William WOODS has a login connected to **EA Standard** profile: he can connect only to the **MEGA Architecture:** application.
- Thomas KOCH has a login connected to **EA Standard** and **MEGA Customizer** profiles: he can connect to **MEGA Architecture:** and **HOPEX Solutions** applications.
- Pierre DURAND does not have a login: he cannot connect to **MEGA**.

Profiles Supplied

Profiles are supplied at installation with defined rights and access to applications:

- Administration profiles:
  These profiles provide access only to the **Administration** applications (Web Front-End and Windows Front-End).
  When several users with a MEGA Administration profile connect to MEGA Administration at the same time, certain actions are exclusive (example: user management).
  - **MEGA Administrator**
    ☛ *See "MEGA Administrator profile", page 94.*
  - **MEGA Administrator - Production**
    ☛ *See "MEGA Administrator - Production profile", page 95.*
  - **User Management Administrator**
    ☛ *See "User Management Administrator profile", page 95.*
  - **User Management Web Administrator**
    ☛ *See "User Management Web Administrator profile", page 96.*
  - **Repository Management Administrator**
    ☛ *See "Repository Management Administrator profile", page 98.*
- other profiles specific to each application, such as:
  - **EA Standard**, which gives access to **MEGA**
    ☛ *See "EA Standard profile", page 98.*
  - **Explorer (Writing)**/**Explorer (Reading)**, which give access to **HOPEX Explorer**.
  - **Teamwork User**, which gives access to **HOPEX Collaboration Manager**.
  - **Audit Director**, which gives access to **HOPEX Internal Audit**.

☛ *If necessary you can modify the rights and access to applications defined on these profiles, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 106 and "Configuring a Profile", page 109.*

MEGA Administrator profile

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

The **MEGA Administrator** accumulates the rights:

- of the **User Management Administrator** profile
  - ☛ *See "User Management Administrator profile", page 95.*
- of the **Repository Management Administrator**
  - ☛ *See "Repository Management Administrator profile", page 98.*
- (Windows Front-End) of management:
  - of an environment:
    - ☛ *See "Managing Environments", page 221.*
  - of objects
    - ☛ *See "Managing objects", page 259.*

MEGA Administrator - Production profile

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

User Management Administrator profile

The **User Management Administrator** profile gives access to:

- user management
- tools

It is used to create, configure and modify the properties:

- of a *user*:

  A user is a person (or person group) with a login.

  - **Person**

    See "Configuring a Person", page 61.

  - **Login**

    See "Creating Users", page 65.

    See "Configuring a Login", page 75.

- of a *user group*:

  A Person Group groups persons in a group. These persons share the same connection characteristics.

  - **Person group**

    See "Creating a Person Group", page 68.

    See "Defining a Person Group", page 70.

    See "Defining a dynamic person group with LDAP", page 72.

    See "Defining a dynamic person group with a Macro", page 73.

  - **Login**

    See "Configuring a Login", page 75.

- of a **Profile**

  See "Creating a Profile", page 105.

  See "Configuring a Profile", page 109.

- of a **Business Role** (assignment of business roles to persons)

  See "Creating Business Roles", page 120.

  See "Configuring a Business Role (Object Assignment)", page 122.

It is also used to perform tasks linked to **Tools**:

- Excel file import/export

  *See **MEGA Common Features** guide, "Exchanging Data With Excel" chapter.*

- XMG/MGL/MGR file import/export

  See "Importing command files", page 162.

  See "Exporting Objects", page 260.

- Visio file import

  See HOPEX Studio Visio Import technical article.

- use of the Scheduler

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

User Management Web Administrator profile

The **User Management Web Administrator** profile gives access to:

- user management
- lock management

It is used to create, configure and modify the properties:

- of a *user*:

  A user is a person (or person group) with a login.

  - **Person**

    See "Configuring a Person", page 61.

  - **Login**

    See "Creating Users", page 65.

    See "Configuring a Login", page 75.

- of a *user group*:

  A Person Group groups persons in a group. These persons share the same connection characteristics.

  - **Person group**

    See "Creating a Person Group", page 68.

    See "Defining a Person Group", page 70.

    See "Defining a dynamic person group with LDAP", page 72.

    See "Defining a dynamic person group with a Macro", page 73.

  - **Login**

    See "Configuring a Login", page 75.

- of a **Profile**

  See "Creating a Profile", page 105.

  See "Configuring a Profile", page 109.

- of a **Business Role** (assignment of business roles to persons)

  See "Creating Business Roles", page 120.

  See "Configuring a Business Role (Object Assignment)", page 122.

It gives access to lock management.

See "Managing Locks", page 215.

Repository Management Administrator profile

The **Repository Management Administrator** profile gives access to:

- repository management
  - ☛ *See "Managing Repositories", page 137.*
- workspace management
  - ☛ *See "Managing Private Workspaces", page 185.*
- tasks relating to **Permissions**
  - ☛ *See "Managing UI Access (Permissions)", page 282.*
- tasks linked to **Tools**:
  - Excel file import/export
    - ☛ *See **MEGA Common Features**guide, "Exchanging Data With Excel" chapter.*
  - XMG/MGL/MGR file import/export
    - ☛ *See "Importing command files", page 162.*
    - ☛ *See "Exporting Objects", page 260.*
  - Visio file import
    - ☛ *See HOPEX Studio Visio Import technical article.*
  - use of the Scheduler
    - ☛ *See **HOPEX Studio - Scheduler** guide.*

EA Standard profile

EA Standard profile gives access to applications:

- **MEGA (Windows Front-End)**
- **MEGA (Web Front-End)**, other than solutions

By default, **EA Standard** profile cannot configure or modify properties of users or user groups.

Business Roles Supplied

☛ *Business roles are supplied, in the case of mode: assignment of business roles by assignment of business roles to persons, see "Assignment of business roles to persons mode", page 91.*

Business roles supplied at installation with rights and access to defined applications are:

- **MEGA Administrator**
- **MEGA Administrator - Production**
- **User Management Web Administrator**
- business roles associated with specific applications

MEGA Administrator business role

MEGA Administrator business role is connected to **MEGA Administrator** profile.

☛ *See "MEGA Administrator profile", page 94.*

So that a person with business role MEGA Administrator can access administration applications (Windows Front-End and Web Front-End) you must configure its login.

☛ *See "Configuring the MEGA Administrator business role", page 123.*

MEGA Administrator - Production business role

MEGA Administrator - Production business role is connected to the **MEGA Administrator** profile.

☛ *See "MEGA Administrator - Production profile", page 95.*

User Management Web Administrator business role

The **User Management Web Administrator** business role is connected to the **User Management Web Administrator** profile.

☛ *See "User Management Web Administrator profile", page 96.*

Other business roles

Other business roles are supplied with each specific application, for example the business role:

- **Enterprise Architect**, connected to **EA Standard** profile.

  ☛ *See "EA Standard profile", page 98.*
- **Explorer (Writing)**/**Explorer (Reading)**, connected to profiles **Explorer (Writing)**/**Explorer (Reading)** which give access to **HOPEX Explorer**.
- **Workflow Participant**, connected to **Teamwork User** profile, which gives access to **HOPEX Collaboration Manager**.
- **Audit Director**, connected to **Audit Director** profile, which gives access to **HOPEX Internal Audit**

Without Management of Assignment of Business Roles to Persons

By default in environment options, the **Management of assignment of business roles to persons** option is selected. This option is necessary for working with **MEGA** Solutions such as risk management and audit.

Depending on business solutions implemented, localization of assignments may not be used, and the same assignments will be shared by all environment repositories. In this case, there is no need for this option and you can clear it.

See:

- "Without Management of Assignment of Business Roles (Web Front-End)", page 100
- "Without Management of Assignment of Business Roles (Windows Front-End)", page 100

Without Management of Assignment of Business Roles (Web Front-End)

To not manage the assignment of business roles to persons:

1. Connect to the **MEGA Administration** desktop (Web Front-End).

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*
2. In the edit area, click **Environment Options**.
   The environment options window opens.
3. Expand the **Installation** folder and select **Manage Users**.
4. Clear the **Management of assignment of business roles to persons** option.
5. Click **OK**.

   ☛ *So that the option is taken into account, you must close then reopen **MEGA Administration**.*

   Profiles available for a user are those connected to his/her login. Assignment of business roles is no longer available.

The following modifications appear:

- in the **User Management** pane:
  - the **Persons by profile** and **Person groups by profile** sub-folders replace the **Persons by business role** and **Person groups by business role** sub-folders.
  - The **Business Roles** folder disappears.

  You must connect profiles to login of persons, see "Configuring a Login", page 75.
- in the
  - **Person Management** page, the **Assign Business Roles (Connection)** button disappears.
  - properties of a person, the **Assignments** tab disappears.

  You can no longer assign business roles (connection) to persons.
- in the **Characteristics** tab of login properties:
  - the **Profile** attribute appears.
  - the **Administrator Profile** attribute disappears.

Without Management of Assignment of Business Roles (Windows Front-End)

To not manage the assignment of business roles to persons:

1. From **MEGA Administration**, connect to the desired environment.

   ☛ *See "Connecting to an Environment", page 5.*
2. Right-click the environment name and select **Options > Modify**.
   The environment options window opens.
3. Expand the **Installation** folder and select **Manage Users**.

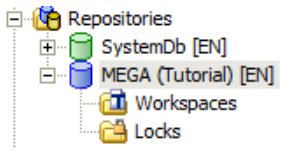
4. Clear the **Management of assignment of business roles to persons** option.
5. Click **OK**.

> ☛ *So that the option is taken into account, you must close then reopen **MEGA Administration**.*

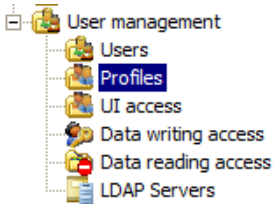
Profiles available for a user are those connected to his/her login. Assignment of business roles is no longer available.

The following modifications appear:

- in each repository of the environment (see "Accessing Repositories", page 138), the **Assignment of Business Roles** folder disappears.
  You can no longer assign business roles to persons.

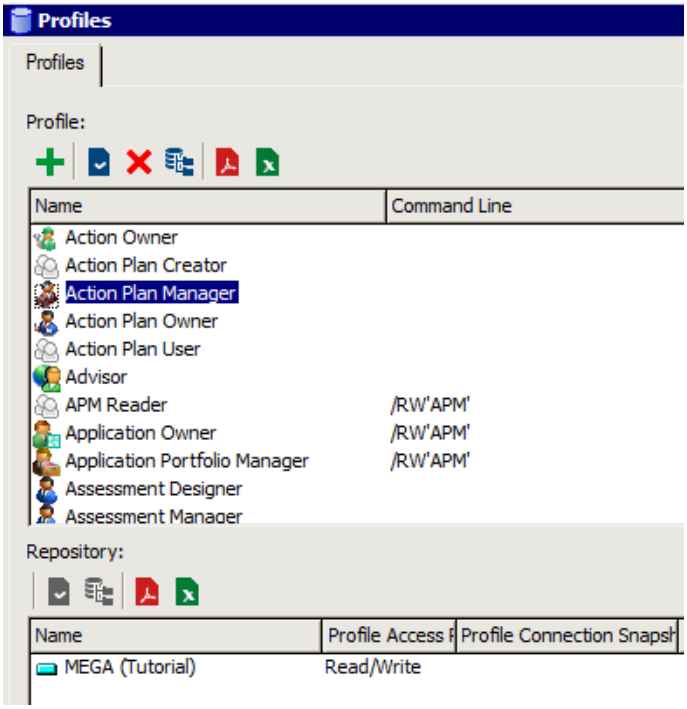


- in the **User management** folder, the **Business Roles and Profiles** folder becomes **Profiles**
  You must connect profiles to login of persons, see "Configuring a Login", page 75.



- the **Business Roles and Profiles** management window becomes the **Profiles** management window (see "Opening the business roles and profiles management window (Windows Front-End)", page 44) and the

Business Roles tab disappears.



- in the **Characteristics** tab of login properties:
  - the **Profile** attribute appears.
  - the **Administrator Profile** attribute disappears.

Profile Properties

Creation of profiles enables definition of the same connection rights to a set of users:

- repository access rights

  ☛ *See "Profile repository access rights", page 104.*

- access rights restricted to certain products

  ☛ *See "Products accessible on the license (Command Line)", page 28.*

  If a user already has access rights restricted by the Command Line attribute on his/her Login (see "Viewing Login Characteristics", page 51), the products accessible to this user are at the intersection of values of the Command Line attribute of the user login and profile.

- access rights to certain Web applications
- connection repository snapshot (available for a profile with repository reading access (example: **HOPEX Explorer**)

☛ *See "Connection repository snapshot of the profile", page 105.*

To manage profiles, see "Managing Profiles and Business Roles", page 88.

Name

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

Products accessible on the license (Command Line)

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

Format of the command is:

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

For example: You have licenses for products **MEGA Process**, **MEGA Architecture: and other MEGA products.** To authorize only **MEGA Process** and **MEGA Architecture:** modules to users that have this profile, enter: /RW'PRO;ARC'

☛ *To determine the product code, see "Product Codes", page 384.*

If a user already has access rights restricted by the Command Line attribute on his/her Login (see "Viewing Login Characteristics", page 51), 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 order	**RW:/'Pro'**	**none**
User A	RW:/'PRO;ARC'	user A has access to **MEGA Process**	user A has access to **MEGA Process** and **MEGA Architecture:**
User B	RW:/'PRO;ARC'	user B cannot access any product	user B has access to **MEGA Architecture:**
User C	none	user C has access to **MEGA Process**	user C can access all products for which he/she has the license (**MEGA Process** and **MEGA Architecture:**

*Restrictions on products for users and profiles that have licenses for **MEGA Process** and **MEGA Architecture:***

Assignable

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

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

☛ *The default value is "No".*

Administrator profile

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

- grant administrator profile to another user.
- declare a profile as administrator.
  That is, specify value "Yes" for the **Administrator Profile** attribute of any profile.

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

Profile 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.

Logins

The **Logins** frame lists all users connected to the current profile.

Profile repository access rights

At creation, a profile can access all repositories by default.

Profile user *access rights* to environment repositories can be restricted by the administrator. He can:

- authorize repository update (**Read/Write**)
- prohibit repository update (**Read-only**)
- prohibit repository access (**Not accessible**)

💣 ***If* a user already has repository access rights restricted by those defined on his/her login, only the restricted access rights will be added to those defined on the profile.**

☛ *See "Defining Profile Repository Access Rights", page 116.*

Connection repository snapshot of the profile

For a profile with reading access to the repository (example: Explorer Reader), the administrator can define a connection *repository snapshot* for users of the profile.

☛ *See "Defining Connection Repository Snapshot for a Profile", page 117.*

Creating a Profile

To be able to connect, a user must be connected to at least one profile (by assignment of a business role to the person, or by definition of a profile on login of the person). Users with the same profile share common characteristics (options, repository access rights, authorized products, read/write and read-only rights on objects).

A profile enables:

- restriction of user access to certain products
- definition of user repository access rights
- definition of access in Multisession mode

Creating a profile (Web Front-End)

To create a profile:

1. Access the Profiles management pages.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

2. In the **Profiles** tab, click **New**  .
3. In the profile creation dialog box that appears, enter the **Name** of the profile.

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

4. Click **OK**.
   The new profile appears in the **All Profiles** list.
   You must:
   - define profile UI access

     ☛ *See "Managing UI Access (Permissions)", page 282.*

     ☛ *You can use configuration of UI access defined on an existing profile, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 106.*
   - configure the profile.

     ☛ *See "Configuring a Profile", page 109.*

Creating a profile (Windows Front-End)

To create a profile:

1. Open the **Profiles** management window.

   ☛ *See "Opening the profile management window (Windows Front-End)", page 42 or "Opening the business roles and profiles management*

window (Windows Front-End)", page 44.

2. In the **Profile** tab, click **New**  .
   A new profile appears in the list of profiles.

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

3. In the profile management window, right-click the profile and select **Properties**  .
   The profile properties dialog box opens.
4. Select the **General** tab.
5. (Optional) In the **Name** field, modify the profile name.
6. Click **OK**.
   The new **Profile** appears in the list of profiles.
   You must:
   - define profile UI access

     ☛ *See "Managing UI Access (Permissions)", page 282.*

     ☛ *You can use configuration of UI access defined on an existing profile, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 106.*
   - configure the profile.

     ☛ *See "Configuring a Profile", page 109.*

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

You can create a profile by aggregation of existing profiles.

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

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

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

1. Create a new profile.

   ☛ *See "Creating a Profile", page 105.*
2. In the properties dialog box of the new profile, select the **Used Profile** tab.
3. Right-click your **Profile** and select **Connect > Profile**.
4. (Optional) In the query field, enter the characters you want to find.
5. Click **Find**  .
6. In the results list, select the profile you want to customize.

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

Viewing Profile Characteristics

See:

- "Viewing Profile Characteristics (Web Front-End)", page 107
- "Viewing Profile Characteristics (Windows Front-End)", page 107

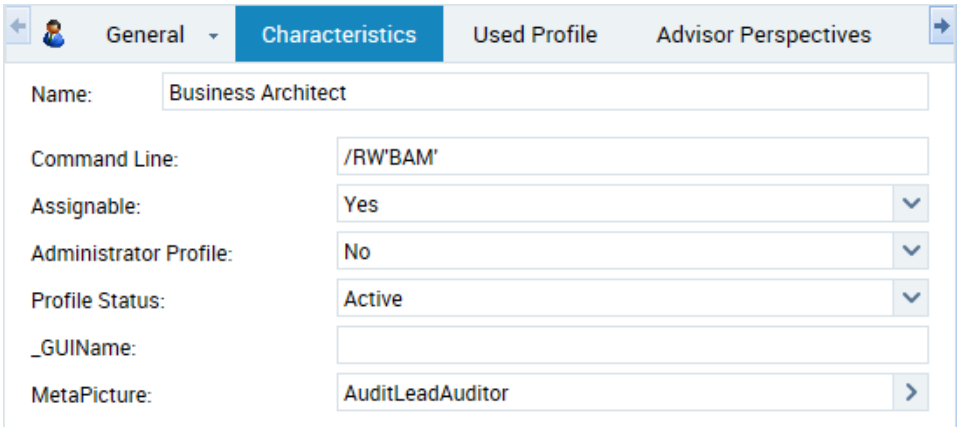
Viewing Profile Characteristics (Web Front-End)

To view profile characteristics:

1. Access the user management pages.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select the **Profiles** sub-folder.
3. In the edit page, select the profile.
4. In the toolbar, click **Properties** .
   The profile **Properties** dialog box opens.

   ☛ *For detailed information on characteristics of a profile, see "Profile Properties", page 102.*



☛ *See "Configuring a Profile", page 109.*

Viewing Profile Characteristics (Windows Front-End)

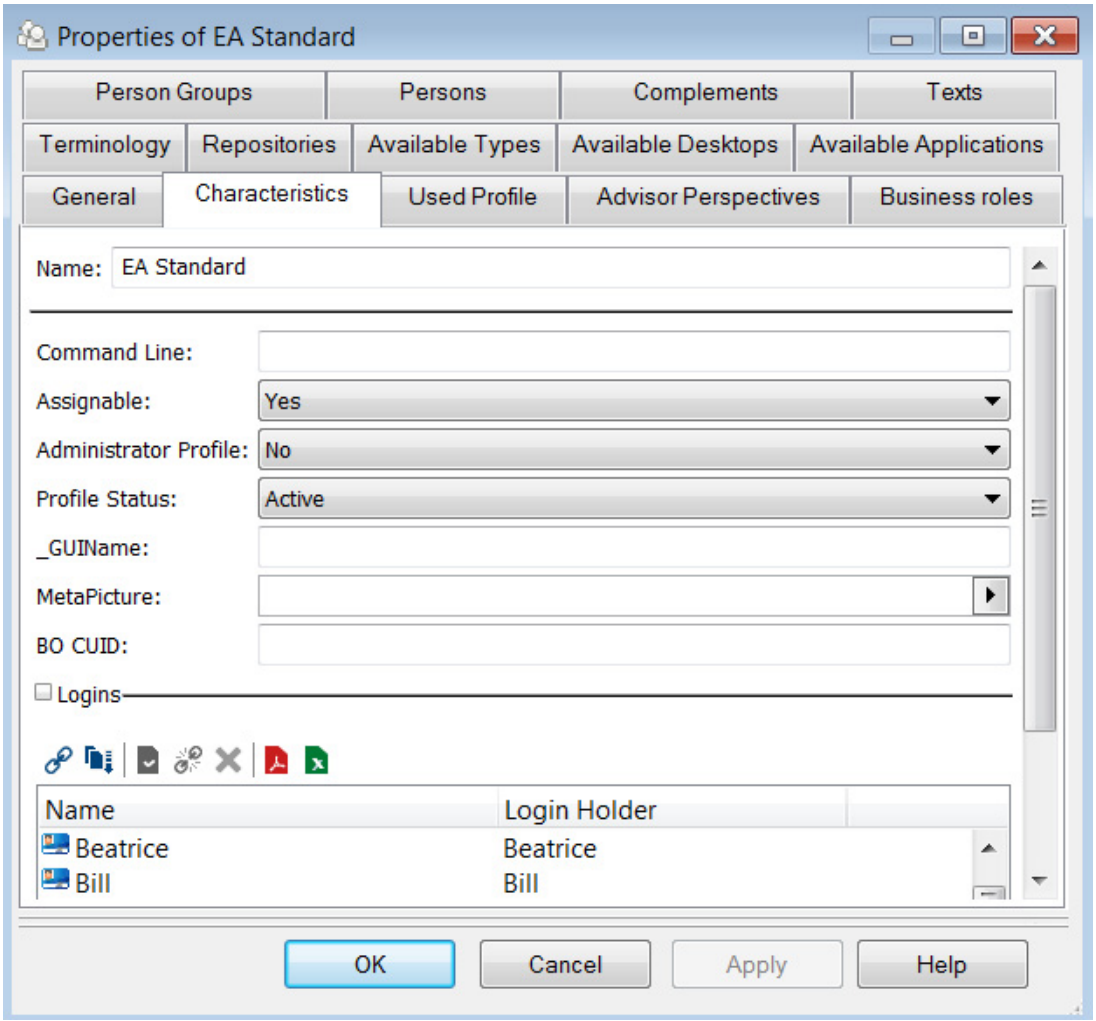
To view profile characteristics:

1. Open the **Profiles** management window.
2. In the **Profile** tab, select the profile.

   ☛ *See "Opening the profile management window (Windows Front-End)", page 42 or "Opening the business roles and profiles management window (Windows Front-End)", page 44.*
3. In the toolbar, click **Properties** .
   The profile **Properties** dialog box opens.

4. Select the **Characteristics** tab.

☛ *For detailed information on characteristics of a profile, see "Profile Properties", page 102.*



☛ *See "Configuring a Profile", page 109.*

Configuring a Profile

From the profile properties dialog box you can define:

☛ *See "Profile Properties", page 102.*

- 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 active or not.

  ☛ *See step 5.*

- icon of the profile

  ☛ *See step 7.*

- users connected to the profile

  ☛ *See "Connecting Users to a Profile", page 115.*

- applications accessible to users of the profile

  ☛ *See "Defining applications accessible to profile users", page 110.*

- desktops accessible to users of the profile

  ☛ *See "Defining application desktops accessible to profile users", page 112.*

- object types available

  ☛ *See "Defining the object types available for a profile", page 114.*

- business roles connected to the profile (case of assignment of business roles to persons)

  ☛ *See "Defining business roles connected to the profile (case of assignment of business roles to persons)", page 114.*

  ☛ *See also "Configuring a Business Role (Connection)", page 122.*

- (**MEGA Advisor** specific) an additional perspective to the Advisor profile

  ☛ *See "Adding a perspective to the Advisor profile", page 115.*

From the profile management tab, you can define the following connection parameters for each profile:

☛ *See "Accessing the User Management Pages (Web Front-End)", page 31 or "Opening the profile management window (Windows Front-End)", page 42.*

- profile repository access rights

  ☛ *See "Defining Profile Repository Access Rights", page 116.*

- (specific to a profile with reading access to repository) connection repository snapshot of the profile

  ☛ *See "Defining Connection Repository Snapshot for a Profile", page 117.*

Configuring profile characteristics

To configure profile characteristics:

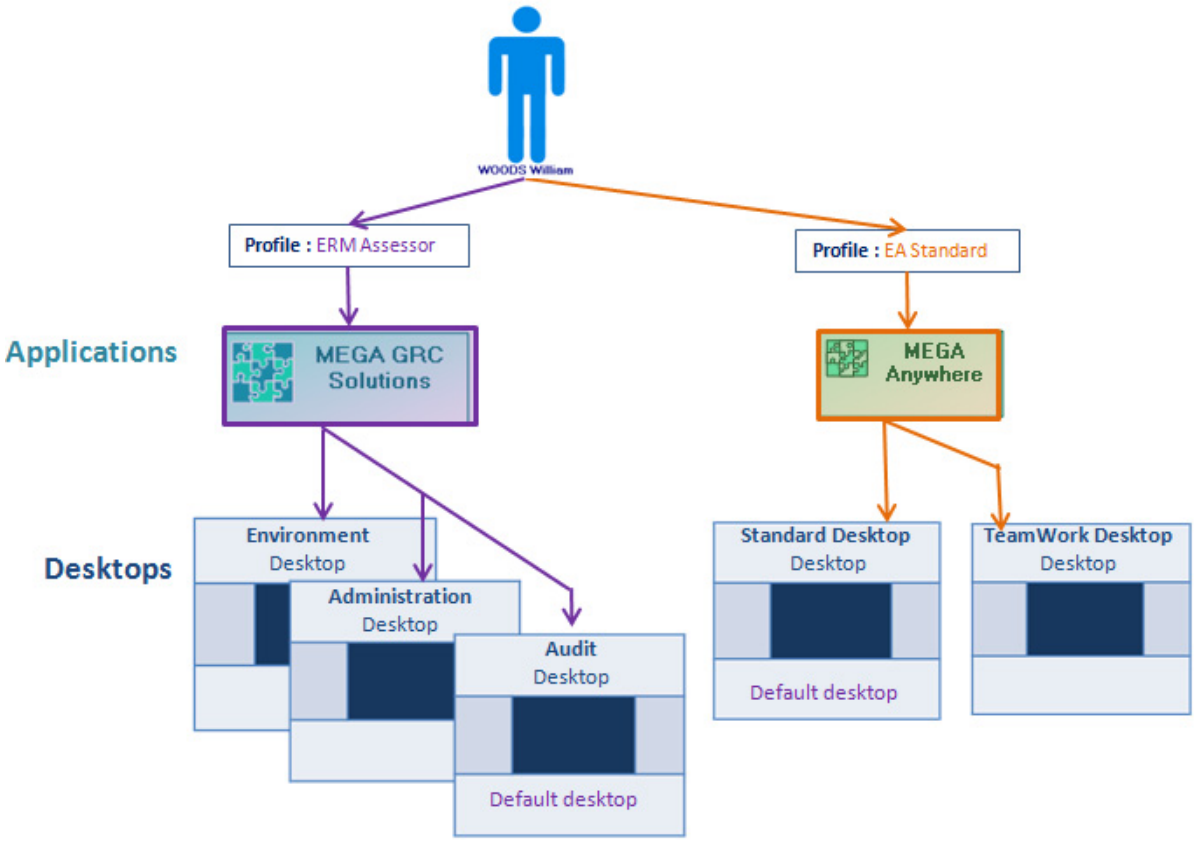
1. Access the properties of the profile.
   ☛ *See "Viewing Profile Characteristics", page 107.*
2. (Optional) In the **Command Line** field, enter the command defining products that can be accessed by users with the current profile.
   ☛ *See "Products accessible on the license (Command Line)", page 103.*
3. (Optional) In the **Assignable** field, modify the attribute value via the drop-down menu. By default, the profile is not assignable.
   ☛ *See "Assignable", page 104.*
4. (Optional) In the **Administrator Profile** field, modify the attribute value. By default, the profile is not an administrator profile.
   ☛ *See "Administrator profile", page 104.*
5. (Optional) In the **Profile Status** field, modify the attribute value.
   ☛ *By default, the profile is active.*
6. (Optional) In the **_GUIName** field, enter the profile name displayed in the interface.
7. (Optional) In the **MetaPicture** field, click the arrow and select **Query MetaPicture**.
   - In the query field, enter the characters you want to find and click **Find**.
   - In the results list, select the icon and click **OK**.

Defining applications accessible to profile users

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 enable access to only certain desktops of the application, see "Defining application desktops accessible to profile users", page 112.

> ☛ *To modify a profile supplied by **MEGA**, you must create a new profile, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 106.*



Example:

The application "MEGA GRC Solutions" is connected to profile "ERM Risk Manager" and the application "MEGA Anywhere" is connected to profile "EA Standard".

No desktop of applications "MEGA GRC Solutions" and "MEGA Anywhere" is directly connected to profiles "ERM Risk Manager" and "EA Standard".

User William WOODS, who has profiles "ERM Risk Manager" and "EA Standard", can access all desktops of the "MEGA GRC Solutions" application and all desktops of the "MEGA Anywhere" application.

To define applications available for a profile:

1. Access the properties of the profile.

   ☛ *See "Viewing Profile Characteristics", page 107.*

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

   ☛ *To select more than one application, use the [Ctrl] key (Windows Front-End).*

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

Defining application desktops accessible to profile users

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

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

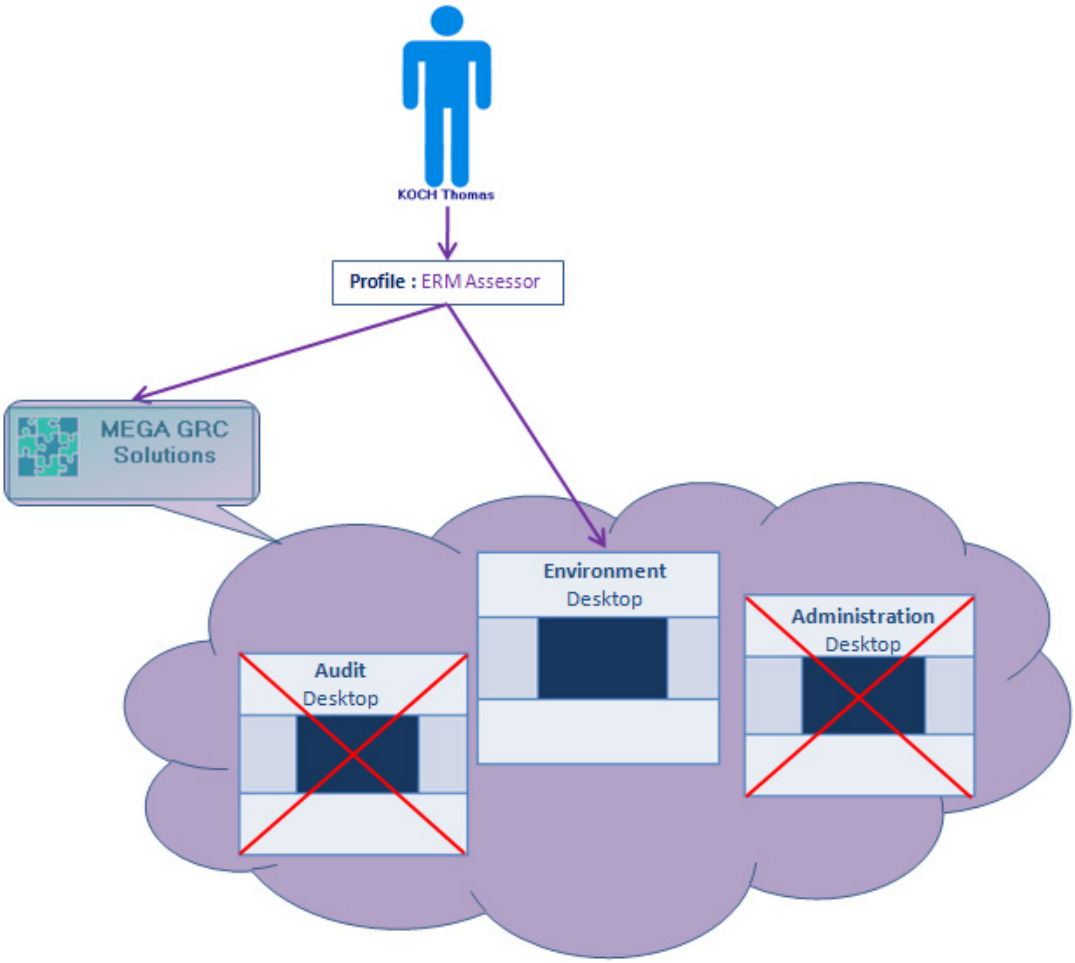
- the application containing the desktops.

  ☛ *See "Defining applications accessible to profile users", page 110.*

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

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

  ☛ *To modify a profile delivered by **MEGA**, you must have rights to modify **MEGA** data. Alternatively, you can create a new profile, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 106.*



Example:

The ERM Risk Manager profile is connected:

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

- to the "Environment" desktop of the application "MEGA GRC Solutions".

User Thomas KOCH with profile "ERM Risk Manager" can connect only to the "Environment" desktop of the application "MEGA GRC Solutions". "Audit" and "Administration" desktops are not authorized.

To define application desktops available for a profile:

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

☛ *See "Defining applications accessible to profile users", page 110.*

1. Access the properties of the profile.
   ☛ *See "Viewing Profile Characteristics", page 107.*
2. Select the **Available Desktops** tab.
3. In the toolbar, click **Connect**  .
   The desktop query tool appears.
4. (Optional) In the second field, enter the characters to find.
5. Click **Find**  .
6. In the query results, select the desktop you want to connect.
   ☛ *To select more than one desktop, use the [Ctrl] key (Windows Front-End).*
7. Click **Add**.
   The desktops are connected to the profile.

Defining business roles connected to the profile (case of assignment of business roles to persons)

In the case of assignment of business roles to persons (see "Assignment of business roles to persons mode", page 91), each user must have at least one business role. Each business role should be connected to only one profile. Several business roles can be connected to the same profile.

☛ *Alternatively, see "Configuring a Business Role (Connection)", page 122.*

To connect business roles to a profile:

1. Access the properties of the profile.
   ☛ *See "Viewing Profile Characteristics", page 107.*
2. Select the **Business Roles** tab.
3. In the toolbar, click **Connect**  .
   The business roles query tool appears.
4. (Optional) In the second field, enter the characters to find.
5. Click **Find**  .
6. In the query results, select the business role you want to connect.
   ☛ *To select more than one business role, use the [Ctrl] key (Windows Front-End).*
7. Click **Add**.
   The business roles are connected to the profile.

Defining the object types available for a profile

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

- document categories
- document models
- definition of a Report DataSet Definition
- Widget

To define the object types available for a profile:

1. Access the properties of the profile.
   ☛ *See "Viewing Profile Characteristics", page 107.*

2. Select the **Available Types** tab.
3. Select **Available Objects**.
4. In the toolbar, click **Connect**  .
   The object type query tool appears.
5. (Optional) In the query tool, in the first field, select the object type category.
6. (Optional) In the second field, enter the characters to find.
7. Click **Find**  .
8. In the query result, select the object types to make available for the profile.
9. Click **Add**.
   The object types selected are made available for the profile.

Adding a perspective to the Advisor profile

You can add a perspective to the Advisor profile.

☛ *The **Default Advisor Perspective** is the perspective with which a user with **Advisor** profile will connect to **MEGA Advisor**. By default this perspective is **Standard 2012**.*

To add a perspective to the Advisor profile:

1. Access the properties of the Advisor profile.

   ☛ *See "Viewing Profile Characteristics", page 107.*
2. Select the **Advisor Perspectives** tab.
3. In the toolbar, click **Connect**  .
   The Advisor perspectives query tool appears.
4. (Optional) In the second field, enter the characters to find.
5. Click **Find**  .
6. In the query results, select the Advisor perspective.
7. Click **Add**.
   The Advisor perspective is added to the list of perspectives.

Connecting Users to a Profile

☛ *Case of definition of profiles on login of persons, see "Definition of profiles to persons mode", page 93*

To connect a user to a profile, you must connect the login of the user to the profile.

☛ *A user can have several profiles.*

A user must have at least one profile.

☛ *Alternatively, you can connect a profile to a user, see "Configuring a Login", page 75.*

Connecting users to a profile (Web Front-End)

To connect users to a profile:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

2. In the result list, select the profile you want to connect to users.
3. In the edit area, click **Connect** .
4. (Optional) In the query field, enter the characters to find.
5. Click **Find** to run the query.
   The list of logins that can be connected to the profile appears.
6. In the results list, select the persons you want to connect to the profile.
7. Click **Add**.
   The persons selected are connected to the profile.

Connecting users to a profile (Windows Front-End)

To connect users to a profile:

1. Open the profile properties dialog box.

   ☛ *See "Viewing Profile Characteristics", page 107.*

2. Select the **Characteristics** tab.
3. In the **Logins** frame, click **Connect** .
4. (Optional) In the query field, enter the characters to find.
5. Click **Find** to run the query.
   The list of logins that can be connected to the profile appears.
6. In the results list, select the logins you want to connect to the profile.

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

7. Click **OK**.
   The users of selected logins are connected to the profile.

Defining Profile Repository Access Rights

Repository access rights defined on a profile determine if users of this profile can access repositories, and with what rights.

Repository access rights depend on the profile used by the user.

If repository access rights are also defined on the login of a user, these rights are added to restrictions on rights defined on the profile, see "Restricting User Repository Access Rights", page 83.

Defining profile repository access rights (Web Front-End)

To modify repository access rights applied to users of a profile:

1. Access the profile properties page.

   ☛ *See "Viewing Profile Characteristics (Web Front-End)", page 107.*

2. Select the **Repositories** tab.
3. For each repository, modify the value of the **Profile Access Rights** field ("Not accessible" or "Read-only if you want to restrict access to the repository concerned).

   ☛ *See "Profile Properties", page 102.*

4. Click **Save**  .

Defining profile repository access rights (Windows Front-End)

To modify repository access rights applied to users of a profile:

1. Open the manage profiles dialog box.

   ☛ *See "Opening the profile management window (Windows Front-End)", page 42 or "Opening the business roles and profiles management window (Windows Front-End)", page 44.*

2. In the **Profile** frame, select the profile.
3. In the **Repository** pane, for each repository modify the value of the **Profile Access Rights** field ("Not Accessible" or "Read-only" if you want to restrict access to the repository concerned).

   ☛ *See "Profile Properties", page 102.*

4. Click **OK**.

Defining Connection Repository Snapshot for a Profile

☛ *Repository snapshots are available for RDBMS repositories.*

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

You can define the connection repository snapshot for a profile, that is the repository state to which users of a profile connect.

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

This profile must have reading access to the repository (example: **HOPEX Explorer**).

☛ *See "Defining Profile Repository Access Rights", page 116.*

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

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

Defining the connection repository snapshot of a profile (Web Front-End)

To define the connection repository snapshot of the users of a profile:

1. Access the profile properties page.

   ☛ *See "Viewing Profile Characteristics (Web Front-End)", page 107.*

2. In the edit area, select the profile.
3. Select the **Repositories** tab.
4. For each repository in the **Profile Connection Snapshot** field, select a repository snapshot.

   ☛ *See "Profile Properties", page 102.*

5. Click **Save** .

Defining the connection repository snapshot of a profile (Windows Front-End)

To define the connection repository snapshot of the users of a profile:

1. Open the manage profiles dialog box.

   ☛ *See "Opening the profile management window (Windows Front-End)", page 42 or "Opening the business roles and profiles management window (Windows Front-End)", page 44.*

2. In the **Profile** frame, select the profile.
3. In the **Repository** pane, for each repository select the value of the **Profile Connection Snapshot** field.

   ☛ *See "Profile Properties", page 102.*

4. Click **OK**.

Deleting a Profile

If you delete a profile that is the only profile connected to the Login of a user, this user can no longer connect to MEGA.

To delete a **Profile**:

1. Open the **Profiles** management window.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31, "Opening the profile management window (Windows Front-End)", page 42, or "Opening the business roles and profiles management window (Windows Front-End)", page 44.*

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

   ☛ *You can select more than one.*

3. Click **Delete** .
   The dialog box for deleting a profile opens.
4. Click **Delete**.
   The profile is deleted from the environment

Business Role Properties

A business role is defined at repository level.

Name

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

Profile

A business role defines the business or function of a person in the enterprise.

For a business role to be used at connection to **MEGA** it must be connected to a profile.

A business role is connected to only one profile. Several business roles can be connected to the same profile.

Case specific to connection to MEGA Administration, see "Configuring the MEGA Administrator business role", page 123, see "Administrator profile", page 30.

Business role status

The **Business Role Status** is used to define the business role as inactive if needed.

MetaPicture

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

Business role display

The **Business Role Display** attribute enables to define that a business role connected to a profile is displayed at connection:

- always, even if the profile to which it is connected is a sub-profile of the profile of another business role of the user (value "Always")

  See "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 106.

- only if it is not included in another business role (value "If not included in another business role"). Default behavior if the field is not specified.

_GUIName

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

Creating Business Roles

In operating mode "assignment of business roles to persons", each user must have at least one business role to be able to connect to **MEGA**. This business role must be connected to a profile.

☛ *"Assignment of business roles to persons mode", page 91.*

To create a business role:

1. (Web Front-End) Access the user management pages and select the **Business Roles** sub-folder.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

   (Windows Front-End) Open the **Business Roles and Profiles** and select the **Business Roles** tab.

   ☛ *See "Opening the business roles and profiles management window (Windows Front-End)", page 44.*

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**.
   (Web Front-End) The new business role appears in the list of **All Business Roles**.

   (Windows Front-End) The new business role appears in the list of **Business Roles**.

   ☛ *To define characteristics of a business role, see "Defining Business Role Characteristics", page 120.*

   ☛ *To configure the business role, see "Configuring a Business Role (Object Assignment)", page 122.*

Defining Business Role Characteristics

☛ *For detailed information on characteristics of a business role, see "Business Role Properties", page 119.*

To define characteristics of a business role:

1. (Web Front-End) Access the user management pages and select the **Business Roles** sub-folder.

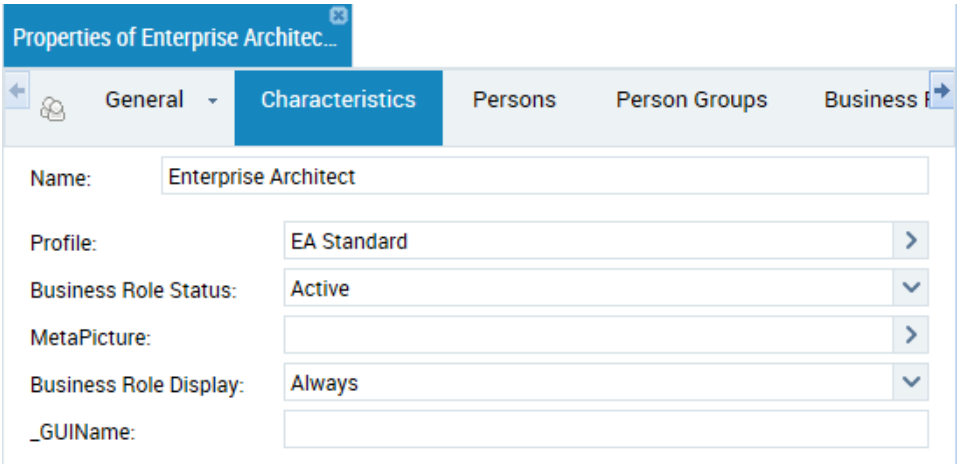
   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

   (Windows Front-End) Open the **Business Roles and Profiles** and select the **Business Roles** tab.

   ☛ *See "Opening the business roles and profiles management window (Windows Front-End)", page 44.*

2. In the list of **Business Roles**, select the business role.

3. In the toolbar, click **Properties** .
The **Properties** dialog box of the business role appears.



4. (Optional) Connect the business role to a profile, see "Configuring a Business Role (Connection)", page 122
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 **Business Role Status** field, modify the attribute value.

   ☛ *By default, the business role is active.*
7. (Optional) In the **Business Role Display** field, click the arrow and modify default behavior of business role display at connection.

   ☛ *See "Business role display", page 119.*
8. (Optional) In the **_GUIName** field, enter the business role name displayed in the interface.
9. Click **Save** (Web Front-End) / **Apply** (Windows Front-End).

Configuring a Business Role

See:

- "Configuring a Business Role (Connection)", page 122
- "Configuring a Business Role (Object Assignment)", page 122
- "Configuring the MEGA Administrator business role", page 123

Configuring a Business Role (Connection)

In operating mode "assignment of business roles to persons" (see "Assignment of business roles to persons mode", page 91), each user must have at least one business role connected to a profile.

A business role can be connected to a profile or not. Only the business role connected to a profile can serve as connection.

☛ *Several business roles can be connected to the same profile.*

☛ *See also "Defining business roles connected to the profile (case of assignment of business roles to persons)", page 114.*

To connect a business role to a profile:

1. Open the business role properties dialog box.
   ☛ *See "Defining Business Role Characteristics", page 120.*
2. Select the **Characteristics** tab.
3. In the **Profile** field, click the arrow and select **Query Profile**.
4. (Optional) In the query wizard, in the second field enter the characters to find.
5. Click **Find**  .
   Profiles found are listed.
6. In the result list, select the profile you want to connect to the business role.
7. Click **OK**.

Configuring a Business Role (Object Assignment)

☛ *See "Assignment of business roles to persons mode", page 91.*

Configuring a business role consists of defining:

- assigned objects and/or
- localizing objects

☛ *See "Assigning a business role to a person", page 123.*

To configure a business role:

1. Display properties of the business role.
   ☛ *See "Defining Business Role Characteristics", page 120.*
2. Select the **Business Role Definition** tab.
3. (Optional) In the **Assignment MetaClass** pane, click **Connect**  .
   You must specify at least one of the two panes, see step 8.
   The MetaClasses query tool appears.
4. (Optional) In the second field, enter the characters to find.
5. Click **Find**  .
6. In the query results, select the MetaClass you want to connect.
   ☛ *Use the [Ctrl] key to select several MetaClasses at the same time.*
7. Click **Add**.
   The MetaClasses are connected to the profile.

8. (Optional) In the **Localizing MetaClass** pane, click **Connect**  .

   You must specify at least one of the two panes, see step 3.

   The MetaClasses query tool appears.
9. (Optional) In the second field, enter the characters to find.
10. Click **Find**  .
11. 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.
12. Click **Add**.
    The Localizing MetaClasses are connected to the profile.
13. Click **Save**  (Web Front-End) / **Apply** (Windows Front-End).
    (Web Front-End) The business role appears in the **Object-Specific Business Roles** list.

Configuring the MEGA Administrator business role

To access the MEGA Administration application with the **MEGA Administrator** business role, you must configure the login of the person who has the MEGA Administrator business role.

1. Display the characteristics of the login of the person in question.

   See "Viewing Login Characteristics", page 51.
2. In the **Administrator Profile** frame, click **Connect**  .
3. Select the **MEGA Administrator** profile (or an equivalent profile).
4. Click **Add**.
   The user can connect to MEGA Administration.

Assigning a business role to a person

For a person to be able to connect to **MEGA**, you must assign a connection business role to the person. You can assign more than one connection business role to the same person.

See:

- Web Front-End:
  - "Assigning a business role to a person (Web Front-End)", page 123
  - "Mass assignment of business roles to persons (Web Front-End)", page 124
- Windows Front-End:
  - "Assigning a business role to a person (Windows Front-End)", page 124

Assigning a business role to a person (Web Front-End)

To assign one or more business roles to one or more persons at a time, see "Mass assignment of business roles to persons (Web Front-

End)", page 124*

☛ *To assign a business role to a person from the user management page, see "Mass assignment of business roles to persons (Web Front-End)", page 124).*

To assign a business role to a person:

1. Access the properties of the person.

   ☛ *See "Viewing person characteristics (Web Front-End)", page 48.*

2. In the **Assignments** tab, click **Business Role Assignments (Connection)**.
3. Click **New**  .
4. In the **Business Role** field, click the arrow and in the drop-down menu, select the business role you want to assign to the person.
5. Click **OK**.

Mass assignment of business roles to persons (Web Front-End)

To perform a mass assignment of business roles to persons:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

2. Select the **Persons** sub-folder.
   The list of persons appears.
3. Select the person to whom you want to assign one or more business roles.

   ☛ *You can select more than one.*

4. Click **Assign Business Roles (connection)**.
   The business role list appears.
5. Select the business role that you want to assign to the selected persons.

   ☛ *You can select more than one.*

6. Click **OK**.
   The business roles selected are assigned to the selected persons.

Assigning a business role to a person (Windows Front-End)

To assign a business role to a person:

1. Connect to the repository in question.

   ☛ *See "Accessing Repositories", page 138.*

2. In the repository tree, right-click **Assignment of Business Roles** and select **Manage**.
3. In the **Persons** frame, select the person to whom you want to assign a business role.
4. In the **Person Assignment** frame, click **New**  .
   The person assignment creation wizard opens.
5. In the **Business Role** field, click the arrow and in the drop-down menu select the business role (connection) you want to assign to the person.

   ☛ *To execute a query on a business role, click the arrow and select **Query Business Role**.*

6. Click **OK**.
   The business role is assigned to the person.

Assigning an Object 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.

  ☛ *Web Front-End, see "Assigning an object to a person (Web Front-End)", page 125 step 5.*

  ☛ *Windows Front-End, see "Assigning an object to a person (Windows Front-End)", page 127 step 6.*

- to a given geographical location

  Example: David Oldfield is Risk Manager at London Branch.

  ☛ *Web Front-End, see "Assigning an object to a person (Web Front-End)", page 125 step 6.*

  ☛ *Windows Front-End, see "Assigning an object to a person (Windows Front-End)", page 127 step 7.*

- to a given geographical location for a specific object

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

  ☛ *Web Front-End, see "Assigning an object to a person (Web Front-End)", page 125 steps 5 and 6.*

  ☛ *Windows Front-End, see "Assigning an object to a person (Windows Front-End)", page 127 steps 6 and 7.*

So that the person can play these business roles, you must assign him/her the necessary rights on tools and data.

☛ *See "Managing UI Access (Permissions)", page 282.*

The business role of a person depends on the repository in which he/she is working. A person can have a given business role in repository R1 and another business role in repository R2.

Assigning an object to a person (Web Front-End)

☛ *To assign one or more objects to one or more persons at a time, see "Mass assignment of objects to persons (Web Front-End)", page 126*

☛ *To assign an object to a person from the user management page, see "Mass assignment of objects to persons (Web Front-End)", page 126).*

To assign an object to a person:

1. Access the properties of the person.

   ☛ *See "Viewing person characteristics (Web Front-End)", page 48.*

2. In the **Assignments** tab, click **Object Assignment**.

3. Click **New**  .

4. Click the drop-down menu in the **Business Role** field and select the business role concerned.
5. (If necessary) In the **Assigned Object** field, click the arrow and select **Find**.

   ☛ *This field appears only if the selected business role has at least one assigned object, see "Configuring a Business Role (Object Assignment)", page 122.*

   In the query dialog box:
   - (if necessary) in the first field, select the object type to find.
   - (Optional) in the field, enter the characters to find.
   - Click **Find**  .
   - Select the object and click **OK**.
6. (if necessary) In the **Assignment Location** field, click the arrow and select **Connect**.

   ☛ *This field appears only if the selected business role has at least one Localizing MetaClass, see "Configuring a Business Role (Object Assignment)", page 122.*

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

Mass assignment of objects to persons (Web Front-End)

To perform a mass assignment of objects to persons:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select a **Persons** sub-folder.
   The list of persons appears.
3. Select the persons concerned.
4. Click **Assign Objects**.
5. In the list of business roles, select the business role in question.

   ☛ *Only the business roles that can be assigned to more than one person at the same time (cardinality >1) are displayed.*
6. In the **Assigned Object** frame, click **Connect**  .
7. (Optional) Using the query wizard:
   - (if necessary) in the first field, select the object type to find.
   - (Optional) in the second field, enter the characters to find.
   - Click **Find**  .
8. Select the object and click **Connect**.

   ☛ *You can select more than one.*
9. Click **Add**.

Assigning an object to a person (Windows Front-End)

To assign an object to a person:

1. Connect to the repository in question.

   ☛ *See "Accessing Repositories", page 138.*

2. In the repository tree, right-click **Assignment of Business Roles** and select **Manage**.
3. In the **Persons** frame, select the person to whom you want to assign a business role.
4. In the **Person Assignment** frame, click **New**  .
   The person assignment creation wizard opens.
5. In the **Business Role** field, click the drop-down menu and in the list, select the business role concerned.

   ☛ *To execute a query on a business role, click the arrow and select **Query Business Role**.*

   If the business role includes:

   - one or several assigned objects, the **Assigned Object** field appears.
   - one or several localizing objects, the **Assignment Location** field appears.

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

   ☛ *This field appears only if the selected business role has at least one assigned object, see "Configuring a Business Role (Object Assignment)", page 122.*

   In the query dialog box,

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

7. (If necessary) In the **Assignment Location** field, click the arrow and select **Find**.

   ☛ *This field appears only if the selected business role has at least one Localizing MetaClass, see "Configuring a Business Role (Object Assignment)", page 122.*

   In the query dialog box,

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

8. Click **OK**.
   The business role is assigned to the person.

Assigning a Business Role to a Person Group (Web Front-End)

To assign a business role to a person group:

1. Access the properties of the person group.

   ☛ *See "Viewing person group characteristics (Web Front-End)", page 50.*

2. In the **Assignments** tab, click **New** .
3. In the **Business Role** field, click the drop-down menu and select the business role you want to assign to the person group.
4. Click **OK**.

Deleting a Business Role

If you delete a business role that is the only business role of a person, this person can no longer connect to MEGA.

To delete a business role:

1. (Web Front-End) Access the user management pages and select the **Business Roles** sub-folder.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

   (Windows Front-End) Open the **Business Roles and Profiles** and select the **Business Roles** tab.

   ☛ *See "Opening the business roles and profiles management window (Windows Front-End)", page 44.*

2. Select the business role you want to delete.

   ☛ *You want to select one or more business roles.*

3. Click **Delete** .
   The business role deletion dialog box appears.
4. Click **Delete**.
   The business role is deleted from the environment.

AUTHENTICATION IN MEGA

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

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

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

This solution offers several advantages, including:

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

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

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

For more details on single sign-on, see:

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

MEGA proposes the following authentication modes:

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

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

Defining Default Authentication Mode

Authentication can be:

- managed within MEGA (by default)
- delegated to a third party service

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

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

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

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

  ☛ *See "Defining default LDAP authentication mode", page 130.*

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

  ☛ *See "Viewing default authentication mode", page 130.*

Viewing default authentication mode

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

To view default authentication mode:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 368.*

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

Defining default LDAP authentication mode

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

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

To define default LDAP authentication mode:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 368.*

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

Defining user authentication mode

User authentication mode is defined on the login by the **Authentication Mode** parameter. The value of this parameter is inherited at user creation from the value of the **Authentication Mode** option defined in the environment options (see "Viewing default authentication mode", page 130).

To define user authentication mode, see "Configuring a Login", page 75.

Windows Authentication

Synchronization with a company directory

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

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

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

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

Associating a Windows user with a MEGA user manually

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

Windows Front-End

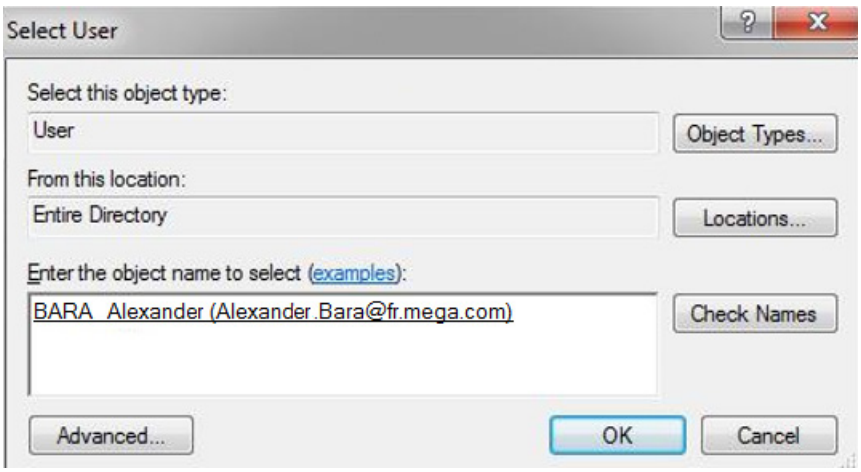
To indicate the Windows identifier of a **MEGA** user from the Administration application (Windows Front-End):

1. Open the properties dialog box of the user login.

   ☛ *See "Viewing Login Characteristics", page 51.*
2. Select the **Characteristics** tab.
3. In the **Authentication Mode** field drop-down list, select "Windows".
   The **Windows Login** field appears.
4. In the **Windows Login** drop-down list  , select **Select Windows User**.
   The **Select User** dialog box opens.
5. In the **Enter the object name to select** frame, enter the user name.

   ☺ *To find users with the help of a wizard, click **Advanced**.*

6. Click **Check Names**.



7. Click **OK**.
   The Windows identifier of the user is displayed.

Web Front-End

To indicate the Windows identifier of a **MEGA** user from the Administration desktop (Web Front-End):

1. Access the Login properties of the user.
   ☛ *See "Viewing Login Characteristics", page 51.*
2. Select the **Characteristics** tab.
3. In the **Authentication Mode** field drop-down list, select "Windows".
   The **Windows Login** field appears.
4. In the **Windows Login** field, enter the user reference in the Active Directory in the following format: Domain name\User login:

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

   ```
   Example: tad
   ```

Connection in case of unique authentication

(Windows Front-End) If the **MEGA** user is:

- different from that identified by the Windows session opened on the workstation, the user must enter his/her own Windows password.
- the same as that identified by Windows session opened on the workstation, the user does not need to enter his/her password.

(Web Front-End) The user must enter his/her Windows password.

Single sign-on precautions

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

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

LDAP Authentication

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

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

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

☛ *Only users (example: Administrator) with a **MEGA Administrator** or **User Administrator** profile, see "Administrator profile", page 30.*

Configuring LDAP authentication

To configure LDAP authentication:

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

   ☛ *See "Creating an LDAP server", page 134.*
2. Specify parameters of your LDAP server.

   ☛ *See "Configuring the LDAP server", page 134.*
3. (Optional) You can:
   - configure LDAP parameters

     ☛ *See "Configuring an LDAP parameter", page 136.*
   - modify LDAP import parameters

     ☛ *See "Modifying LDAP directory import content", page 137.*
4. (Web Front-End) Check the configuration of the LDAP server.

   ☛ *See "Checking the configuration of an LDAP server (Web Front-End)", page 137.*

When LDAP authentication has been configured:

- you can import persons from the LDAP directory.

  ☛ *See "Importing persons from an LDAP server", page 138.*
- or you can manually map a **MEGA** user group with a user group declared in your LDAP server.

  ☛ *See "Associating a MEGA user group with an LDAP user group", page 138.*

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

Accessing LDAP server management

To access LDAP server management:

- Web Front-End:
  From the **Administration** desktop, select the **LDAP Servers** sub-folder.

  ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
- Windows Front-End:
  From **MEGA Administration,** in the **User Management** folder, right-click on **LDAP Servers** and select **Administer**.

  ☛ *See "Accessing User Management and UI Access Management Folders (Windows Front-End)", page 39.*

  ☛ *The **LDAP Servers** folder is available only if you are connected with a user with MEGA Administrator profile (example: **Administrator**), see "Administrator profile", page 30.*

Creating an LDAP server

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

The LDAP directory can be an Active Directory directory.

To create an LDAP server:

1. Access LDAP server management.

   ☛ *See "Accessing LDAP server management", page 134.*
2. In the LDAP server menu bar, click **New**  .
3. In the creation of LDAP server dialog box, enter the **Name** of the LDAP server and click **OK**.
   The new LDAP server appears in the list of LDAP servers.
   You must configure the LDAP server, see "Configuring the LDAP server", page 134.

Configuring the LDAP server

LDAP server configuration is restricted to users with a MEGA Administration or user Administration profile.

To configure an LDAP server:

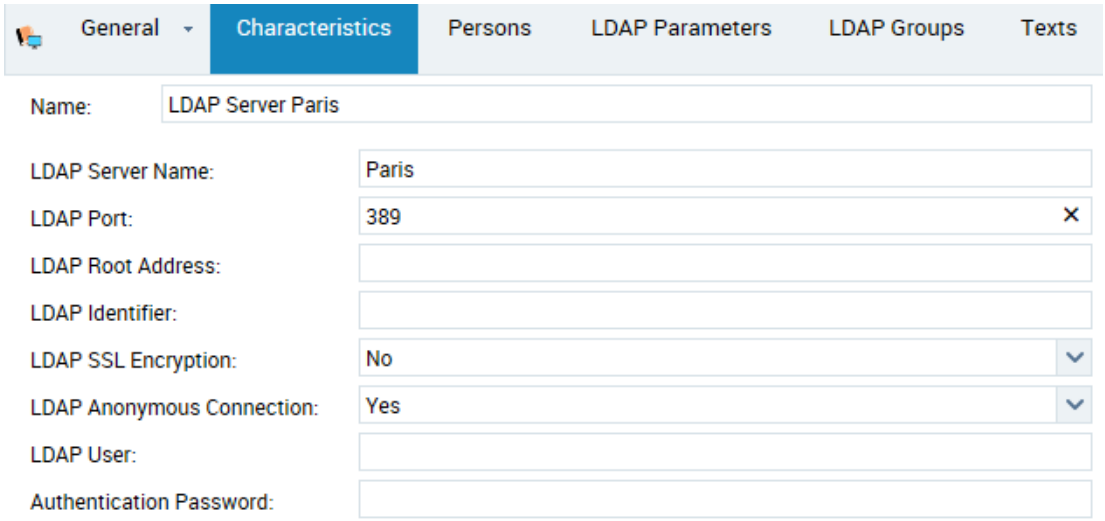
Prerequisite: the LDAP server is already created.

☛ *See "Creating an LDAP server", page 134.*

1. Access LDAP server management.

   ☛ *See "Accessing LDAP server management", page 134.*

2. Select the new LDAP server and click **Properties** .



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

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

     `Example: SAMAccountName, UID`
   - **LDAP SSL Encryption**: select **Yes** if you wish 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 **MEGA** needs to access (example: LDAP person group, membership of a group in LDAP, e-mail in LDAP, etc.).*
   - **Authentication Password**: enter the password of the LDAP user used for LDAP directory connection. If connection is anonymous, this field should not be completed.

4. Click **Save** (Web Front-End) / **OK** (Windows Front-End).
   The LDAP server is configured.
   You can also:
   - configure an LDAP parameter, see "Configuring an LDAP parameter", page 136.
   - modify content of LDAP directory import, see "Modifying LDAP directory import content", page 137.

Configuring an LDAP parameter

An LDAP parameter is a parameter that exists in the LDAP directory and is associated uniquely with a **MEGA** 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 **MEGA**) corresponding to parameters with values stored in the LDAP directory.

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

To configure an LDAP parameter:

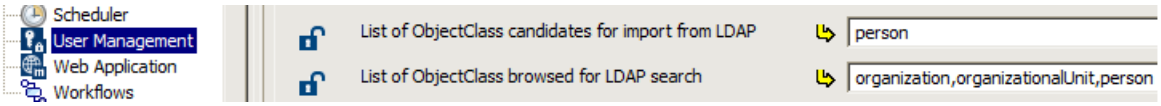
1. Access LDAP server management.
   ☛ *See "Accessing LDAP server management", page 134.*
2. Select the LDAP server for which you want to configure an LDAP parameter and click **Properties**  .
3. In the **LDAP Parameters** tab, click **New**  .
   ☛ *The LDAP parameter enables pre-completion of characteristics of a person corresponding to the LDAP parameters.*
4. Enter the **Name** of the LDAP parameter (example: Mail), then click **Properties**  .
5. (Optionally, access the "expert" metamodel) Select **Index on Persons**, so that the parameter value enables unique identification of a person. If a person in **MEGA** has the same e-mail as a person defined in the LDAP directory, this person is reused (instead of creating a new person and risk duplicating the same person).
6. (Optionally, access the "expert" metamodel) Select **Is available for search** so that an e-mail address can be entered in the import entry area.

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

Modifying LDAP directory import content

You can modify LDAP directory import content:

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



To define content of LDAP directory import:

1. Access the environment options management window.
   ☛ *See "Modifying options at environment level", page 368.*
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 (Web Front-End)

To check the configuration of an LDAP server:

1. Access LDAP server management.
   ☛ *See "Accessing LDAP server management", page 134.*
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 **MEGA**) corresponding to parameters with values stored in the LDAP directory.

☛ *See "Configuring an LDAP parameter", page 136.*

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

An LDAP parameter is a parameter that exists in the LDAP directory and is associated uniquely with a MEGA 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. Open the user management window.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31 or "Opening the user management window (Windows Front-End)", page 40.*
2. In the **Persons** tab, click **Import From LDAP**.
3. The **LDAP Import Wizard** appears.
4. In the **LDAP Server** field, select via the drop-down menu the server from which you want to import persons.

   ☛ *The LDAP server must be created, see"Creating an LDAP server", page 134.*
5. In the **Queried Element** field, enter the queried character string.

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

Associating a MEGA user group with an LDAP user group

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

Having configured the LDAP server (see "Configuring the LDAP server", page 134), you must specify a user group authenticated with the LDAP directory.

☛ *If a default person group is defined (example "Guests") and no LDAP group is specified, a person authenticated in LDAP (with the **Belongs to a person group** option selected, see "Person Properties", page 21) automatically belongs to the group defined by default (example: "Guests").*

To specify a user group authenticated with the LDAP directory:

1. Access LDAP server management.

   ☛ *See "Accessing LDAP server management", page 134.*
2. Select the LDAP server you wish to configure and click **Properties** .
3. In the LDAP server properties dialog box, select the **LDAP Groups** tab.
4. Click **Connect** to connect the existing LDAP user group.
   The LDAP Group query wizard appears.
5. (Optional) In the query field, enter the character string to be queried.

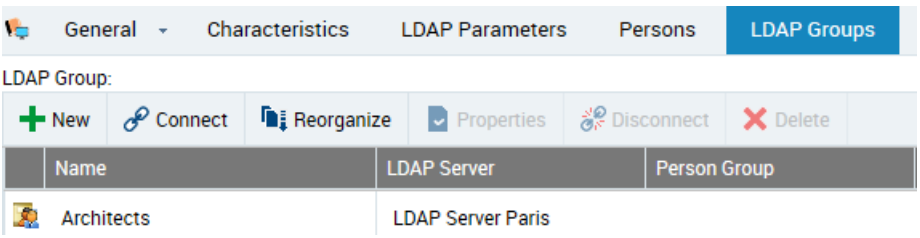
6. Click **Find** .

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

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

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

   The LDAP user group appears in the list.



8. Connect the MEGA user group to the LDAP user group.

   ☛ *See "Defining a dynamic person group with LDAP", page 72.*

Authentication and a user created on the fly (RDBMS repository)

Creation of a person on the fly concerns only RDBMS repositories.

Users created on the fly concern cases of connection to MEGA via the Web in read-only mode (example: *HOPEX Explorer*). Creation of a user on the fly is not available for connection to MEGA (Windows Front-End).

When a user has been created on the fly, the LDAP parameters can be used as indexing identifier (**Index on Person** attribute, see "Configuring an LDAP parameter", page 136) to check that a person with an attribute with the same value as the LDAP directory already exists in **MEGA**.

Example of use:

Anne, responsible for sending questionnaires, wishes 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 the Web application (**HOPEX Explorer**), with tkh:

1. The authentication service authenticates tkh with the LDAP directory: the "mail" parameter exists and is indexing identifier type (**Index on Person** is selected),
2. The authentication service checks if a person already has this e-mail.

   ☛ *Answer: Yes.*
3. The authentication service creates the login associated with the person.

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

WEB-SPECIFIC CONFIGURATION

Some configurations are specific to **MEGA** users on the Web.

☛ *To connect to the d'**Administration** desktop (Web Front-End), see "Connecting to the Administration Desktop (Web Front-End)", page 7).*

The following points are detailed here:

Review of Web Application-Linked Installation Options

For detailed information on the installation options linked to Web applications, see the **MEGA Web Front-End Installation Guide**.

☛ *To manage languages in Web applications, see "Managing Languages in Web Applications", page 379.*

Specifying the Web applications access path

To specify the Web applications access path:

1. Access the environment options management window.

   ☛ *See "Modifying options at environment level", page 368.*
2. In the options tree, expand the **Installation** folder and select **Web Application**.
3. In the right pane, specify the **Web Application Path** option.

   `Example: http://<Server Name>/HOPEX`

Specifying SMTP configuration

To specify SMTP configuration:

1. Access the environment options management window.

   ☛ *See "Modifying options at environment level", page 368.*
2. In the options tree, expand the **Installation** folder and select **Electronic Mail**.
3. The following options should be specified in the right pane:
   - **Default address of sender via SMTP**

     `Example: server@company.com, AdministratorName@company.com`
   - **SMTP Server**

     `Example: exa.fr.company.com`

Initializing and 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.

☛ *See "Authentication mode", page 28.*

Initializing a user Web account

Prerequisites

Before initializing the Web account of a user:

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

  ☛ *See "Viewing Person Characteristics", page 47.*

- check that the following options relating to Web applications are specified:
  - "Specifying the Web applications access path", page 141
  - "Specifying SMTP configuration", page 141

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

To initialize the Web account of a user:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select the **Persons** sub-folder.
3. In the Persons list, select the person concerned.
4. Click **Initialize the Account**.
   An e-mail is sent to the person concerned with a limited life link (48 hours by default), allowing the person to define a password and the reply to a security question.

   In the characteristics of the person, if the e-mail address is not specified, the person cannot receive the message.

   ☛ *To modify the life of the first connection link, see "Modifying the life of the first connection link", page 142.*

Modifying the life of the first connection link

To modify the life of the first connection link:

1. Connect to the **MEGA Administration** desktop (Web Front-End).

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*
2. In the edit area, click **Environment Options**.

   ☛ *Alternatively, from **MEGA Administration** (Windows Front-End), open the management window for environment options, see "Modifying options at environment level", page 368.*
3. In the options tree, expand the **Installation** folder and select **User Management**.

4. In the right pane, modify the value of the **Life of first connection link** option.

Modifying password management configuration

To modify configuration linked to password management:

1. Connect to the **MEGA Administration** desktop (Web Front-End).

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

2. In the edit area, click **Environment Options**.

   ☛ *Alternatively, from **MEGA Administration** (Windows Front-End), open the management window for environment options, see "Modifying options at environment level", page 368.*

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

     ☛ *Default value: 3*

   - **Password expiry**

     ☛ *Default value: 40 days*

Modifying password definition rules

To modify password definition rules:

1. Edit the **CheckPasswordFormat** macro.

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

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

Reinitializing a User Password

Prerequisite:

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

- "Specifying the Web applications access path", page 141
- "Specifying SMTP configuration", page 141

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

To reinitialize the password of a user:

1. Access the user management page.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select a **Persons** sub-folder.
3. In the edit area, select the person for whom you want to initialize the password.
4. Click **Initialize the Account**.
   An e-mail is sent to the person concerned with a limited life link (48 hours by default), allowing the person to define a password and the reply to a security question.

Specifying Data Language for a User or User Group (Web Front-End)

The data language is the language with which the user connects by default the first time. If the user changes data language in the interface, this is kept for the next connection.

By default, the data language is defined in the environment options. If necessary, you can define the data language for each user or user group.

💣 **The data language defined at user or user group level takes priority over the language defined in the environment options.**

To modify:

- the interface language in Web applications, see "Modifying the interface language in Web applications at environment level", page 379.
- the data language at environment level, see "Modifying the data language in Web applications at environment level", page 379.

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

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

☛ *See "Configuring a Person", page 61.*

☛ *See "Viewing Person Group Characteristics", page 49.*

MANAGING REPOSITORIES

A **MEGA** repository constitutes the workspace in which modeling data is stored. Several users can connect to it and work simultaneously on the same project.

By default, any user of an environment can access all repositories of the environment. The **MEGA** administrator can restrict these rights.

Repository management is carried out with the **MEGA Administration** application.

The **MEGA** repository server type has an influence on the functionalities available (for example: management of repository snapshots and collaborative workspace.

☛ *Certain recommendations may concern only RDBMS or GBMS type storage. Absence of a warning indicates that the recommendation is valid for all types of storage.*

This chapter covers points relating to working in a repository and the use of repositories:

USING REPOSITORIES

A repository depends on an *environment*. Different policies of data distribution can be implemented. You can, for example, work on two repositories:

- a Development repository, which groups all projects
- a Production repository, which groups stable states of each project.

The following points are covered here:

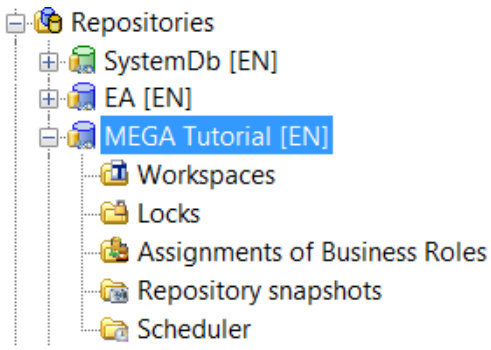
Accessing Repositories

To access a repository:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **Repositories** folder.
The list of the repositories in the environment appears.



Each repository is represented by:

- an icon defining its storage type
- its installation language.

Repository storage type			
GBMS		***RDBMS***	
	MEGA owner format		ORACLE
			SQL Server

Repository Structure

The files enabling use of a repository are all in the same folder, the location of which is stored in the *system repository* (SystDb).

> 🕮 *SystDb is a particular repository containing the metamodel and technical data (descriptors, Web site templates, queries, etc.). The metamodel and technical data are common to all repositories in the same environment. Definition of users and their rights are stored in this repository, essential for operation of the software.*

By default, a **MEGA** repository is stored in GBMS format (**MEGA** proprietary format). You can choose another storage type for your **MEGA** repository: an RDBMS format (relational database management system) such as Oracle or SQL Server.

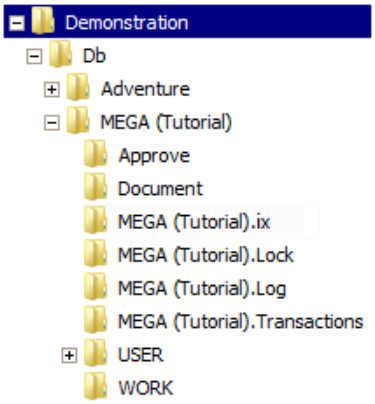
> ☛ *For more details on structure and the advantages of the different server types, see **RDBMS Installation** deployment guide.*

A repository comprises "RepositoryName".XXX files of which type and format XXX depend on the repository server type:

Information type	MEGA repository storage type		
	GBMS	RDBMS	
		Oracle	SQL Server
Semaphore of administration	.EMA (protects simultaneous accesses to the EMS)	N/A	N/A
Managing active private workspaces	.EMS	N/A	N/A
Repository evolution logfile (creation, update, etc.)	.EMV	.EMV	.EMV
Data	.EMB inseparable from .EMA, .EMS and .EMV files)	.EMO*	.EMQ*

*: this file does not contain data; it is a pointer to data stored on the relational database server.

For each repository, folders are created dynamically while the user is working:



- ***Approve***: contains validated reports (MS Word) detached from MEGA.
- ***Data:*** contains all business documents created in **MEGA**.
- ***Document***: contains all reports (MS Word) generated from **MEGA**.
- ***RepositoryName.ix***: contains the result of indexing for quick search.

  ☛ *See "To allow the user to execute quick searches in MEGA solutions, the repository must first be indexed.", page 144.*
- ***RepositoryName.Lock***: contains locks created on objects during user working (when a GBMS repository is used). These files have .EMK extension.

  ☛ *See "Managing Locks", page 215.*
- ***RepositoryName.Log*** (repository backup logfile): contains repository backup logfiles (enabled by default). Each private workspace is saved in logfile, .MGL format.

  ☛ *See "Backup logfile", page 147.*
- ***RepositoryName.PrivateWorkspaces*** (private workspace backup logfile: contains files linked to active private workspaces of repository users.

  ☛ *The presence of these files depends both on the server type used and on the options enabled for this repository.*

  These files are:
  - "CCC.MGL" files, where CCC is the code associated with the user (the **Backup logfile** option is enabled for the repository).

    ☛ *See "Backup logfile", page 147.*
  - "CCC.EMB" and "CCC.EMS" files (similar to those of the repository) containing data of the GBMS private workspace, where CCC is the code associated with the user.
- ***USER***: contains a folder for each user, in which all work files generated by the user are stored. It groups the files created by backup and extraction procedures, as well as control files.

  ☛ *Each folder is named "CCC", where CCC is the code associated with the user.*
- ***WORK***: contains work files created by administration operations carried out using the administration application.

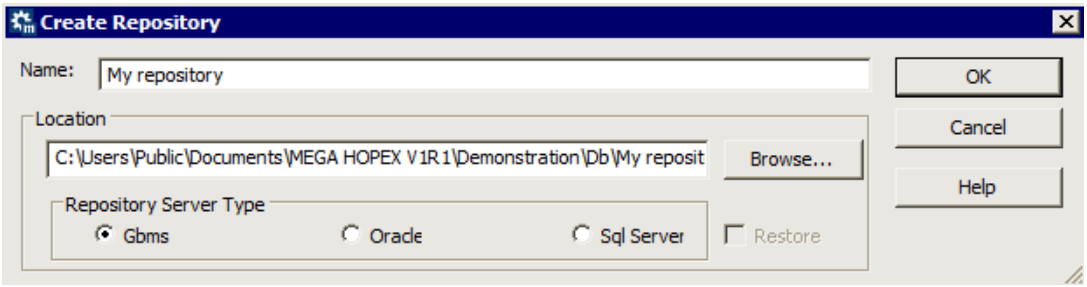
Creating a Repository

To create a repository:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Right-click the **Repositories** folder and select **New**.
   The **Create Repository** dialog box opens.



3. Enter the **Name** of the repository.
   The repository name should start with a letter and not exceed 60 characters. It can contain letters (A-Z), figures (0-9) and certain special characters (_$#).

   ☛ *The name of an Oracle repository should not be an Oracle reserved word (see DBA Oracle).*

   ☛ *The name of an SQL Server repository is prefixed by the environment name. This prefix is not included in the 60 characters limit.*

   ☛ *If you use strange characters, you must be in the same system language as these characters so that they will be recognized by **MEGA**.*

4. (Optional) By default, the repository is created in the **Db** folder of the selected environment; to modify this, click **Browse** and define another location.
5. Select the repository server type and click **OK**.

   ☛ *For more details on repository server type, see **RDBMS Installation Guide**.*

   The repository folder and its files are created.

   ☺ *At creation of a repository, a sub-folder carrying the name of your new repository is automatically created in the **Db** folder of the environment folder to store corresponding repository files.*

The repository created is empty. You can transfer data from another repository into it by importing updates or by restoring a backup file.

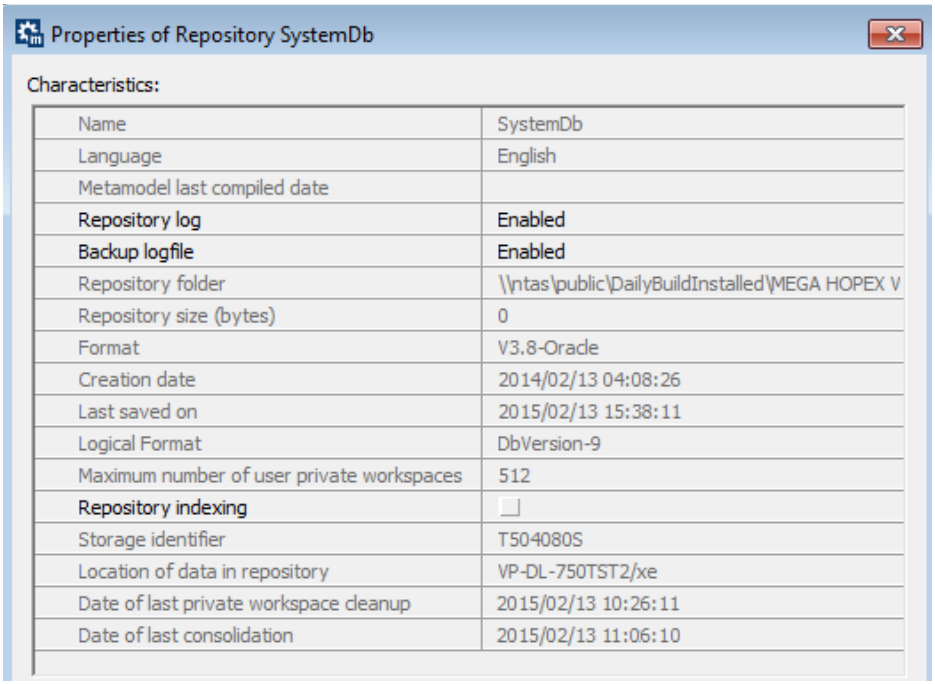
Consulting and Modifying Repository Properties

To consult and/or modify certain repository properties:

1. From **MEGA Administration**, connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **Repositories** folder.
3. Right-click the concerned repository and select **Properties**.
   The **Repository Properties** dialog box opens.



From the **Repository Properties** dialog box, you can:

- click the row of one of the following characteristics to:
  - modify the **Name** of the repository
  - modify the repository **Language**

    Only if you need to modify the repository language right after its creation. Never change the repository language at any time, to avoid irreparable loss of object names.
  - enable/disable the **Repository log**

    For more details, see "Enabling the repository log", page 149.
  - enable/disable the **Backup logfile**

- consult its following characteristics:
  - **Metamodel last compiled date** (SystemDb repository specific)
  - location of the **Folder** in which the repository is stored
  - **Repository Size** presents the size of the .EMB file of the GBMS database.
  - **Format** is information used only for internal operation of MEGA on GBMS repositories.
  - **Dates** of repository creation and last save
  - repository **Logic Format**.
  - **Date of last private workspace cleanup** and **Date of last consolidation** (RDBMS specific), which provide useful information for the maintenance plan of an RDBMS repository.

    ☛ *See "Deleting RDBMS Repository Temporary and History Data", page 187.*
- enable/disable the backup logfile

  ☛ *See "Enabling and Customizing Repository Indexing", page 144.*

Enabling and Customizing Repository Indexing

To allow the user to execute quick searches in **MEGA** solutions, the repository must first be indexed.

Indexing runs automatically every 10 minutes (modifiable default value) with the indexing scheduler (RDBMS specific). This indexing is incremental (indexing modified objects only).

☛ *To modify scheduler default configuration, see "Customizing the indexing scheduler (RDBMS)", page 145. For detailed information on the scheduler, see the technical article **HOPEX Studio - Scheduler**.*

☛ *The initial indexing can take some time depending on the size of your repository (eg: more than 30 hours for a 2 GB repository, of which business documents constitute a major part), and can slow the performance of **MEGA**. Remember to run this initial indexing when other **MEGA** users are not connected.*

Take care to allow sufficient disk space before enabling indexing: statistically for a large repository (eg: 2 GB) of which business documents constitute a major part, the indexing size can represent twice the repository size.

Enabling/Disabling repository indexing for quick search

By default, repository indexing is not enabled.

To enable/disable repository indexing:

1. Access properties of the repository concerned.

   ☛ *See "Consulting and Modifying Repository Properties", page 142.*
2. Select/Clear **Repository Indexing** to enable/disable repository indexing.

3. Click **OK**.
   The scheduler (RDBMS specific) updates indexing every 10 minutes.

   ☛ *To modify scheduler default configuration, see "Customizing the indexing scheduler (RDBMS)", page 145.*

   Indexing is carried out for all of the languages installed.

   When indexing is completed, the "Repository Name".IX folder is created in the corresponding folder of the repository. This folder contains indexing results.

Indexing a repository manually

When the scheduler is unavailable (GBMS), or for initial indexing, the administrator can index the repository manually.

To index a repository manually:

☛ *To be able to manually index the repository, the repository indexing option must be selected, see "Enabling/Disabling repository indexing for quick search", page 144.*

1. From **MEGA Administration**, connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **Repositories** folder.
3. Right-click the repository to be indexed and select **Index for Quick Search**.
   Indexing is carried out for all of the languages installed.

   ☛ *For initial indexing, the "Repository Name".IX folder is created in the corresponding folder of the repository. This folder contains indexing results.*

Customizing the indexing scheduler (RDBMS)

You can modify indexing scheduler default configuration.

To modify indexing scheduler default configuration:

1. Access the repository concerned.

   ☛ *See "Accessing Repositories", page 138.*

2. Right-click **Scheduler** and select **Manage Triggers**.
3. Select the **System Triggers** tab.
4. Right-click **Indexing Automaton** and select **Update Scheduling**.
   The indexing scheduler configuration window appears.
5. Modify the configuration.
6. Click **OK**.

   ☛ *For detailed information on the scheduler, see the technical article **HOPEX Studio - Scheduler**.*

Consulting RDBMS Repository Performance

Before starting work in an RDBMS repository, **MEGA** recommends that you run the RDBMS diagnostic tool.

This tool indicates repository performance compared to optimized performance.

To run the RDBMS repository diagnostic tool:

1. From **MEGA Administration**, connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **Repositories** folder.
3. Right-click the RDBMS repository concerned and select **RDBMS Administration > RDBMS Diagnostics**.

   ☛ *For more information on the RDBMS repository diagnostic tool, see deployment **RDBMS Installation Guide**.*

Generating a Health File for an RDBMS Repository

MEGA enables to generate a file containing information on the fragmentation and the statistics of an RDBMS repository.

To generate a health file for an RDBMS repository:

1. From **MEGA Administration**, connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **Repositories** folder.
3. Right-click the RDBMS repository concerned and select **RDBMS Administration > Information about fragmentation and statistics**. A report file is generated with the information returned by Oracle or the SQL Server on the repository health state.

Accessing the Log of Repository Changes (.EMV file)

The .EMV file contains repository changes (eg: creation, update).

To directly access the .emv file of a repository:

1. From **MEGA Administration**, connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **Repositories** folder.
3. Right-click the desired repository and select **See EMV File**.

MANAGING REPOSITORIES

☛ *For management operations specific to an RDBMS repository, see **RDBMS Installation Guide**.*

The following points are covered here:

Managing logfiles

At repository creation, by default:

- the backup logfile is enabled (value **Enabled**).
- the repository log is not enabled (value **Disabled**).

See:

Backup logfile

The repository is configured so that changes made by users are saved simultaneously in the repository and/or in a specific file called the *backup logfile*.

Backup logfile process

When opening a private workspace, the backup logfile process is as follows:

Step	User A...	Result
1	...connects to **MEGA**.	The MEGA workspace opens. XXX.MGL logfile is created in folder \Db\RepositoryName\RepositoryName.Private Workspaces of the environment directory.
2	...dispatches work.	XXX.MGL logfile is consolidated (*): under YYYY-MM-DD_hh.mm.ss_XXX.mgl name in "\Db\RepositoryName\RepositoryName.Log\ folder
	...discards work.	There is no copy of XXX.MGL logfile.
3	...reconnects to **MEGA**.	A new private workspace opens. XXX.MGL logfile of folder RepositoryName.Transactions is reinitialized

XXX: Code of User A

YYYY-MM-DD: dispatch date (year-month-day)

hh.mm.ss: dispatch time (hour.minute.second)

(*): Consolidation consists of search and deletion of useless commands. For example:

```
When an object is created then deleted, the information is
not saved in the consolidated logfile.

When a comment is created, then modified several times, only
the final modification is saved in the consolidated
logfile.
```

☺ *To avoid overloading the* RepositoryName.Transactions directory, MEGA recommends that you regularly archive the old logfiles.

Modifications made by a user to the system repository are logged in the same way.

If you have a problem

In the event of a problem on the repository, you can restore the last repository backup and import backup logfiles saved in the RepositoryName.Log folder from this backup up to time of the problem.

☛ *It is highly recommended that you synchronize backup logfile archiving with repository backup.*

Dispatched modifications are logged in a new repository log.

In the event of a problem on a user private workspace, you can copy the user backup logfile saved in the RepositoryName.Log folder, delete the current private workspace and import the backup logfile in a new private workspace.

Enabling the repository log

By default, the repository log is disabled for a GBMS repository and enabled for an RDBMS repository.

To keep a history of the actions performed on the repository after dispatch, you must activate the repository log.

> **Enabling the repository log generates a large volume of objects. This volume can adversely affect MEGA performance, particularly at dispatches. It is not recommended with a GBMS repository.**

To enable the repository log:

1. Open the **Properties** dialog box of the repository.

   ☛ *See "Consulting and Modifying Repository Properties", page 142.*

   The repository properties dialog box opens.
2. Click **Repository Log** line and select **Enabled**.

The repository log is enabled.

The repository log lists all modifications made in the repository. It gives users a better understanding of actions dispatched in the repository from private workspaces.

Each time an action is executed, an occurrence of Change Item is created.

> *A **ChangeItem** is a MetaClass corresponding to a change made in a **MEGA** repository.*

A repository log comprises **MEGA** occurrences. These occurrences can be handled using **MEGA** APIs.

☛ *See "Viewing the Repository Update Log", page 151.*

Configuring the logging for an inter repository consolidation

To improve performance you can define some MetaClasses or MetaAssociationEnds as non loggable.

☛ *See "Modifying MetaClass loggability", page 183.*

Logging

Logging of updates enables:

- mainly to view the repository activity, i.e. actions performed on objects.

  ☛ *See "Viewing the Repository Update Log", page 151.*

  In that case, an incomplete (**Consolidate** command) or truncated (**Delete** command) log is functionally satisfactory.

  ☛ *See "Deleting a log or reducing the log size", page 180 step 7.*

  This is the default configuration.
- to transfer the commands performed from a repository to another.

  ```
  Example: you want to transfer all the commands performed
  during the day from a development repository to a production
  repository.
  ```

  In that case a complete log, including all the actions performed by the users, is necessary so that the inter repository *consolidation* is performed correctly. You must modify the default log behavior.

  ☛ *See "Modifying the log behavior", page 150.*

Modifying the log behavior

To include in your log the MetaClasses and MetaAssociations defined as non loggable, you must modify the log behavior.

To modify the log behavior:

1. Access the options.

   ☛ *See "Accessing Options", page 368.*
2. In the Options tree, select **Repository**.
3. In the right pane, for the **Log behavior** option, select "Logging all updates" value.
   All of the updates are included in the logs, including MetaClasses and MetaAssociations that are defined as non loggable.

   ☛ *See "Modifying MetaClass loggability", page 183.*

Viewing the Repository Update Log

You can view the history of the actions performed in the repository after dispatch from:

- the **Administration** desktop (Web Front-End)

  ☛ *See "Accessing repository dispatches from the Administration desktop (Web Front-End)", page 151.*

- the **MEGA Administration** application (Windows Front-End)

  ☛ *See "Viewing the repository update log using MEGA Administration (Windows Front-End)", page 152.*

- **MEGA** (**Repository Activity** navigation window)

  ☛ *See "Viewing the repository update log using MEGA Administration (Windows Front-End)", page 152.*

- the object **History**

Accessing repository dispatches from the Administration desktop (Web Front-End)

To access the repository dispatches from the **Administration** desktop (**Web Front-End**):

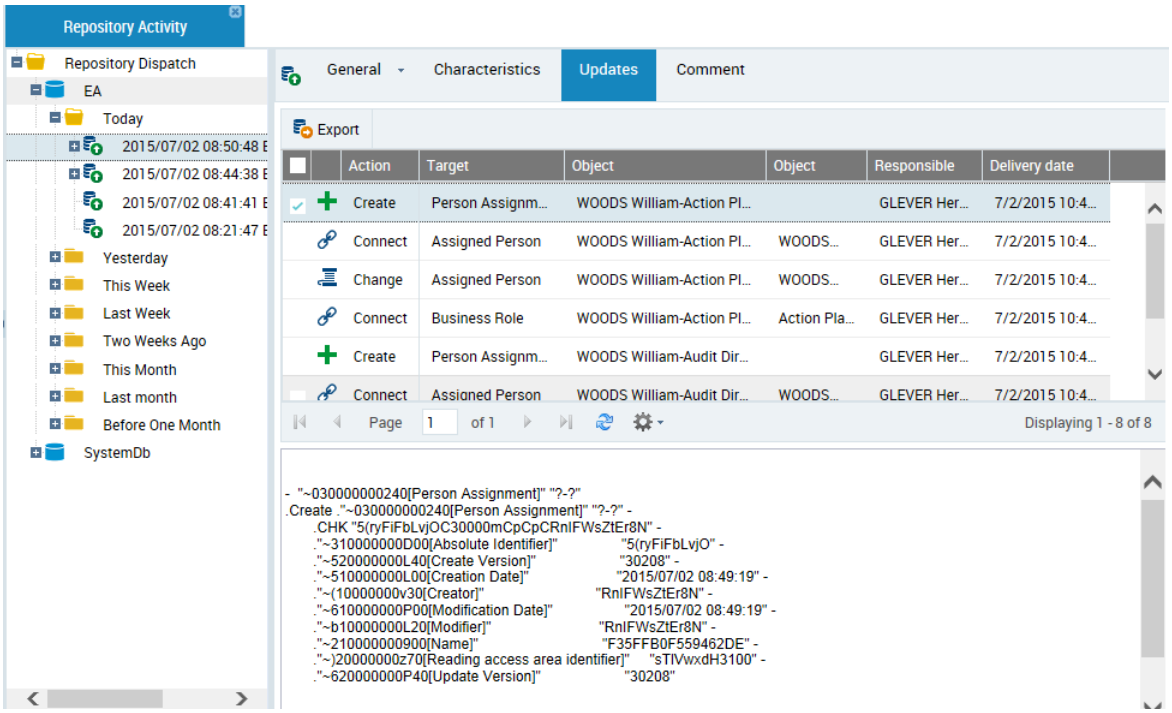
1. Connect to the **Administration** desktop.

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

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. Dispatches are filed by day, week and month.
3. Click a dispatch.
   Its properties appear in the edit page.
   The **Updates** tab details the content of the dispatch in the form of a list of actions displayed in chronological order.

4. Select a line to display the details of the action in the lower frame.

   ☛ *See "Exporting Updates", page 154.*



Viewing the repository update log using MEGA Administration (Windows Front-End)

To view the repository update log using **MEGA Administration** (**Windows Front-End**):

1. From **MEGA Administration**, connect to the desired environment.

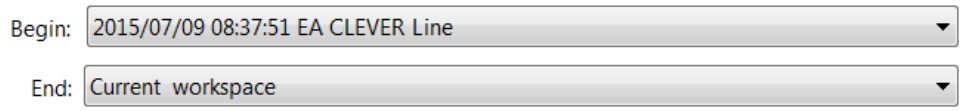
   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **Repositories** folder.
3. Right-click the repository concerned and select **Repository Log > Open**.
   The **View repository updates log** appears.

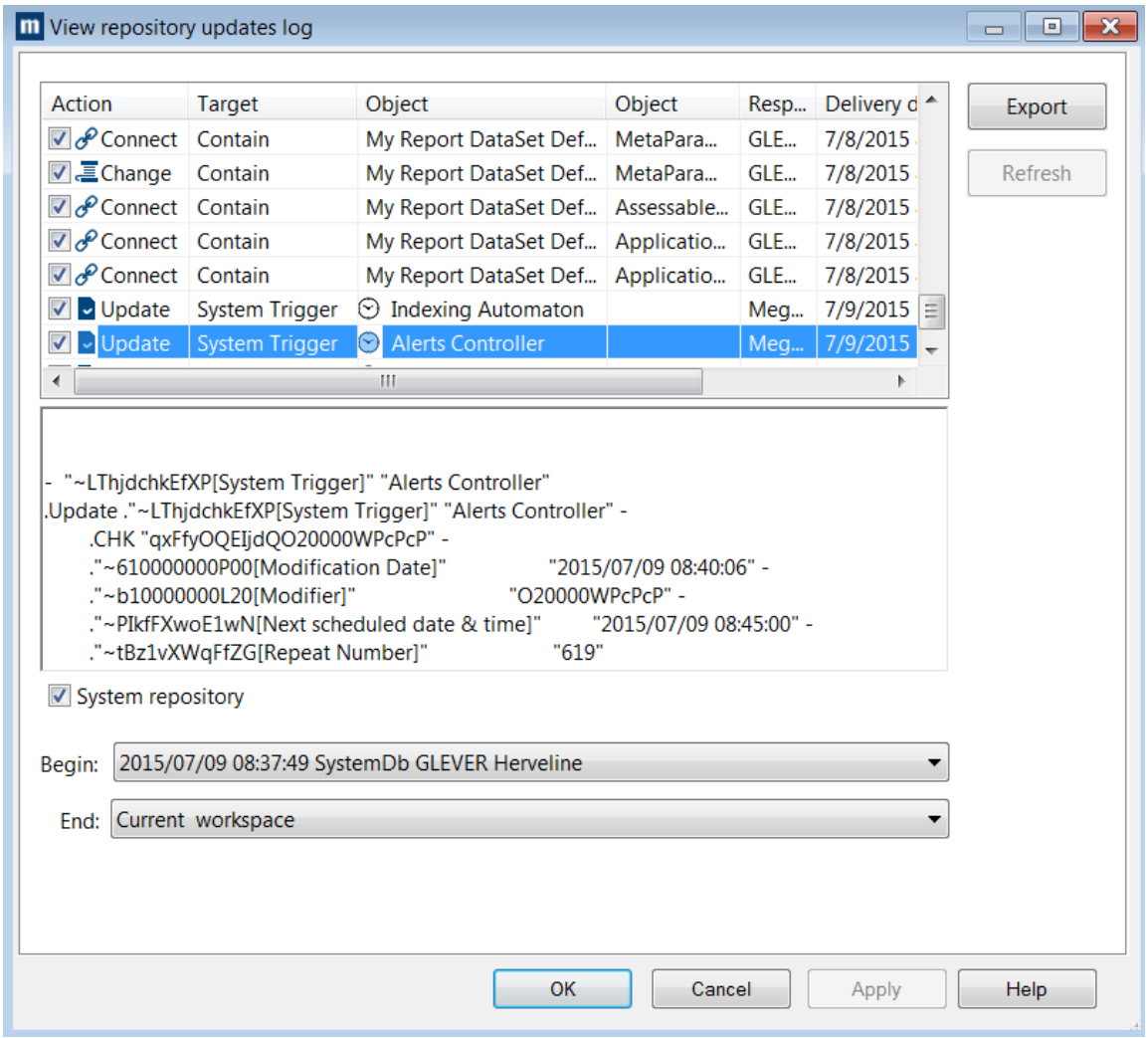
   ☛ *Alternatively, from **MEGA** (with access to the **Expert** metamodel level, see "Configuring metamodel access", page 77), select the **File > Properties** menu. In the dialog box that appears, select the **Update** tab. The log of the current private workspace is displayed by default.*

4. In the **Begin** and **End** fields, select the dispatch interval that you want to display.

   ☛ *You can view the repository log in its totality, or between two given dispatches. In the **Begin** drop-down list, the first element corresponds to the first dispatched private workspace of this repository.*



5. Click **Refresh**.
   The repository log appears as a list of actions displayed in chronological order.



☛ *See "Exporting Updates", page 154.*

Exporting Updates

To export updates:

1. Access the repository update log.

   ☛ *See "Viewing the Repository Update Log", page 151.*

2. Select the updates to be exported.
3. Click **Export**.
4. Select the export format:
   - *.mgr: text format
   - *.xmg: MEGA XML format.
5. Click **Export**.
   You can open or save the export file.

Deleting a Repository

You can delete a GBMS or Oracle repository.

☛ *To delete an SQL Server repository, you need the appropriate administration rights (db_owner database).*

To delete a repository:

1. From **MEGA Administration**, connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the folder containing repositories of this environment.
3. Right-click the repository concerned and select **Delete**.
   A dialog box appears asking you for confirmation.
4. Click **Yes** to confirm deletion.

Converting a Repository

Repository conversion is only necessary:

- at migration.

  ☛ *For more information on repository conversion, consult the technical note **How to migrate to HOPEX V1R3**.*

- on request from **MEGA** support.

Importing Libraries into a Repository

You can import the libraries you need for your work into a repository.

To import a library into a repository:

1. Connect to:
   - the **MEGA Administration** desktop (Web Front-End).

     ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*
   - **MEGA Administration** (Windows Front-End) and select the repository concerned.

     ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*
2. (Web Front-End) In the **Administration** tab, click the **Tools** pane and select the **XMG/MGL/MGR > Import** sub-folder.
   The **Mega File Import - Parameterization** page appears.
   (Windows Front-End) Right-click the repository concerned and select **Object Management > Import**.
   The **Import MEGA Data** dialog box opens.
3. Alongside the **Command File** field, click **Browse** ....
4. From the **MEGA** installation folder, select in the **MEGA_Std** folder the desired Library (*.mol).
5. Click **Upload** (Web Front-End) / **Open** (Windows Front-End).
6. In the dialog **Import MEGA data**, click **Import**.
7. When import has been completed, click **Close**.

Repository Physical Backup

In event of a problem, you must have a valid and recoverable data backup.

A physical backup consists of copying the files of a repository from their original location to another one.

Data is stored at **MEGA** environment level. Data to be backed up varies according to repository server type.

☛ *See "Repository Structure", page 139.*

The following points are covered here:

Backup frequencies

For a **MEGA** environment used by an active project, **MEGA** recommends:

- daily backup of the environment
- backup before any major data update

  Example: system database customization, data reprocessing, CP/RP update of **MEGA** data.
- that you keep:
  - daily backups of the last 30 days
  - monthly backups of the last 12 months

Whatever your repository server type, **MEGA** recommends cold backup (no **MEGA** user should be connected).

☛ *In SQL server type mode, hot backup is possible.*

Elements to be backed up

Identify environments that require regular backup.

Example: design environment.

From the environment folder, you must backup complete folders:

- **Db**
- **SysDb**
- **Mega_usr**

For repositories in format:

- GBMS
  Db and **SysDb** folders contain all EMA, .EMB, .EMS and EMV files of the system database and repositories.

  ☛ *The daily physical backup should include at least the .EMB, .EMS and .EMA files of the GBMS repository.*
- RDBMS
  Db and **SysDb** folders contain an .EMV file and (respectively) an .EMO .EMQ .EMY file that points to other folders that you must back up:
  - for Oracle:
    system database and repository schemas.
  - for SQL Server:
    system database and repository databases.

GBMS format repository recommendations

To obtain a valid backup, ensure that files are not accessible during backup:

1. Access environment options.

   ☛ *See "Modifying options at environment level", page 368.*
2. In the tree, select the **Options\Repository** folder.
3. In the right pane, for option **Authorize dispatch for the environment**, select "Prohibit".

Elements that can be excluded from the backup file

To save space and time it is not necessary to back up the complete content of the environment folder. You need not back up for example folders that contain:

- user work files
  These files are contained in the **SysDb\USER** and **Db\USER** folders.
- work files linked to the Administration application
  These files are contained in the **SysDb\WORK** and **Db\WORK** folders.
- lock files:
  - **Systemdb.Lock** contained in **SysDb** folder
  - **RepositoryName.Lock** contained in **Db\<RepositoryName>** folder

Other elements to be backed up

MEGA recommends that you back up folders concerning:

- configuration:
  the **Cfg** folder (in the **MEGA** installation directory) containing the **megasite.ini** configuration file.
- licenses:
  the file containing licenses (.Must or .ELF).

(Optional) You can back up folders concerning:

- your java customization:
  lib_usr folder (in the **java** folder of the **MEGA** installation directory)
- your installation customization:
  Mega_Usr folder
- your delivered data
  in the **MEGA** installation directory, the following folders:
  - **Document**, which contains shared documents
  - **Intranet**, which contains the Web sites generated
  - **Approve**, which contains detached documents.

Elements that could be useful to back up

You may need to back up:

- private workspaces in progress
- technical data modifications in progress

To back up private workspaces in progress:

1. copy the "RepositoryName.Transactions" folder in the repository folders tree.

   ☛ *The **USER** and **WORK** folders contain the work documents of users.*

To back up technical data modifications in progress:

1. copy the **SysDb** folder and its sub-folders in the tree of the *system repository*.

Checking and Physically Restoring a GBMS Repository

This section describes how to:

- check a GBMS repository
- physically restore a GBMS repository.

☛ *A repository should be physically restored only in the event of system failure or to check that the backup is valid.*

Checking a GBMS repository

To facilitate the decision on repository reorganization, breakdown of volumes in the repository is presented during the check.

A repository check enables physical and logical verification of the repository on the main data storage file (.EMB extension). A repository check consists of:

- reading the file block by block
- checking the data
- checking all data indexing mechanisms contained in these data blocks.

As well as this physical integrity check, repository check gives a full technical report that can help the administrator decide whether or not to *reorganize* the repository to improve data access times (slow diagram loading, slow workspace opening, etc.).

To start the check:

1. Connect to **MEGA Administration** and select the repository concerned.

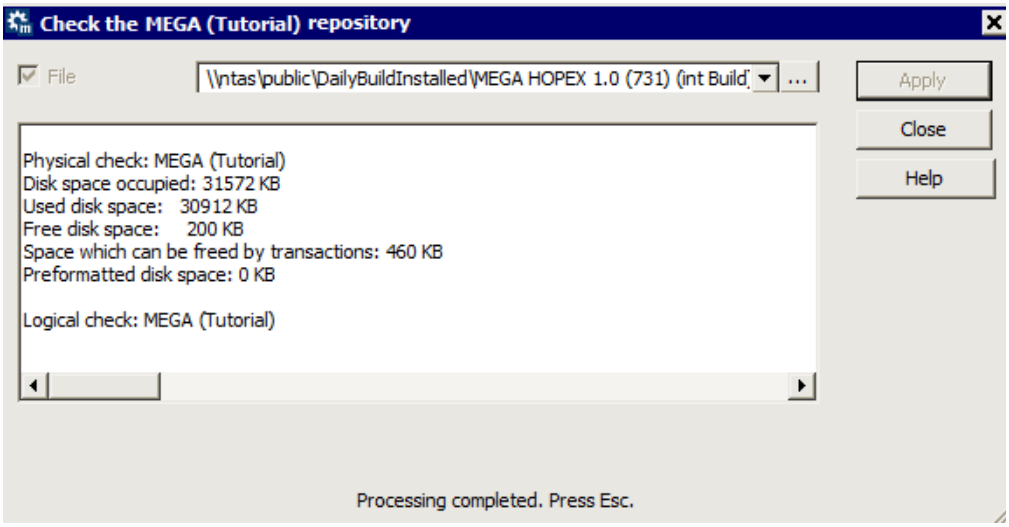
   ☛ *See "Accessing Repositories", page 138.*

2. Right-click the repository and select **Check**.
   The **Repository Check** dialog box opens.
3. (Optional) Select the **File** option if you want to create a report file.
   By default when you run a check at level:
   - of a "Test" repository, the Testxxxx.txt file is generated in the Test folder (eg: MyEnvironment\db\test).
   - of the "systemdb" system repository, the SystemDb0000.txt file is generated in the sysDb folder (eg: MyEnvironment\SysDb).

   No writing access should occur during this process.

   This repository check does not check private workspaces. It does not detect defective private workspaces.

4. Click **Apply** to start checks.
   The report is displayed in the dialog box.



The following table explains the meaning of the different disk spaces used:

Type	Definition
Disk space occupied	Physical size of repository data file (.EMB). Sum of the used, free, reserved and freeable space. This space is not limited.
Disk space used	Disk space used by data limited to 4 GB.
Free disk space	Free disk space for consumption by progressive updates.
Freeable space by private workspaces	Space required for multi-user management and not compressible while older private workspaces remain (see "Managing Private Workspaces", page 185).
Reserved space	Space temporarily reserved for updates without validation (generally zero).

From a physical standpoint, a repository is usually divided into four parts if it has never been reorganized:

- 80% usable space
- 10% or less free space
- 10% or less space that can be freed by private workspaces
- 0% preformatted space

> ☺ *We recommend that you reorganize the repository when the space occupied by its logical backup represents less than 3 times the disk size*

occupied by the repository itself or when space used by the data represents less than 20% of disk size occupied.

For more information on repository reorganization, see "Reorganizing a repository", page 160.

Physical restore

A physical restore consists of copying previously saved repository files.

The following table shows different problems that may impact your repository. If any of these problems occur, you may have to *restore* your repository.

Cause	check
Problems of disk integrity	The following system tools can detect errors on your disk: - Run the Scandisk utility if Dos > V6 or Win95 - Run the server utility if server disk
Server saturation (lack of space, disk controller failure)	- Consult the server log. Other applications are also encountering errors.
Server disk controller is operating incorrectly	- Consult the server log. Other applications are also encountering errors.

Restore the *lock* file only if restoring recent files.

Reorganizing a repository

You can reorganize a repository:

- to optimize storage space and GBMS repositories performance.

  ☛ *This space increases rapidly when users begin accessing and updating the repository.*

- when you want to change storage type, for example: from GBMS repository to Oracle repository.

Before reorganizing a repository, you must check that there is no other active or passive private workspace on this repository, see "Workspace Administration", page 200.

The repository reorganization process is automated. It consists of:

1. physical backup of repository files (GBMS only).
2. logical backup of the repository, to obtain the *command file* which contains creation orders of repository objects and their links.
3. repository initialization.
4. repository restore by import of the command file in an empty repository.

Recommendations concerning GBMS repositories

Repository reorganization frequency depends on activity (dispatch frequency, number of users, functionalities used, etc.)

MEGA recommends that you:

- reorganize your repository:
  - twice a month for configurations of more than 100 users.
  - once every two months for smaller configurations.
- not forgetting to also reorganize the system repository SystemDb.

Reorganizing a repository

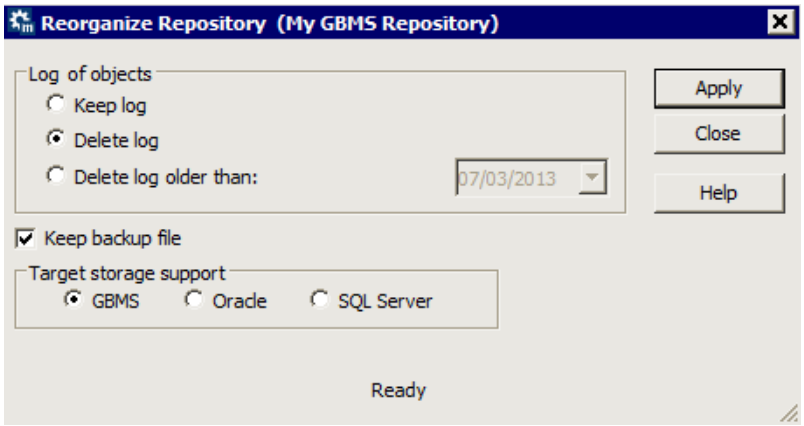
☺ *To improve reorganization times and performance of **MEGA**, remember to delete old log elements before repository reorganization.*

To reorganize a repository:

1. Connect to **MEGA Administration** and select the repository concerned.

   ☛ *See "Accessing Repositories", page 138.*

2. Right-click the repository concerned and select **Reorganize**.



3. (Optional) In the **Log of objects** frame, you can select the actions to be executed on the log at reorganization.
4. (Optional) If you do not want to keep the repository log, clear **Keep log**.

   ☛ *The log is generated in the work folder WORK of the repository, in format Bkp_<YYYY-MM-dd_HH.mm.ss>_<repository name>.mgr*

   ☛ *By default, the target server type is the same as the repository server type.*

5. Click **Apply**.
   When the repository has been reorganized, a reorganization completed message is displayed.

Repository Logical Backup

Before you make a repository backup, dispatch all current private workspaces so that their changes are included in the backup. To view private workspaces active on your repository, use the private workspaces administration tool, see "Workspace Administration", page 200.

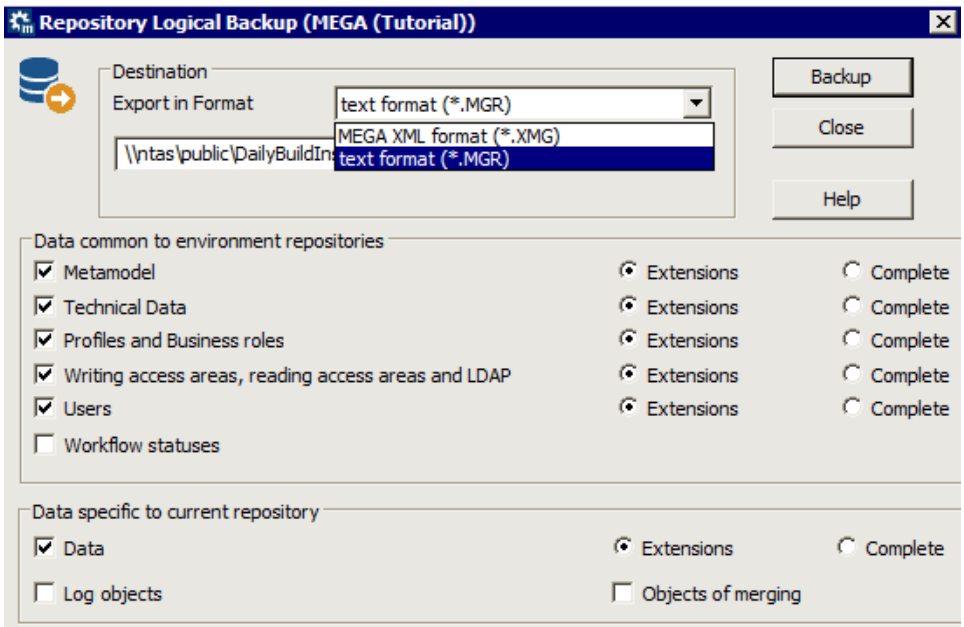
Logical *backup*:

- creates a *command file* that allows you to reconstruct the repository by update of an empty repository.
- analyzes all repository content.
- is safer than a physical backup since it checks that all data in the repository is readable.
- can be used as a long term archive or to merge repositories.

> **You can execute updates on the repository after starting logical backup by dispatching a private workspace. Note, however, that these modifications are not included in the backup.**
>
> ☺ *You can temporarily prohibit users from updating the repository by clearing the **Authorize Dispatch** option in the environment or user options.*

To execute a logical backup of a repository:

1. Connect to **MEGA Administration** and select the repository concerned.
2. Right-click the repository concerned and select **Logical Backup**.
   The **Repository Logical Backup** dialog box opens.



3. In the **Destination** frame, select the export format of the backup file:
   - **text format** (*.MGR).

     ☺ *For more details on .MGR file syntax, see "Command File Syntax", page 349.*
   - **MEGA XML format** (*.XMG)
     This format is reserved for exchange of data between **MEGA** and other applications. It includes commands or data (objects and links).
     This format cannot be used to extract the metamodel or technical data.

     ☺ *For more details on MEGA XML data exchange format, see technical article **MEGA Data Exchange XML Format EN**.*

     ☛ *Environment options enabling configuration of **MEGA** data export (XMG encoding, default export format, etc.). See "Managing Options", page 365.*

4. (Optional) In the **Destination** frame, click **Browse** ... to browse the folder tree and modify the name and/or location of the backup file.
   By default, the backup creates a file "RepositoryName.mgr" in the WORK *work folder*.

   ☛ *We recommend that this backup be made to a physical device other than the device on which the repository is located. Selection of a different logical device, such as a different partition on the same disk, does not protect your backup in the event of disk failure.*

5. Select the type of data you want to save.

   ☛ *The **Extensions** buttons correspond to data created by users.*

   💣 **Carry out a complete backup only if technical support asks you to do so.**

   ☺ *You can choose what you want to save: extensions common to environment repositories and data specific to current repository. It is recommended that you save all these elements in separate specific files, with names indicating their contents.*

   ☛ *For a standard logical backup, simply select the **Data** and its **Extensions**.*

   In the frame **Data common to environment repositories**, select the data type of the system repository to be saved:
   - **Metamodel** allows extraction of the *metamodel*, if the standard metamodel has been modified.
   - **Technical Data** allows extraction of data such as *descriptors*, *queries*, and *report templates (MS Word)*.

     💣 **A complete logical backup of the repository including the Technical Data can take time and occupies considerable space.**
   - **Profiles and Business roles** allows extraction of created profiles and business roles (those not provided by MEGA).
   - **Writing access areas, reading access areas and LDAP** allows extraction of created writing and reading access areas (those not

provided by MEGA) and LDAP parameters (parameters, servers, groups).

- **Users** allows extraction of created users (persons, person groups, logins).
- **Workflow statuses** enables extraction of workflows (workflow instances, transitions and statuses, tasks, validations, requests for change).

In the frame **Data specific to current repository**:

- **Data** allows extraction of repository data. This data includes assignment of business roles to persons.
- **Log objects** allows you to include object histories in the extraction of **MEGA** data.

  ☛ *For more information on object logs, see "Viewing Object History", page 177.*

- **Objects of merging** allows you to export technical objects resulting from merging objects (_TransferredObject).

  ☛ *For further information on merging objects, see "Merging Two Objects", page 277.*

6. Click **Backup** to start backup.
   During execution of backup, a series of messages keeps you informed of progress.
   The backup report is displayed in the **Report** area.

   ☛ *For more information on this file, see "Viewing the Environment Report File", page 173.*

To update a repository, import the repository backup file.

☛ *For more details on importing a command file, see "Updating a Repository", page 167.*

Duplicating a Repository

See:

- "Duplicating a GBMS repository", page 164
- "Duplicating an Oracle repository", page 165

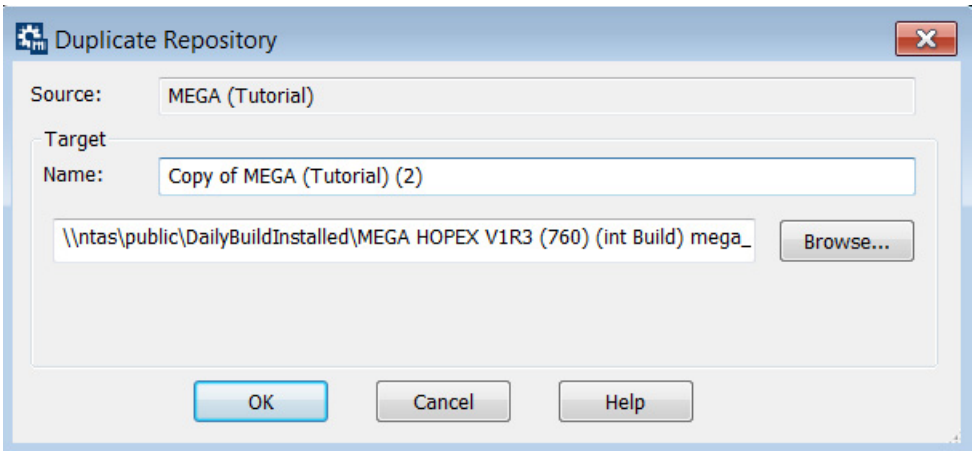
Duplicating a GBMS repository

Prerequisite: before duplicating a repository, check that there is no other active or passive private workspace on this repository, see "Workspace Administration", page 200.

To duplicate a GBMS repository:

1. Connect to **MEGA Administration** and select the GBMS repository concerned.

2. Right-click the repository concerned and select **Duplicate**.
   The **Duplicate a Repository** dialog box appears.



   The name of the **Source** repository is indicated.
3. In the **Name** field of the **Target** frame, enter the name of the repository to be created.
4. (Optional) Click **Browse** to select the location where the repository will be created.
5. Click **OK**.

Duplicating an Oracle repository

> ☛ *For detailed information on duplicating an environment and an RDBMS repository, see the **RDBMS Environment Duplication** technical article. Also see the **RDBMS Installation Guide** deployment guide.*

Prerequisite: before duplicating a repository, check that there is no other active or passive private workspace on this repository, see "Workspace Administration", page 200.

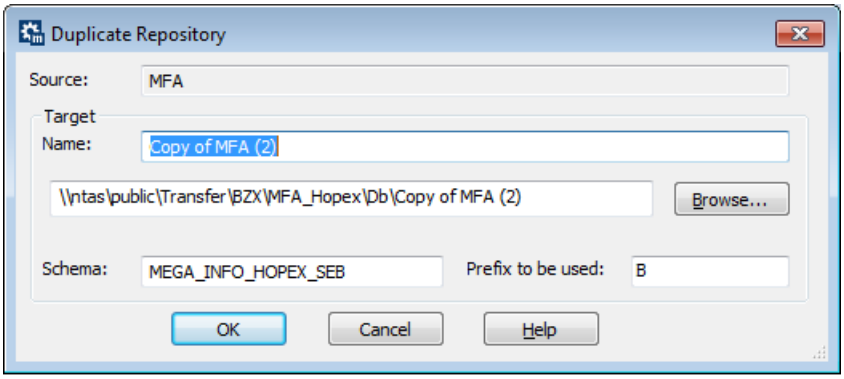
To duplicate an Oracle repository:

1. Connect to **MEGA Administration** and select the Oracle repository concerned.
2. Right-click the RDBMS repository concerned and select **RDBMS Administration > Duplicate Oracle Storage**.
   The **Duplicate a Repository** dialog box appears.
   The name of the **Source** repository is indicated.
3. (Optional) In the **Name** field of the **Target** frame, modify the name of the repository to be created.
4. (Optional) Click **Browse** to select the location where the repository will be created.
5. (Optional) In the **Schema** field, modify the schema.

   > ☛ *The source schema is used by default. You should use a different schema for a different repository.*

6. (Optional, if you have kept the name of the source schema) In the **Prefix to be used** field, enter a prefix to distinguish the source schema from the target schema.

   ☛ *The prefix must start with an alphabetic character.*



7. Click **OK**.
8. In the connection window, enter the password to access Oracle.
9. Click **Test connection**.
   You must validate the test before continuing the procedure.
10. Click **Test GRANTs**.
    You must validate the test before continuing the procedure.
11. Click **OK**.
    The repository is duplicated.

Initializing an Existing GBMS Repository

To reinitialize a GBMS repository:

1. Connect to **MEGA Administration** and select the GBMS repository concerned.
2. Right-click the repository concerned and select **Initialize**.
   This empties the repository of its data so that a backup can be reinserted, for example.
   A message box asks for confirmation.
3. Click **Yes** to confirm reinitialization.

   💣 **This operation deletes all repository data irreversibly.**

   ☺ *Initialization of the GBMS repository, as well as repository reorganization, keeps the absolute identifier of the processed repository. This can be useful if you use the absolute identifier of your repository in a macro or query.*

   💣 **Repository reinitialization does not keep repository configuration options. You must update configuration of the newly-initialized repository.**

Updating a Repository

Importing command files

You can update a repository by importing the command file produced by the repository backup tool, export of an object or any other means of command file production.

You can import two types of command file into a **MEGA** repository:

- **text format** (.MGR).

  ☛ *For more details on .MG* file syntax, see "Command File Syntax", page 349.*

- **MEGA XML format** files. 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**.*

To import a command file:

1. Connect to:
   - the **MEGA Administration** desktop (Web Front-End).

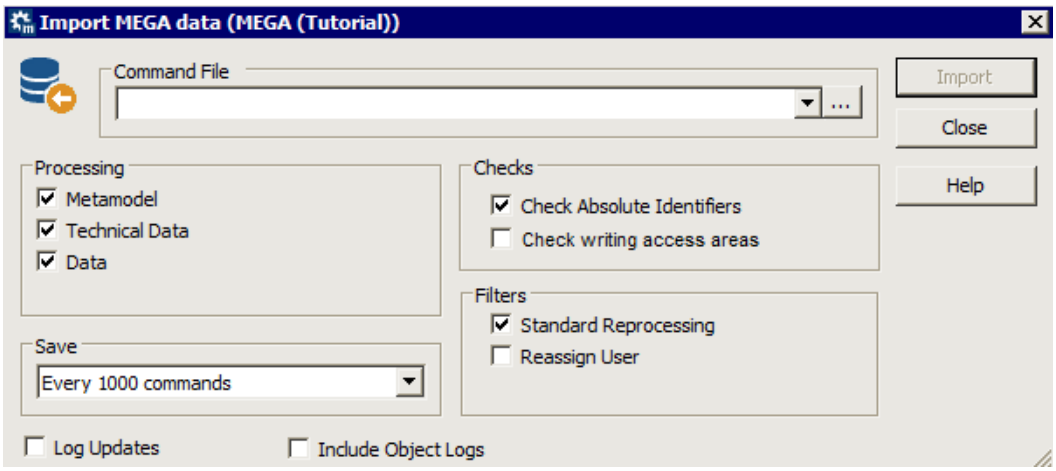
     ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

   - **MEGA Administration** (Windows Front-End) and select the repository concerned.

     ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. (Web Front-End) In the **Administration** tab, click the **Tools** pane and select the **XMG/MGL/MGR > Import** sub-folder.
   The **Mega File Import - Parameterization** page appears.
   (Windows Front-End) Right-click the repository concerned and select **Object Management > Import**.
   The **Import MEGA Data** dialog box opens.

   ☛ *To import a command file from **MEGA**, select **File > Import > MEGA File**.*



3. In the **Command File** frame, click **Browse** ... to browse the folders and select the backup file.
4. (Web Front-End) Click **Upload**.
5. Select the types of **Processing** to be executed:
   You can update:
   - the **Metamodel** (repository structure)
   - the **Data** (most frequent case)
   - the **Technical Data** (*descriptions*, *requests*, as well as *users*).

     ☛ *If the file includes commands that do not match the type you have selected, these commands are ignored.*
6. 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.*
   - ***Every 5000 commands**: each save is quite long. You can speed things up or slow them down by saving **every 100, 200, 500, 1000** or **5000 commands**.*

   ☛ *Large files may cause memory problems when updating. To avoid such problems, you should decrease the intervals between saves.*

7. In the **Checks** frame, the checks to be carried out are selected automatically, based on the file extension:
   - **Check Absolute Identifiers** is not selected in the case of a command file that does not come from a **MEGA** repository.
   - **Control writing access areas** is selected when the **MEGA 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.*
8. In the **Filters** frame, select the import behavior to be applied:
   - **Standard Reprocessing** changes creation of an already existing object into a modification, or into creation of an object of the same name preceded by a number if their absolute identifiers are different.
   - **Reassign User** ignores the writing accesses contained in the imported file. All elements in the imported file are given the same writing access level as the user executing the import. This is useful when you have the **MEGA 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.*
9. (Optional: **Windows Front-End**) Select the **Log Updates** option if you want to update the *repository log*, if this log will be exported to another workstation without the file being imported.

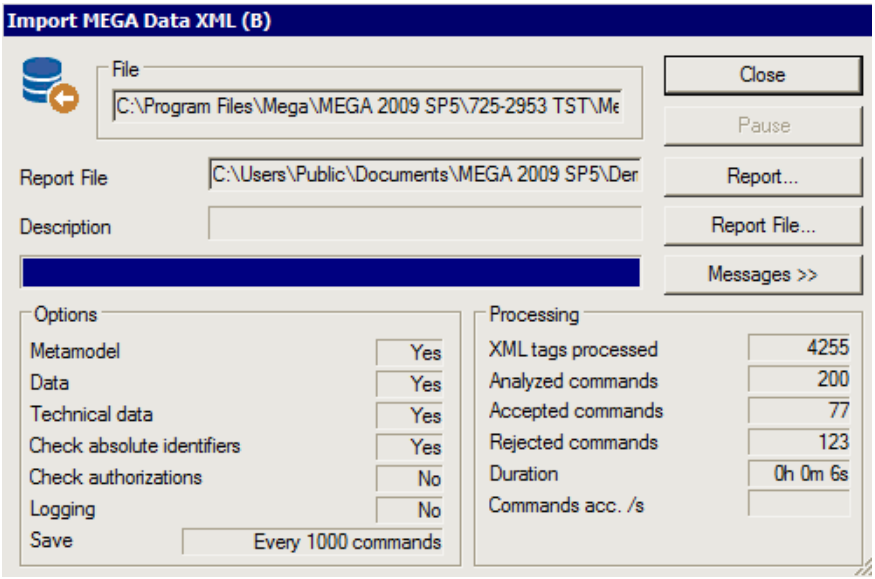
   This option is an advanced operation, MEGA recommends that you contact MEGA support before selecting this option.
10. (Windows Front-End) Selecting **Include Object Logs** allows you to also import object histories.

    ☛ *For more information on object logs, see "Viewing Object History", page 177.*

    The options you select are controlled by the software, based on the file extension and the standard processing to be applied. If your choices are not consistent with the file extension, a message box informs you of this fact and its possible consequences.

    ☛ *For more details on the main causes of rejects, see "Dispatch Conflicts", page 192 and "Rejects When Dispatching", page 193.*

11. Click **Import**.
    (Web Front-End) The report page appears.
    (Windows Front-End) The report window appears showing the import progress.



    (Windows Front-End) The **Processing** frame details the number of commands accepted and rejected.

When the import contains errors:

- a reject report file is generated.

  ☛ *See "Viewing rejects", page 170.*

- (Windows Front-End) an execution report file is available.

  ☛ *See "Viewing the environment report file (Windows Front-End)", page 172.*

Viewing rejects

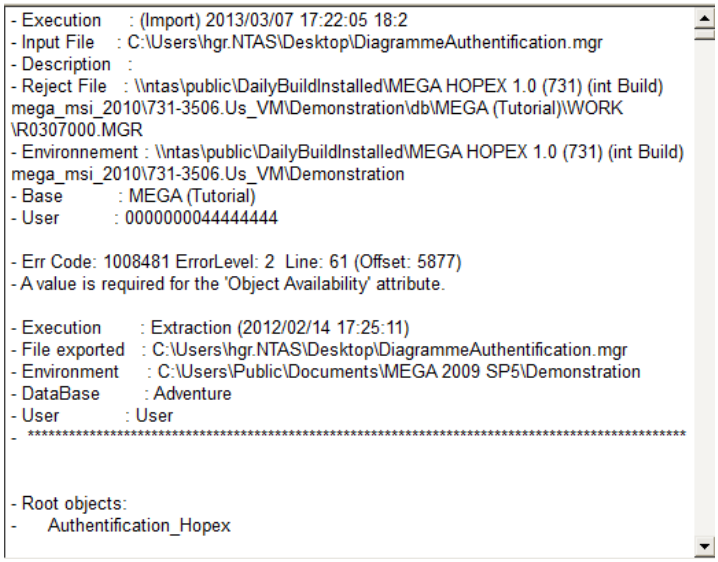
To view the rejects (or errors) recorded during the import of the command file:

- (Web Front-End) In the **Report** frame, click the arrow in the **Report File** field and select **Open**.
- (Windows Front-End) Click the **Report File** button.

  ☛ *The contents of the report file depend on import options. For more details on importing a command file, see "Managing Options", page 365.*

Case of a text file import (MGR, MGL)

The report file appears and details all the rejects.

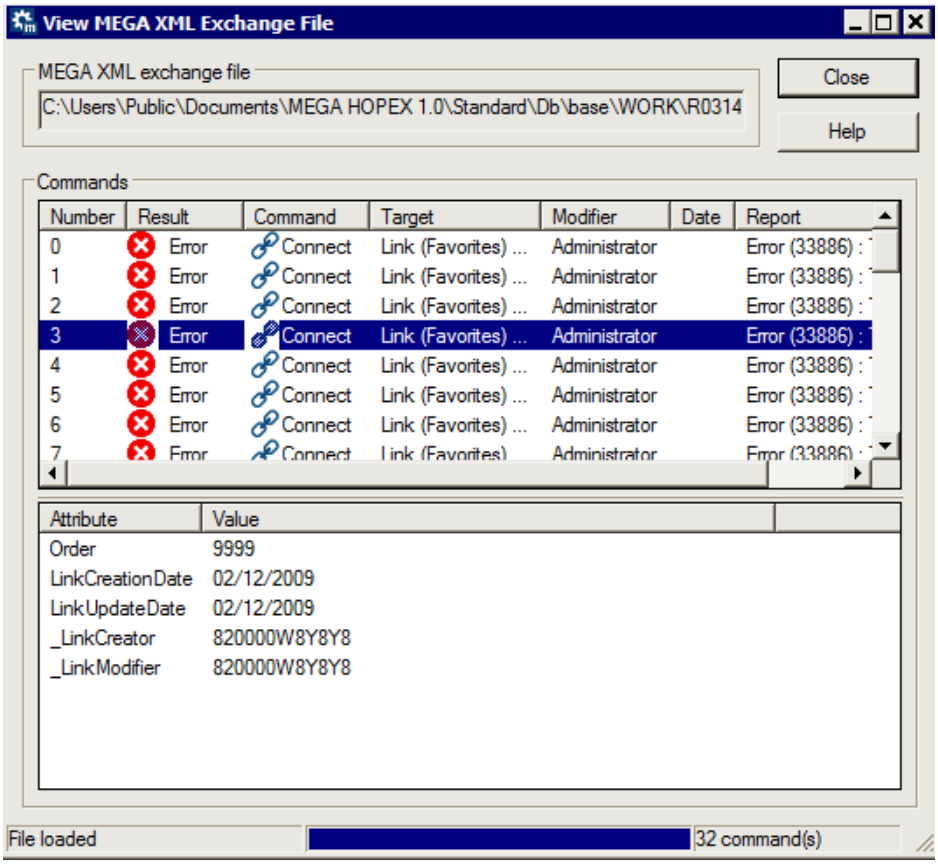


Example of rejects file at MGR file import

Case of a MEGA XML import (Windows Front-End)

The view window for the report file appears and details the **Commands** contained in the imported file and the **Result** of execution of each command:

- ***Accepted***: the command is accepted
- ***Rejected***: the command is rejected
- ***Warning***: the command is accepted, but contains errors



Viewing the environment report file (Windows Front-End)

To view the import execution report:

1. Click **Report**.
   The report details the number of commands analyzed, executed and rejected for each command type.

Viewing the Environment 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.

After you have executed backup and restore operations on a repository, you can view the environment *report file*.

Viewing the environment report file

To open the environment report view window:

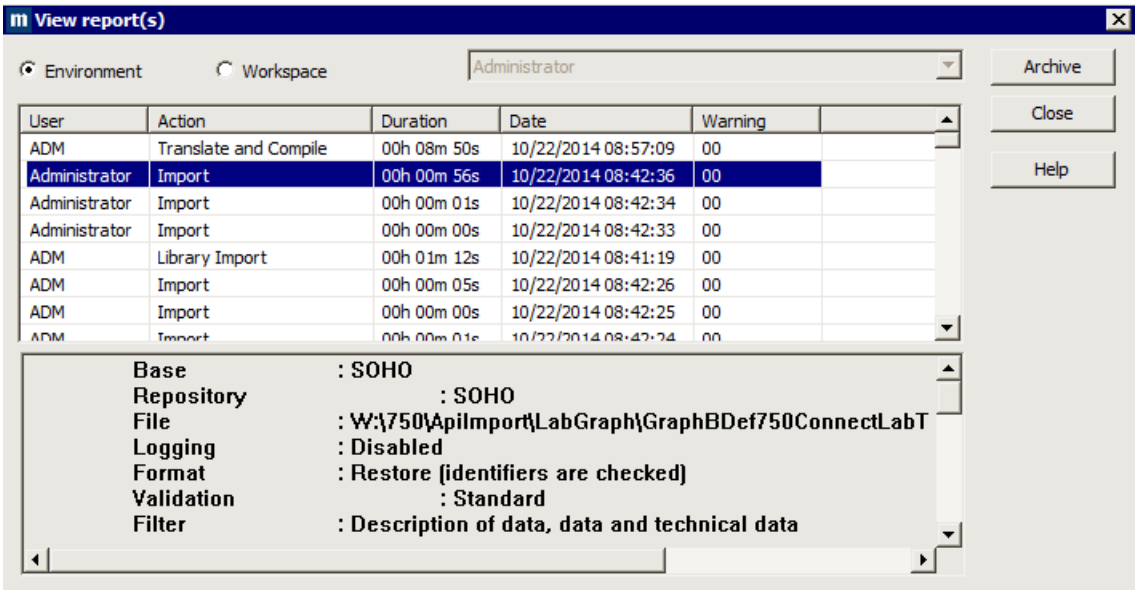
1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. Connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

3. Right-click the environment and select **Reports > Open**.



This dialog box also allows you to view report files of each user of the environment. Indicated for each action are:

- **User** who executed the operation.
- **Action** executed: dispatch, import, installation, translation, export, derivation, extraction, backup, update, user diagram extraction, user diagram import, repository translation, repository or environment check,

repository creation, repository deletion, log initialization, object protection, etc.
- **Date** the operation began.
- **Duration** of the operation.
- return code in the **Warning** column:
  - Error level 0: no error.
  - Error level 2: minor errors such as attempts at creating already existing objects or links.
  - Error level 4: the actions involved nonexistent objects or links.
  - Error level 8: a system error was encountered during the update.
  - Error level 16: update aborted because of a problem such as insufficient disk space.

when you select an action, the lower frame displays:
- the repository concerned
- the file used
- details of the action.

Copying the environment report file

To copy and reinitialize the environment report file:

1. In the **View Report(s)** window (see "Viewing the Environment Report File", page 173), click **Archive**.
   A confirmation request message appears.
2. Select **Yes**.

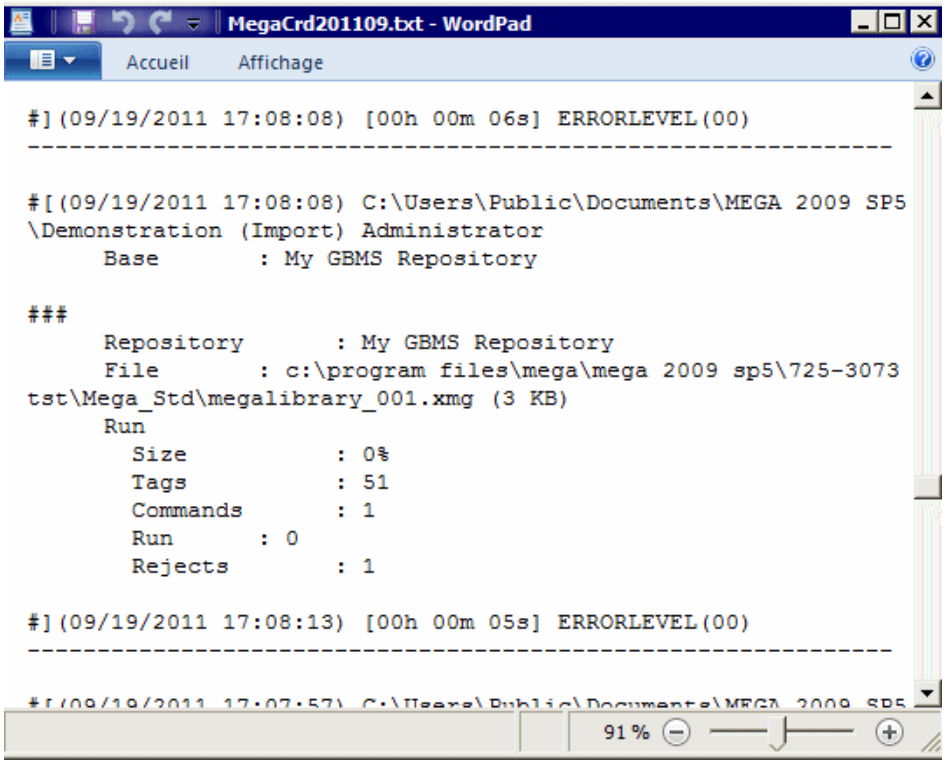
   ☛ *You should reinitialize this file (or archive with the network version) from time to time.*

Opening the environment report file

To open the "MegaCrdYYYYmm.txt" file with Wordpad:

1. From the explorer, localize the "MegaCrdYYYYmm.txt"" file in the environment folder.

2. Right-click the file and select **Open with > Wordpad**.



Viewing User Process Error Trace Files

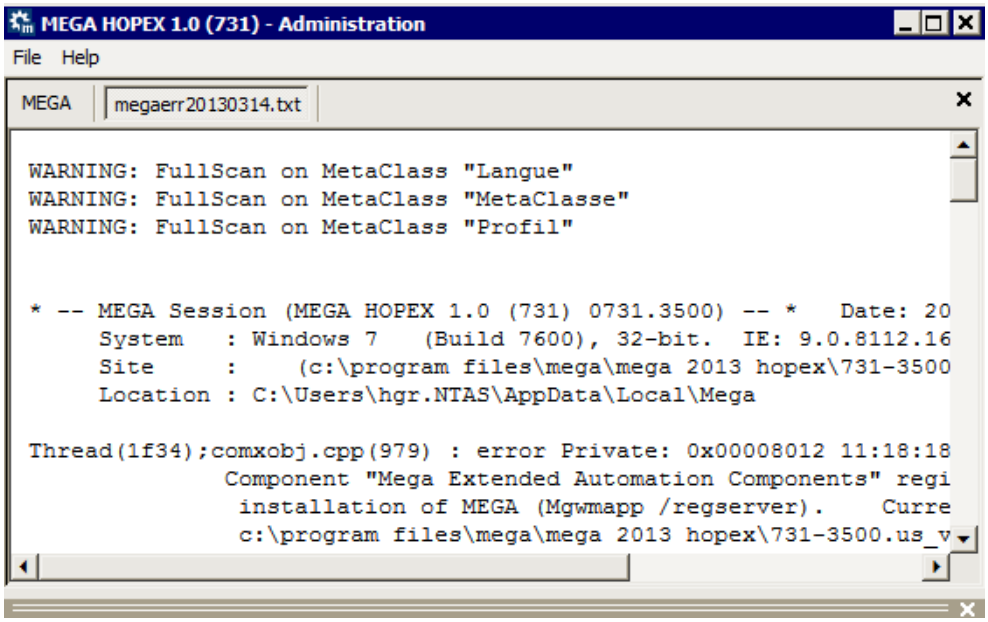
Trace files of errors in user processes contain information on operations executed and possible anomalies.

If there is a problem with a repository, this file will help the **MEGA** Research Center to analyze it.

Each *trace file* has the following characteristics:

- format: *.txt
- name: megaerrAAAAmmJJ
  where YYYYmmDD represent the year, month and day when the file was generated

  ```
  Example: file Megaerr20110204.txt was generated on 04
  February 2014).
  ```
- information on errors:
  - date and time of the error
  - action that produced the error
  - associated error message



You can open the trace file from:

- **MEGA Administration**
- the **Mega Server Supervisor** tool
- **MEGA**

Opening the trace file from MEGA Administration

To open the trace file from **MEGA Administration**:

1. Start **MEGA Administration**.
2. In the navigation tree, right-click **Workstation** and select **Trace File > Open**.
   The file is opened in the main pane of the window.

Opening the trace file from the Mega Server Supervisor tool

To open the trace file from the **Mega Server Supervisor** tool:

1. (Prerequisite) The **MEGA Server Supervisor** tool is started, see "Starting Mega Server Supervisor", page 244.
2. In your workstation system tray, right-click **MEGA Server Supervisor** and select **Mega Logs > Open Daily Logs**.

Opening the trace file from MEGA

To open the trace file from **MEGA**:

1. In the **MEGA** menu bar, select **Help > About MEGA**.
   The **About MEGA** dialog box appears.
2. In the dialog box that opens, click **System Information**.
3. In the **System Information** dialog box, select **Error Log > Edit**.

Saving the Error Zip file for Diagnostics

The **Mega Server Supervisor** tool allows you to save a zip file containing information required by the **MEGA** Research Center to help in repository problem diagnostics.

This zip file of errors contains in particular the trace files of errors related to user processes and/or SSP (megaerrAAAAmmJJ.txt and ssperrAAAAmmJJ.txt).

Prerequisite: **MEGA Server Supervisor** is started, see "Starting Mega Server Supervisor", page 244.

To save the error zip file for diagnostics:

1. In your workstation system tray, right-click **MEGA Server Supervisor** and select **Logs > Daily Logs manager**.
2. Click **Zip**.
3. Specify a saving location and enter the zip file name.
4. Click **Save**.

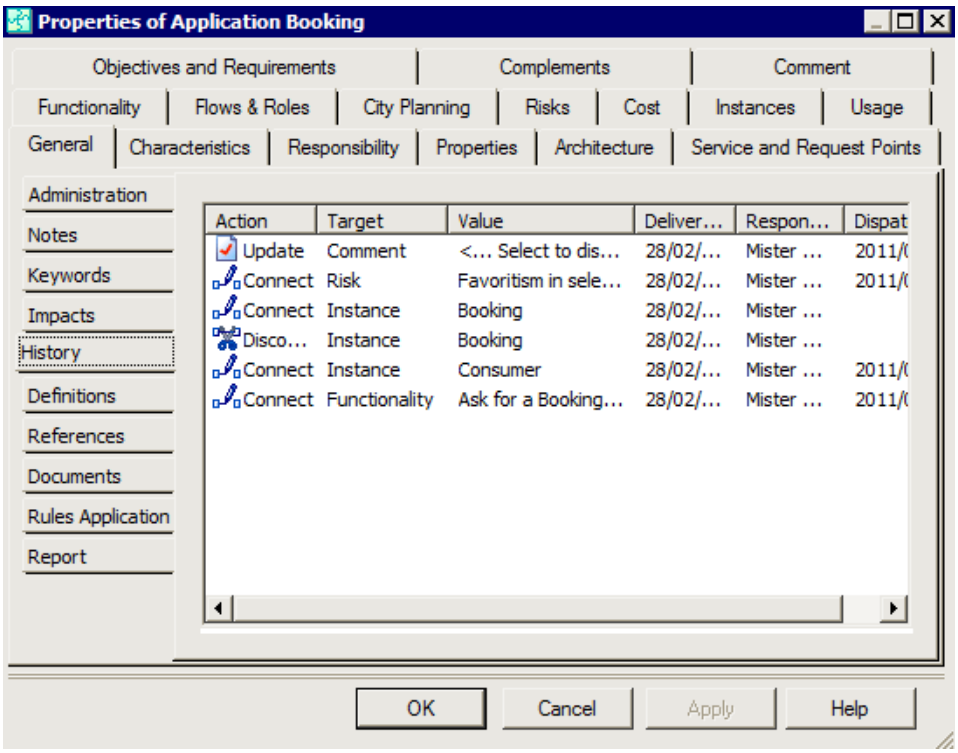
Viewing Object History

The object history is a different view of the repository log: instead of browsing actions performed by a user in a dispatch, the object history shows actions carried out from an object for all dispatches and users.

> ☛ *The repository log must be enabled so that the object history can be supplied, see "Enabling the repository log", page 149.*

In the properties dialog box of an object, the **History** subtab of the **General** tab gives an overview of actions on each object in the repository. At each update

concerning the object (Create, Modify, Connect, Disconnect), the corresponding action is added to the list.



OPTIMIZING REPOSITORY ACCESS PERFORMANCE

To optimize the performance of **MEGA**, you must also remember to optimize your repository size. You must:

- reduce the log size
  - ☛ *See "Managing Log Size", page 179.*
- increase the cache size
  - ☛ *See "Increasing RDBMS cache size (memory)", page 184.*
- delete temporary data and history data (RDBMS repository) regularly
  - ☛ *See "Deleting RDBMS Repository Temporary and History Data", page 187.*
- perform regular maintenance tasks of RDBMS repositories
  - ☛ *See "Performing regular maintenance tasks (RDBMS repository)", page 187.*
- reduce quantity of status indicators
  - ☛ *See "Managing Status Indicators", page 186.*
- reduce quantity of locks
  - ☛ *See "Managing GBMS Repository Locks (Windows Front-End)", page 187.*
- clean up repository
  - ☛ *See "Cleaning up a Repository", page 188.*
- configure anti-virus actions
  - ☛ *See "Configuring the Anti-Virus According to MEGA Data", page 189.*
- reorganize repository
  - ☛ *See "Reorganizing a repository", page 160.*

Managing Log Size

☛ *Managing the log size is only necessary if you have enabled the repository log, see "Enabling the repository log", page 149.*

To reduce the log size, you can:

- delete or consolidate all the log commands earlier than a selected date
  - ☛ *See "Deleting a log or reducing the log size", page 180.*
- (SQL Server) select and delete log elements, earlier than a selected date
  - ☛ *See "Deleting log elements to reduce the log size (SQL server)", page 182.*
- modify MetaClass loggability
  - ☛ *See "Modifying MetaClass loggability", page 183.*

Log size management frequency

You must reduce the log size:

- every month, for configurations of less than 50 users.
- every week, for configurations of more than 50 users.

Deleting a log or reducing the log size

To delete a log or to reduce its size:

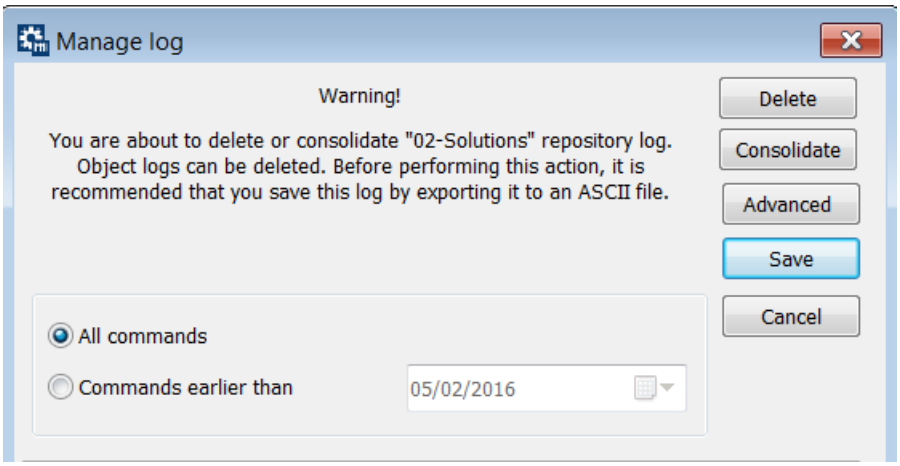
1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. Connect to the environment in which the repository is referenced.

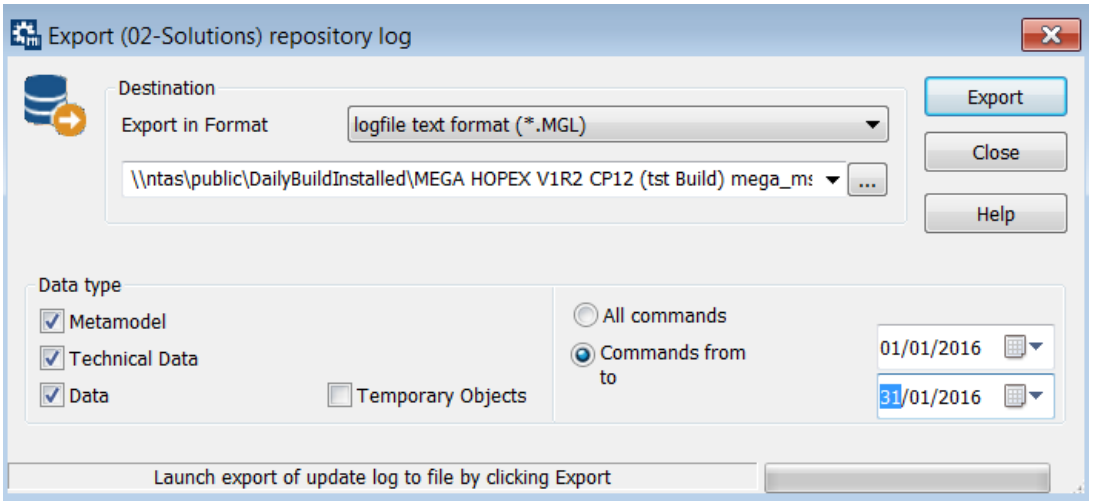
   ☛ *See "Connecting to an Environment", page 5.*

3. Expand the **Repositories** folder.
4. Right-click the repository and select **Repository Log > Manage Repository and Object Log**.
   The **Manage Log** dialog box opens.



5. Before deleting your log (complete or partial deletion), **MEGA** recommends that you back up your log.
   - Click **Save**.

   The **Export repository log** dialog box opens.



For more details on how to specify log export information, see "Exporting Your Private Workspace Log", page 211.

☺ *Select the option **Commands from** "selected date" **to** "selected date".*

There is no duplication of backup and you save backup time and size.

Select a starting date (From) corresponding to the end date of your last backup, and select the ending date (To) you require.

   - Click **Export**.

   The log backup is performed.

6. In the **Manage log** window, define the commands to be deleted. Select either:
   - **All commands** or
   - **Commands earlier than** and select the date using the drop-down menu calendar.
7. Click either:
   - **Delete** to delete all the commands contained within the selected time interval.

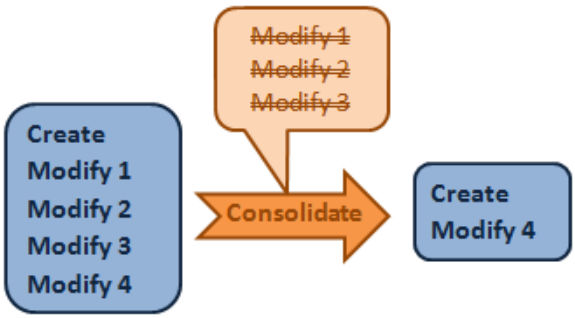
☛ *(GBMS, Oracle) If you did not follow the recommendation regarding log management frequency, this action may take a very long time, see*

"Log size management frequency", page 180.

☛ *(SQL Server) For a more specific deletion, see "Deleting log elements to reduce the log size (SQL server)", page 182.*

- **Consolidate** to delete only the intermediate commands contained within the selected time interval.

  ☺ *You can consolidate the latest information.*



Deleting log elements to reduce the log size (SQL server)

With an SQL Server repository storage, you can delete log elements more specifically: you can delete only log elements relating to specific MetaClasses, earlier than a selected date.

☛ *If you do not want to have to delete log elements you are not interested in, see "Modifying MetaClass loggability", page 183.*

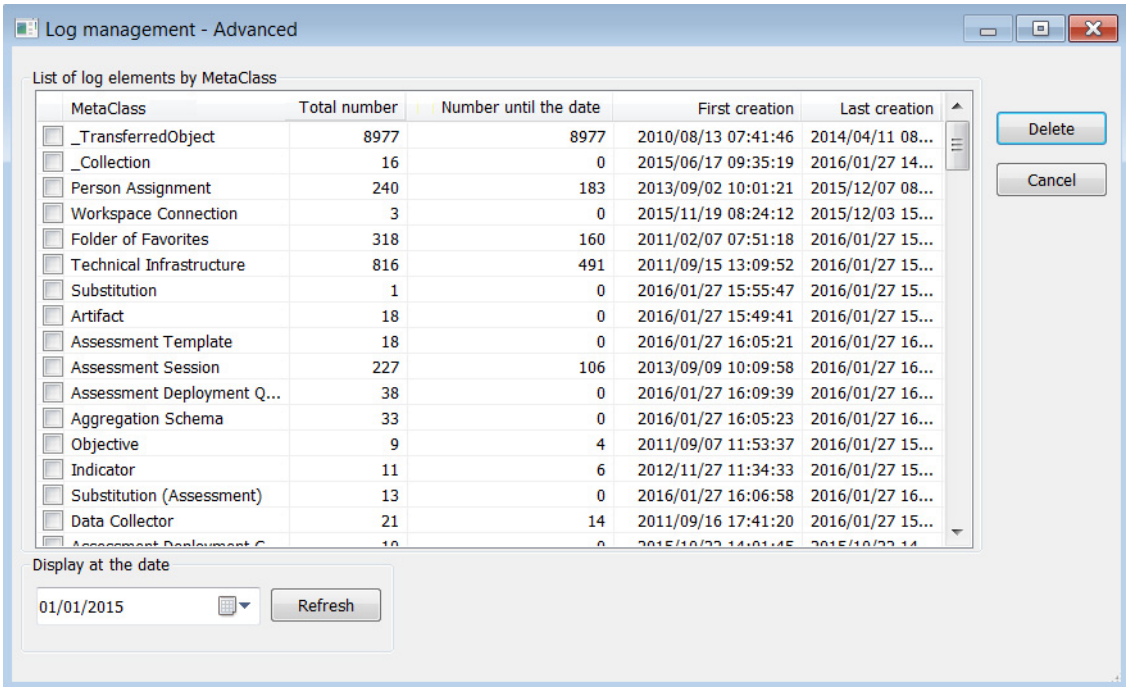
To delete log elements regarding specific MetaClasses:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*
2. Connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*
3. Expand the **Repositories** folder.
4. Right-click the repository and select **Repository Log > Manage Repository and Object Log**.
   The **Manage Log** dialog box opens.

5. Click **Advanced**.
   The **Log Management - Advanced** window shows the log element number by MetaClass and specifies the first and last creation date.



6. In the **Display at the date** pane, select the date until which you want to delete the log elements.
7. Click **Refresh**.
   The **Number until the date** column shows for each MetaClass the log element number until the selected date.

   ☺ *Click the **Number until the date** column header to sort the MetaClasses, with the most populated at the top.*
8. In the **MetaClass** column, select the MetaClass for which you want to delete the log elements until the selected date.

   ☛ *You can select several MetaClasses.*
9. Click **Delete**.
   Log elements are deleted.

Modifying MetaClass loggability

To reduce the number of objects generated in logs, you can modify logging of MetaClasses you do not want to track.

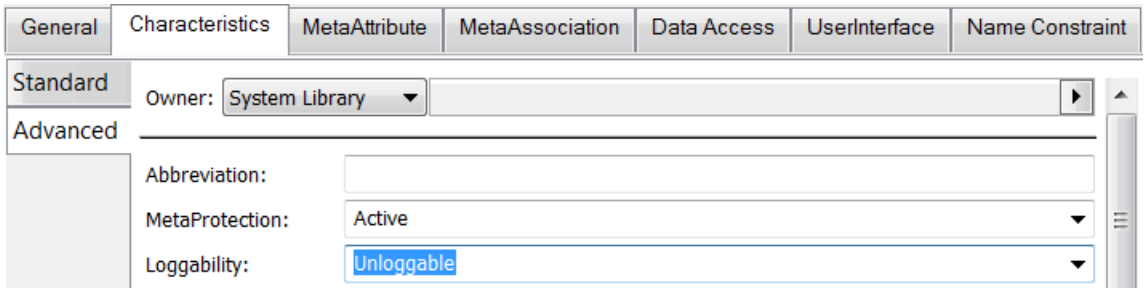
☛ *In case of inter-repository consolidations, see "Modifying the log behavior", page 150.*

To modify MetaClass loggability:

1. From **MEGA**, open the **MetaStudio** navigation window and expand folders **MetaClass > MetaModel**.

   ☛ *Or you can click **Explore** , and from the explorer find the **MetaClass** or **MetaAssociation** object.*

2. Open the properties dialog box of a **MetaClass** or **MetaAssociation**.
3. In the **Characteristics > Advanced** tab, for the loggability attribute, select **Unloggable** value.



Occurrences created, updated or deleted in a private workspace are dispatched, but certain commands are not available in object histories or in repository activity.

Managing cache in RDBMS environments

In RDBMS environments, you can:

- increase RDBMS cache size (memory) (see "Increasing RDBMS cache size (memory)", page 184)
- manage RDBMS local cache:
  - "RDBMS data local cache (files)", page 185
  - "Modify location of the RDBMS local cache files", page 185

Increasing RDBMS cache size (memory)

In RDBMS storage case, with repositories including a large amount of objects, we advise you to increase the size of RDBMS caches. The larger your cache space, the fewer the network exchanges and the better your **MEGA** performance.

To increase cache size:

1. Connect to **MEGA Administration**.

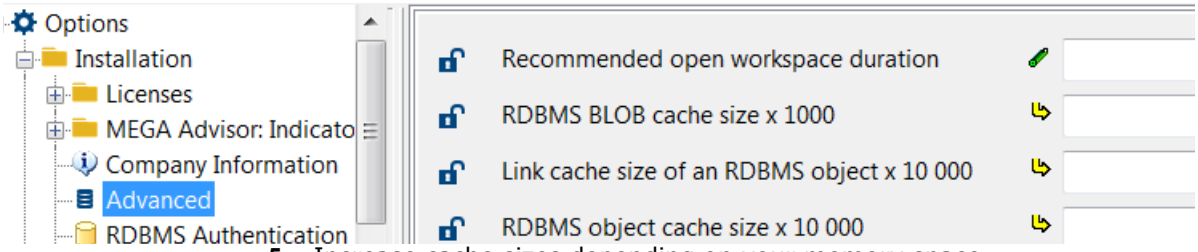
   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. Connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*

3. Right-click the environment and select **Options > Modify**.

4. In the environment options, select **Options > Installation > Advanced**.



5. Increase cache sizes depending on your memory space.

RDBMS data local cache (files)

Activate RDBMS local cache option:

- adds an additional cache level for RDBMS repository objects.
  This RDBMS local cache avoid multiple requests when multiple users are on the same repository view. Access for the following users is speed up.

  ☛ *This option is accessible from the environment options (**Options > Installation > Advanced**).*
- is selected by default.
  You must configure your anti-virus accordingly.

  ☛ *See "Configuring the Anti-Virus According to MEGA Data", page 189.*

Cache files are generated in .mgc format in **RDBMS Data cache** folder. This folder is accessible from <ProgramData>\MEGA\MEGA HOPEX 1.0\.

☛ *To modify this location, see "Modify location of the RDBMS local cache files", page 185.*

Cyphering of RDBMS local cache option enables cyphering data included in the RDBMS local cache. Selecting this option decreases the benefit of RDBMS local cache activation. In that case, balance the benefit of **Activate RDBMS local cache** option activation.

☛ *This option is accessible from the environment options (**Options > Installation > Advanced**).*

Modify location of the RDBMS local cache files

If needed you can change **RDBMS Data cache** folder location.

To modify **RDBMS Data cache** folder location:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*
2. Connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*
3. Right-click the environment and select **Options > Modify**.
4. In the environment options, select **Options > Installation > Advanced**.

5. In **RDBMS local cache path** field, enter a location.

   ☛ *For this location select a local drive that has a good access time.*

Managing Status Indicators

Use of status indicators generates large quantities of queries on repositories. Select only those indicators you require.

To modify indicator backup selection:

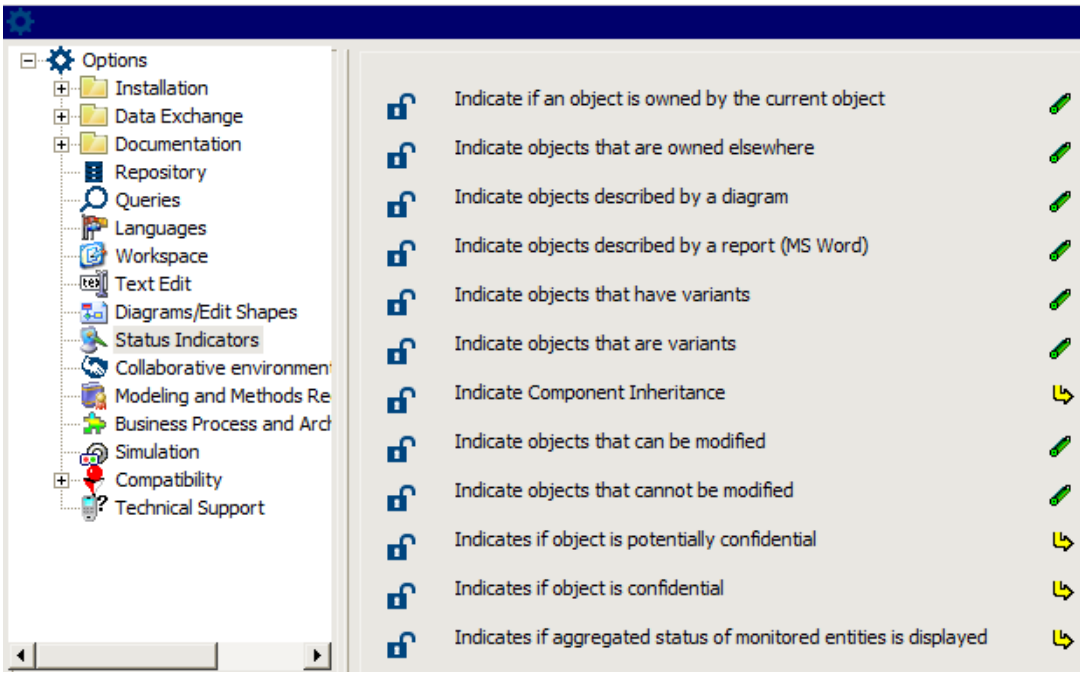
1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. Connect to the environment in which the repository is referenced.

   ☛ *See "Connecting to an Environment", page 5.*

3. Right-click the environment and select **Options > Modify**.
4. In the **Environment Options** dialog box, select **Status Indicators**.



5. In the right pane, select only those indicators you require.
6. Click **OK**.

Deleting RDBMS Repository Temporary and History Data

To prevent repository size increase and keep optimized performances, you should regularly delete data of the completed private workspaces of **MEGA** users.

MEGA recommends that you delete all RDBMS repository temporary and history data:

- every week for less than 10 users
- every evening if you have more than 10 users.

To delete the temporary and history data of an RDBMS repository, you (or your database administrator) must include the following procedures in your regular maintenance tasks:

> ☛ *To perform these procedures, see **RDBMS Repository Installation Guide** deployment guide.*

- SP_CLEAN_MEGA_DATABASE

  > ☛ *To consult the date of last private workspace cleanup (last execution of this procedure), see "Consulting and Modifying Repository Properties", page 142.*

- SP_CONSOLIDATE_MEGA_DATABASE

  > ☛ *To consult the date of last consolidation (last execution of this procedure), see "Consulting and Modifying Repository Properties", page 142.*

Performing regular maintenance tasks (RDBMS repository)

With RDBMS repositories you must include a regular maintenance plan. You (or your database administrator) should, for each repository (SystemDb repository included), perform the following maintenance tasks regularly (at least once a week):

- rebuild indexes
- update the statistics
- (optional) shrink the logs regarding the policies
- perform the stored procedures

  > ☛ *See "Deleting RDBMS Repository Temporary and History Data", page 187.*

  - SP_CLEAN_MEGA_DATABASE
  - SP_CONSOLIDATE_MEGA_DATABASE

Managing GBMS Repository Locks (Windows Front-End)

In a GBMS repository, a file is associated with each lock. When private workspaces are deleted manually, certain files may persist despite lock deletion.

A folder with more than 1000 files:

- is costly to manage for Windows
- slows down operation of **MEGA**.

To delete locks that persist, for example after deletion of a user private workspace:

- Delete locks for a user whose private workspace has been manually deleted.

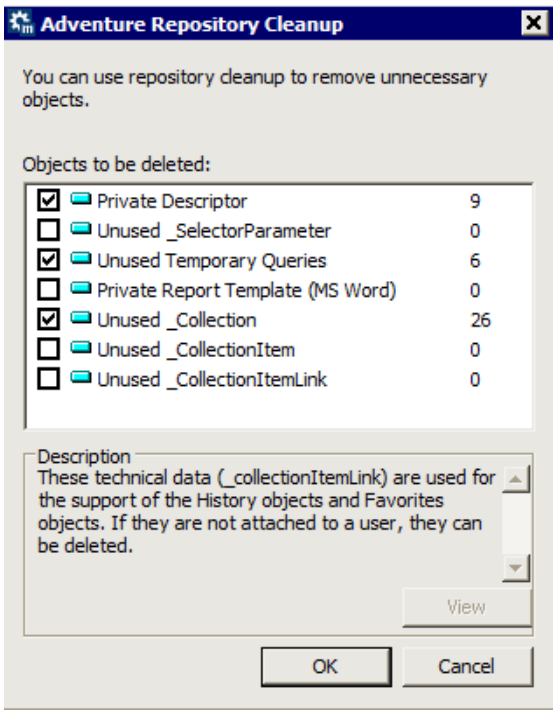
  ☛ *See "Managing Locks from Administration (Windows Front-End)", page 220.*

Cleaning up a Repository

During modeling work, handling different objects results in creation of temporary objects (temporary queries, etc.). It is probable that these objects will subsequently be unnecessary. To avoid unnecessarily increasing repository size, you can delete these temporary objects.

To clean up a repository:

1. From the **MEGA** menu bar, select **File > Properties**.
   The properties dialog box of the repository to which you are connected appears.
2. In the **Characteristics** tab, click **Repository Cleanup**.
   The **Repository Cleanup** dialog box opens.



3. Select the object groups to be deleted and click **OK**.

   ☛ *To view the content of an object group, select the group and click **View**.*

   Selected object groups are deleted from the repository.

Configuring the Anti-Virus According to MEGA Data

To optimize anti-virus activity and to avoid unnecessary slowdown, you must configure what should be managed or not by the anti-virus.

You must exclude the following files from anti-virus scanning:

	Access mode	Location	File type
Program files external to MEGA Files used by **MEGA** to display user interface elements in Web or Windows interfaces	***Read***	Program Files (x86) \ MEGA\ MEGA-STD and sub-folders	Proprietary format: ****.mgs*** (vectorial shapes in diagrams) Public formats: ****.gif***, ****.ico*** and ****.bmp***
Quick search indexes Files used by the workstation or server executing the search	***Reading*** by the workstation or node executing the search ***Writing*** by the Administration station and by the server programming index creation	<Environment folder>\Db\ <Repository name>\ <Repository name>.ix	Proprietary format: ****.ix*** (indexes) Public formats: ****.log*** and ****.dat***
Data cache Files used by **MEGA** to improve its performance In RDBMS environment, **RDBMS data cache** subfolder is automatically populated, see "RDBMS data local cache (files)", page 185	***Read/Write***	<ProgramData>\MEGA \MEGA HOPEX 1.0	Public format: ****.mgc***
Import/export files Files generated or read during import/export/logical backup processes	***Reading*** by the import function ***Writing*** by export and logical backup functions	Selected by the user	Proprietary formats: ****.mgr*** or ****.xmg***

	Access mode	Location	File type
Logfiles Files generated by **MEGA** for each repository when the **Backup Logfile** option is activated. Files generated by the Export command	***Writing***	<Environment folder>\Db\<Repository name>\ <Repository name>.transaction or <Repository name>.Log	Proprietary format: ***.mgl***
MUST license Note: if the anti-virus does not allow such a configuration, allow ***Reading/Writing*** for all of the files on the license oath and sub folders.	***Reading/Writing*** of the files on MUST license path and under this path	<Installation folder>\Cfg\megasite.ini gives the MUST License path: [must license] path=	Public format: ***.ini*** Proprietary formats: ***.tnk*** and ****.usr****
	Reading of the files on MUST license path and under this path		Proprietary format: ***.must***

REFERENCING AND UNREFERENCING A REPOSITORY

Referencing and unreferencing a repository is carried out via the drop-down menu of the repository.

See successively:

- "Referencing a Repository", page 191
- "Unreferencing a Repository", page 192

Referencing a Repository

If you have moved or copied a repository without using MEGA move or restore commands, you will have to reference the repository so that the environment recognizes it.

☛ *To reference a repository in another environment, the two metamodels must be identical.*

To do this:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. Connect to the environment in which you want to reference the repository.

   ☛ *See "Connecting to an Environment", page 5.*

3. Right-click the **Repositories** folder and select **Create reference**.
4. Several options are proposed, select for example a **Repository in MEGA format**.

   ☛ *You can also reference a repository from SQL Server or Oracle. For more details on **MEGA** repository server type, see the **MEGA** deployment guide.*

   The **MEGA Repository Selection** dialog box opens. This dialog box allows you to create a reference for a new repository in the environment.

5. Indicate where the .EMB (or .EMO, .EMQ, .EMY) file for the repository is located. The repository name is automatically indicated and cannot be modified.

The repository is accessible exactly as repositories created in the normal way.

☛ *you must save and then restore a repository to move it from one environment to another. The users and metamodel of the two environments must be defined identically so that transfer occurs without reject.*

☛ *To also copy these objects, import the missing part of the metamodel. One way of doing this is to upgrade the site or the environment. Then, import the rejected commands if you used the backup-restore procedure.*

☛ *Check that the repository is not simultaneously referenced in two different environments. Compatibility errors may occur if the environments are not identical.*

Unreferencing a Repository

You can delete a repository reference from an environment. This action does not delete the repository.

To delete a repository reference:

1. Connect to **MEGA Administration** and select the repository concerned.

   ☛ *See "Accessing Repositories", page 138.*

2. Right-click the repository of which you want to delete the reference and select **Delete Reference**.
   A message requests confirmation.
3. Click **OK** to delete the repository reference.
   The repository reference is deleted, and can be created in another environment on condition that the metamodel is identical.

   ☛ *A repository must be referenced in only one environment. It is important to check that the reference for your repository was deleted in its original environment.*

MANAGING PRIVATE WORKSPACES

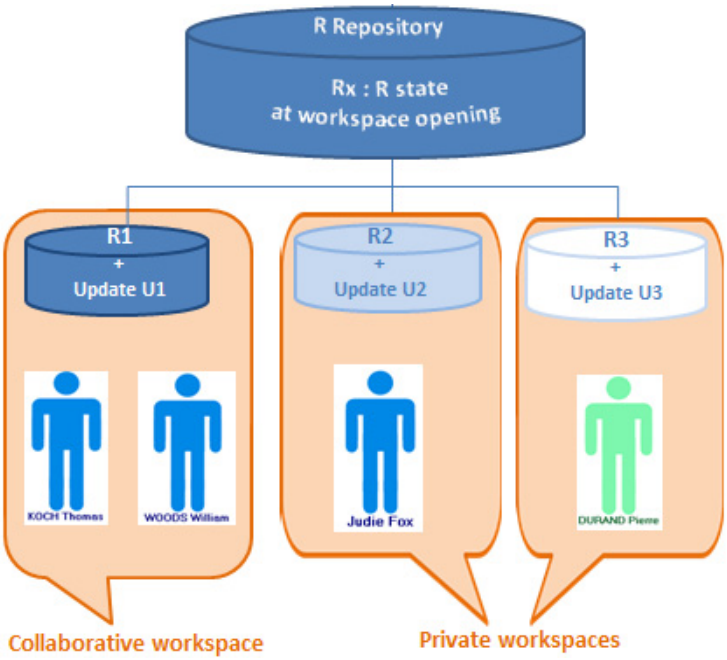
Workspaces are managed by the administrator.

The following points are covered here:

PRIVATE WORKSPACES 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 **MEGA** the user controls management of his/her workspace: opening, closing, dispatch, refresh.



Private Workspace

When a user connects to a **MEGA** desktop (**Windows Front-End**) and to certain **Web Front-End** 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 wishes to integrate his/her repository updates and make these visible to other users. To do this, he/she dispatches modifications.

☛ *See "Dispatching Your Work", page 192.*

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

> ☛ *The private workspace is open for each user on both his/her repository and on the system repository. A private workspace always exists on system repository even if the user is not using any of the system repository objects.*

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

> ☛ *Locks inform the user of objects modified by others. See "Managing Locks", page 217.*

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

> ☛ *See "Refreshing Data", page 195.*

MEGA allows several users to work at the same time.

Collaborative Workspace

> ☛ *This functionality is available with an RDBMS format repository only.*

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 **MEGA 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 MEGA

When you connect to **MEGA**, you can:

- create a private workspace (if you do not already have one).

  ☛ *You can only have one private workspace open in the same environment.*

  ☛ *The private workspace is open for each user on both his/her repository and on the system repository. A private workspace always exists on system repository even if the user is not using any of the system repository objects.*

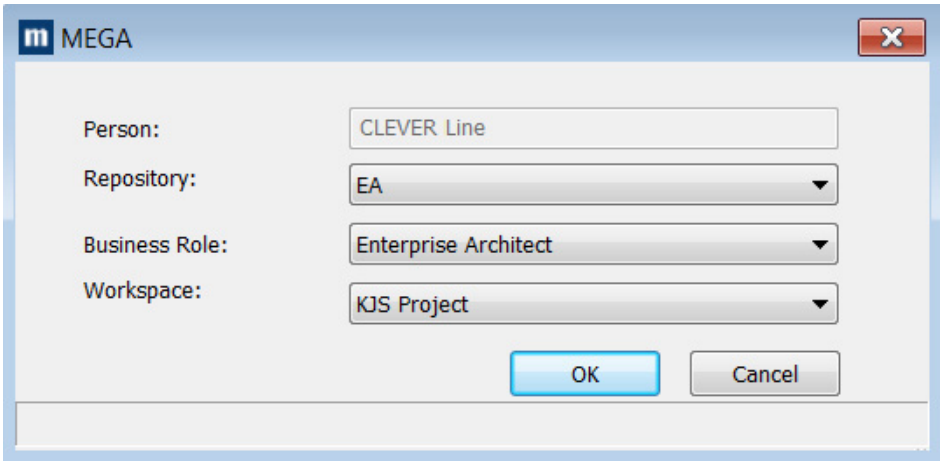
- resume work in your private workspace
- resume work in a collaborative workspace

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

To connect to **MEGA**:

1. Start the **MEGA** application.
   The authentication dialog box appears.
2. In the **Login** field, enter your login.
3. (Optional) In the **Password** field, enter your password if required.

4. In the **Environment** field, select your work environment.
5. Click **OK**.
   You are authenticated, your name appears in the **Person** field.



6. In the **Repository** field, select your work repository.

   ☛ *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.*
7. In fields **Business Role**/**Profile**, select the business role/profile with which you want to work.
   If you have **HOPEX Collaboration Manager**, go to step 9.
8. Click **OK**.
   A private workspace is created and your desktop opens.
9. If:
   - you do not have a collaborative workspace available, the **Workspace** field is not available. Click **OK**.

   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 business role/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 **OK**.

     ☛ *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.

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 MEGA. 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:

- In the **MEGA** menu bar, 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", page 192.*

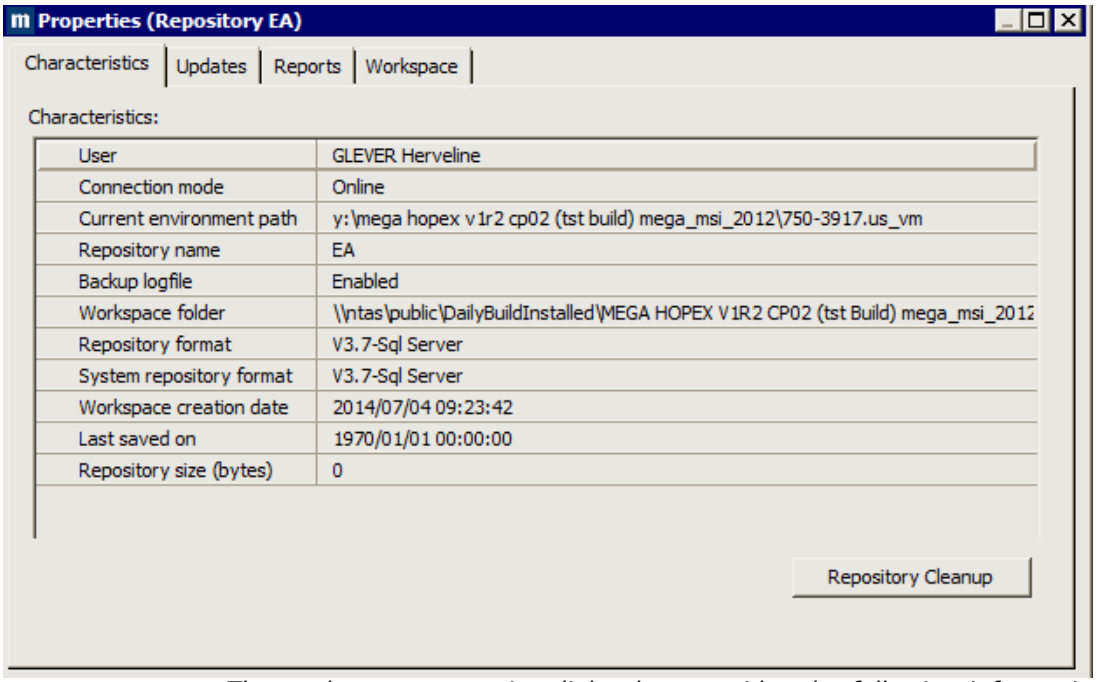
Private Workspace Properties

To consult properties of your workspace:

1. Connect to **MEGA**.

   ☛ *See "Connecting to MEGA", page 188.*

2. In the **MEGA** menu bar, select **File > Properties**.
   The properties dialog box of your workspace appears.



The workspace properties dialog box provides the following information on the current workspace:

- current **User**
- information on the current repository: its **Name**, **Backup logfile**, **Format**, **Workspace creation date**, **Last saved on**, **size**
- **Repository Cleanup** option.

MEGA Repository State Changes

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

☛ *See example "Private Workspace Life: Example", page 208.*

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

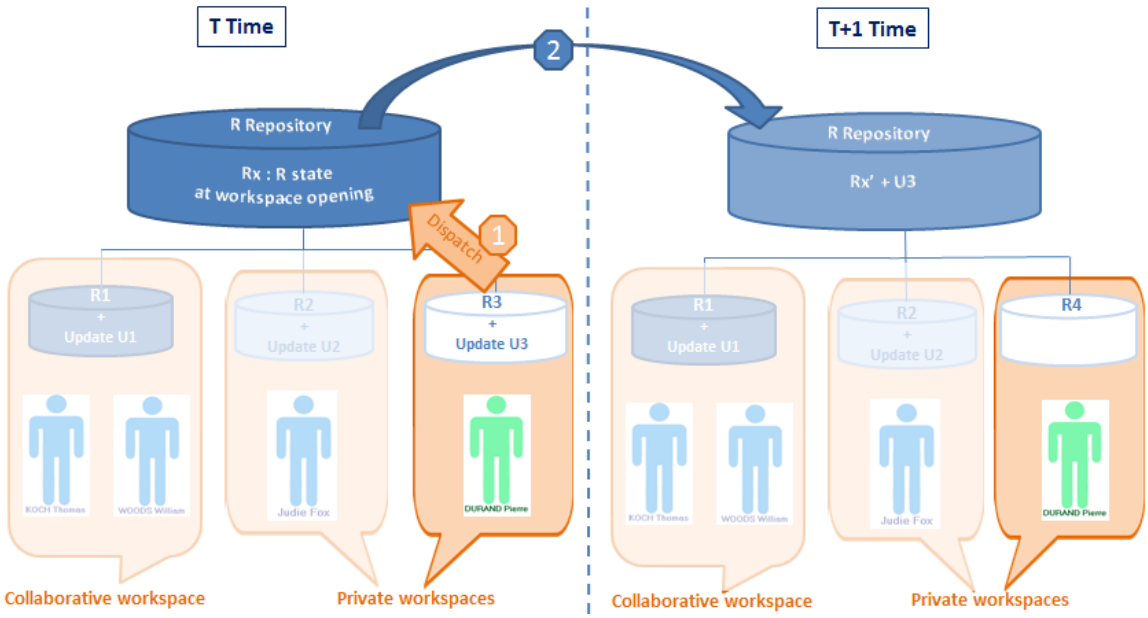
The repository changes from state N to state N+1 with memorization of new data related to the previous situation (state N).

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 **MEGA** 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 **MEGA** 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 **MEGA** without having to wait until the works from other queued private workspaces are dispatched.

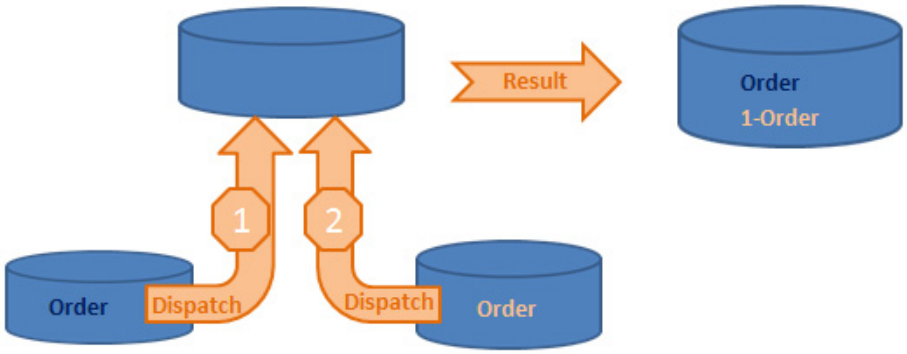
☛ *See "Dispatch Conflicts", page 193.*

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.

☛ *See "Merging Two Objects", page 277.*

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 you dispatch a private workspace. Most conflicts are managed automatically.

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

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

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

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

Rename/create collisions

A user renames an object in his/her private workspace, for example, from "Customer" to "Customer***s***". Then another user dispatches his/her private workspace in which he/she created an object having the same name "Customer***s***".

When the first user dispatches his/her private workspace, since the "Customer***s***" object already exists, the object "Customer" cannot be renamed "Customer***s***". The rename command will therefore be rejected.

Verifying link uniqueness

A user creates a link for which there is a uniqueness check. For example, he/she indicates that the "Order" message is sent by the "Customer" org-unit. In the meantime, another user indicates in his/her private workspace that the "Order" message is sent by the "Customers" org-unit. When the second user dispatches his/her private workspace, the link is rejected if the uniqueness control imposes that a message can be sent by only one object.

☛ *See the **HOPEX Studio** Technical Article for information on uniqueness verification for a MetaAssociation.*

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.

Dispatch Report

The report file can be accessed from **MEGA Administration**.

To view the report file:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Right-click the environment and select **Reports > Open**.
   A new window allows you to view report contents.

   ☛ *See "Viewing the Environment Report File", page 165 for more details on these dialog boxes.*

The error level is indicated in the dispatch report.

- Error level 0: no error.
- Error level 2: minor errors such as attempts at creating already existing objects or links.
- Error level 4: the actions involved nonexistent objects or links.
- Error level 8: a system error was encountered during the update.
- Error level 16: update aborted because of a problem such as insufficient disk space.

  ☛ *These error levels are the same as those used for manual file imports.*

  ☛ *When manually importing a file, rejects concerning the creation of already existing objects or links can be filtered out using the Reprocess option.*

Objects that were renamed are also listed in the report.

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:

- from 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.

- from 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.

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

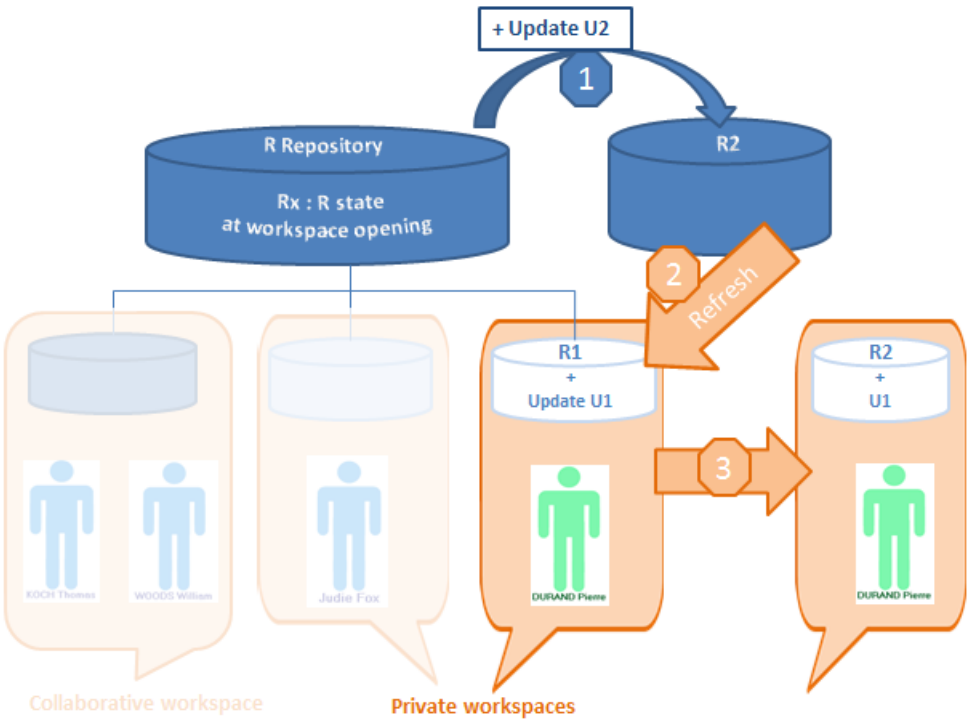
  Refreshing allows a user to incorporate repository and system repository changes made by other users, without dispatching current work.

Refreshing a private (or collaborative) workspace.

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

  ☛ *see "Managing Locks", page 217.*

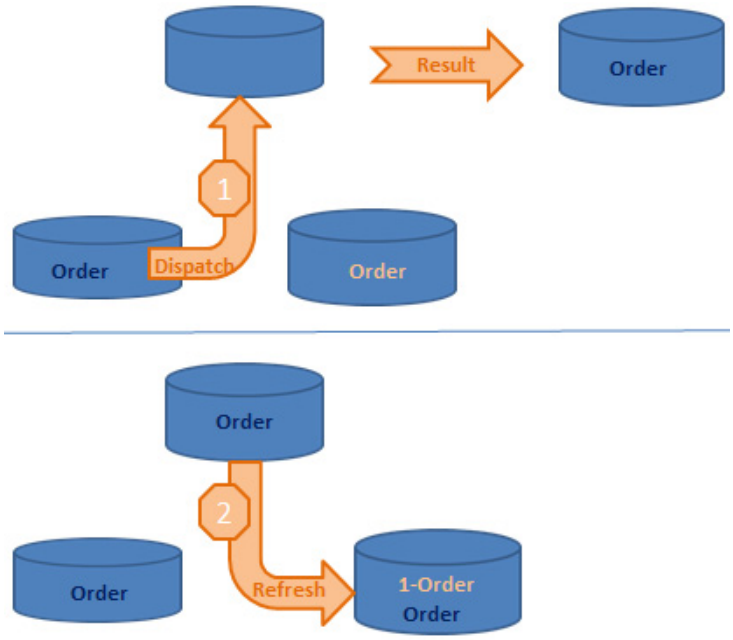
When a user resumes work on his/her private space that has lasted longer than the limit set by the administrator (the default is 6 days), **MEGA** proposes that the user refreshes or dispatches his/her work.



Conflicts When Refreshing

Conflicts at refreshing are the same as at dispatch, but they apply to the private workspace only.

☛ *For more details on the main causes of rejects, see "Dispatch Conflicts", page 193 and "Rejects When Dispatching", page 194.*



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

In **MEGA**, to discard your private workspace:

1. (Optional) It is advisable to export the private workspace before confirming the discard, see "Elements that could be useful to back up", page 155.
2. In the **MEGA** menu bar, select **File > Discard**.

☛ *You can also discard your private workspace at disconnection, see "Exiting a Session", page 198 (choose not to dispatch modifications).*

Discarding work from a collaborative workspace

Only the collaborative workspace **Owner** can discard the collaborative workspace.

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

In **MEGA**, to discard your collaborative workspace:

1. (Optional) It is advisable to export the collaborative workspace before confirming discard, see "Elements that could be useful to back up", page 155.
2. In the **MEGA** menu bar, select **File > Workspace > Discard**.

Exiting a Session

When you exit **MEGA**, 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

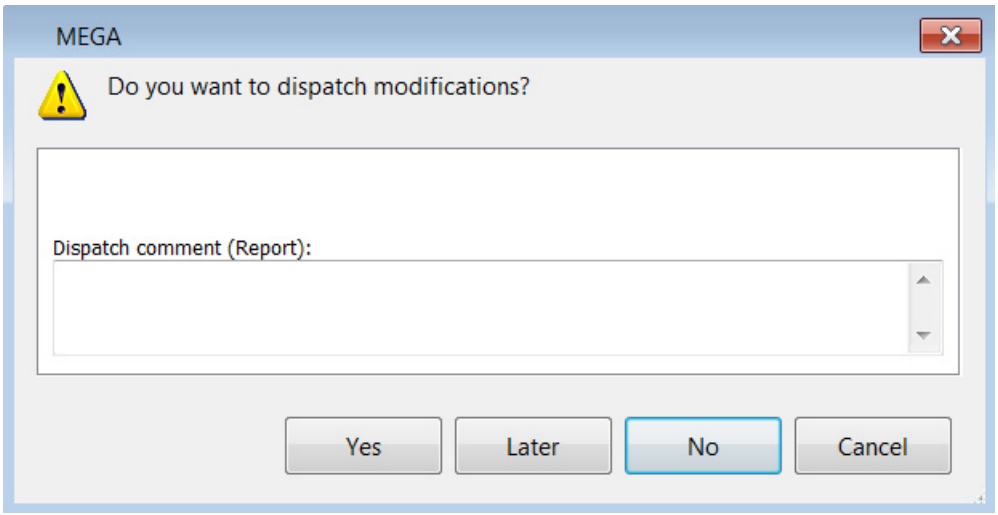
    ☛ *These modifications are saved in the collaborative workspace. These modifications are not saved in the repository until the collaborative workspace is closed.*
  - cancel modifications you have made.

Exiting a session from a private workspace

From **MEGA**, to exit your work *session*:

1. From your **MEGA** desktop:
   - **Windows Front-End**: in the **MEGA** menu bar, select **File > Exit**.
   - **Web Front-End**: in the **Miscellaneous** toolbar, click **Disconnect**.

   The **MEGA** 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 **MEGA** exit mode.
   - **Yes**

     Modifications you have made in your private workspace are saved in the repository.

     ☺ *In order to work effectively as a team, it is recommended that you dispatch frequently and regularly. Other users can update their own private workspace without dispatching their work (menu **File > Refresh**).*

     ☛ *This exit mode also allows the user to select a different repository the next time he/she logs in.*
   - **No**

     All modifications you made since your last dispatch will be lost. You can use this option if you want to view data quickly and exit without impacting the repository.

     ☛ *Modifications to your desktop are also lost.*
   - **Later**

     This option allows you to keep your changes without impacting the repository. You can open your session later and continue working but other users are not yet seeing the changes you have made.

     ☛ *Click **Cancel** to not exit your private workspace.*

Exiting a session from a collaborative workspace

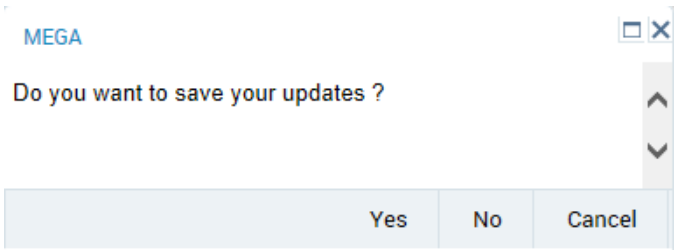
Exiting **MEGA** from a collaborative workspace is the same whether you are its owner or not.

For as long as the collaborative workspace is not closed, participants can exit and rejoin the collaborative workspace at any time.

From **MEGA**, to exit your work *session*:

1. From your **MEGA** desktop:
   - **Windows Front-End**: in the **MEGA** menu bar, select **File > Exit**.
   - **Web Front-End**: in the **Miscellaneous** toolbar, click **Disconnect**.

   The **MEGA** 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 Workspace Management (Web Front-End)", page 201
- "Accessing Workspace Management (Windows Front-End)", page 204
- "Deleting a Private Workspace", page 206

Accessing Workspace Management (Web Front-End)

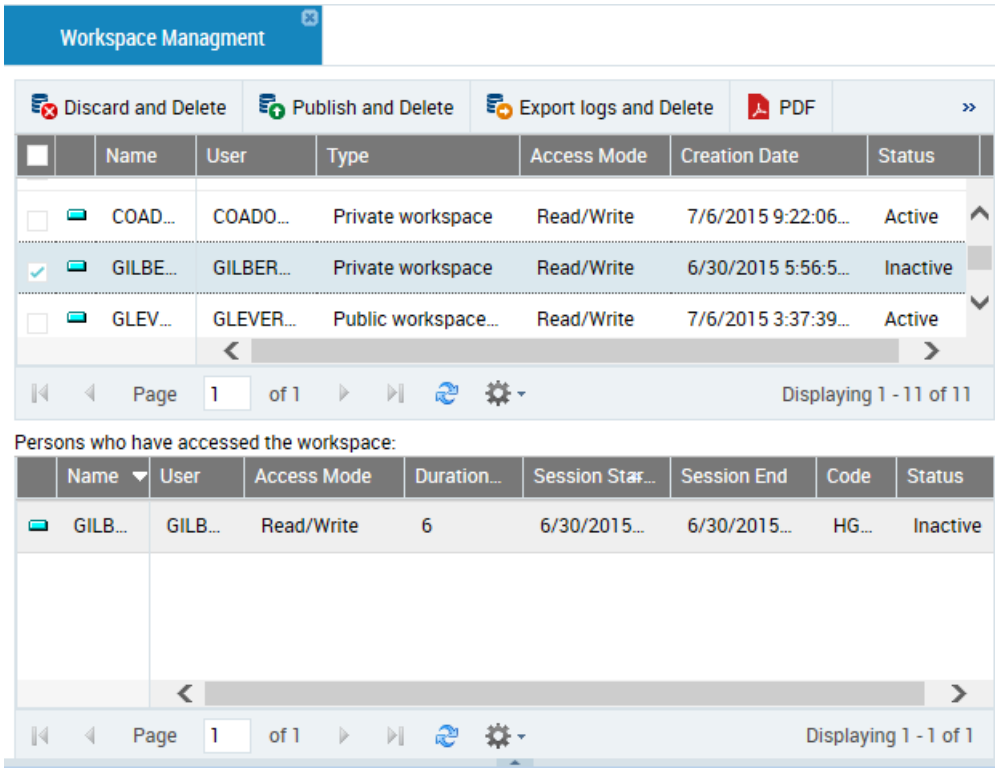
To access the list of current workspaces in an environment:

1. Connect to the **MEGA Administration** desktop (Web Front-End).

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

2. In the **Administration** tab, click the **Repository Management** pane.

3. Click the **Workspace Management** sub-folder.
The management page for workspaces currently in progress in the environment appears.



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

> ☛ *To sort workspaces according to a column, click the header of the corresponding column.*
>
> ☺ *You can also arrange columns in the order you want. To do this, click the header of the column to be moved and, holding down the mouse button, move it to the required position.*

- the **User** of the workspace
- the **Type** of workspace:
  - "Private Workspace":
  The user can modify data. His/her updates are kept in his/her private workspace until dispatched.
  - "Public Workspace":
  The user can modify data. His/her updates are immediately visible to all other users.
- the **Access Mode** of the workspace, for example:
  - "Read/Write" when a session is open.
  - "Read-only" when the user is in consultation only.
  - no value, if the private workspace is passive (the user has saved his/her session but is not currently connected to **MEGA**).
  - no value if the user is in offline mode
- its **Creation** date and time
- the **Status** of the workspace
  - enabled
  - disabled

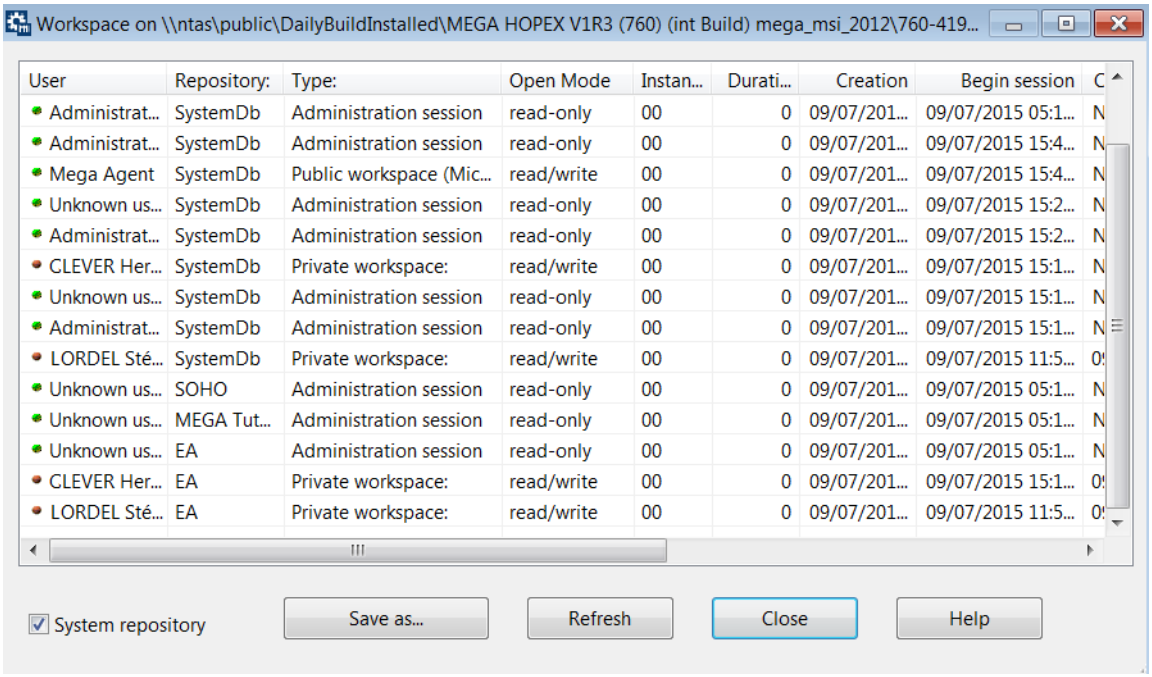
The **Persons who have accessed the workspace** frame details:

- 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**

Accessing Workspace Management (Windows Front-End)

To see the list of current workspaces in an environment:

1. From **MEGA Administration**, connect to the environment concerned.
   ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **Repositories** folder.
3. Expand the folder of the repository concerned, right-click **Workspaces** and select **Manage**.
   The dialog box for management of workspaces currently in progress in the environment appears.



4. (Optional) Select **System Repository** to view system repository workspaces and the user connected to **MEGA Administration**.

The private workspace dialog box 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.*

- its state:
  - the green button indicates that the workspace is open (private workspace) or in consultation (public workspace)
  - a red button indicates that the workspace is passive or that the user is disconnected.
- the **User** who created it and his/her **Code**.

  > ☛ *In the case of collaborative workspaces, only the collaborative workspace owner appears.*
- the **Repository** to which it relates
- the **Type** of workspace:
  - "Private Workspace":

  The user can modify data. His/her updates are kept in his/her private workspace until dispatched.
  - "Collaborative Workspace":

  The participants of a collaborative workspace can, depending on their access level, modify the data. Their updates are kept in the collaborative workspace until the owner of this workspace decides to dispatch them.
  - "Administration Session":

  The user is Administrator type. The user cannot modify data.
  - "Public Workspace":

  The user can modify data. His/her updates are immediately visible to all other users.
- the **Open 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 **MEGA**).
  - no value if the user is in offline mode
- its **Duration** in days
- its **Creation** date and time
- the **Start** and **End** dates and times of the last **Session**
- the **Location** where it is stored
- its **Dispatching Delay**, which indicates its state compared to the current state of the repository (number of saves since the private workspace began, whether manual or automatic).
  Each time the repository is updated, the difference between the private workspace view and the repository state increases. This difference is measured by the private workspace delay. Dispatching or refreshing the private workspace reduces the delay to zero.

  > ☺ *It is recommended that you refresh your workspace if its delay is greater than 50.*

Deleting a Private Workspace

The **MEGA** administrator can delete a private workspace when this is passive.

See:

- "Deleting a Private Workspace (Web Front-End)", page 206
- "Deleting a Private Workspace (Windows Front-End)", page 206

Deleting a Private Workspace (Web Front-End)

To delete a workspace:

1. Access the workspace management page.

   ☛ *See "Accessing Workspace Management (Web Front-End)", page 201.*

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.

Deleting a Private Workspace (Windows Front-End)

The result is equivalent to discarding it.

To delete a workspace:

1. Open the workspace management dialog box.

   ☛ *See "Accessing Workspace Management (Windows Front-End)", page 204.*

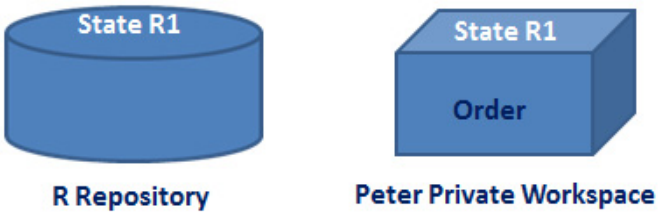
2. Right-click the workspace concerned and select **Delete**.

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.

PRIVATE WORKSPACE LIFE: EXAMPLE

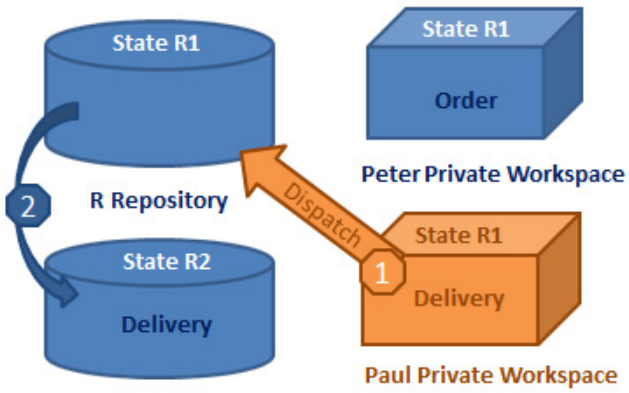
To illustrate how private workspaces work, the following is an example of some steps in the work of several users:

Private Workspace 1



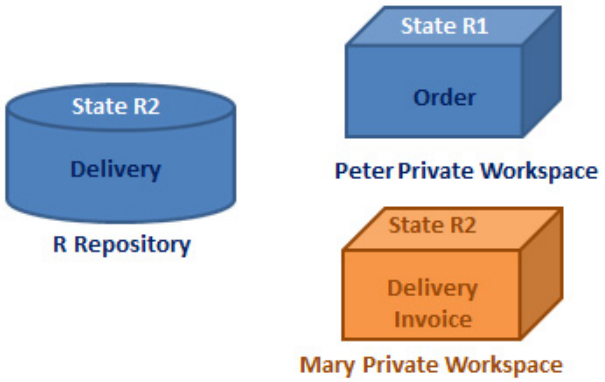
- Peter opens a private workspace, his repository view is state "n" (R1).
- He creates the "Order" message, which he links to the "Customer" org-unit.
- In parallel, Paul dispatches his private workspace...

Private Workspace 2



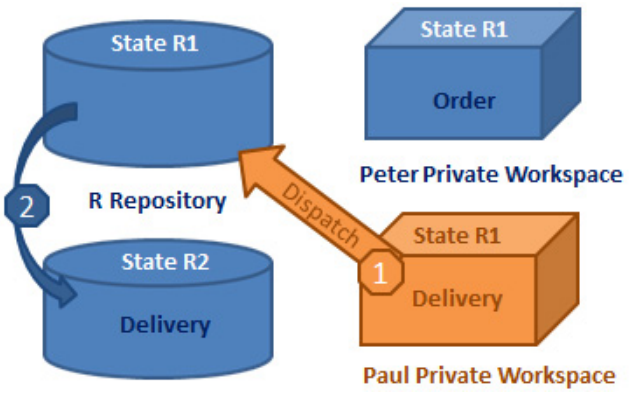
- The private workspace that Paul dispatched created the "Delivery" message, linked to the "Customer" org-unit.
- Paul's dispatch changes the repository to state "n+1" (R2).
- This new message is not seen from Pierre's private workspace...

Private Workspace 3



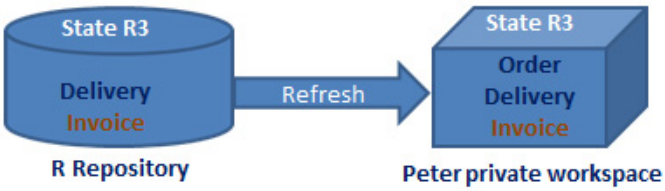
- Mary opens a new private workspace, her repository view is state "n+1" (R2).
- Mary creates the message "Invoice" connected to the "Customer" org-unit...

Private Workspace 4



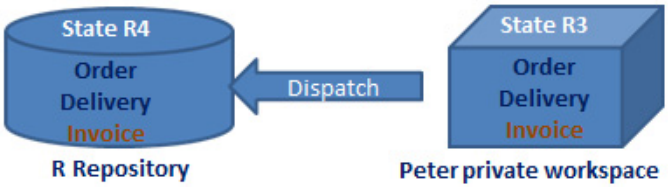
- Mary dispatches her private workspace.
- The repository passes to state "n+2" (R3).
- Peter's view is still in state "n" (R1).
- Peter refreshes his private workspace...

Private Workspace 5



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

Private Workspace 6



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

MANAGING UPDATES

During their modeling work, users make additions to a **MEGA** 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 logfile, which can be exported in the form of a command file.

The following points are detailed here:

Viewing Updates

You can view updates:

- in your private workspace
- in the repository

Private workspaces

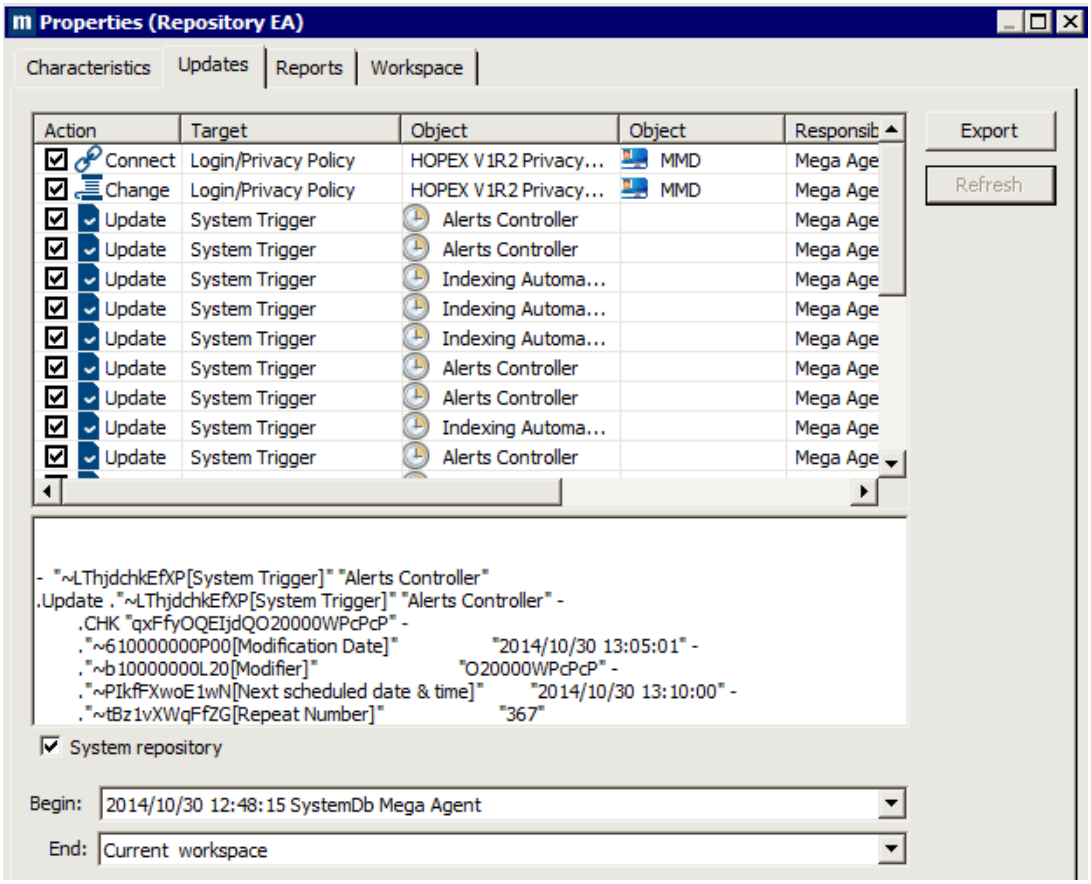
To view updates you have made in your private workspace:

1. From the **MEGA** menu bar, select **File > Properties**.

   ☛ *This process may take some time if there are many updates.*

   The properties dialog box of your private workspace appears.

2. Select the **Updates** tab.



The **Properties** dialog box shows the commands you have executed in your private workspace or in your collaborative workspace. For each command, the following are indicated:

- the **Date** the command was executed.
- **Action** executed:

  ```
  Example: "Create", "Connect", "Update".
  ```

  ☛ *See "Command File Syntax", page 349 for more information on operators.*
- Object Type concerned in the **Target** column.
- the name of the **Object** concerned.
- the name of the second **Object** concerned in the case of a "Connect", "Disconnect" or "Change" action.
- when you select the line of a command, the complete text of the update appears (lower frame of dialog box).

To sort the updates list:

❱ Click the column header.

To copy a command from the logfile (to paste it in the notepad for example):

1. Select the command.
2. In the lower frame of the dialog box, select the command text and simultaneously press keys <CTRL> + <C>.

To display only those commands concerning objects stored in the system repository (for example Person):

- Select the **System repository** check box.

In the logfile dialog box, the **Export** button enables export of selected commands in MGL or XMG format.

> ☛ *For more details on private workspace log export, see "Exporting Your Private Workspace Log", page 213.*

Dispatches

> ☛ *See "Viewing the Repository Update Log", page 149.*

The **Repository Dispatches** folder contains private workspaces dispatched in the current repository and in the system repository. Dispatches are filed by day, week and month.

To display private workspaces dispatched and the content of their updates:

1. From:
   - (Web Front-End) the **Administration** desktop, in the **Repository Management** pane, select the **Repository Activity** sub-folder. Select a dispatch.

     > ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

     > ☛ *To access the content of the **Repository Management** pane, you must have **Expert** metamodel access (see "Configuring metamodel access", page 77).*

     The dispatch properties appear in the edit area.
   - (Windows Front-End) **MEGA**, in the navigation window **Repository Activity> Repository Dispatch**, right-click the dispatch and select **Properties**.

     > ☛ *To access the content of the **Repository Activity** navigation window, you must have **Expert** metamodel access (see "Configuring metamodel access", page 77).*

     Private workspaces dispatched on the current repository and system repository are contained in the repository folder.
2. Select the **Updates** tab.

Exporting Your Private Workspace Log

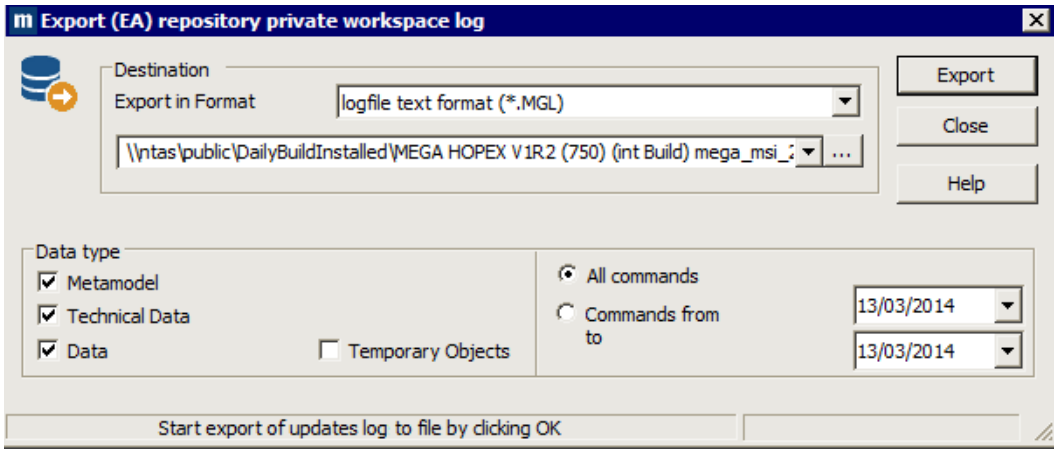
You can create an export file (*private workspace logfile*) and save it in your *work folder*.

The export file can be exported in:

- **logfile text format** (.mgl).
  Name format of the exported file is "LOGmmdd.mgl", where "mmdd" represents the month and day of the logfile export.
- **MEGA XML format** (.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 the current private workspace in the form of a command file:

1. From the **MEGA** menu bar, select **Tools > Manage > Export Updates Logfile**.
   The **Export repository private workspace log** dialog box opens.



2. Select export format.
3. (Optional) If necessary, modify the data export file name and save folder proposed as default. The **Browse** button ... allows you to browse the folder tree and select the folder in which the file will be placed.
4. In the **Data Type** frame, select the type of exported modifications:
   - **Metamodel** if you want to extract the metamodel from the system repository. This is useful if the standard metamodel has been modified.
   - **Technical Data** if you want to include in your file the changes made to data such as descriptors and queries.
   - **Data** if you only want to export changes made to repository data, particularly the workspace.
   - **Temporary Objects** - these objects are created when you execute requests, when you consult objects (stored in the history), etc. Generally you will not need to export these objects.
5. (Optional) If you want to export only those commands that correspond with a defined period, select **Commands from** / **to** and specify the dates.
6. Click **Export**.
   The **Execution Report** appears.

7. Click **OK**.
   The file is exported and saved in the specified folder.

The user can subsequently import this logfile, for example into a new private workspace.

Private Workspaces and Repository Size

Private workspace life

A private workspace gives a user a frozen view of a repository.

When the repository is modified by other dispatched private workspaces, this private workspace keeps the view it had when created.

Since the data corresponding to these views is kept in the repository, its size grows, and may become disproportionate to the actual repository contents.

☛ *See "Dispatching Your Work", page 192 and "Refreshing Data", page 195.*

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 **MEGA** repository.

☛ *See "Refreshing Data", page 195 and "Discarding Work", page 197.*

In his/her private workspace, modifications made by the user are saved in a temporary space (file for GBMS repository and data for RDBMS repository) dedicated to data of his/her private workspace. The repository is updated only when the user dispatches these changes.

☛ *See "Dispatching Your Work", page 192.*

All data accessed by a user is "frozen" for the duration of the private workspace.

Example:

> For example, if an object is renamed in the reference repository after the private workspace is opened, the user sees the previous name unless the private workspace is refreshed. However, users connecting after the modification has been dispatched will have a view reflecting the most recent state of the repository.
>
> If other users connected before you dispatch your updates, and are accessing the same data as you, they will have an obsolete view of the data until they refresh their private workspace. Note that when you dispatch your updates, your view is refreshed automatically.

This means that data being accessed by user A and modified at the same time by user B is duplicated. It is stored in its initial state for each user private workspace; if a user makes a change, the previous state is stored along with the new one.

When the updates are dispatched and all users accessing the updated data have refreshed their private workspaces, the previous state is no longer required.

If a user does not want to dispatch his/her private workspace, refreshing it allows the user to avoid a large increase in the **MEGA** repository size.

The administrator can set the maximum duration of a private workspace. If your private workspace exceeds the duration defined by your administrator, then each time you establish a connection, a message box appears asking you to dispatch or refresh your private workspace.

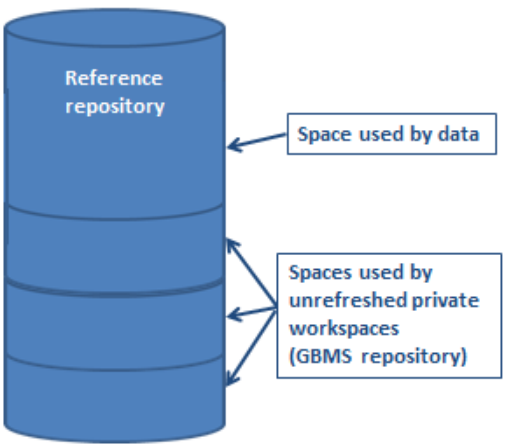
You can audit private workspaces with the **MEGA Administration** application.

> **A private workspace that began before significant modifications were made may cause a considerable increase in repository size, since an image of the previous state of the modified elements is kept until the private workspace is refreshed.**

The default option when a user disconnects is indicated in the user configuration. It is defined for the entire environment.

The greater the number of private workspaces and the longer their duration, the more the volume of the temporary space (file for GBMS repository and data for RDBMS repository) dedicated to private workspace data will increase. This volume can be reduced by repository backup or deletion, new repository creation or logical backup restoration.

☛ *For more information on reorganization of repositories, see "Reorganizing a repository", page 157.*



MANAGING LOCKS

When several users are connected to the same repository simultaneously, there may be conflicts when they modify the same object in their different private workspaces.

See:

- "Principle", page 217
- "Managing Locks on Objects (Web Front-End)", page 219
- "Managing Locks on Objects (Windows Front-End)", page 221

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 by the administrator, or at desynchronization of clocks.

> ☛ *For more details on clock synchronization, see "Clock synchronization", page 218.*

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.

Clock synchronization

When lock management is active, workstation and environment clocks must be synchronized.

> **If clock times differ by more than 5 minutes when you connect to MEGA, an error message appears and your work is saved at your workstation time. This situation can create consistency problems when dispatching your work.**

To be able to start **MEGA**, you must synchronize the clocks:

Times relating to the network object locking system are always expressed in GMT0. For network workstations on which executables are decentralized, ensure that clocks are synchronized with a reference server. To do this, it is possible to use the "Net-Time" command or a Web clock synchronization service.

- With Windows NT and 2000, this can be done using a network command such as "Net time \\Workstation name/set" with LAN Manager or Windows NT.
- With Windows XP, setting is carried out from the Windows **Control Panel**, **Date/Time** icon.

> *For more information on clock synchronization, see Windows online Help.*

Details on lock operating

MEGA only indicates that objects are locked when their attributes are modified (unlike links for example).

Alert 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 (Web Front-End)

The lock management page of the **Administration** desktop (Web Front-End) provides access to:

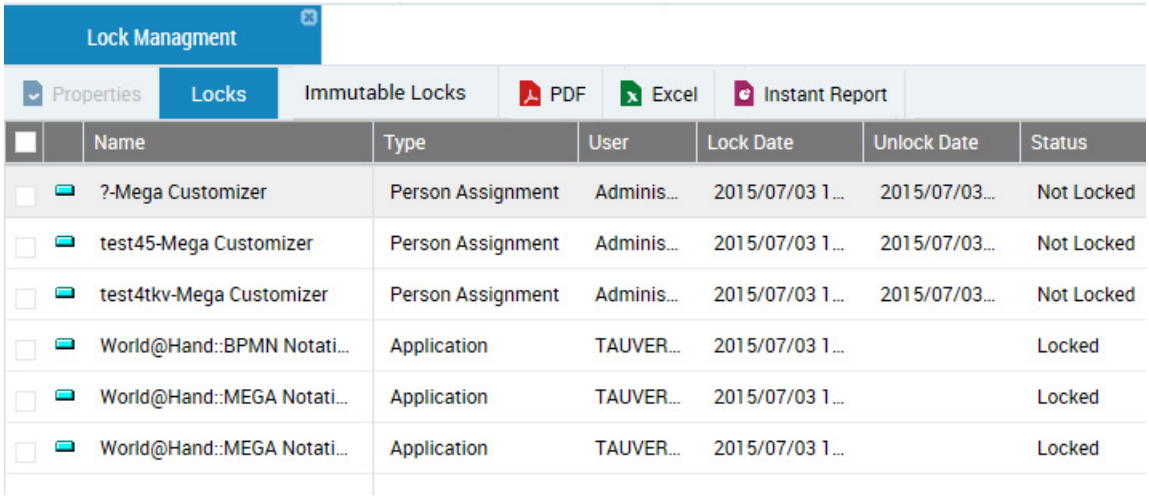
- the **Locks** page, which details for each lock:
  - the **Name** of the object concerned
  - the **Type** of object concerned
  - the **User** who owns the lock
  - the date and time (GMT0) of the **Lock**, and, if applicable, **Unlock**
  - the lock **Status** (locked or not locked).
- the **Immutable 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 lock **Status** (locked or not locked).

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.



Viewing locks on objects (Web Front-End)

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

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

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

2. In the **Repository Management** pane, click the **Lock Management** sub-folder.
   The **Lock Management** page appears and lists the locks.
3. (Optional) To sort locks according to column, click the column header.

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

4. Select a lock and click **Properties** to view the details of the lock.
   With **General > History** you can view the history of modifications performed on the object.

Managing immutable locks on objects (Web Front-End)

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

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

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*

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 Locks on Objects (Windows Front-End)

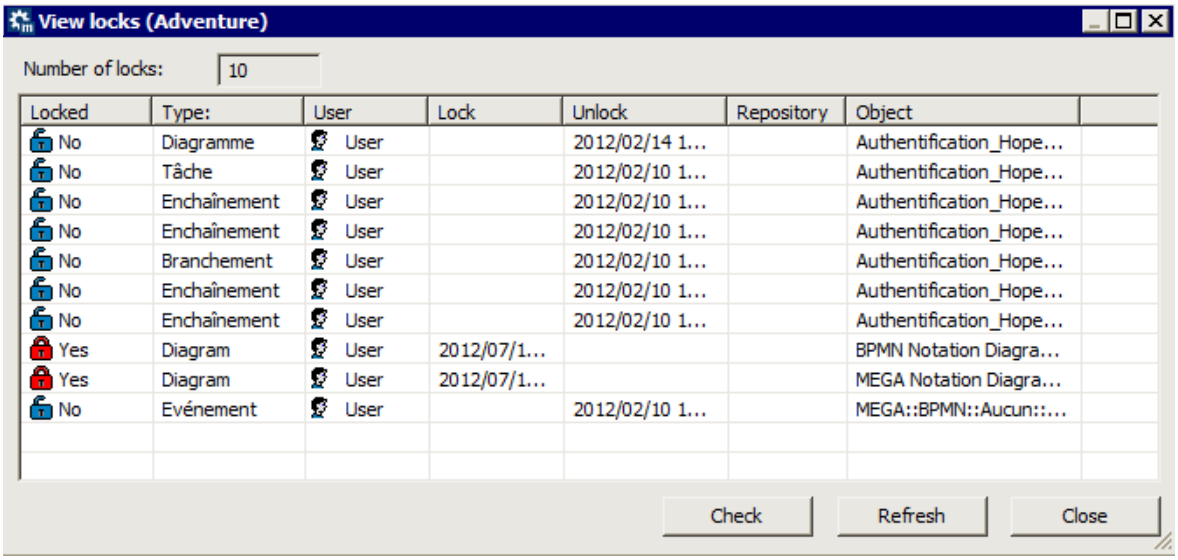
The management window for locks is accessible from:

- the **Administration** application (**Windows Front-End)**

  ☛ *"Managing Locks from Administration (Windows Front-End)", page 222*

- the **MEGA** application (**Windows Front-End)**.

  ☛ *"Managing locks with MEGA (Windows Front-End)", page 222*



The **Display Locks** window displays the locks created since the creation of the oldest private workspace. The following information is provided for each lock:

- the lock state (**Locked**):
  - **Yes**: When a user locks an object, other users can only view it, even if they dispatch their work.
  - **No**: the object is locked when its modifications are dispatched. Other users must dispatch their work or refresh their private workspaces before they can modify the object.

    ☛ *To unlock an object or delete a lock, see "Managing Locks from Administration (Windows Front-End)", page 222*
- 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 name of the **Repository** to which the lock relates.

Managing Locks from Administration (Windows Front-End)

To manage locks from the **Administration**application:

1. Connect to the environment concerned.

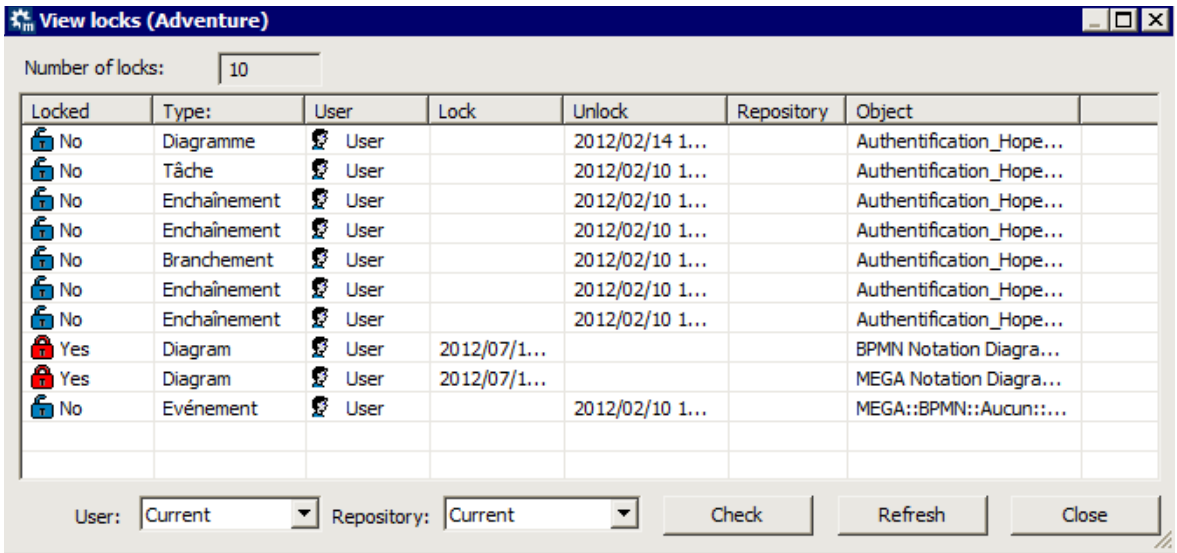
   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **Repositories** folder, then that of the repository concerned.
3. Right-click the **Locks** folder and select **Manage**.
   The **View locks** dialog box opens.
4. To:
   - unlock an object, right-click the lock concerned and select **Unlock**.
   - delete an object, right-click the lock concerned and select **Delete**.

Managing locks with MEGA (Windows Front-End)

To view the locks with **MEGA**:

1. Connect to **MEGA (Windows Front-End)**.
2. Select **Tools > Manage > View Object Locks**.
   The **View locks** dialog box opens.



   The locks appear grayed, except that of the current user.

3. To:
   - delete an object, right-click the lock concerned and select **Delete**.
   - unlock an object, right-click the lock concerned and select **Unlock**.

MANAGING ENVIRONMENTS

When multiple users are working together across a network, it may be useful to create several work environments. Another reason for creating a new environment is to provide the administrator with an environment where report templates (MS Word), queries, etc. can be modified and tested without interfering with users' work.

Environment management functions are used when several environments are available and they need to exchange data or repositories.

The following points are covered here:

ENVIRONMENT STRUCTURE

> 🕮 *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.*

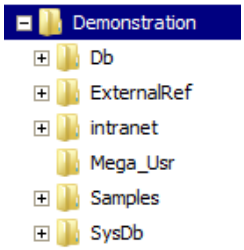
An *environment* comprises:

- A configuration file.
- A system repository (see "System Repository", page 223)
- Shapes, if they are different from the site standard shapes.
- A "Db" folder for the repositories used in this environment.

In most cases, there is only one environment per site. It is possible to define several environments when the *site* includes repositories on which users work with different resources (such as specific report templates (MS Word) or metamodel extensions).

> ☛ *All users must have full access rights to the resources of the environments and repositories (creation and deletion of files and folders).*

The folder structure of an environment is as follows:



- ***Db***: contains the environment repositories

  > ☛ *Each repository is located in a folder carrying its name. See "Repository Structure", page 138.*

- ***ExternalRef***: contains external references of the environment
- ***intranet***: contains the Web sites generated in the environment
- ***Mega_Usr***: contains shapes specific to the environment
- ***Samples***: contains examples
- ***SysDb***: the system repository

The "Demonstration" environment is provided as an example with all versions of **MEGA**, and it is managed differently from environments created by the user.

MEGA recommends:

- that you do not work in the "Demonstration" environment, even in a specific repository.
- that you create a new environment (see "Creating an Environment", page 225) and you work in this.

System Repository

The system repository (SysDb) contains the configuration required to run **MEGA**:

- the metamodel, constituting the structure of repositories
- programmed *queries* and macros
- the elements to produce outputs: report templates, *report templates (MS Word)*, Web site templates
- users and their rights.

A system repository exists for each environment, automatically created in the **Sysdb** folder at creation of the environment.

MS WORD REPORT TEMPLATES (WEB FRONT-END)

So that users of **MEGA (Web Front-End)** can create reports (MS Word), you must convert report templates (MS Word) of the environment to RTF format. This operation is necessary for integrity of **MEGA** data.

If you use MEGA (Windows Front-End) only, do not carry out this operation. Reports (MS Word) converted to RTF format significantly increase file size.

Converting report templates (MS Word) to RTF format

This operation is irreversible.

To convert report templates (MS Word) to RTF format:

1. Connect to **MEGA Administration** and select the **SystemDb** repository.
   See "Accessing Repositories", page 138.
2. Right-click the **SystemDb** folder and select **Conversions > Utilities**.
3. In the **Utilities of repository SystemDB** dialog box, select option "MEGA Repository - Convert Report Templates (MS Word) to RTF format".
   This operation is irreversible. It is mandatory only for users of MEGA (Web Front-End) only.
4. Click **OK**.
   Report templates (MS Word) of the environment are converted to RTF format.
   User reports (MS Word) will be generated in RTF format, not only for users of MEGA (Web Front-End) but also for users of MEGA (Windows Front-End).

USING ENVIRONMENTS

The following points cover certain basic operations that can be executed on an environment:

Creating an Environment

To create an environment:

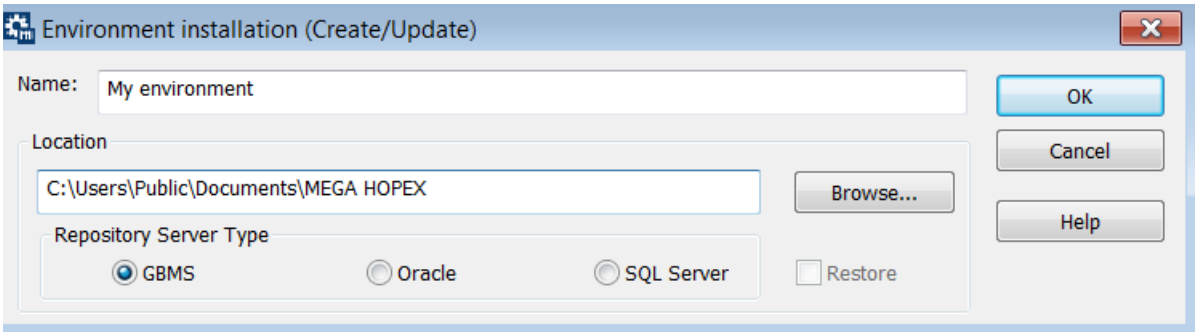
1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. In the navigation tree, right-click **Environments** and select **New**.
3. Enter the **Name** of the new environment.

   ☛ *The environment name must respect Windows folder naming constraints.*

4. (Optional) To modify the default environment location, click **Browse**.



5. Select the repository server type for the new environment.

   ☛ *Possible server types are: GBMS (**MEGA**) and RDBMS (Oracle and SQL Server). For more details on **MEGA** repository server type, see the **MEGA** deployment guide.*

6. Click **OK**.
   Creation and installation of the new environment are started.

   ☛ *(GBMS) The SystemDb repository is rebuilt and environment creation takes several minutes.*

   (RDBMS) The SystemDb repository is built dynamically and environment creation can take several hours.

   A directory is created. It hosts the environment structure.

   ☛ *When you create a new environment, it is automatically referenced, and it appears in the list of environments.*

   ☛ *The environment is identified by the complete path of its root directory. It is therefore essential that all users see the network resource in which it is located under the same name.*

Copying a GBMS Environment

💣 **Prior to this operation, check that there is no private workspace active on the environment.**

To copy an environment:

- With Windows explorer, copy the following files and folders:
- The environment root directory, which contains:
  - the environment system repository
  - all or some of the repositories that it references
  - the shared reports (MS Word) folder, "Document"
  - the "MEGA_Usr" folder containing the custom shapes and style sheets.
- Directories of repositories that are not stored under the environment root.

  ☛ *At the time of this operation, it can be useful to delete work folders of users and administrators.*

  💣 **When the operation is completed, you should check in each repository that the reports (MS Word) and Web Sites point to the correct network locations.**

Deleting a GBMS Environment

💣 **Prior to this operation, check that there is no private workspace active on the environment.**

To delete an obsolete environment with all its repositories:

1. Delete the reference for the old environment.

   ☛ *See "Deleting a Reference to an Environment", page 228.*

2. From the Windows explorer, delete the root directory of the environment and the folders of repositories that will not be hosted under this root.

MOVING AND REFERENCING AN ENVIRONMENT

During administration of **MEGA**, you may need to move an environment. When an environment is moved, you must create a new reference for it to be able to use it.

When you delete an environment, it is recommended that you delete its reference. It will then no longer appear in the list of environments available in the corresponding **MEGA** site.

For more details on these options, see:

- "Moving an Environment", page 227
- "Referencing an Environment", page 227
- "Deleting a Reference to an Environment", page 228

Moving an Environment

When you need to move an environment, such as when you have to place it on a different drive:

1. Copy the root folder of the environment in its new location.
2. Delete the reference for the old environment.
3. Create a reference for it at its new location.
4. Carry out the same operations for each of the repositories not hosted in the environment structure.
5. Check that the reports (MS Word) and Web sites of each repository point to the correct files.

Precautions to be taken:

- Verify that there is enough free space in the destination folder.
- It is not necessary to dispatch private workspaces before moving the environment. They will be moved with the environment.
- No user should be connected during movement of environments. No private workspace should be active.

Referencing an Environment

When an environment has been moved by the user, it is necessary to create a reference for this environment so the site will recognize it.

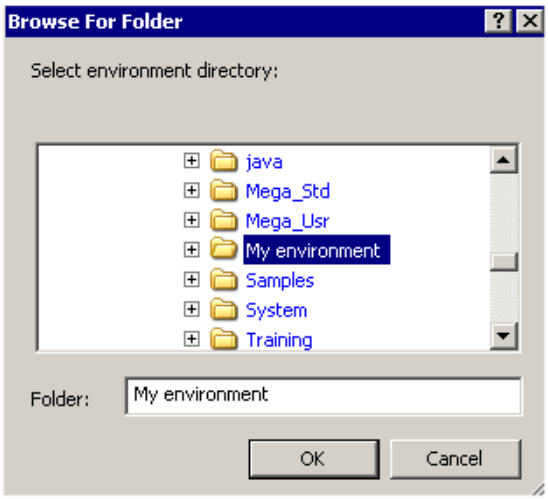
To create a reference to an environment:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. In the navigation tree, right-click **Environments** and select **Create Reference**.

3. In the dialog box that opens, select the folder in which the environment to be referenced is located.



4. Click **OK** to validate.
The new environment reference is created and appears in the list of available environments.

Deleting a Reference to an Environment

To delete a reference to an environment:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. In the navigation tree, right-click the desired environment and select **Delete Reference**.
A confirmation request appears.
3. Select **Yes**.
The environment reference is deleted and no longer appears in the list of available environments.

DEACTIVATING AN ENVIRONMENT (RDBMS)

In an RDBMS environment, for administration requirements, you can prevent users from connecting to **MEGA**.

You can block all users or Web users only.

The users already connected are not disconnected and can continue to work.

(Web Front-End) Prerequisite: You can notify the Web users that the environments are going to be inaccessible; see "Edit Area", page 15.

To deactivate an environment:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*

2. In the navigation tree, right-click the environment (RDBMS) that you want to make inactive and select **Environment Activity** then:
   - **Inactive environment**: only the **Administration (Windows Front-End)** application is accessible. Users cannot connect to **MEGA** (Windows Front-End and Web Front-End).
   - **Active environment with Windows-Front-End only**: access to **MEGA** (Web Front-End) is blocked.

CUSTOMIZING ENVIRONMENTS

Administration tasks may involve you in modifying configuration of an environment so that it meets your particular requirements.

With **MEGA Administration** you can perform the following actions:

Backing Up Environment Customizations

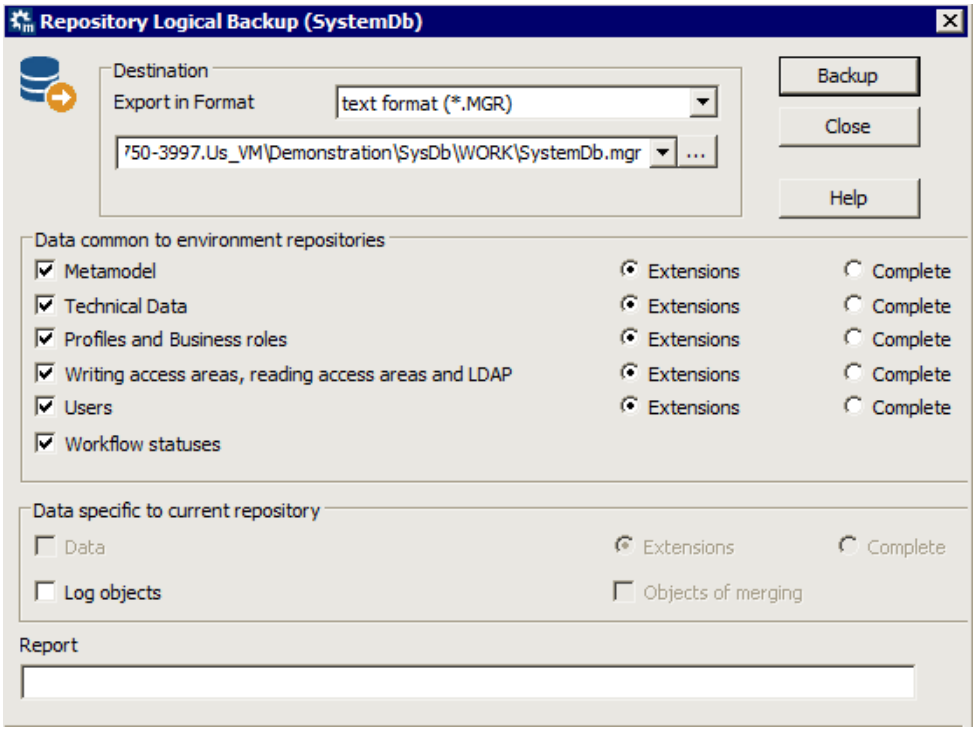
The following operations allow you to back up modifications made to the standard environment so that these can be imported into a new environment. This backup contains modifications you have made to *report templates (MS Word)*, Web site templates, *descriptors*, *queries* etc. It also contains the list of users and their configuration if this exists. You can also save any extensions to the metamodel.

To back up customizations:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. In the **Repositories** folder, right-click the system repository (SystemDb) and select **Logical Backup**.
   The **Repository Logical Backup** dialog box opens.



3. In the **Destination** frame, select the export format of the backup file:
   - **text** (.MGR)
   - **XML MEGA** (.XMG)

     ☛ *This format cannot be used to extract the metamodel or technical data. This format is reserved for exchange of data between **MEGA** and other applications. It includes commands or data (objects and links).*

4. (Optional) In the **Destination** frame, click **Browse** ... to browse the folder tree and modify the name and/or location of the backup file.

   ☛ *By default, the backup is saved in the "SystemDb.mgr" file in the \SysDb\WORK\ folder of the repository.*

5. Select the type of data you want to save.

   ☛ *The **Extensions** button corresponds to data created by users.*

   Carry out a complete backup only if technical support asks you to do so.

   ☺ *It is recommended that you save the extensions of the metamodel and technical data in different files.*

   In the frame **Data common to environment repositories**, select the data type of the system repository to be saved:

   - **Metamodel** if you want to extract the metamodel from the system repository. This is useful if the standard metamodel has been modified.
   - **Technical Data** allows extraction from the system repository of data such as *descriptors*, *queries*, and *report templates (MS Word)*.
   - **Profiles and Business roles** allows extraction of created profiles and business roles (those not provided by MEGA).
   - **Writing access areas, reading access areas and LDAP** allows extraction of created writing and reading access areas (those not provided by MEGA) and LDAP parameters (parameters, servers, groups).
   - **Users** allows extraction of created users (persons, person groups, logins).
   - **Workflow statuses** enables extraction of workflows (workflow instances, transitions and statuses, tasks, validations, requests for change).

   In the frame **Data specific to current repository**:

   - **Log objects** allows you to also save object logs.

     ☛ *For more information on histories, see "Deleting a Repository", page 152 and "Viewing Object History", page 169.*

6. Click **Backup** to start backup.
   A series of messages keeps you informed of backup progress.

Restoring Environment Customizations

You can restore environment customizations that you have backed up.

☛ *See "Backing Up Environment Customizations", page 230.*

To restore environment customizations:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Under the **Repositories** folder, right-click the repository concerned and select **Object Management > Import**.

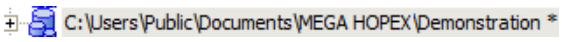
   ☛ *See "Updating a Repository", page 162.*

Compiling an Environment

The metamodel and technical data must be compiled after migration or customization. This is to check configuration of the environment concerned. When compilation has been completed, processing for all users of this environment is speeded up.

MEGA can function in "interpreted" (not compiled) mode but with reduced performance.

In the **MEGA Administration** navigation tree, an asterisk after the environment name indicates that the metamodel or/and technical data (excluding permissions) of this environment is/are in "interpreted" (not compiled) mode.



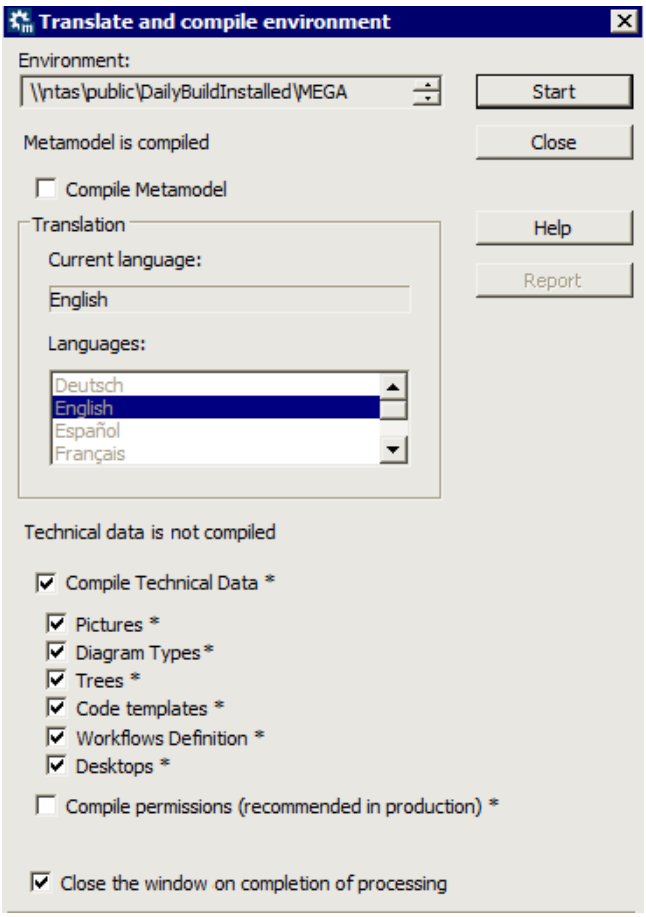
Metamodel compilation includes in parallel translation in the current language. You can also translate the metamodel into another language.

Prerequisite:

1. Ask **MEGA** users to exit their application:
   - mandatory for **Web Front-End** users
   - recommended for **Windows Front-End** users.
2. Start the **Mega Server Supervisor** tool.
   ☛ *See "Starting Mega Server Supervisor", page 244.*
3. In the identification area of your workstation, right-click **MEGA Server Supervisor** and select **System > Stop HOPEX Processes Services and Web Application**.

To translate and compile the metamodel and/or compile technical data:

1. From **MEGA Administration**, connect to the environment concerned.
   ☛ *See "Connecting to an Environment", page 5.*
2. In the navigation tree, right-click the desired environment and select **Metamodel > Translate and Compile**.
   The **Translate and compile environment** dialog box opens.



* : the asterisk indicates interpreted (not compiled) mode.

In the **Translation** frame, the **Current Language** field indicates the current language of the system repository.

3. If the metamodel is not compiled, keep **Compile Metamodel*** selected.
4. (If **Compile Metamodel*** is selected) In the **Translation** frame, in the **Languages** list of the system repository, select the target translation language.

   ```
   Example: "English"
   ```

5. If technical data is not compiled, keep **Compile Technical Data*** selected.

   If technical data and metamodel are not both compiled, you must also keep Compile Metamodel* selected.

   By default, all technical data (images, diagram types, trees, code templates, workflow definitions, desktops) is selected.

6. If you are in a production environment, keep the **Compile Permissions*** option selected; otherwise, you can erase the selection. This compilation improves **MEGA** loading times.

   ☛ *Compilation of permissions can take some time (more than an hour) and is recommended only in a production environment. The fact of not compiling permissions (permissions interpreted mode) has no impact on correct operation of **MEGA**.*

7. Keep **Close the window on completion of processing** option selected.

   ☛ *This option enables automatic closing of the **Translate and Compile Environment** window when compilation is completed, allowing **MEGA (Windows Front-End)** users to resume their work.*

8. Click **Start** to run compilation and translation.

   ☛ *If **MEGA (Windows Front-End)** users have remained connected, they are blocked during processing.*

   Metamodel and/or technical data compilation (excluding permissions) takes several minutes.

   If you selected metamodel compilation with a different target language, after execution the system repository is available in the new language.

9. When compilation processing is completed, **MEGA (Windows Front-End)** can resume their work.

   ☛ *If at step 7 the **Close the window on completion of processing** option was not selected, click **Close** to close the **Translate and Compile Environment** window and allow **MEGA (Windows Front-End)** users to resume their work.*

10. In the identification area of your workstation, right-click **MEGA Server Supervisor** and select **System > Restart HOPEX Processes Services and Web Application**.

    ☛ ***MEGA (Web Front-End)** users can connect to Web applications.*

COMPARING ENVIRONMENTS

The environment comparator enables evaluation of the differences between two environments and production of an update file that enables switching between one and the other. It enables detection of all changes to an environment or focuses only on certain aspects of customization by carrying out a comparison by topic. You therefore have available a tool enabling detection of metamodel extensions.

This comparator only functions if both environments have the same level of metamodel, meaning that they must share the same list of languages and the same MetaClass and MetaAttribute definitions.

☛ *This tool is written using **MEGA** APIs, and it is essential that the **MEGA** version is correctly referenced in the registry.*

See:

- "Comparison Types", page 236
- "Environment Comparator Configuration", page 237
- "Running the Environment Comparison", page 238

Comparison Types

You can run an analysis:

- standard (selected by default)
  It is a complete comparison of the two environments.
- by topic
  If you do not wish to carry out standard analysis due to lack of time, or if you need to compare a certain object type only.

Standard analysis

💣 ***Both environments must be compiled in the same language.***

☛ *Standard analysis is an extremely long process: it takes 8 - 12 hours.*

Standard Analysis consists of comparing:

- **Metamodel**:
  The metamodel analysis phase spots metamodel changes. If these changes are significant and concern addition of a language or modification of **MEGA** "core" data, comparison will not continue.
- **Technical data**:
  The technical data analysis phase detects all customizations of the system repository, excepting the metamodel.

This analysis produces:

- a report file (**XML report**)
- an update command file (Upgrade **MGR file**)
  This command file applied to the source environment allows us to obtain the target environment.

Analysis by topic

You can carry out comparison by topic:

- **Metamodel** to compare **MEGA** core metamodel elements:
  - MetaClasses
  - MetaAssociations
  - MetaAttributes
- **Diagram settings** to compare all diagram configuration elements.

  `Example: DIAGRAMTYPEFIELD, MODELTYPELINK, DIAGRAMTYPEPARAM.`
- **Report templates (MS Word)** to compare Report Templates (MS Word).

  ☛ *This option does not cover comparison of report template (MS Word) descriptors and queries.*
- **Descriptors** to compare descriptors.
- **Queries**to compare queries.
- **Web supplies** to compare the main components of Web sites: Site Web template.

  ☛ *Web site descriptors and queries are not analyzed.*
- **MOKA supplies** to compare the main components of MOKA supplies:
  - Project type
  - Phase
  - System diagram
  - Deliverable
  - Project context
- **Generators** to compare the main components of generators:
  - Generator
  - Generation rule
  - Generation kinematics

  ☛ *Generator descriptors and queries are not analyzed.*

This comparison produces a report covering only the differences detected (**XML report**).

Environment Comparator Configuration

You can configure:

- "Configuring the comparison", page 238
- "Configuring the XML Report File", page 238

Configuring the comparison

You can alter comparator behavior depending on your knowledge of modifications carried out in your environment. Avoiding unnecessary comparisons significantly reduces total analysis time.

You can:

- **Compare Translation**

  ☛ *Clearing this option deactivates comparison of translations and reduces processing time by around 20%.*

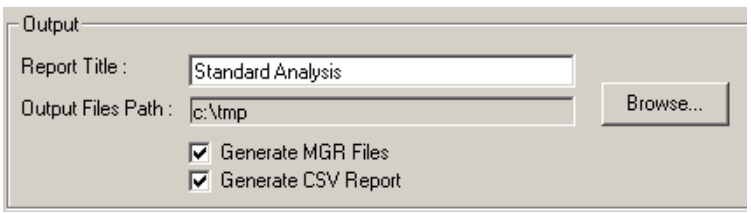
- **Compare Comments**

  ☛ *Clearing this option deactivates comparison of object comments and reduces processing time.*

Configuring the XML Report File

To configure the XML report file, you can modify:

- its name in the **Report Title** field.
- its path in the **Output Files Path** field.



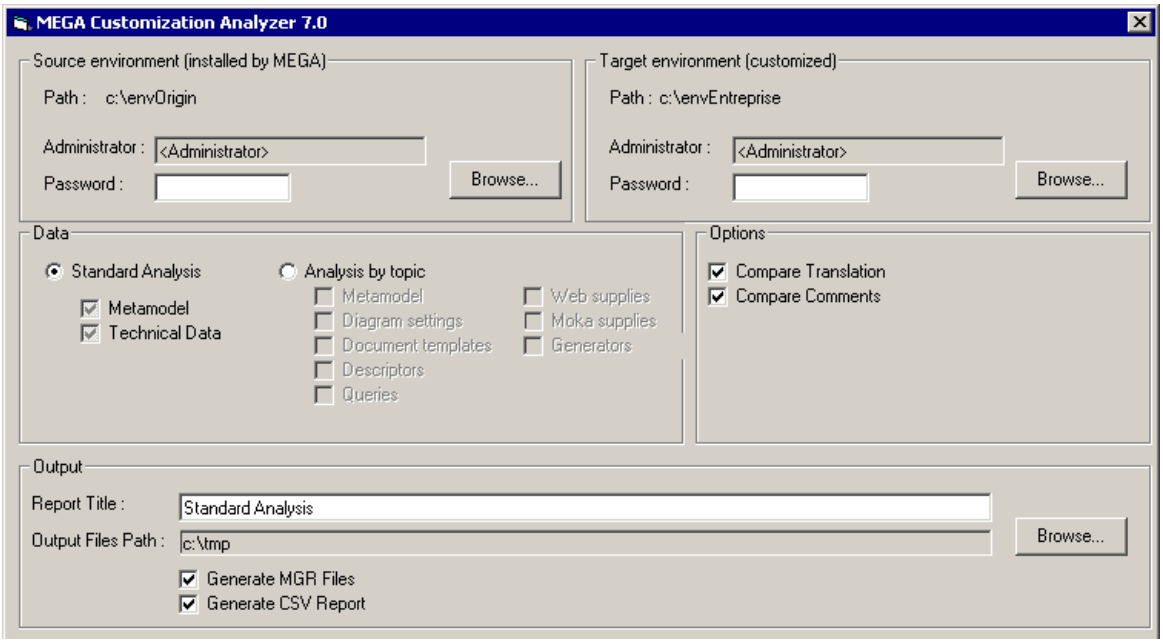
The XML comparison file opens automatically on completion of processing.

Running the Environment Comparison

To compare environments:

1. In the **MEGA** site directory, open **Utilities** folder.

2. In the **MEGA Customization Analyzer** folder, double-click "mgwenvc.exe" file .
   The **MEGA Customization Analyzer** application opens.



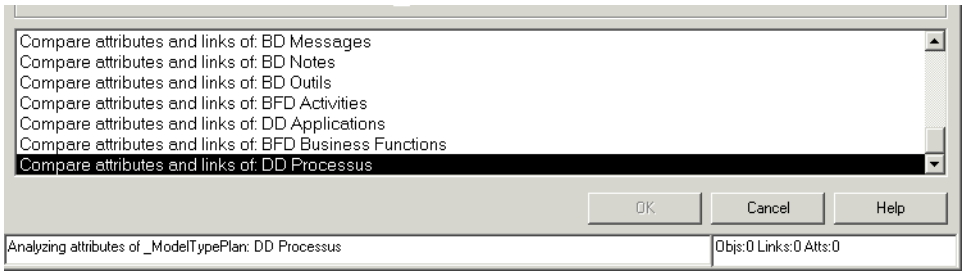
If you have modified your work environment (Target environment) by importing corrective files of type .mol provided by MEGA, you must also apply these to the source environment. In this way the comparison will check out only your modifications.

3. In the **Source environment** pane, click **Browse** to define the **Path** of the source environment installed by **MEGA**.
4. Click **OK**.
   The source environment **Path** is displayed.
5. In the **target environment** pane, click **Browse** to define the **Path** of the target (or customized) environment.
6. Click **OK**.
   The target environment **Path** is displayed.
7. (Optional) The environment standard administrator is selected. If you have deleted this, enter the name of your administrator and password if necessary.
8. Select data to be compared/

   ☛ *See "Comparison Types", page 236.*
9. Define comparison parameters.

   ☛ *See "Environment Comparator Configuration", page 237.*

10. Click **OK**.
    Messages indicate progress of comparison.



The XML report file is generated:

Depending on configuration, it includes a list of objects, links, characteristics and translations, indicating the differences detected. You can change results sort order simply by clicking the different columns.

MANAGING EVENTS

MEGA provides a supervision tool (**MEGA Server Supervisor**) that enables management of events.

The following points are covered here:

INTRODUCTION TO SUPERVISION

The **MEGA Server Supervisor** supervision tool is used to collect messages from **MEGA** applications (**Windows Front-End** and **Web Front-End**). These messages include indicators to ensure that **MEGA** is operating correctly.

```
Example: information or error messages.
```

A message corresponds to a supervision event, which has been previously coded in the executable. A client cannot create a new event.

The following points are covered here:

Prerequisites to Supervision

Before starting supervision function, you must check the following points:

- MegaSSP web application is up and running.
  MegaSSP web application collects all of the messages.
- SSP service is started.
  The SSP stores messages in the supervision log file.
- The Megasite.ini file is configured.

☛ *See "Supervision configuration file: MegaSite.ini", page 241.*

Supervising Events

A supervision event can include about fifty pieces of information.

```
Example: "Event infos" information is a json (or a text)
that can provide details regarding the event context. The
json structure depends on each event.
```

To consult and analyze a supervision event, see "Consulting a supervision event file", page 250.

Event types

Events are sorted by type

- A (Action): user action
- W (Warning): alert
- E (Error): erreur
- S (Snapshot): process snapshot

A type A event is characterized by:

- a start, which corresponds to its creation.
- an end, which corresponds to the moment the message is actually sent. Only one message is sent at the end. It summarizes the indicators of the process for the event duration.

Type W and type E events are immediate.

Type S events summarize the indicators of the process since the last sent snapshot.

Supervision files

Supervision files include supervision events.

Each supervision files represents a day.

Supervision file name format: SSPSPRVSmm-jj-aa.TXT.

```
Example: SSPSPRVS02-10-15.TXT
(supervision file for the 10th of February 2015)
```

To find the supervision file location, see "Finding the supervision file location", page 246.

Supervision configuration file: MegaSite.ini

Configuration of some of the supervision behaviors is performed in the MegaSite.ini file (<**MEGA** installation directory>\Cfg) in [Supervision] section.

In addition, Supervision components need to communicate with the SSP and access the [SSP] section content.

```
[Supervision]
StateInterval=<time interval>
Filter=<Filter>

[SSP]
url=<SSP url>
```

MegaSite.ini	Description
[Supervision]	Supervision parameter section
StateInterval	Time interval (in millisecond) between two supervision events of snapshot type. Minimum value: 1000 By default this parameter value corresponds to 3' (180000) (do not modify this parameter)
Filter	Enables definition of executables to be supervised. Other executable supervision is deactivated. If not specified, there is no filtering and all of **MEGA** executables are supervised. Example: `Filter=AM` Displays only **MEGA Windows Front-End** (code A) and its Administration (code M) events. See "Executable code", page 242. To modify the filter, see "Modifying processes to be supervised (MegaSite.ini filter)", page 246
[SSP]	
Url	SSP url If the url is not specified, supervision is deactivated.

Executable code

Each application is associated with a code:

Windows Front-End:

- A: Administration
  (mgwmapp.exe /DesktopAppGbm.Administration)
- M: MEGA
  (mgwmapp.exe)
- N: Automation
  (API mgwmapp.exe/Automation)

Web Front-End

- R: Session holder (mgwspro.exe)
- T: site (mgwmapp.exe)
- O: SSP environment holder (mgwspro.exe)
- I: SSP site (mgwmapp.exe)

SUPERVISION TOOL: MEGA SERVER SUPERVISOR

The **MEGA Server Supervisor** tool enables reading supervision files.

The **MEGA Server Supervisor** tool gives access to calculated/filtered views of supervision events.

You can activate/deactivate the supervision of certain processes to filter messages. Only selected executables send messages.

☛ *See "Supervision configuration file: MegaSite.ini", page 241.*

See:

Starting Mega Server Supervisor

To start the **MEGA Server Supervisor** tool:

1. In the **MEGA** installation folder, expand the **Utilities** folder, then **MEGA Server Supervisor**.
2. Right-click **MEGA Server Supervisor** and select **Execute as administrator**.

   The **MEGA Server Supervisor** icon appears in the system tray of your workstation.

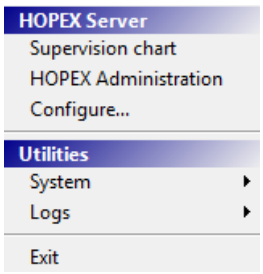
   ☛ *The green button on the icon indicates that the SSP is ready and that IIS is started, else the button is red:* .

Extend MEGA Server Supervisor functionalities

By default, at **MEGA** installation, **MEGA Server Supervisor** menus are minimum.

To extend access to **MEGA Server Supervisor** functionalities:

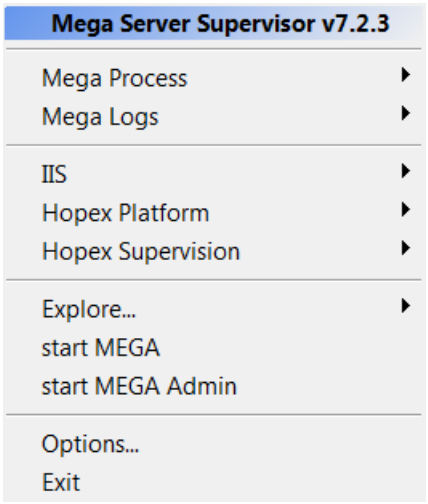
1. In your workstation system tray, right-click **MEGA Server Supervisor** .



2. Click HOPEX Server .
   The **Command** field is displayed.
3. Enter "swl 1" and press "Enter".

All of **MEGA Server Supervisor** functionalities are available.

☛ *To come back to a minimum display, perform step 2 to 3 again.*



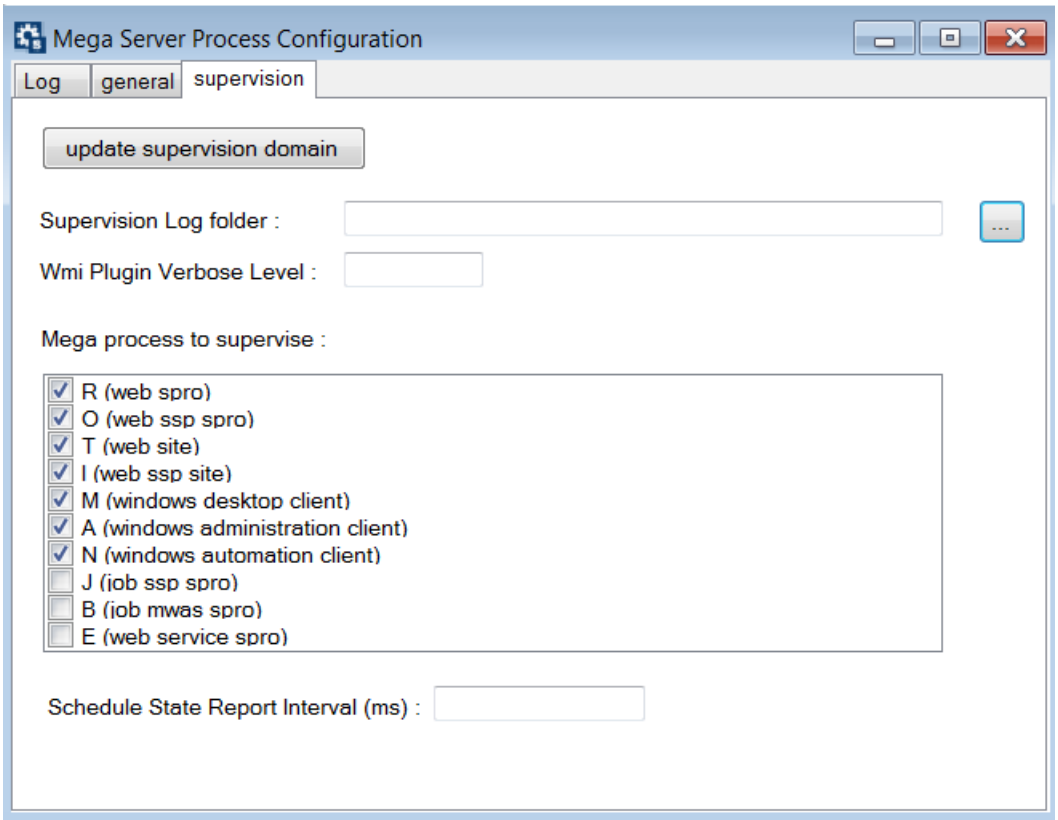
Modifying processes to be supervised (MegaSite.ini filter)

MEGA Server Supervisor enables to configure the **Filter** section of MegaSite.ini file:

☛ *For information on MegaSite.ini file, see "Supervision configuration file: MegaSite.ini", page 241*

To configure the **Filter** section of MegaSite.ini file:

1. In your workstation system tray, right-click **MEGA Server Supervisor** and select **Hopex Supervision > Supervision configuration**.
2. From **Mega Server Process Configuration** window, **Supervision** tab, select the processes you want to supervise.



Your modifications are immediately taken into account in MegaSite.ini file.

Finding the supervision file location

To open the folder where the supervision files are stored:

1. Open **MEGA Server Supervisor** in extended configuration.

☛ *See "Extend MEGA Server Supervisor functionalities", page 245.*

2. From **MEGA Server Supervisor**, select **Mega Logs > Daily Logs Manager**.
3. Right-click the daily log line (sprvs_log_<mm-jj-aa>.txt) and select **Open Folder**.

> ☛ *To modify the supervision file location, see "Modifying the supervision file location", page 247.*

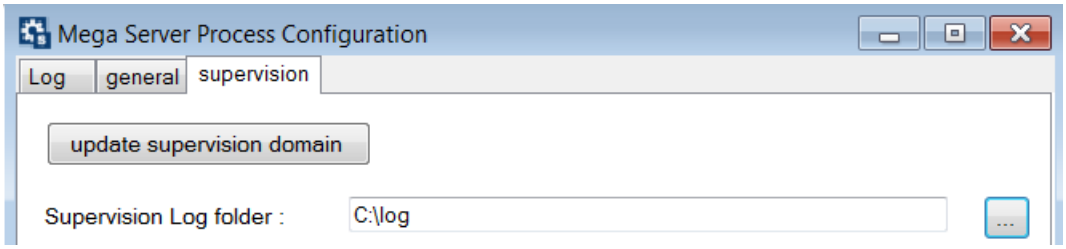
Modifying the supervision file location

To modify the supervision file location:

1. Create the directory where you want the supervision files to be stored.

   `Example: c:\log`
2. From **MEGA Server Supervisor**, select **Hopex Supervision > Supervision configuration**.
3. Select the **Supervision** tab.
4. In the **Supervision Log folder** field, use the browse button **...** to define the directory path where the supervision files are stored.

   `Example: c:\log`



These modifications are immediately taken into account. Supervision files are stored in the specified directory (e.g.: c:\log).

SUPERVISING EVENTS

Event supervision is performed from the **Supervision** tool of **MEGA Server Supervisor**.

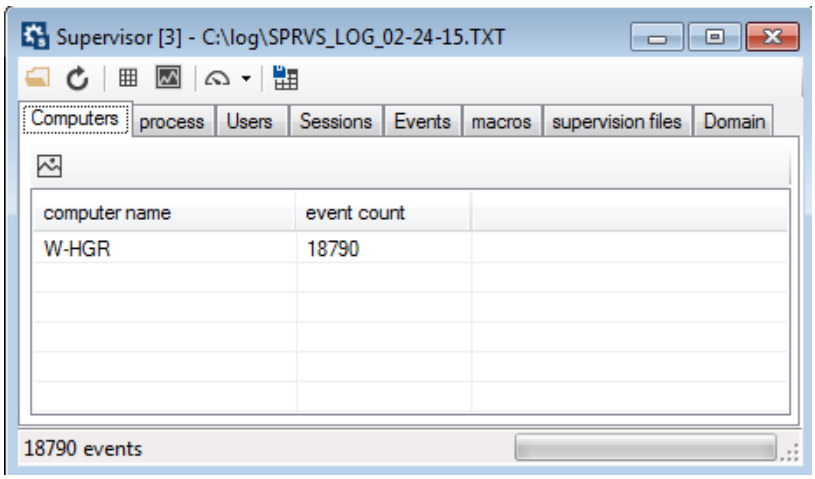
See:

- "Supervision tool", page 248
- "Consulting a supervision event file", page 250
- "Actions from an event supervision window", page 252

Supervision tool

The **MEGA Server Supervisor Supervision** tool opens and analyzes **MEGA** event files.

☛ *To launch* **Supervision** *tool, see "Consulting a supervision event file", page 250.*



For detailed information on event files, see:

- "Supervising Events", page 240
- "Supervision files", page 241.

Supervision tool toolbar

From **Supervision** tool toolbar, click:

-  to open one or several specific supervision files
-  to refresh calculated view data of the current supervision file
-  to open the set of snapshots that have been created on the different servers.
  A consolidated snapshot gives an application calculated view over the last three minutes.
-  to view the load state, object consumption on the set of supervised processes.
-  to load a supervision domain (reference domain - Standard) so that comparisons can be made.
-  export data in CSV format.

Supervision tool tabs

In the **Supervision** tool, events are grouped by calculated view that gives access to the corresponding list of prefiltered events. Views correspond to the following tabs:

- **Computers**
  This tab shows the list of servers used and its associated event number.
- **process**
  This tab shows the set of supervised processes of the set of servers.
- **Users**
  This tab shows the list of users who logged on the application.
- **Sessions**
  This tab shows the list of current or past sessions of all the servers or workstations supervised.
- **Events**
  This tab shows the list of HOPEX events that have been recorded.
- **macros**
  This tab enables to view macros, for which execution time is high.
- **supervision file**
  This tab shows analyzed supervision files.
- **Domain**
  This tab enables to show activity synthesis according to the supervision domain

Consulting a supervision event file

To consult an event of a supervision file:

1. From your workstation system tray, right-click **MEGA Server Supervisor** and select **Supervision**.

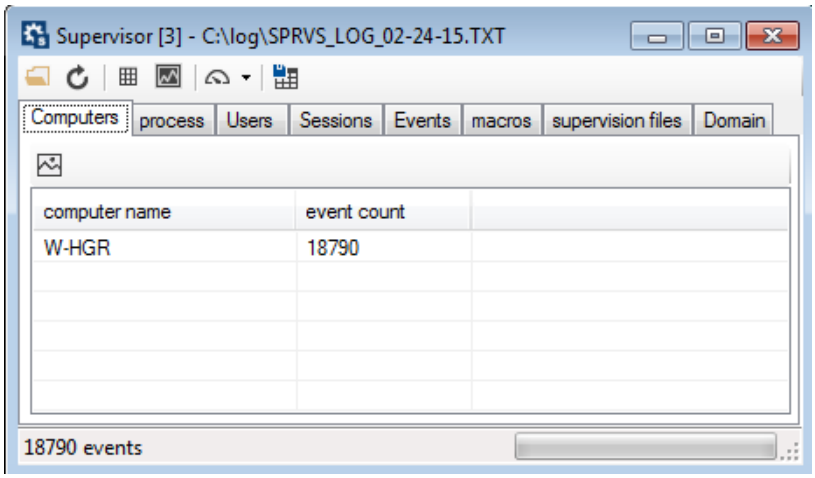
   ☛ *If **MEGA Server Supervisor** is in extended configuration (see "Extend MEGA Server Supervisor functionalities", page 245), select **Hopex Supervision > Supervision**.*

   The current supervision file opens.

   ☛ *To open another (or several) supervision file , if **MEGA Server Supervisor** is in extended configuration select **Hopex Supervision > Supervision from file** and select the files.*

   *Alternatively, from **Supervision chart** toolbar, click **Open Supervision data file** and select the files.*

   See "Finding the supervision file location", page 246.



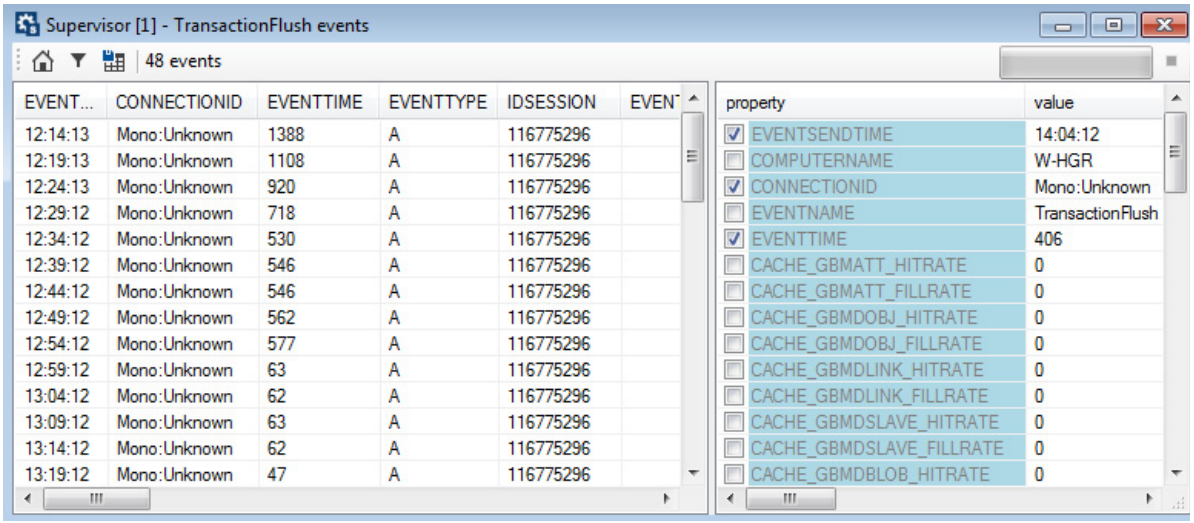
2. (optional) If you are on the current supervision file, click **Refresh** anytime you want to immediately refresh the view data.

   ☛ *See "Supervision tool tabs", page 249.*

3. Click the tab regarding the view you want to consult:

   ☛ *See "Supervision tool tabs", page 249.*

4. Double-click the line of the view you want to consult the events.
Events regarding this view are displayed in table format.



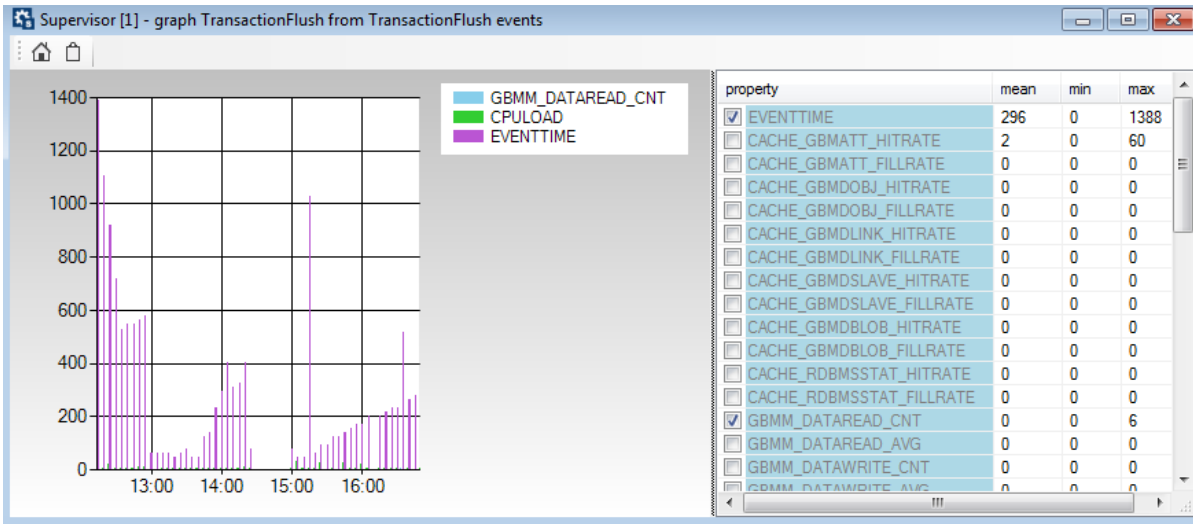
Each line represents an event of which characteristics are detailed.

☛ *See "Actions from an event supervision window", page 252.*

5. (optional) In the **property** pane, select the indicators (columns) you want to be displayed in a table column.
6. (optional) Right-click the event for which you want to display a graph and select **show graph for <event name>**.

☛ *You cannot get a graph for an Error type or Warning type event.*

The graph is displayed.



7. In the **property** pane, select the indicators you want to be displayed in the graph.
   The graph is calculated on the set of the prefiltered original view, taking into account the event selected.
8. (optional) Click **copy graph image to clipboard** to copy the graph image in the clipboard.

Actions from an event supervision window

From the supervision window, which lists the events in table format, you can:

- access the window of the source **Supervision chart** tool.

  Click **Supervisor Home** .
- create filters to filter displayed events.

  Click **Filters** .
- export current events in .txt format.

  ☛ *Example: to import events in Excel.*

  Click **Export the current filter view as supervision format** .
- interrupt data downloading.

  ☛ *Example: when experiencing long downloading times.*

  Click **Interrupt loading** .

EVENTS TO BE MONITORED (PRODUCTION SERVER)

To keep your HOPEX production server in the best operating conditions, here are the events you have to monitor:

In the following tables, each event **Type** column indicates the importance level of the event as follows:

- severity ++: requires an immediate action
- severity ++: requires a rapid analysis
- severity -: requires your attention
- severity --: informative

Events: Login and Authentication

Events you have to monitor in a login and authentication context are listed in the following table:

Event	Type (severity)	Context / JSON	Description / Content
LoginPasswordChangeFailure	Alert (+)	***Password update***	***Error during a password update***
		`"Login Name":`	`Name of the login`
LoginAuthenticationFailure	Alert (-)	***Authentication***	***Failure in the authentication process***
		`"Login Name":`	`Name of the login`
		`"Failure reason":`	`Error message`
LicenseLoginFailure	Alert (+)	***License***	***Error while obtaining a license token***
		`"Failure reason":`	`Error message`

Events: Configuration Management

Events you have to monitor in a configuration management context are listed in the following table:

Event	Type (severity)	Context / JSON	Description / Content
GraphCompile	Action (--)	***Writing access diagram compilation***	***Should never happen on a production server*** Except after the update of a new writing access hierarchy definition
MetaDataCompile	Action (--)	***Environment compilation***	***Should never happen on a production server*** Except after the update of new customization
CompiledDataReset	Alert (+)	***Meta or technical data modification***	***Should never happen on a production server*** If this event is raised on a server, it means that a person is carrying out MetaModel extensions directly on the server
		`"User":`	`User responsible for the update`
		`"CompiledDataUpdated":`	`Modified object`
		`"CompiledDataResetOrigin":`	`Executed command.` This information is written during the upgrade or import process
GraphUpdate	Alert (+)	***Writing access diagram modification***	***Should never happen on a production server*** Except after the update of a new writing access hierarchy definition

		`"GraphUpdated":`	`"Authorization"`
			if the writing access diagram has been updated
			`"Visibility"`
			if the reading access diagram has beenupdated

Events: Workspace Activity

Events you have to monitor in a workspace activity context are listed in the following table:

Event	Type (severity)	Context / JSON	Description / Content
TransactionFlushFailure	Alert (++)	***Workspace flush***	***Unable to validate data update***
		`"Failure reason":`	`Error message`
TransactionDispatchFailure	Alert (++)	***Workspace publication***	***Failure in the authentication process***
		`"Failure reason":`	`Error message`

Events: Repository Connections

Events you have to monitor in a repository connection context are listed in the following table:

Event	Type (severity)	Context / JSON	Description / Content
RepositorySessionConnect	Action (--)	***Connection (session)***	***This event enables to monitor the connection times***
		`"GBMSESSIONOPENMODE":`	One of the following values: `GBMSESSION_OPENMODE_READWRITE` `GBMSESSION_OPENMODE_READONLY_PHYSICAL` `GBMSESSION_OPENMODE_READONLY_LOGICAL` `GBMSESSION_OPENMODE_READONLY_REALTIME` `GBMSESSION_OPENMODE_READWRITE_REALTIME`
		`"Login":`	`IdAbs of the login`
		`"User":`	`IdAbs of the user`
		`"Profile":`	`IdAbs of the profile`
		`"Role":`	`IdAbs of the business role`
		`"pathDB":`	`Path of the SystemDb repository of the Environment`

Event	Type (severity)	Context / JSON	Description / Content
RepositorySessionConnectFailure	Alert (+)	**Connection**	**Error during the session connection phase**
		"GBMSESSIONOPENMODE":	One of the following values: GBMSESSION_OPENMODE_READWRITE GBMSESSION_OPENMODE_READONLY_PHYSICAL GBMSESSION_OPENMODE_READONLY_LOGICAL GBMSESSION_OPENMODE_READONLY_REALTIME GBMSESSION_OPENMODE_READWRITE_REALTIME
		"Login":	IdAbs of the login
		"User":	IdAbs of the user
		"Profile":	IdAbs of the profile
		"Role":	IdAbs of the business role
		"pathDB":	Path of the SysDb repository of the Environment
		"Failure reason":	Error message
RepositoryOpenFailure	Alert (+)	**Repository opening phase**	**Error detected when opening a repository**
		"RepositoryName":	Name of the repository
		"Failure reason":	Error message
RepositoryCloseFailure	Alert (-)	**Repository closing phase**	**Error detected when closing a repository**
		"RepositoryName":	Name of the repository
		"Failure reason":	Error message
RepositorySessionReconnect	Alert (++)	**The connection with the database server has been lost**	**HOPEX is trying to reconnect automatically to the server, each try generates an alert (5 by default)**
		"RepositoryServerName":	Name of the repository

Events: Service Execution

Events you have to monitor in a service execution context are listed in the following table:

Event	Type (severity)	Context / JSON	Description / Content
ScheduledJobExecutionFailure	Alert (+)	**Job execution**	**Error when running a scheduled job**
		`"Failure reason":`	`Error message`
SchedulerError	Error (+)	**Scheduler service start**	**Unable to run the scheduler service due to a lack of license or other reason (see msg)**
		`"Msg":`	`Error message`
ProcessException	Error (++)	**Important exception occurred**	**Important error occurred when running HOPEX**
ERQLExcessiveInvocationTime	Alert (-)	**An ERQL query executing more than 5000 GBM commands**	**Optimizing the query manually**
		`"QueryId": or "QueryName":`	Query identifier
		`"GBM Get count":`	Number of readings generated by the query
		`"GBM Get count":`	Number of searches generated by the query

7

MANAGING OBJECTS

The following points are covered here:

EXPORTING MEGA OBJECTS

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 **MEGA** objects from a library includes objects present in the library and their dependent objects.

The following points are detailed here:

Export

You can export common modeling objects as well as configuration and parameterization objects.

```
Examples: report templates (MS Word), queries, metamodel
extensions, users.
```

To access these objects, you must select the extended metamodel options in your configuration. This option is available in user options, from the **Repository** icon.

☛ *See "Managing Options", page 365.*

Export uses the propagation mechanism, which can be configured using perimeters.

☛ *For detailed information, see the **Perimeters** chapter in the **HOPEX Studio - MetaStudio** guide.*

Propagation steps in organizational process (major) export:

1. For an organizational process (major) you also export its operations (minor).
2. For an operation you export the event messages or result messages (minor) of the operation (major)
3. Propagation continues step by step until all links have been explored.

   ☛ *Export takes account of link types: for certain link types, search in depth of other links stops.*

   All keywords are also exported.

Exporting Objects

You can export **MEGA** objects from:

- Web Front-End:
  - the **Administration** desktop
- Windows Front-End:
  - the **MEGA Administration** application
  - of your **MEGA** workspace.

You can export objects in the following formats:

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

  ☛ *For more details on .MGR file syntax, see "Command File Syntax", page 403.*
- **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".*
- **Excel**

  ☛ *See **MEGA Common Features** guide, "Exchanging Data With Excel" chapter.*

Exporting MEGA Objects from the Administration desktop (Web Front-End)

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

1. Connect to the **MEGA Administration** (Web Front-End) desktop.

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*
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 **Mega 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).

     ☛ *For further information on merging objects, see "Merging Two Objects", page 280.*
   - **Propagate** exports the objects listed together with their dependent objects.

     ☛ *To view objects before export, see "Viewing Objects Before Export", page 267*
6. In the **Objects to export**, click **Add objects to list**  .
   The selection 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.

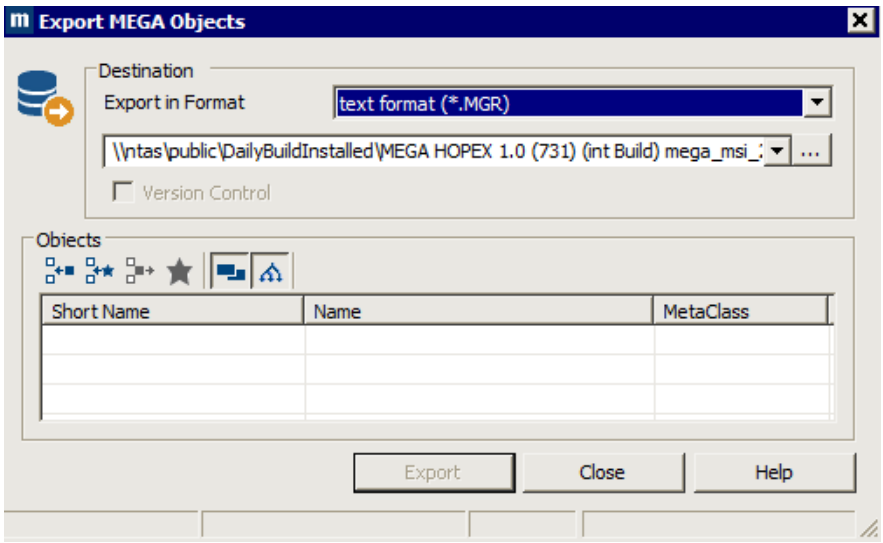
    ☛ *For more details on updating a repository by command file import, see "Updating a Repository", page 162.*

Exporting MEGA objects from MEGA Administration

To export **MEGA** objects from **MEGA Administration**:

1. Open **MEGA Administration** and select the repository from which you want to export objects.

   ☛ *See "Accessing Repositories", page 138.*
2. Right-click the desired repository and select **Object Management > Export Objects**.
   The **Export MEGA Objects** dialog box opens.



3. In the **Export in Format** field, select the export file format.
   Several options enable object export configuration.

   ☛ *See "Managing Options", page 365.*
4. (Optional) Enter a different name and folder if the default values are not suitable.

   ☛ *Button ... enables you to browse the folder tree and select where the export file will be located.*
5. In the **Objects** frame, click **Add Objects to List**.

   ☺ *To simplify the query, click* **Add objects to list from favorites**.

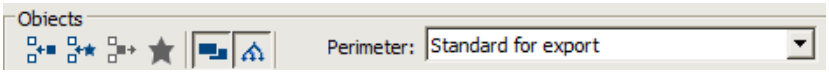
   The selection dialog box appears.
6. Start the query and select the appropriate objects in the result window.

7. Click **OK**.
   The selected objects are added to the **Export MEGA Objects** dialog box list, preceded by their type.
   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.*
8. In the **Objects** group box, by default two export configuration options are proposed:
   - **Include Objects of Merging**, which allows you to export technical objects resulting from merging objects (_TransferredObject).

     ☛ *For further information on merging objects, see "Merging Two Objects", page 280.*
   - **Propagate**, which allows you to export listed objects together with their dependent objects.

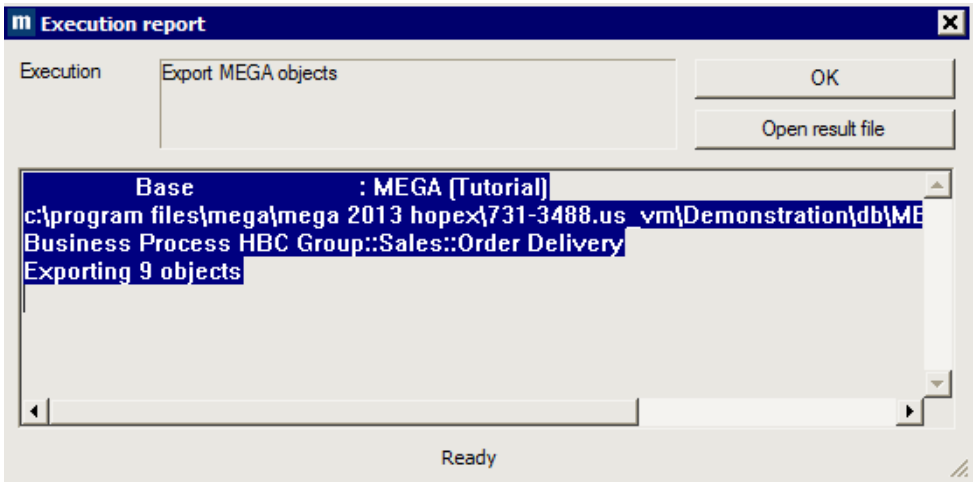
     ☛ *To view objects before export, see "Viewing Objects Before Export", page 267*
9. (Optional) By default, the export perimeter is as defined in the properties of the Export tool. To modify the export default perimeter, you must have previously activated export perimeter selection, see "Activating the export perimeter selection option", page 267.
   In the **Objects** frame, select the **Perimeter** of export using the drop-down menu.



10. When selection is complete, click **Export**.
    The export process begins.

    ☛ *To interrupt export during execution, click **Cancel**.*
    During export, the name and type of the objects being exported appear at the bottom of the dialog box, together with duration of export. On

completion of export, the **Execution Report** displays the number of exported objects.



☛ *See "Viewing an export file (Windows Front-End)", page 266.*

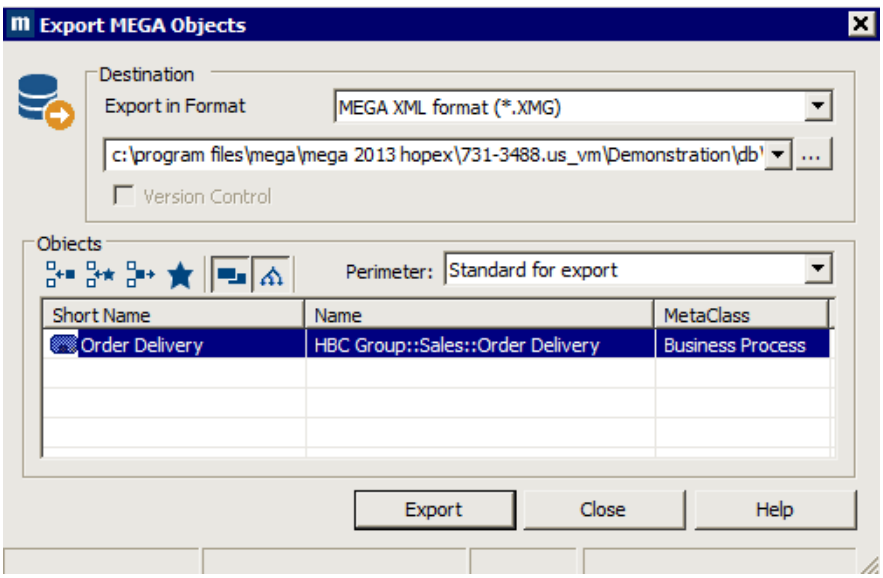
Exporting MEGA objects from the MEGA desktop

To export a **MEGA** object from the **MEGA** desktop:

1. In the **Main Objects** navigation window, right-click the object you want to export and select **Manage Export**.

   ☛ *You can also export **MEGA** objects by selecting **File > Export > MEGA Objects** in the workspace.*

   The **Export MEGA Objects** dialog box opens.



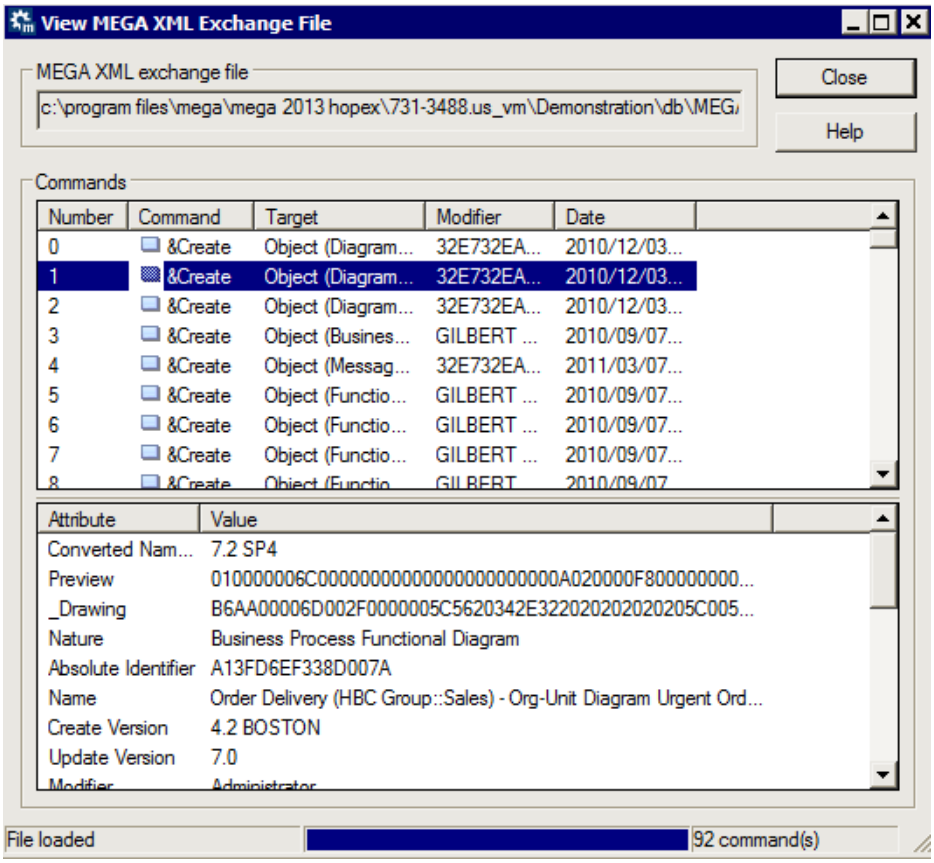
   In the **Objects** frame, the object to be exported is already selected.

2. Refer to the procedure "Exporting MEGA objects from MEGA Administration", page 262.

Viewing an export file (Windows Front-End)

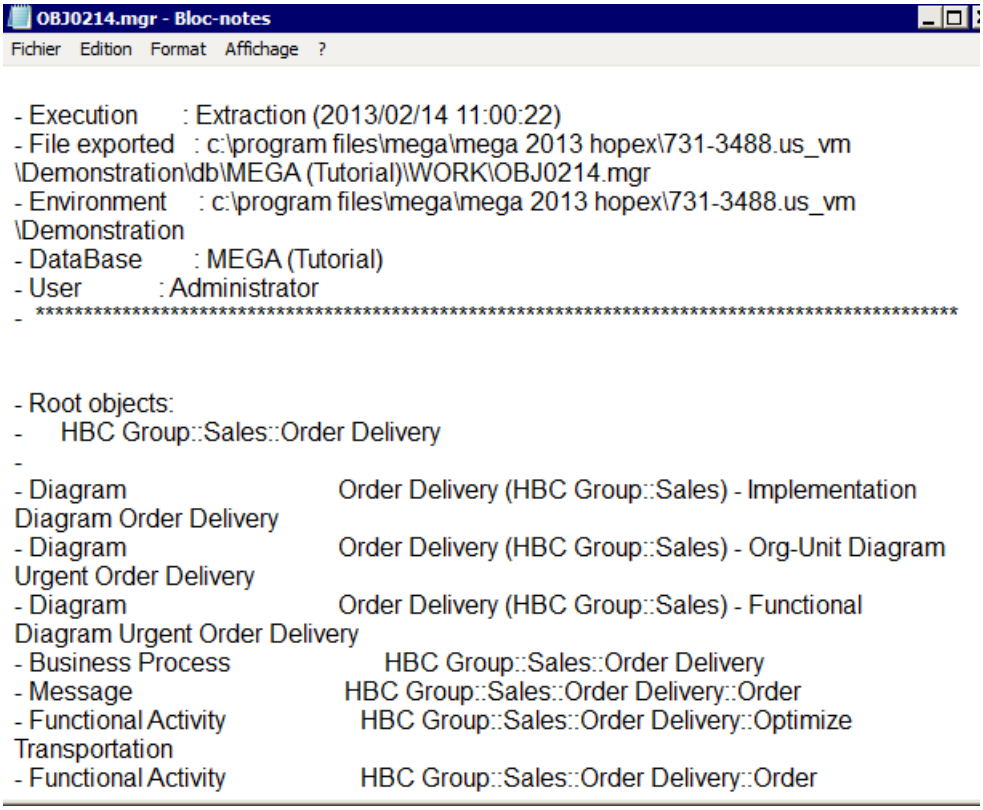
To view the exported file:

1. In the export **Execution Report** dialog box, click **Open result file**
   In the case of:
   - an export in **MEGA** XML format, the view MEGA XML exchange file dialog box appears.



This file is presented in the form of a table showing a list of commands. Corresponding to each command ("Create", "Connect", etc.) there is a an object, object modification date and name of the last modifier.

- export in text format, the Notepad dialog box appears:



This file lists all objects in text format.

The exported file can then be imported into another repository.

☛ *For more details on updating a repository by command file import, see "Updating a Repository", page 162.*

Activating the export perimeter selection option

At the time of export, to be able to select export perimeter, you must activate the **Activate export perimeter selection** option:

1. From your **MEGA** workspace, select **Tools > Options**.
2. In the MEGA **Data Exchange > Export > Files** option group: **Generic Options** select the **Activate export perimeter selection** option.

Viewing Objects Before Export

☛ *Viewing of objects is available with the **MEGA Supervisor** technical module.*

Viewing models with a perimeter allows preview of the operation result before its execution, and modification of the operation if required. You can therefore:

- see default impact of the applied perimeter, see "Viewing objects", page 268.
- modify behavior of the perimeter according to the different types of links browsed from the root object, see the **MetaStudio** guide.

In the case of object export, other objects (connected to the root object) are also exported - they are determined by behavior of the "***Standard for export***" perimeter related to links existing around the root object.

☺ *Before exporting one or several **MEGA** objects, you may find it useful to view all objects that will be exported. These can be objects you have selected as well as those deduced by the propagation mechanism.*

☛ *For more information on perimeters, see the **HOPEX Studio - Mega Studio** guide.*

Enabling the view option

To view objects that will be exported, you must enable the **View objects before export** option:

1. From your **MEGA** workspace, select **Tools > Options**.
2. In the MEGA **Data Exchange > Export > Files** option group: **Generic options** select **View objects before export** option.

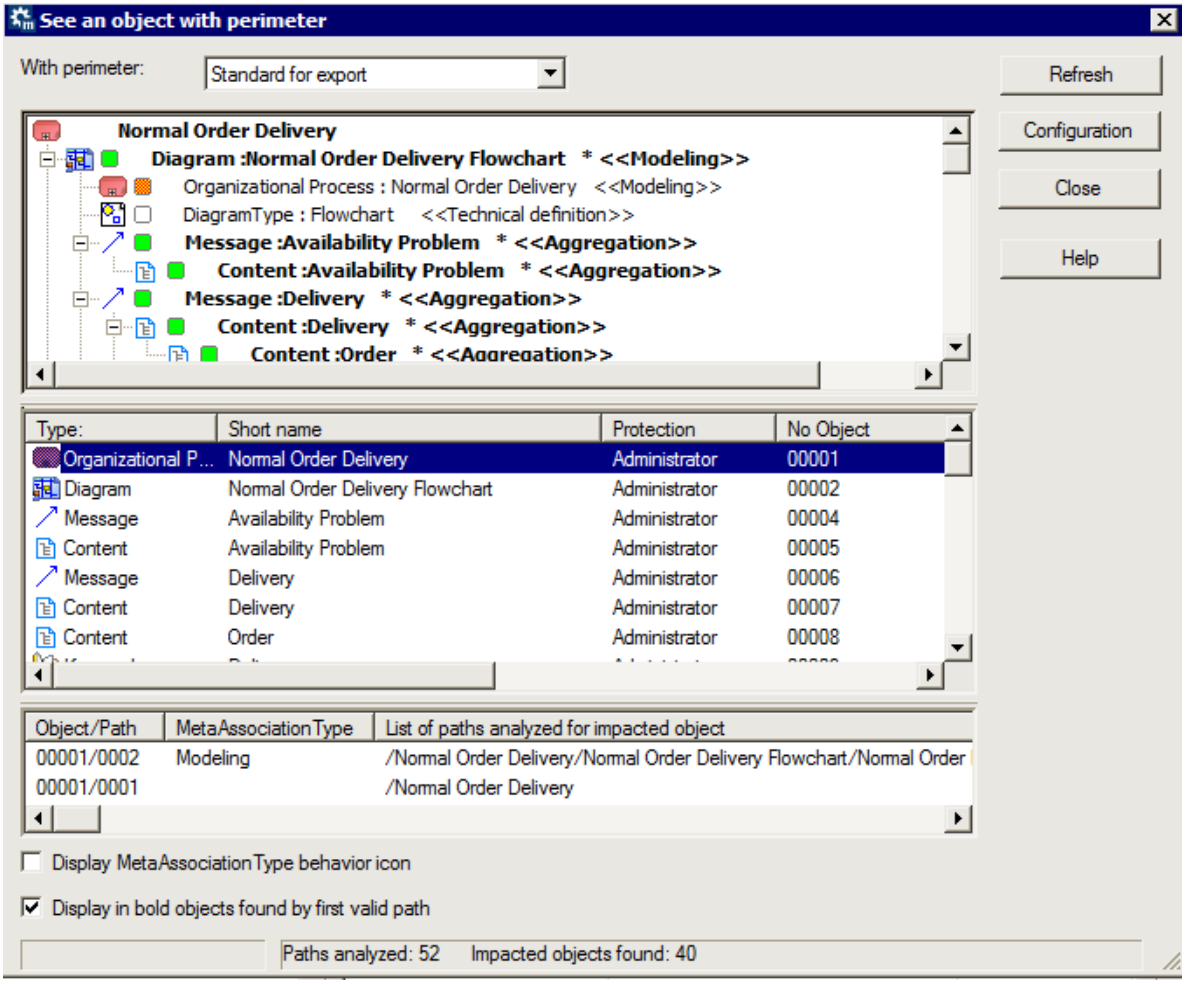
Viewing objects

To view objects that will be exported:

1. Select menu **Tools > Options**.
2. In the MEGA **Data Exchange > Export > Files** option group: select the **View objects before export** option.

   The **View** button  appears in the **Objects** frame.

3. In the **Export MEGA Objects** dialog box, select an object in the list and click **View** .
The object detailed view window appears.



The ***See an object with perimeter*** window presents all exported objects in two ways (result of propagation applied to the root object):

> ☛ *To view the impact of other perimeters on the object concerned, select another **Perimeter** in the drop-down list.*

- The top frame presents, in tree form, the objects that will be exported with the root object. For each object it details:
  - the propagation behavior defined by the "***Standard for export***"perimeter for the link browsed.

The behavior of this operator depends on the various link types and will determine the objects that will also be exported.
- the corresponding link type (for example ***Modeling***).
- the propagation type (identified by an icon) that will be executed on the object.

Table: Description of propagation behaviors

Icon	Value	Propagation description
	***Deep***	***Recursive complete propagation***: Takes into account this link and the opposite object only. Propagation continues.
	***Standard***	***Simple propagation***: Takes into account this link and the opposite object only. Propagation stops.
	***Link***	***Limited propagation:*** Takes into account this link but not the opposite object. Propagation stops.
	***Abort***	***No propagation:*** Does not take into into account this link or the opposite object. No propagation:

You can customize display of these results by selecting:
- **Display MetaAssociationType behavior icon**, which presents propagation behavior defined for the MetaAssociationType.
- **Display in bold objects found by first valid path**.

- the middle table lists objects that will be exported with the root object. For each object it details:
  - the number of paths linked to the object.
  - the comment associated with the object.
  - the bottom table details all paths by which the object selected in the middle table has been found, together with the corresponding link type (MetaAssociationType).

To locate an object/path in the tree:

1. From one of the tables, right-click the object/path you want to locate and select **Find in tree**.

The **Configuration** button accesses the perimeter configuration tool.

☛ *For detailed information, see how to configure a perimeter in the **HOPEX Studio - MEGA Studio** guide.*

PROTECTING OBJECTS

The object protection function is available with the **MEGA Supervisor** technical module.

An object has the writing access level of the user who created it. The writing access level of an object can be modified:

- directly
- by its dependence on another object (project, process, etc.) by propagating the authorization level for that object. This dependence may be indirect.

  ☛ *See "Viewing Objects Before Export", page 267 for more details.*

See:

- "Accessing the Object Protection Management Window", page 271
- "Assigning a Writing Access Area to an Object", page 272
- "Propagating Authorizations Between Linked Objects", page 273

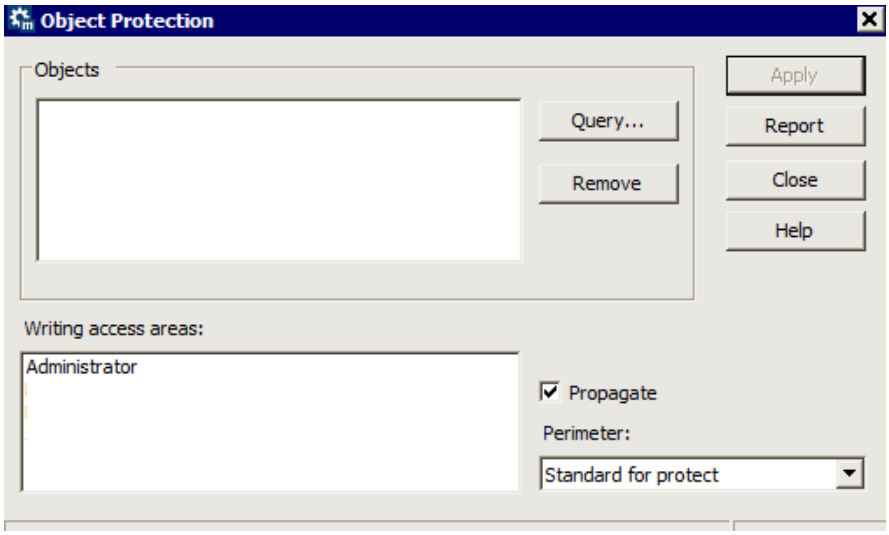
Accessing the Object Protection Management Window

To access the object protection management window:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **Repositories** folder.

3. Right-click **SystemDb** and select **Object Management > Protect Objects**.
   The **Protect objects** dialog box opens.



   The **Writing Access Areas** list presents the writing access area of the user accessing the dialog box, and if appropriate, its dependent access areas (it is not possible to assign writing access areas higher than its own writing access area).

   Writing access areas are identified by level.

   When you open this dialog box, its **Objects** list is empty.

   ☛ *See "Assigning a Writing Access Area to an Object", page 272.*

   ☛ *See "Propagating Authorizations Between Linked Objects", page 273.*

Assigning a Writing Access Area to an Object

To assign a writing access area to an object:

1. Access the **Object Protection** window.

   ☛ *See "Accessing the Object Protection Management Window", page 271.*

2. In the **Writing Access Areas** list, select a writing access area.
3. Click **Query** to start a query.
4. Run the query, select the appropriate objects from the results, and click **OK**.
   The selected objects are added to the **Protect objects** dialog box list. Their types are also displayed.

   ☛ *You can carry out this procedure several times, allowing you for example to protect objects of different types.*

   ☛ *In event of error, select the unwanted object in the list and click **Delete**.*

5. Select the objects in the list.

6. When selection is complete, click **Apply**.
   The objects are assigned the selected protection level.

   ☛ *You can select some objects in the list and assign one authorization to these, then select other objects and assign a different writing access level without executing a new query.*

Propagating Authorizations Between Linked Objects

You can automatically assign writing access level of an object to objects linked directly or indirectly to it.

1. Access the **Object Protection** window.

   ☛ *See "Accessing the Object Protection Management Window", page 271.*
2. Click **Query** to select the objects concerned.
3. In the **Writing Access Areas** list, select a writing access area.
4. Select the **Propagate** check box.
5. Click **Apply**.
   Objects dependent on those for which propagation is requested are protected with the same writing access level.

   ☛ *For more details, see "Viewing Objects Before Export", page 267.*

   ☛ *Note that this type of propagation may modify the authorizations for objects shared by several projects or diagrams.*

Comparing and Aligning Objects Between Repositories

☛ *The object compare and align feature is available with the **MEGA Supervisor** or the **HOPEX Collaboration Manager** technical module.*

MEGA enables comparison and alignment of:

- two complete repositories
- objects in different repositories
- objects of the public repository with those of the current private workspace.
- a file and a repository (or repository objects)
- two repository archived states

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

See:

- "Compare and Align Principle", page 274
- "Compare and Align Warnings", page 275
- "Comparing and Aligning Two Repositories", page 275

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 **MEGA** 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.

☛ *For more details on repository log, see "Managing logfiles", page 146.*

The repository log is not transferred from one repository to the other: a newlog 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.

☛ *For more details on writing and reading access management, see "Managing Data Reading Access", page 321 and "Managing Data Writing Access", page 297.*

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**.*

Comparing and Aligning Two Repositories

☛ *Before comparing and aligning, see "Compare and Align Warnings", page 275*

To compare and align two repositories:

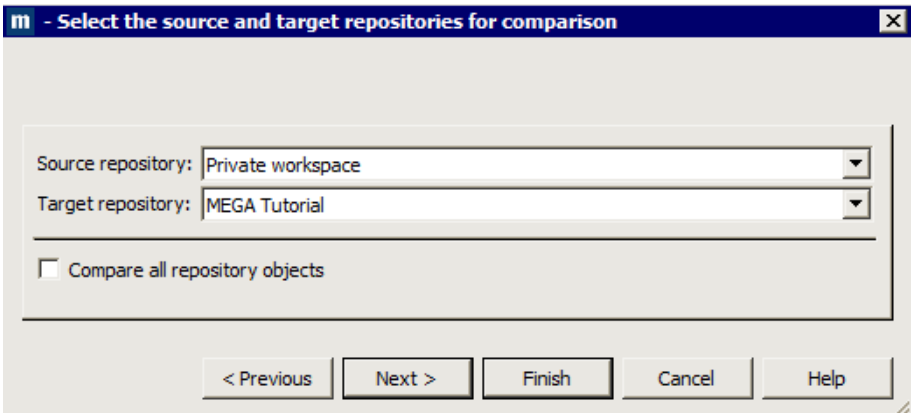
1. From your **MEGA** desktop:
   - **(Windows Front-End)**, in the **MEGA** menu bar, select **Tools > Manage > Compare and Align**.

     ☛ *Alternatively, right-click the object and select **Manage > Compare and Align**.*

     ☛ *Or, from **MEGA Administration**, in the environment concerned, right-click the repository concerned and select **Compare and Align**.*
   - **(Web Front-End)**, right-click the object and select **Manage > Compare and Align**.

   The object comparison wizard opens.
2. Indicate if you want to compare:
   - two repositories
   - two current repository archived states (RDBMS repository only)
   - a file and a repository
3. Click **Next**.
4. Select:
   - the **Source repository**
   - the **Target repository**, which is the repository to be updated.

     ☛ *It can be a private workspace of the repository.*



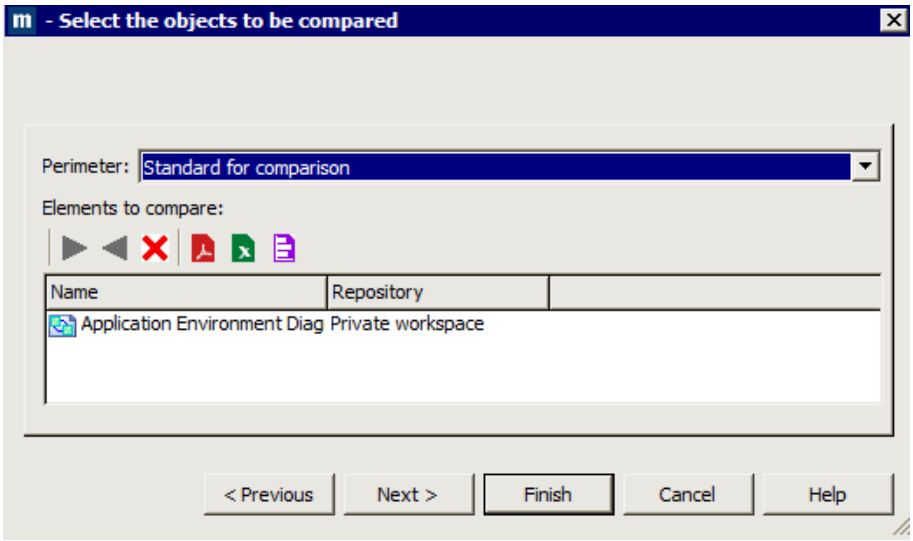
5. (Optional) If required, you can choose to **Compare all repository objects**.

   ☛ *Processing of this option can take some time.*
6. Click **Next**.
   The dialog box for selection of objects to be compared opens.
7. In the **Perimeter** field, select the perimeter type (by default **Standard for Comparison**)

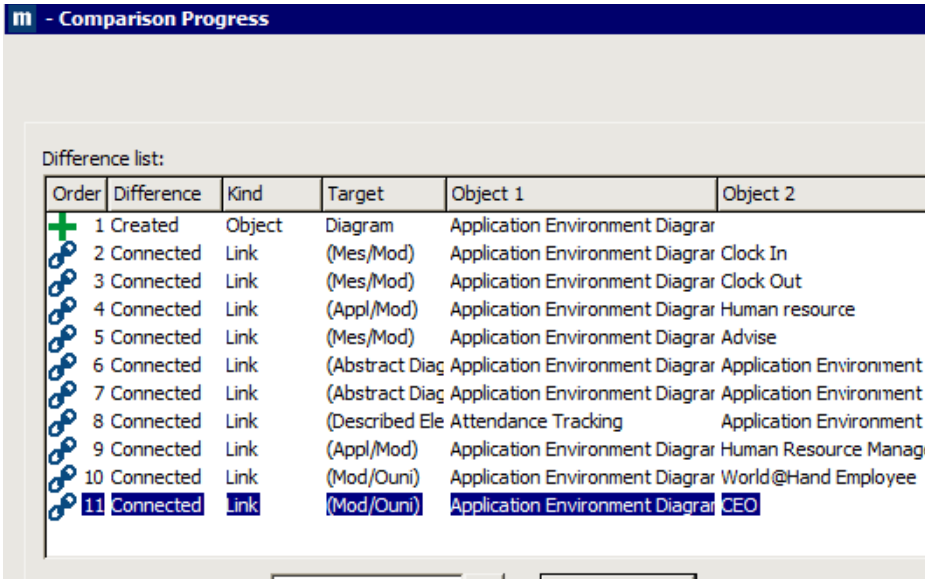
   ☛ *For detailed information on perimeters, see **HOPEX Studio - MEGA Studio** Technical Article.*

8. In the **Elements to compare** pane, select:
   - to add objects from the source repository, or
   - to add objects from the target repository, or

     ☛ *If you opened the comparison wizard from an object, this is automatically added in the list of objects to be compared.*



9. Click **Next**.
   The **Comparison Progress** window opens. It presents the differences between compared objects and their modifications.



   The **Difference** column presents differences by update category:
   - ***Created***: objects not existing in the target repository.
   - ***Deleted***: objects existing in the target repository but not in the source repository.

     ☛ *Deletion commands of compare and align can be generated in a separate file. To do this, activate the corresponding option in **Options > 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.
10. (**Windows Front-End**) In the **Generate a difference file** field (.mgr format):
    - Click ... and enter the name and location of the comparison file, then click **Save**.
    - Click **Generate** to generate the .mgr file that contains the list of differences detected.
11. (Optional) Click **Generate Report** to generate the report (.pdf format) which contains:
    - the list of differences detected
    - statistics

12. Click **Next**.
    Differences are imported in the target repository.
    The target repository is aligned with the source repository.

    ☛ *An alignment file with the content of differences (align-YYYY-MM-DD-hh-mm_555.mgr) is automatically saved in folder <Environment Name>\Db\<Repository Name>\USER\<User Code>.*

    ☛ *If the alignment contains rejects, click **Display Rejects** to open the alignment rejects file (format .mgr).*

    A rejects file is automatically saved in folder <Environment Name>\Db\<Repository Name>\USER\<User Code> (rejects file-reject-YYYY-MM-JJ-hh-mm_555.mgr). This file is empty if alignment does not contain rejects.
13. Click **Finish**.

MERGING TWO OBJECTS

The object merge feature is available with the **MEGA Supervisor** technical module.

When you merge two objects, you obtain a single object by transferring the *characteristics* and *links* from one object to the other. The source object is deleted. It is therefore recommended that merges be done in a new private workspace, so you can discard the changes if the result is not satisfactory.

You must have administration rights to merge two objects.

Choice of the objects to be merged

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

- its characteristics are not modified
- merging proposes addition of source object links.

The **Source** object is the object of which:

- you want to reuse certain characteristics or certain links
- characteristics and links will be transferred to the **Target** object.

When the link is to be a unique link (e.g., for sub-typing where the type is unique), the link of the target object is kept by default.

When merging is completed, the source object is deleted.

*You can **Explore** objects using the corresponding command. It can also be used to explore their links.*

Merging Two Objects

To merge two objects:

1. Connect to **MEGA**.

   "Connecting to MEGA", page 188.

2. In the menu bar, select **Tools > Manage > Merge Two Objects**.
   The first step of the **Merge Objects** wizard appears: **Object selection**.

   To have the right to merge two objects, you must have the right to delete objects.

3. In the **Object** pane, select the object type to be merged.

   See "Choice of the objects to be merged", page 280.

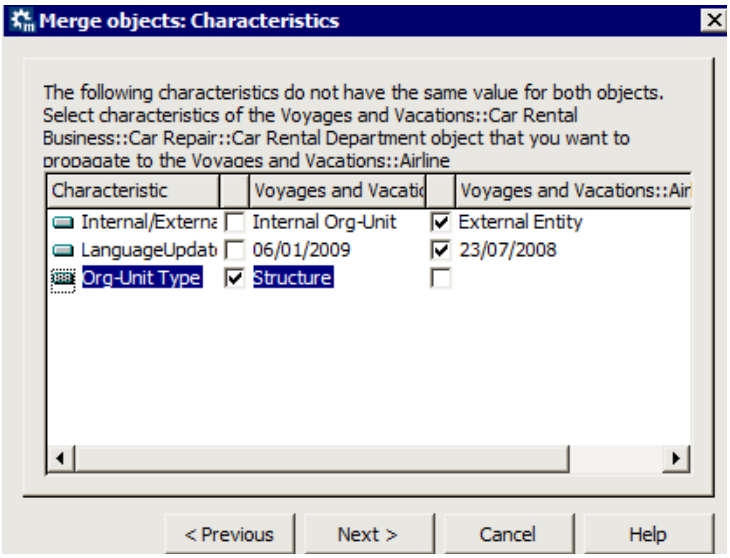
4. In the **Source** field, click the arrow and select the source object.
5. In the **Target** field, click the arrow and select the target object.

6. Click **Next**.

   ☛ *If the target and source objects are the same, the **Next** button is disabled.*

   The second step of the **Merge Objects** wizard appears: **Characteristics**. It presents the differences found in characteristic values of both objects.

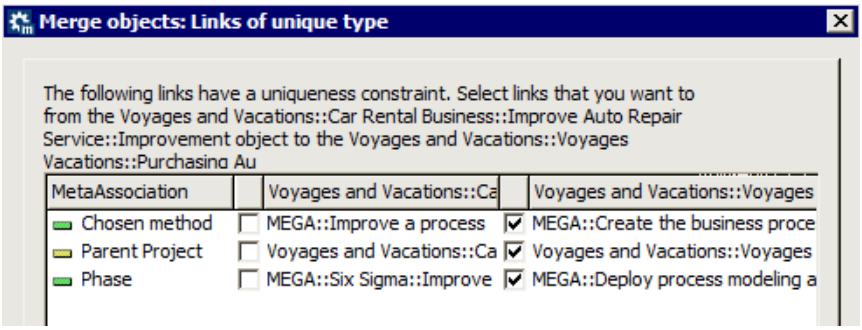
7. Select the source object characteristics you want to transfer to the target object. Characteristics that remain selected in the target object are kept.



8. Click **Next**.
   The third step of the **Merge Objects** wizard appears: **Unique links** (those that can only exist once for a given object).

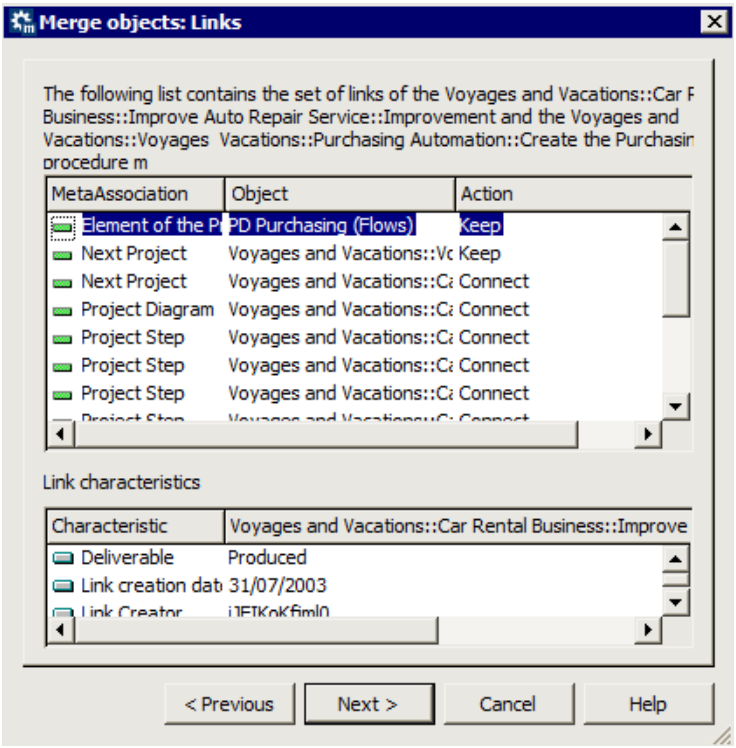
   `Example: a message can have only one super-type.`

   ☛ *This step appears only if the objects to be merged have unique links connecting them to different objects.*



9. Select the links to be transferred.

10. Click **Next**.
    The **Merge Objects** wizard presents: **Links**.



- When the link does not exist for the target object, the default is to connect the target object (**Action** : "Keep"). You can select the **Do not connect** command so as not to transfer the link.

You can **Keep** existing links, or **Disconnect** them.

- When the two objects are linked to the same object by the same link, it is possible to **Not change characteristics** of the link for the target object, or to **Copy characteristics** of the link for the source object. In this case, you can indicate for each characteristic whether to use the value of the source object, or keep the value of the target object.

11. Click **Next**.
12. Click **Finish** to start merging.
    The gauge indicates progress of the operation.
    When merging has been completed, the source object no longer exists and the selected *characteristics* and *links* have been transferred to the target object.

> ☛ *"_TransferredObject" temporary merge objects are created on this occasion. Merge objects of a repository can all be exported at export of **MEGA** objects.*

QUERYING ISOLATED OBJECTS

The Query isolated objects function is available with the **MEGA Supervisor** technical module.

Isolated objects are objects unconnected to other objects, and are therefore almost certainly not used.

Querying isolated objects

1. From **MEGA Administration**, connect to the environment concerned.

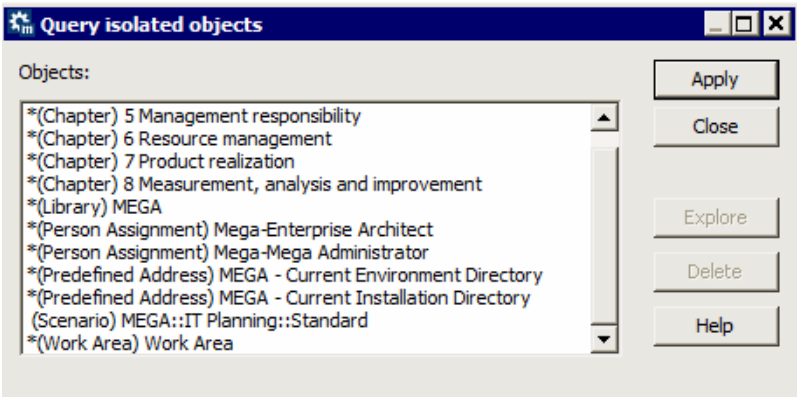
   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **Repositories** folder.
3. Right-click a repository and select **Object Management > Query Isolated Objects**.

   ☛ *Alternatively, in the **MEGA** workspace, select **Tools > Manage > Query Isolated Objects**.*

   The **Query Isolated Objects** dialog box appears.

4. Click **Apply** to run the query.
The system scans the repository, and lists the **Objects** not connected to higher level objects in the hierarchy, preceded by their type.



☛ *Objects not preceded by an asterisk are not linked to any other object and can be deleted.*

☛ *Objects preceded by an asterisk are connected only to lower objects in the hierarchy. An example is an org-unit that sends messages but does not appear in any diagram.*

☛ *Querying for isolated objects involves searching the entire repository and for this reason the operation may take some time.*

The **Explore** button allows you to explore links around the selected object.

The **Delete** button allows you to delete selected objects.

It is normal to find projects, processes, applications and keywords in the list. Do not delete these types of object.

In the "Extended metamodel" configuration, objects of type _deskitem are listed. These are user workspaces: Do not delete them.

QUERYING OBJECTS TO BE TRANSLATED

In the case of multilingual use of **MEGA**, you can query objects to be translated in the repository.

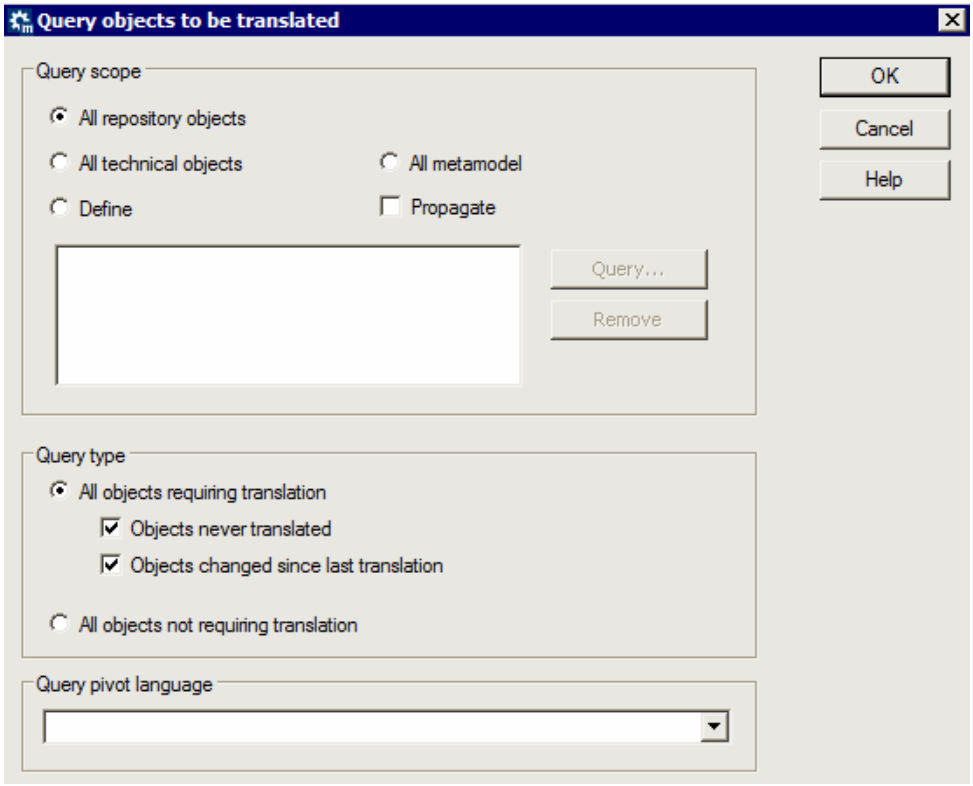
> ☛ *For more details on translation of objects, see in the **MEGA Common Features guide** "Workspace" chapter, "Using **MEGA** in a Multilanguage Context" paragraph.*

To query objects to be translated:

1. Connect to **MEGA**.

   > ☛ *"Connecting to MEGA", page 188.*

2. In the menu bar, select **Tools > Manage > Query Objects to be Translated**.
   The **Query objects to be translated** dialog box opens.



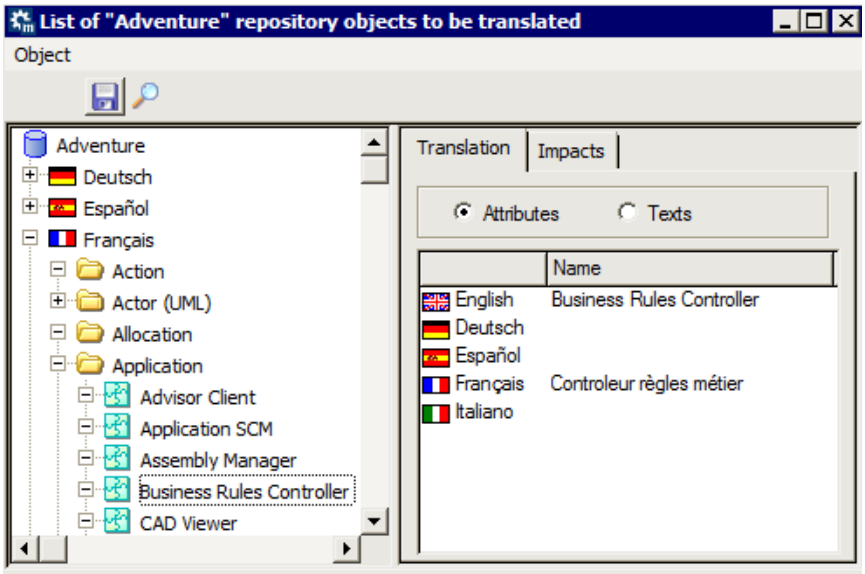
3. In the **Query scope** pane, define the query perimeter of the objects not translated:
   - on **All repository objects**
   - on **All technical objects**
   - on **All metamodel**
   - on specific items: select **Define** and click **Query**.

4. By default the search is performed on **All objects requiring translation**.
   You can refine your query by clearing one of the options:
   - **Objects never translated**
   - **Objects changed since last translation**

   ☛ *If needed, you can perform the query on **All objects not requiring translation**.*
5. Click **OK**.
   The query starts.

   ☺ *Click **Stop** to interrupt the query in progress.*

   The **List of objects to be translated** dialog box opens. It indicates objects to be translated, classified in the menu tree by language and object type.
6. Enter translation of the object names directly in this dialog box.



☛ *When you want to change language for display of the **MEGA** interface, it is necessary to close then reopen a session. The names of menus and tabs will then be refreshed.*

IMPORTING REFERENCE FRAMEWORKS IN MEGA

You can import the following reference frameworks in **MEGA**:

- solution packs
- regulation frameworks

Importing a Solution Pack

Prerequisites: the solution packs that you import are decompressed (**MEGA** > **Utilities > Solution Pack** installation folder, or **Solution Pack.R3**, double-click the solution pack to extract it).

To import a solution pack in a MEGA repository:

1. From **MEGA Administration**, connect to the environment concerned.
2. Expand the **Repositories** folder.
3. Right-click the repository and select **Object Management > Import Solution Pack**.
   The **Solution Pack Import** dialog box appears.
4. Select one or more solution packs that you want to import.
5. Click **OK**.
   The **Import MEGA Data XML** dialog box displays import progress.
   The selected solution packs are imported into the repository.

Importing a Regulation Framework

To import a regulation framework in MEGA:

1. From **MEGA Administration**, connect to the environment concerned.
2. Expand the **Repositories** folder.
3. Right-click a repository and select **Object Management > Import a regulation framework**.
   The **Import a regulation framework** dialog box opens.
4. Select the regulation framework(s) you want to import.
5. Click **OK**.
   The regulation frameworks are imported into the repository.

MANAGING UI ACCESS (PERMISSIONS)

☛ *UI access management is only available with the **MEGA Supervisor** technical module.*

To modify profile UI access, you must have modification authorization rights on this profile.

To modify a profile for which you do not have modification rights, you can create a new profile from this profile, see *"Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 96*.

UI access is managed at profile level.

You can manage:

- *object UI access*

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

  ☛ *For information on management of workflow UI Access, see the **HOPEX Collaboration Manager - Workflows** guide ("Managing Workflows" Chapter, "Managing workflow authorizations" section, "Configuring permissions on objects" paragraph).*

- *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)*

Opening the UI Access Management Window (Permission)

The **UI Access** window (Windows Front-End) and the **Permission** (Web Front-End) pane is used to manage UI access for the complete environment and for each profile:

To modify UI access of a profile, you must have modification authorization rights on this profile.

To modify a profile supplied by MEGA, you must create a new profile, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 96.

- **Object UIs**, which details for the selected profile its access to UI of objects and its access to tools specific to these objects.

  ☛ *See "Object UI Access Values", page 289.*

  ☛ *See "Managing UI Access", page 291.*

- **General UIs**, which details for the selected profile its access to general UIs.

  ☛ *See "Object UI Access Values", page 289.*

  ☛ *See "Managing General UI Access", page 301.*

See:

- *"Accessing the management pages for UIs (Web Front-End)", page 289.*
- *"Opening the UI Access Management Window (Windows Front-End)", page 289*

Accessing the management pages for UIs (Web Front-End)

To access the UI access management pages (Web Front-End)

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

   ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*
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**

Opening the UI Access Management Window (Windows Front-End)

To open the UI Access Management Window (Windows Front-End)

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*
2. Expand the **User management** folder of the environment.
3. Right-click the **UI access** folder and select **Manage**.
   The dialog box for managing **UI Access** opens.
4. Click the tab:
   - **Object UIs**
   - **General UIs**

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.
  ```

See:

- "MetaClass occurrence access permissions", page 290
- "MetaAssociationEnd access permissions", page 290
- "MetaAttribute access permissions", page 290
- "Permissions on a tool", page 290

MetaClass occurrence access permissions

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

- C: Create
- R: Read
- U: Update
- D: Delete

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

- **R**: read occurrences of the MetaClass
- **CRU**: create, read and update occurrences of the MetaClass
- **CRUD**: create, read, update and delete occurrences of the MetaClass
- **RU**: read and update occurrences of the MetaClass
- **RUD**: create, read, update and delete occurrences of the MetaClass

MetaAssociationEnd access permissions

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

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

A permission on a MetaAssociationEnd can take combinations of values:

- R
- CRU
- CRUD
- RU
- RUD

MetaAttribute access permissions

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

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

A permission on a MetaAttribute can take combinations of values:

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

Permissions on a tool

A tool can be available or not.

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

The permission on a tool can take value:

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

Managing UI Access

To modify UI access on an object for a given profile, you must have modification authorization rights on this profile.

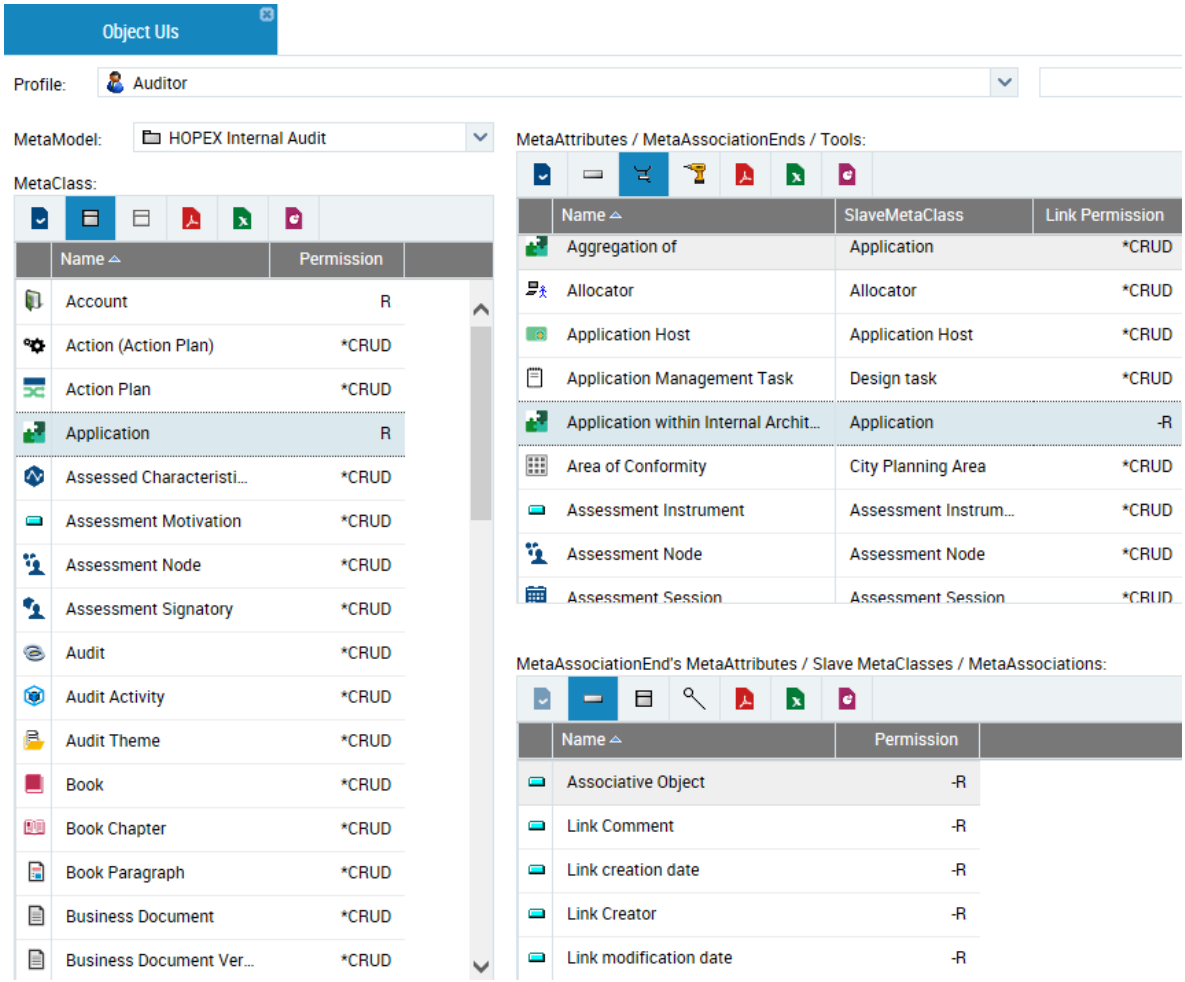
*For information on management of accesses to user interface workflows, see the **HOPEX Collaboration Manager - Workflows** guide.*

For a new profile, access permissions on an object of this profile are by default:

- inherited from the Default profile, if the profile is not an aggregation of profiles (in profile parameters, the profile does not contain sub-profiles, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 96).
- inherited from permissions defined on owned profiles, if the profile is an aggregation of profiles (in profile parameters, the profile contains one or

several profiles, see "Customizing an Existing Profile/Creating a Profile from an Existing Profile", page 96).

☛ *See "Rules on permissions at profile aggregation", page 299.*



In the **Object UIs** tab:

- the **Profile** field enables definition of the profile for which you want to define access permissions.
- the **MetaModel** field enables filtering of MetaClasses displayed in the **MetaClass** frame according to the selected MetaModel.
  - value "All" lists all existing MetaClasses.
  - value Extensions lists all MetaClasses that are not stored in standard MetaModels (MEGA Products products)

To define access permissions on objects, see:

- "Modifying access permissions on occurrences of a MetaClass for a profile", page 293.
- "Modifying access permissions of MetaAttributes of a MetaClass for a profile", page 295.
- "Modifying access permissions to tools of a MetaClass for a profile", page 296.
- "Modifying access permissions of a link around a MetaClass for a profile", page 297.
- "Modifying access permissions on links around a MetaClass for a profile", page 298.

Modifying access permissions on occurrences of a MetaClass for a profile

To modify access permissions on occurrences of a MetaClass for a profile:

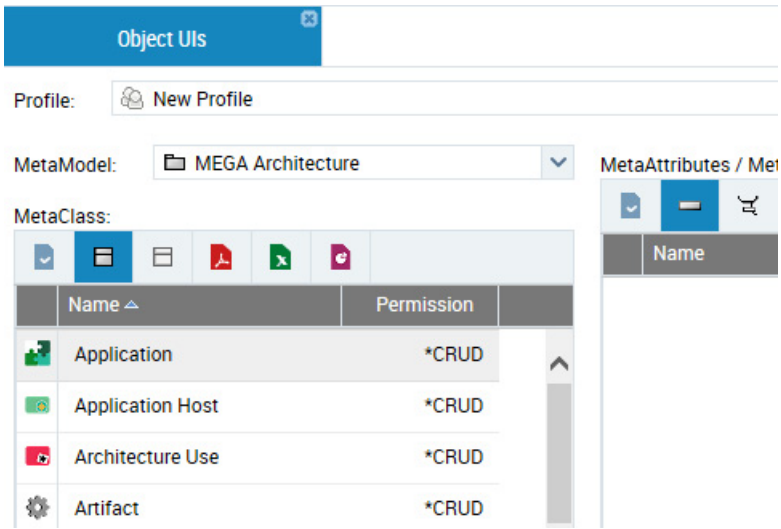
1. Access the UI access management window and select the **Object UIs** tab.

   ☛ *See "Opening the UI Access Management Window (Permission)", page 288.*

2. In the **Profile** field, select the profile using the drop-down menu.

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

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

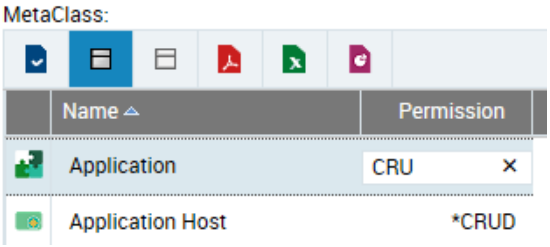


4. In the **MetaClass** frame, select the MetaClass for which you want to modify configuration of access permissions.

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

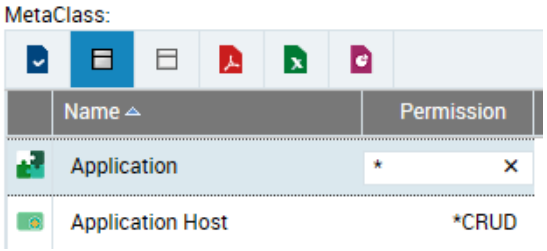
5. In the **Permission** field, enter the new value.

☛ *See "MetaClass occurrence access permissions", page 290.*

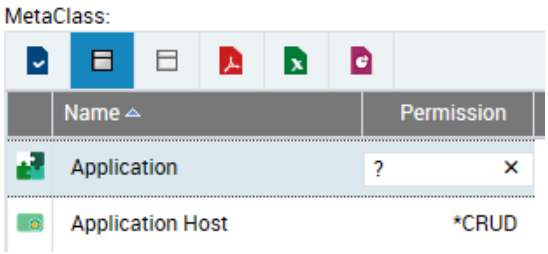


6. Press "Enter".
The value of the MetaClass permission is modified.
In the **MetaAttributes/MetaAssociationEnds/Tools** frame, the values of permissions of elements of the MetaClass are also modified.

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



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



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

- "Modifying access permissions of MetaAttributes of a MetaClass for a profile", page 295.
- "Modifying access permissions to tools of a MetaClass for a profile", page 296.
- "Modifying access permissions of a link around a MetaClass for a profile", page 297.
- "Modifying access permissions on links around a MetaClass for a profile", page 298.

Modifying access permissions of MetaAttributes of a MetaClass for a profile

To modify access permissions of MetaAttributes of a MetaClass for a profile:

1. Access the UI access management window and select the **Object UIs** tab.

☛ *See "Opening the UI Access Management Window (Permission)", page 288.*

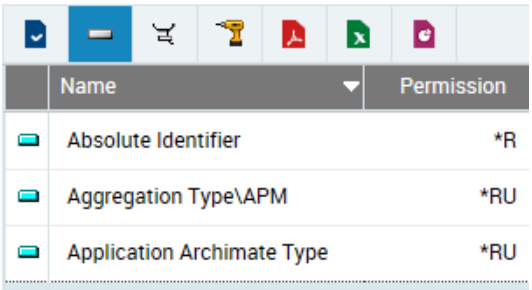
2. In the **Profile** field, select the profile using the drop-down menu.

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

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

   ☛ *See "MetaAttribute access permissions", page 290.*

MetaAttributes / MetaAssociationEnds / Tools:



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

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

   ☛ *To obtain information on origin of an inherited value, enter the character ?.*

Modifying access permissions to tools of a MetaClass for a profile

A tool can be available or not.

To modify access permissions to tools of a MetaClass for a profile:

1. Access the UI access management window and select the **Object UIs** tab.

   ☛ *See "Opening the UI Access Management Window (Permission)", page 288.*

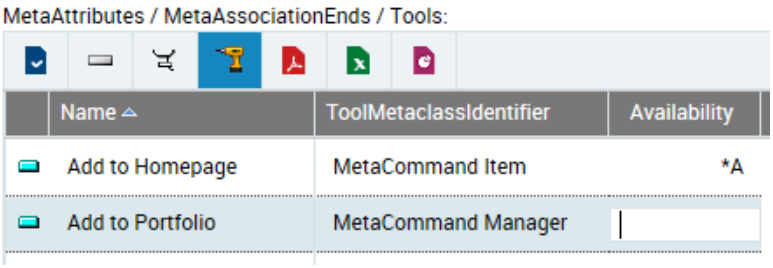
2. In the **Profile** field, select the profile using the drop-down menu.

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

3. In the **MetaModel** field, select the MetaModel concerned.
   In the **MetaClass** frame, the listed MetaClasses are filtered according to the selected MetaModel.
4. In the **MetaClass** frame, select the MetaClass concerned.
5. In the toolbar of the **MetaAttributes/MetaAssociationEnds/Tools** frame, click **Tools** .

6. Select the tool for which you want to modify access permissions.
7. In the **Permission** field, enter the new value.

   ☛ *See "Permissions on a tool", page 290.*



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

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

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

Modifying access permissions of a link around a MetaClass for a profile

To modify access permissions of a link around a MetaClass for a profile:

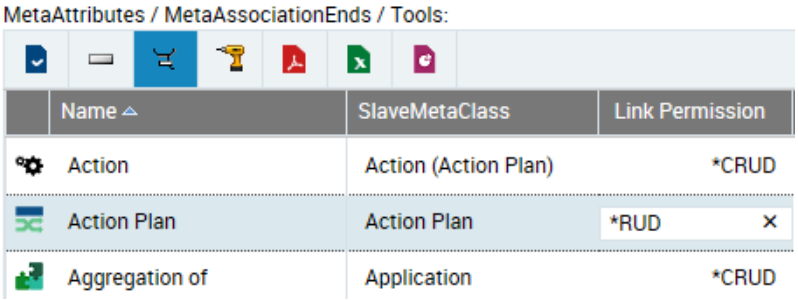
1. Access the UI access management dialog box and select the **Object UIs** tab.

   ☛ *See "Opening the UI Access Management Window (Permission)", page 288.*
2. In the **Profile** field, select the profile using the drop-down menu.

   ☛ *The <Default> profile defines default permissions of each MetaClass, MetaAttribute, MetaAssociationEnd and tool.*
3. In the **MetaModel** field, select the MetaModel concerned.
   In the **MetaClass** frame, the listed MetaClasses are filtered according to the selected MetaModel.
4. In the **MetaClass** frame, select the MetaClass concerned.
5. In the toolbar of the **MetaAttributes/MetaAssociationEnds/Tools** frame, click **MetaAssociationEnd** .
6. Select the MetaAssociationEnd for which you want to modify link access permissions.

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

   ☛ *See "MetaAssociationEnd access permissions", page 290.*



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

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

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

   See also "Modifying access permissions on links around a MetaClass for a profile", page 298.

Modifying access permissions on links around a MetaClass for a profile

You can modify access permissions on:

- the link according to the MetaClass accessed via the link
- one of the MetaAttributes of the link
- one of the MetaClasses accessed via the link

```
Example: You can grant rights to connect (but not to create)
an IT Service to an Application via this same link.
```

To modify access permissions on links around a MetaClass for a profile:

1. Select the MetaAssociationEnd.

   ☛ *See "Modifying access permissions of a link around a MetaClass for a profile", page 297, 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, enter the new value.

   ☛ *See "MetaAttribute access permissions", page 290.*

   ☛ *See "MetaClass occurrence access permissions", page 290.*

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

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

   ☛ *To obtain information on origin of an inherited value, enter the character ?.*

Rules on permissions at profile aggregation

When a profile aggregates several sub-profiles, its permissions are defined by the addition of permissions defined on its sub-profiles.

```
Example:

Profile 1 is the aggregation of sub-profiles 1.1 and 1.2.

If the permission on an object A of sub-profile 1.1 has
value CR, and that of sub-profile 1.2 has value RUD, then
the value of this permission on object A for profile 1 is
CRUD.
```

Attention to default values

A permission value with * means that this value is the default permission value and that it has not been specifically defined. Only those values specifically defined are taken into account in aggregation.

```
Example:

Profile 1 is the aggregation of sub-profiles 1.1 and 1.2.

If the permission on an object A of sub-profile 1.1 has
value *CRUD, and that of sub-profile 1.2 has value R, then
the value of this permission on object A for profile 1 is R.
```

Managing Data Access Dynamically

Writing and reading access diagrams define data access statically. A person sees objects belonging to his/her reading access area, and can modify objects belonging to his/her writing access area.

☛ *See "Managing Data Writing Access", page 297, "Managing Data Reading Access", page 321.*

You can define dynamic rules for reading or writing data access.

Dynamic rule:

- defines for a person, his/her reading or writing access rights on a given object
- can be based on characteristics of:
  - an object
  - of a person
  - an object or person
- can be associated with one or several profiles

Creating permission rules

A permission rule is defined by a macro. A permission rule can define reading or writing access rights to an object.

To create a permission rule:

1. From the **MEGA** explorer, click **Create** ✚.
2. Select **Data Access Rule** and click **OK**.

3. In the **Creation of Data Access Rule** dialog box, enter a **Name** for the rule and click **OK**.
4. Access properties of the rule.
5. From the **Characteristics** tab, in the **Macro** field, click the arrow and connect the macro.
6. In the **Data Access Type** field, select the data access type (**Reading** or **Writing**).
   In the **User Profile** frame, if no profile is connected to the rule, the rule applies to all profiles.

   ☛ *See "Associating a permission rule with a profile", page 300.*

Associating a permission rule with a profile

☛ *To associate a dynamic permission rule to an object, you must have rights to modify **MEGA** data, see "Authorizing MEGA Data Modification", page 78.*

To associate a permission rule with a profile:

1. Open permission rule properties.

   ```
   Example: "Action Plan - Writing"
   ```

2. Click the **Characteristics** tab.
3. In the **User Profile** frame, click **Connect** and select the profile with which you wish to associate the permission rule.

Associating a permission rule with an object

☛ *To associate a dynamic permission rule to an object, you must have rights to modify **MEGA** data, see "Authorizing MEGA Data Modification", page 78.*

To associate a permission rule with an object:

1. Open object properties.

   ```
   Example: MetaClass "Risk"
   ```

2. Select the **Data Access** tab.
3. In the **Data Access Rule** frame, click **Connect** and select the rule you wish to associate with the object.

Generating a Report on Permissions by Profile

A report allows you to generate the detail of permissions for a given workflow.

Generating the report

To generate this report:

1. In the menu bar of **MEGA** (**Windows Front-End**), select **Tools > Profile and Permission Management > Profile Permissions Report**.
   A wizard opens.

2. (Optional) In the **Report File Name** field, modify the name and/or location in which to save the report by default. By default this is your user folder.

   ☛ *See "Repository Structure", page 138.*

3. Select report parameters:
   - In the **MetaModel** field, select the MetaModel concerned.

     ☺ *For a more rapid result, do not select <All>, but just the metamodel concerned.*

   - in the **Profile** frame, click **Add Profile**  (you can add several).

     ☺ *For a more rapid result, do not select a large number of profiles.*

4. Click **OK**.
   The report is generated as an Excel worksheet.

   ☛ *Generation can take some time, depending on the parameters you have selected.*

Report content

All MetaClasses of the selected metamodel appear in the report.

Presented for each MetaClass are:

- 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

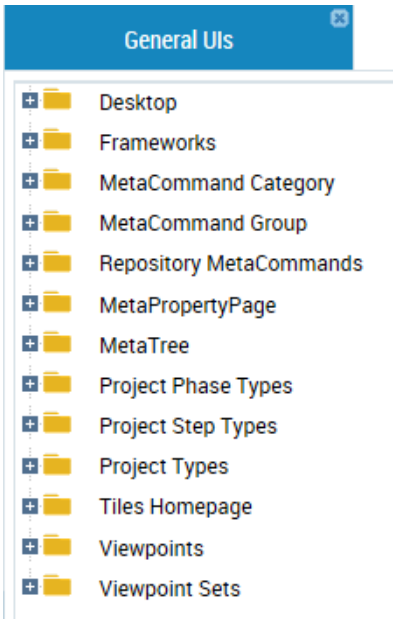
You can manage general UI access for a profile. General UIs are classified by category:

- desktop
- command category
- command group
- general command
- properties page
- tree

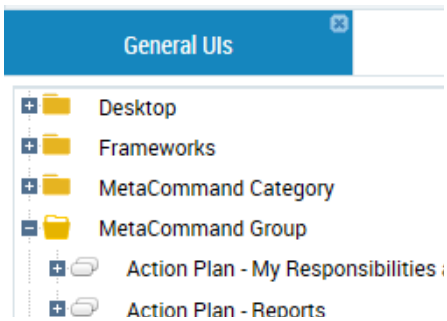
To manage general UI access:

1. Access the UI access management dialog box and select the **General UIs** tab.

   ☛ *See "Opening the UI Access Management Window (Permission)", page 288.*

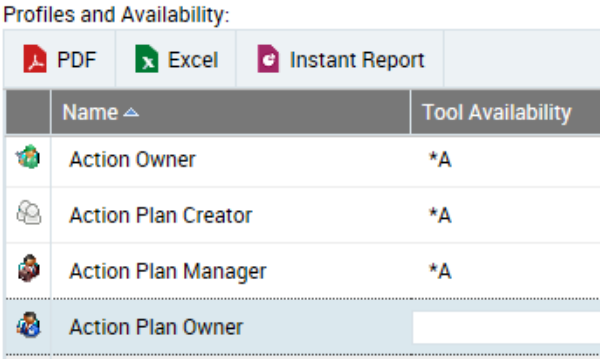


2. In the **SystemDb** tree, expand the folder of the category concerned.
3. In the list, select the tool concerned.



4. In the **Profiles and Availability** frame, select the profile for which you want to modify access on the tool.

5. In the **Tool Availability** field, enter the availability value.



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 SHAPES

MEGA provides several sets of shapes used to represent the various objects in diagrams.

MEGA Administration, allows you to consult the list of shapes:

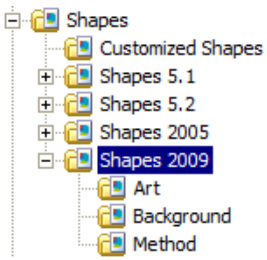
- shapes customized by users
- shapes supplied by **MEGA**
  Each set of shapes (5.1 / 5.2 / 2005 / 2009) contains three shape categories:
  - Art
  - Background
  - Method

Accessing Shapes

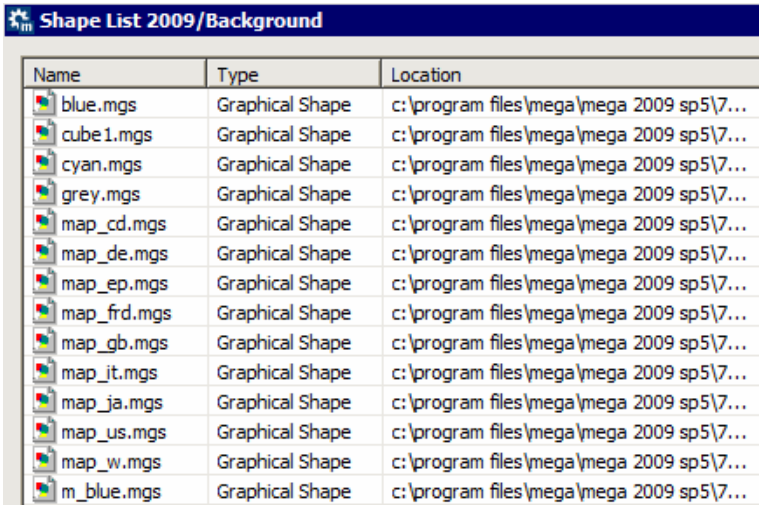
To access shapes:

1. Connect to **MEGA Administration**.

   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*
2. Expand the **Shapes** folder.
3. Expand the sub-folder of the desired shapes.



4. Right-click the category of the desired shapes and select **Manage**.
A table appears listing the images of this category and their location.



8

MANAGING DATA WRITING ACCESS

MEGA Administration is provided with tools required for writing access management.

This chapter explains how to create a *writing access diagram* and how to customize its characteristics.

The following points are covered here:

INTRODUCTION TO WRITING ACCESS MANAGEMENT

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

The administrator declares the users and defines the writing access.

The structure of *writing access* is defined in the *writing access diagram*. There is a hierarchical link between writing access.

☺ *Implementation of this function does not replace a structured management of projects. To operate, the writing access diagram must model itself on organization of projects.*
Clear functional breakdown of your projects simplifies management of operational follow-up of writing accesses.

Users

user

A user is a person with a login.

At creation of an environment, two users are declared by default. These two users have administration rights to manage repositories and users:

- the "Administrator" person, with Login "System" (without password)

  ☛ *The "Administrator" user cannot be deleted. It has no profile (it has all rights). It is recommended that you define a password to restrict use of the "Administrator" user code.*

- The "Mega" person, with Login "mega" (without password)

You must declare other users who will access repositories.

If several environments are defined for a site, users must be defined in each of these environments. To do this, export the user diagram from the reference environment, and import it into each of the other environments.

💣 **Do not manually create a user with the same name in other environments. If you do, the user will have a different absolute identifier in each environment, and you would actually have created different users with the same name.**

☺ ***MEGA** recommends that you create the repositories before defining the users, so you can declare the user access rights when they are created.*

To access a repository, a user must identify himself/herself. Then, depending on user writing access area, he/she is able to modify the repository.

User groups

A person can belong to one or more groups. A user group is a group of persons with a login.

Persons belonging to a group:

- depend on the same environment.
- share the same connection characteristics defined on the **login** of the group.
- share the assignments defined for the group:
  - (Web Front-End) persons accumulate their assignments and those defined for the group.
  - (Windows Front-End) the assignments defined for the person are ignored.
- connect to the application
  - (Web Front-End) with the group **login**
  - (Windows Front-End) with their **login**, but with access rights to the repository defined on the **login** of the group.

☛ *see "Login Properties", page 26.*

By default at creation of an environment, a group of users is created:

- the "Guests" person group, with Login "Guest".

Writing Access Areas

Each user or group of users is connected to a writing access area. It is the person or person group that carries the writing access area.

Each object is connected to a writing access area.

☛ *At creation, the object inherits the writing access area of the person who created it.*

MEGA delivers by default the "Administrator" writing access; this writing access area:

- cannot be deleted.
- is the highest level writing access area; it does not depend on any other writing access area. In principle it should be reserved for repository administration.
- is the writing access area to which "Administrator", "Mega" and "Guests" are connected.
  When the writing access diagram has been installed, **MEGA** recommends that you change the writing access area levels of "Mega" and "Guests". It is not desirable that default users have such extensive rights.

All other writing access areas depend on at least one writing access area.

Writing access areas are interconnected by hierarchical links. This is a strict hierarchy, with no circular dependencies: a writing access area cannot be declared at a higher level than the writing access area on which it depends, either directly or via a succession of dependencies.

A user can modify an object connected to his/her writing access area or to a hierarchically lower writing access area.

The writing access area of an object can be modified by the administrator:

- by specifically changing the object writing access area
- when modifying the writing access area of another object (project, process, diagram, etc.) if the propagation option is enabled.

Writing Access Diagram

There is one writing access diagram per environment.

☛ *If several environments use the same protection configuration, the same user diagram must be used in all these environments.*

Rules

Installation of a writing access diagram diagram must respect the following rules so as to minimize user management costs:

- Any object must be modifiable by users that may need to modify it, without administrator intervention.
- The administrator should intervene only in exceptional circumstances.

Use

The writing access diagram is used similarly to a diagram. The persons, person groups and writing accesses are handled just like standard objects:

- Creation and modification of the name, etc., are done in the same way as for standard objects.
- Be careful however when you delete a writing access.

☛ *See "Deleting Writing Access Areas", page 309.*

Avoid using the Cut command for a person or person group, as this can result in errors in the writing access diagram if the person or person group is not deleted from the repository or not linked to a writing access.

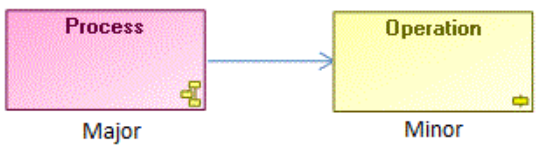
Link Orientation: Major and Minor Objects

When two objects are linked, one object is *major* and the other *minor*.

You cannot delete a minor object if you do not have writing access on the major object.

The major object in the link is the one whose nature changes with the presence or absence of the link. For example a process, defined as a succession of operations, is modified if you remove an operation. The process is then major for the link. If the objects are protected, you must have the correct authorization for modifying the major object in order to create or delete the link.

The minor object in a link is the one whose nature is not modified or only slightly modified by presence or absence of this link. For example, removing an operation from a process does not change characteristics of this operation. Therefore the process is minor in the link.



In the above example, you must have writing access on the org-unit (the major object) to disconnect or delete the message (minor object).

Opening the Writing Access Diagram

☛ *To access the writing access diagram, you must have a license for the **MEGA Supervisor** technical module.*

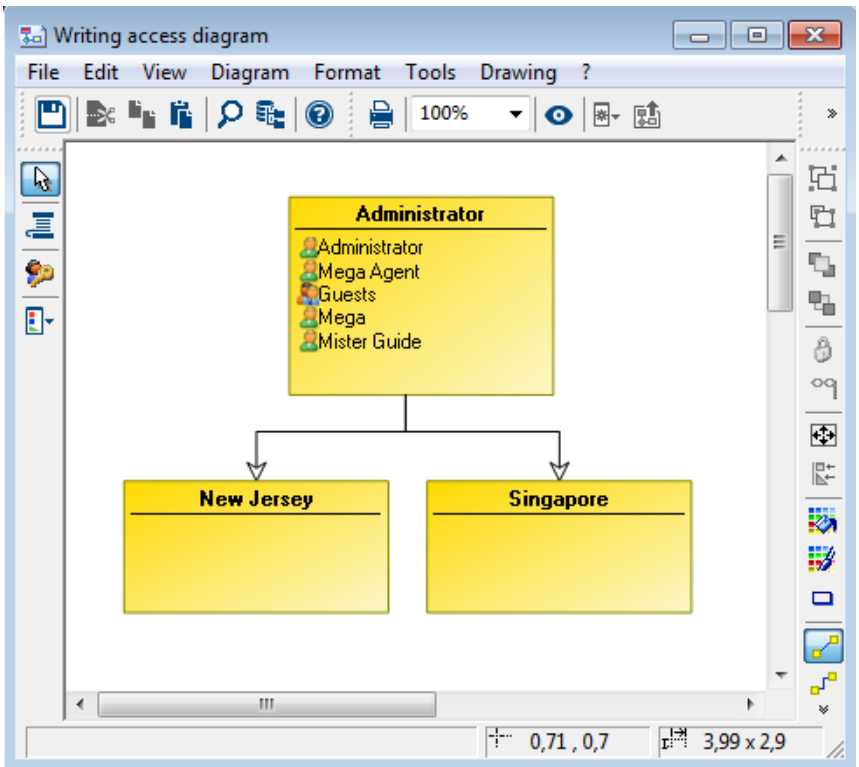
See:

- "Opening the Writing Access Diagram (Windows Front-End)", page 302
- "Opening the Writing Access Diagram (Web Front-End)", page 303

Opening the Writing Access Diagram (Windows Front-End)

To open the writing access diagram:

1. From **MEGA Administration**, connect to the desired environment.
   ☛ *See "Connecting to an Environment", page 5.*
2. In the **User Management** folder, right-click **Data Writing Access** and select **Open Diagram**.
   The diagram opens in a new window.



Opening the Writing Access Diagram (Web Front-End)

To open the writing access diagram:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

2. Select the **Persons by writing access area** or **Person groups by writing access area** sub-folder.
3. In the edit area, click **Diagram** .
   The diagram appears.

COMPILING THE WRITING ACCESS DIAGRAM

Running writing access diagram compilation assures consistency of behavior of **MEGA** with declarations of the diagram.

If the diagram is not compiled, there is a risk that certain users will be able to update objects that are normally protected.

When modifying the writing access diagram, so as to warn of rejects due, for example, to writing access restrictions or deletions before compilation it is recommended that:

- all changes made on the user workstations should be uploaded to the administrator workstation, or
- all private workspaces dispatched.

To compile the writing access diagram from the **Administration** application:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **User Management** folder of the environment.
3. Right-click the **Data Writing Access** folder and select **Compile**.
   When compilation is complete, a message indicates whether the operation was successful or whether the diagram contains errors.

   ☛ *The most frequent errors are:*

   A writing access area (other than '"Administrator") is not attached to any other.

   A person or person group is not attached to any authorization.

DEFINING WRITING ACCESS AREAS

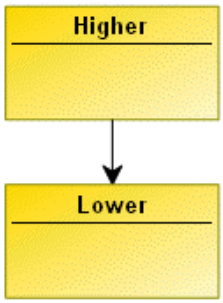
The writing access diagram is available if you have the MEGA Supervisor technical module. With this diagram, you can create users and manage their writing access rights for repositories and product functions. By default only one writing access area is defined, named "Administrator". Attached to it are 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.

The *writing access diagram* enables creation of writing access areas.

Creating a Writing Access Area

To create a writing access area:

1. In the diagram insert toolbar, click icon **Writing Access Area** then click in the diagram.
2. Enter the name of the writing access area.
   Dependency of writing access access areas is determined by creation of a "lower" link which starts from the higher writing access area to the lower writing access area.



Defining Writing Access Area Persons or Person Groups

(Web Front-End) See "Defining Writing Access Area Persons or Person Groups", page 305 and "Connecting a Person to a Writing Access Area (Web Front-End)", page 73.

To define persons or person groups of a writing access area:

1. **From the** Administration tool, open the writing access diagram.
   See "Opening the Writing Access Diagram", page 302.
2. Right-click the writing access area and select **Properties**.
3. Select the **Users** tab and click **Connect**.

4. In the query tool, click the arrow in the first field and select the target (*Access Area Member*, Person or Person Group).

   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.

5. (optional) In the second field, enter the character string to be queried.
6. Click **Find**.
7. In the results list, select the required access area member and click **Connect**.

   ☛ *Press the [CTRL] key to select several members simultaneously.*

   The person or person group you have connected appears in the list of access area members of the selected writing access area.

Defining a Writing Access Area at Creation

To assign to all objects created by a user a writing access area different from the writing access area of this user, you must associate a writing access area at creation with the user concerned.

To define a writing access area at creation of a user:

1. Open the properties dialog box of the person.
2. Select the **Characteristics** tab.
3. In the **Writing Access Area at Creation** field, select the required writing access.

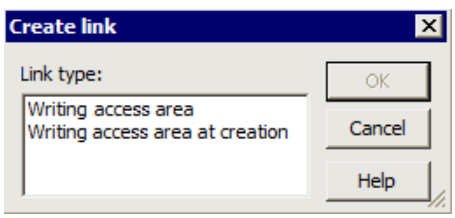
   ☛ *See "User writing access area and writing access area at creation", page 22.*

To define a writing access area at creation of a user:

1. **From the** Administration tool, open the writing access diagram.

   ☛ *See "Opening the Writing Access Diagram", page 302.*

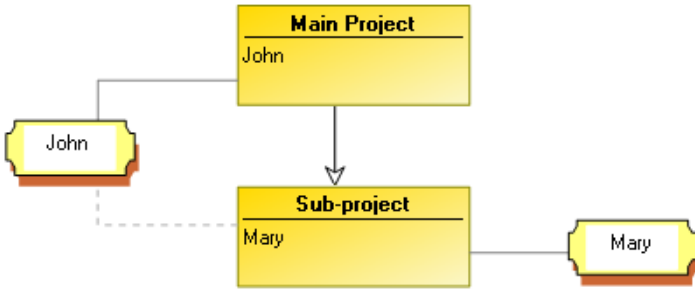
2. If this is not already done, place the person and the writing access area concerned in the diagram.
3. Draw a link between the person and the required writing access area. The **Create Link** dialog box opens.



4. Select **Writing Access Area at Creation** and click **OK**.

   ☛ *Value "None" of **Writing Access Area at Creation** signifies that the user creates objects in the same writing access area as that to which he/she belongs.*

When the writing access area at creation has been created, it is represented by a dotted line link between the person and the writing access area in the writing access diagram.



In the above example, user John has:

- a writing access area of level "main project"
- a writing access area at creation of level "sub-project"

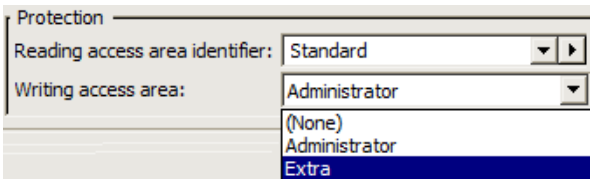
Objects created by John can therefore be modified by Mary.

Modifying Writing Access Areas of Objects

If you have a writing access area of level higher than or equal to that of an object, you can modify the writing access area of this object in the object properties dialog box.

To modify writing access area of an object:

1. From your **MEGA** desktop, open the object properties dialog box, select the **General** tab, then the **Administration** subtab.
2. In the **Protection** frame, in the **Writing Access Area** field, select a writing access area via the drop-down menu.



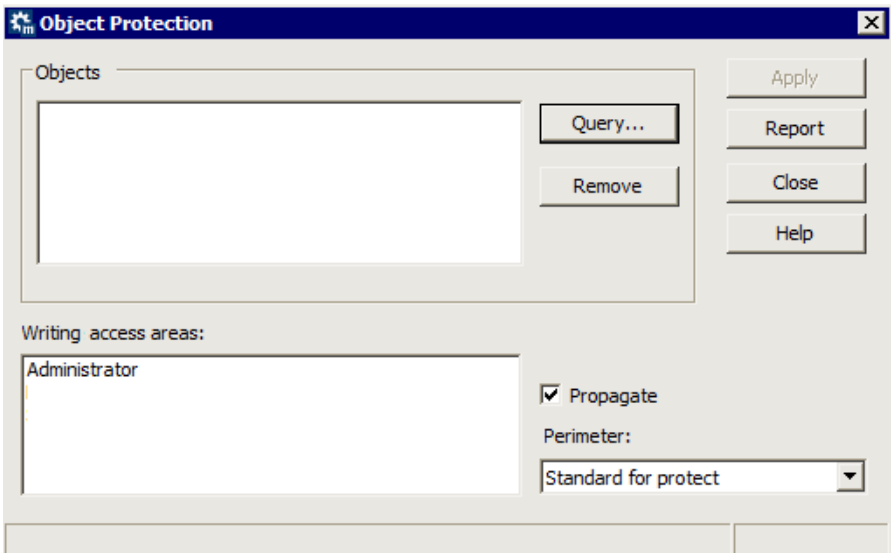
3. Click **OK**.

Modifying Writing Access Areas of an Object Group

If you have a writing access area of level higher than or equal to that of an object group, you can modify the writing access area of this object group.

To modify the writing access area of an object group:

1. From your **MEGA** workspace, select **Tools > Manage > Protect Objects**.
   The **Protect Objects** dialog box opens.
2. In the **Objects** frame, click **Query** and select the object group.
3. In the **Writing Access Areas** frame, select the writing access area you want to assign to the object group.
4. (Optional) Select **Propagate** if you want the writing access area to be propagated to all dependent objects of the object group, as a function of the perimeter selected.



5. Click **Apply**.
   Object protection is applied.
6. Click **Report** to check if a conflict has been encountered at protection propagation in the repository.

Propagating Object Writing Access Areas to Child Objects

You can propagate writing access areas from all objects connected to dependent objects, for all environment repositories.

> ☛ *This action can take some considerable time, depending on repository size.*

To propagate a writing access area:

1. From the **Administration** tool, open the writing access diagram.
   > ☛ *See "Opening the Writing Access Diagram", page 302.*
2. Right-click the writing access area to be propagated and select **Propagation of writing access area to associated occurrences**.
3. Click **Yes** to confirm.

Deleting Writing Access Areas

To delete a writing access area:

1. From the **Administration** tool, open the writing access diagram.

   ☛ *See "Opening the Writing Access Diagram", page 302.*
2. Open the properties dialog box of the writing access area concerned.
3. Select the **Users** tab and disconnect all **Access Area Members** of the writing access area, and connect these **Access Area Members** to another writing access area.
4. Delete the writing access area.

The writing access areas dependent on the deleted writing access area are, after updating, no longer attached to the writing access areas tree. It is therefore preferable to first delete their links with the obsolete writing access area and attach them to a writing access area that will be retained.

Objects which had this writing access area can be protected with another writing access area. Otherwise, they are considered as being protected at the highest level, with "Administrator" writing access area level.

☛ *For more details on protection of objects, see "Protecting Objects", page 269.*

Associating Objects with Writing Access Areas

The **Administration** navigation window of the **MEGA** workspace allows:

- access to writing access areas
- simple automation of writing access area propagation to connected and child objects.

To connect an object to a writing access area:

1. In the **MEGA** workspace menu, select **View > Navigation Windows > Administration**.
2. Expand the **Writing Access Area** folder.
3. Right-click the required writing access area and select **Connect > Object**.
4. In the query dialog box, find the required object and click **OK**.

To display the list of objects associated with a writing access area:

- Right-click the writing access area and select **Objects associated with writing access area**.
  A dialog box displays a list of these objects.

Tips on Using Writing Access Areas

Common data

MEGA recommends that you manage data common to several projects in a specific project. This simplifies control of their evolutions.

Tips

MEGA recommends:

- definition of certain users:
  - with writing access area level higher than projects so as to manage conflicts between projects, for example "Project Management".
  - with writing access area at creation at the level of the project, to avoid creation of objects that cannot be modified by the project.

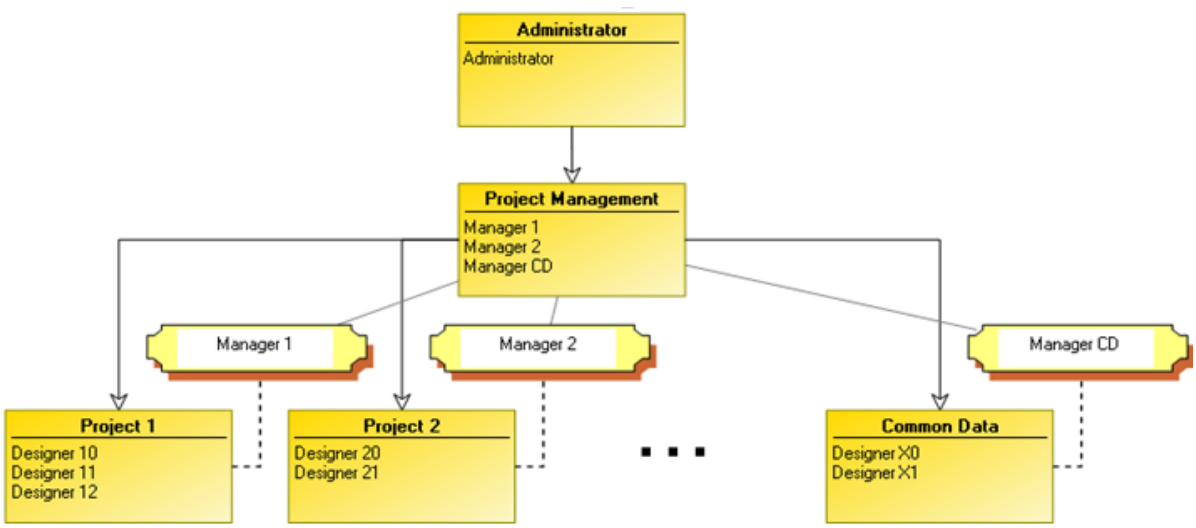
    ☛ *See "Defining a Writing Access Area at Creation", page 306.*
- that only the "Administrator" user should be connected to the "Administrator" writing access area.
- that if a person produces on several projects, the person should have one **MEGA** user per project.
  Objects are therefore directly created in the correct owner project, greatly simplifying management.

Typical example

The following example presents a typical case of writing access area use:

- Only the Administrator user has "Administrator" writing access area level.
- All managers can modify objects of all projects.
- Objects created by a manager are attached to a dedicated project.

  ☛ *Manager 1 can modify objects of all projects, by default the objects he/she creates are in project 1.*
- Data common to different projects ("Common Data") is managed in a dedicated project with a specific writing access area.



CUSTOMIZING WRITING ACCESS AREA MANAGEMENT

This section describes how to use and customize management of writing access areas:

Calculated Writing Access Area

As standard, the writing access area of an object is stored in the "_Authorization" MetaAttribute and takes the value of the writing access area absolute identifier. It is assigned at creation and you can modify it.

You can install up calculated writing access area.

```
For example, you can deduce the writing access area of an
operation from that of the process on which it depends. You
need only change the writing access area of a process, and
those of the dependent operations will automatically adapt.
```

In this case, watch performance.

To customize the writing access area of an object:

- Replace the "_Authorization" MetaAttribute (which carries the object writing access area) by a calculated MetaAttribute.

Calculated MetaAttribute

A calculated MetaAttribute is a software device enabling deduction of the MetaAttribute value of an object as a function of data around the object or dependent on other sources (system, current user, etc.).

MEGA uses a set of "conventional" MetaAttributes (including the writing access area) that do not require metamodel definition.

A substitution device is available in **MEGA**; it enables replacement of an implicit MetaAttribute by another for a MetaClass.

This device is required when you need to alter behavior of an existing MetaAttribute by implementing a calculated MetaAttribute.

To customize writing access area of an object, you must:

1. Create a MetaAttribute with characteristics close to those of the "_Authorization" MetaAttribute.

2. Substitute the "_HexaIdAbs" value of the new MetaAttribute by the "_HexaIdAbs" value of the "_Authorization" MetaAttribute.
3. Calculate the writing access area.

Installing a Writing Access Diagram

To install a writing access area diagram in an environment already in production:

1. **From the** Administration tool, open the writing access diagram.

   ☛ *See "Opening the Writing Access Diagram", page 302.*

2. Ask users who have a private workspace in progress to close this.
3. Create an "Old Data" writing access area

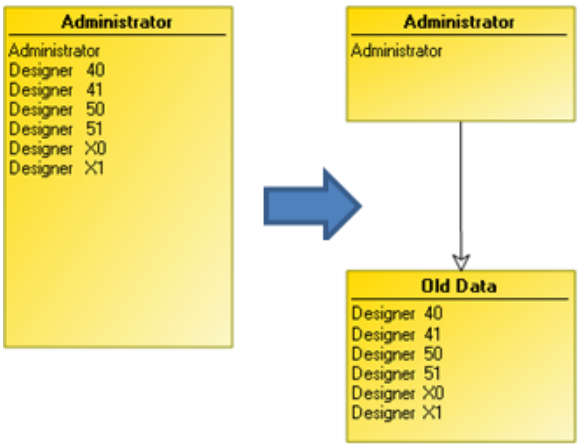
   ☛ *See "Creating a Writing Access Area", page 305.*

4. Attach all users (except the "Administrator" user) and all objects of all repositories to the "Old Data" writing access area.

   ☛ *See "Defining Writing Access Area Persons or Person Groups", page 305.*

   ☛ *See "Associating Objects with Writing Access Areas", page 309.*

   Users may resume working.

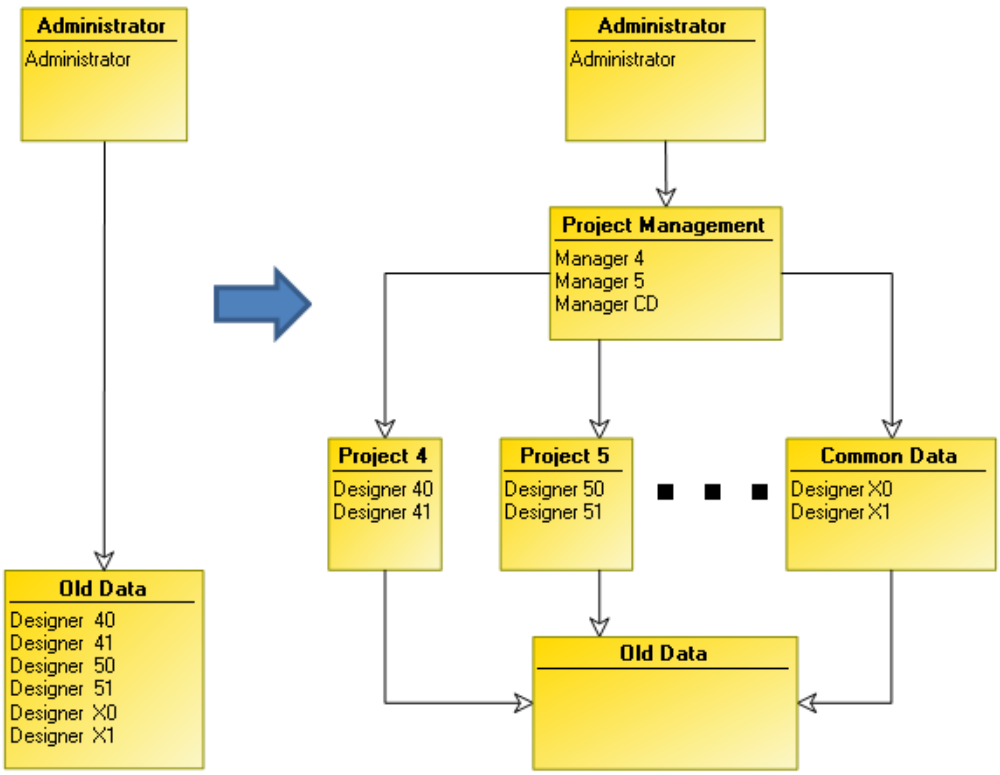


5. Create new writing access areas according to projects.
6. Distribute users between these writing access areas.
7. Distribute objects between these projects/writing access areas for all repositories of the environment.

   ☛ *See "Associating Objects with Writing Access Areas", page 309.*

   Until this distribution is completed, projects can interfere with each other, since they have rights to modify objects created before distribution.

8. (Optional) When all objects of all repositories have been distributed, you can delete the "Old Data" writing access area.



☛ *If the environment is new and there is no data to be distributed between the new writing access areas, you do not need to draw the diagram with the "Old Data" writing access area.*

Locking Validated Objects

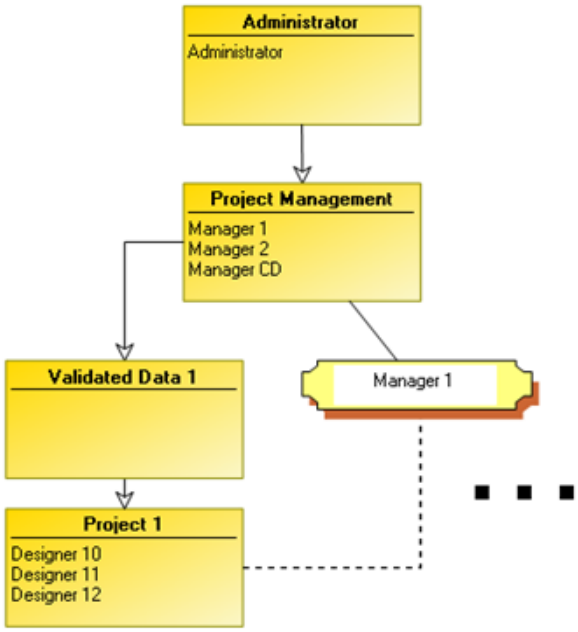
When objects have been validated, you can configure the writing access diagram so that these objects cannot be modified.

To lock objects:

1. **From the** Administration tool, open the writing access diagram.

   ☛ *See "Opening the Writing Access Diagram", page 302.*

2. Between the writing access area "Project Management" and that of the project, insert a writing access area dedicated to validated data of the project.



3. When data is validated, modify its writing access area from "Project" level to the higher level "Validated Data" writing access area.

   ☛ *See "Modifying Writing Access Areas of Objects", page 307.*

4. (Optional) If validated data must be modified:
   - it is modified by a user of "Project Management" writing access area level.
   - it is lowered to the "Project" writing access area level.

So the project perimeter is distributed between two writing access areas, but remains perfectly determined.

Merging Two Projects

To merge two projects:

1. **From the** Administration tool, open the writing access diagram.

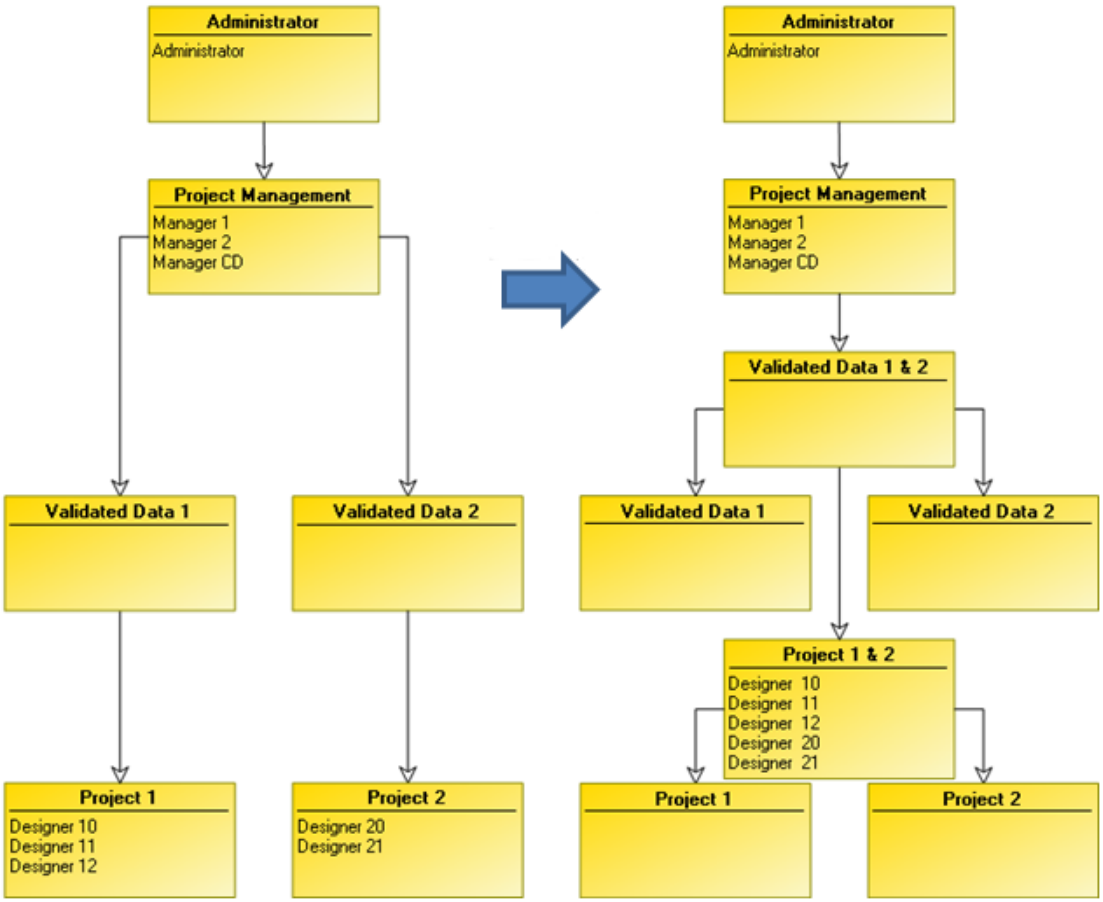
   ☛ *See "Opening the Writing Access Diagram", page 302.*

2. Create a new writing access area for the new project.

   ☛ *This new writing access area must be of higher level than the writing access area it will replace.*

3. Connect users of merged projects to this new writing access area.

☛ *See "Defining Writing Access Area Persons or Person Groups", page 305.*



Splitting a Project

To split a project:

1. **From the** Administration tool, open the writing access diagram.

☛ *See "Opening the Writing Access Diagram", page 302.*

2. Create writing access areas connected to new projects.
These writing access areas must be of must be of higher level than the writing access areas they will replace.

☛ *See "Creating a Writing Access Area", page 305.*

3. Ask users who have a private workspace in progress to close this.

4. Distribute users between these writing access areas.

   ☛ *See "Defining Writing Access Area Persons or Person Groups", page 305.*

   ☛ *Users may resume working.*

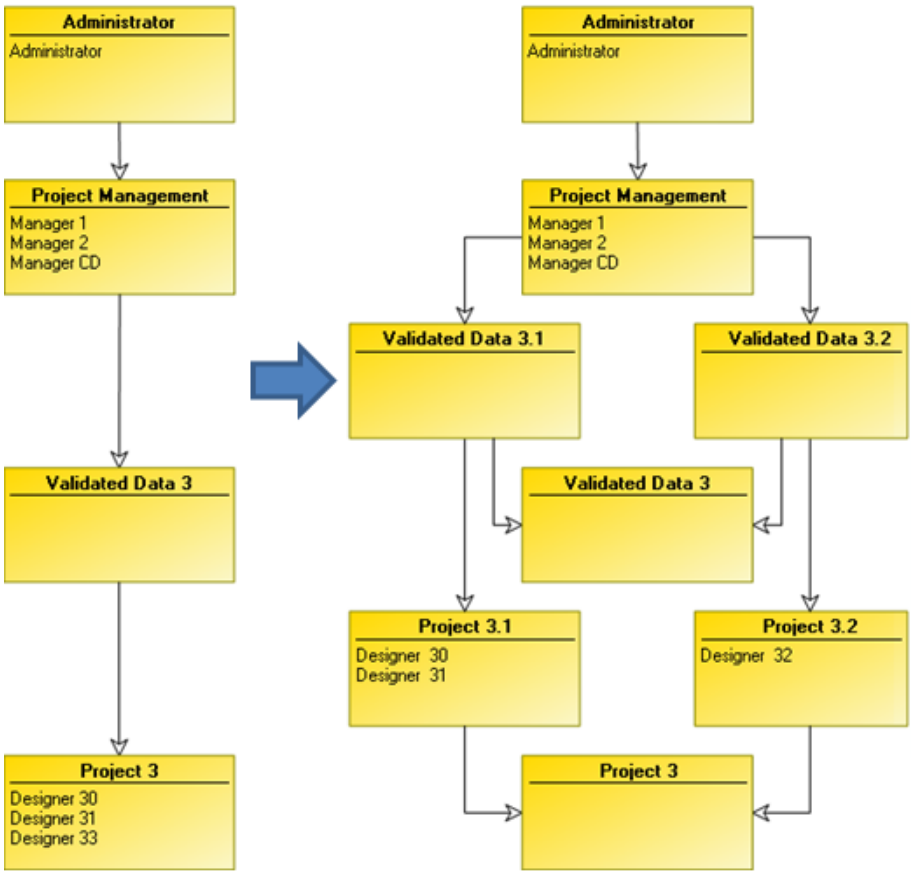
5. Distribute the objects between the new projects.

   ☛ *See "Associating Objects with Writing Access Areas", page 309.*

   Until this distribution is completed, projects can interfere with each other, since they do not yet have rights to modify objects created before distribution.

6. (Optional) Delete the old writing access areas.

   ☛ *(Optional) When all objects of all repositories have been distributed, you can delete old writing access areas.*



MANAGING USERS FROM THE WRITING ACCESS DIAGRAM

This section presents how to:

Creating Persons with Writing Access Areas

At creation, the user is not connected to any writing access area. To implement protection, the person should be connected to a writing access area by creation of a link between person and writing access area.

To create a person with a writing access area, from the writing access diagram:

1. From **MEGA Administration**, open the writing access diagram.
   ☛ *See "Opening the Writing Access Diagram", page 302.*
2. In the writing access diagram, right-click a writing access area and select **Properties**.
3. In the **Users** tab, click the **New** button  .
   A selection dialog box appears.
4. In the **MetaClass** field, select **Person**.
   The **Creation of Person** dialog box opens.
5. Follow the procedure "Creating a Person", page 54.
   The person is created and connected to the selected writing access area.
   ☛ *A person depends on a single writing access area.*

Creating Person Group with Writing Access Areas

To create a person group with a writing access area, from the writing access diagram:

1. **From the** Administration tool, open the writing access diagram.
   ☛ *See "Opening the Writing Access Diagram", page 302.*
2. In the writing access diagram, right-click a writing access area and select **Properties**.
3. In the **Users** tab, click the **New** button  .
   A selection dialog box appears.
4. In the **MetaClass** field, select **Person Group**.
   A new person group appears in the list of access area members. The new group is connected to the selected writing access area.

5. (optional) Modify the **Short Name** of the new person group.

Managing Users from the Writing Access Diagram

User access rights to repositories and functions can be restricted by the administrator. You can carry out this modification user by user, or on all users simultaneously.

☛ *To manage user access rights, the **MEGA Supervisor** technical module is required.*

To manage users from the writing access diagram:

1. **From the** Administration tool, open the writing access diagram.

   ☛ *See "Opening the Writing Access Diagram", page 302.*

2. From the writing access diagram, select **Diagram > Described Object > Manage Users**.
   The **Users** administration dialog box opens.

   ☛ *See "Introduction to User Management", page 18.*

Compiling the Writing Access Diagram

Changes to the writing access diagram only take effect after it has been compiled.

To compile the diagram:

- Select **Diagram > Described Object > Compile Writing Access Diagram**.

If the diagram has been modified, it is automatically compiled at closing. This allows you to check the validity of the user diagram.

When modifying the writing access diagram, so as to warn of rejects due, for example, to authorization restrictions or deletions before compilation it is recommended that:

- all changes made on the user workstations should be uploaded to the administrator workstation, or
- all private workspaces dispatched.

When compilation is complete, a message indicates whether the operation was successful or whether the diagram contains errors. The most frequent errors are:

- A writing access area (other than '"Administrator") is not attached to any other.
- A person or person group is not attached to any authorization.

Transferring the Writing Access Diagram

On workstations where the network is not available, when the user diagram has been updated and compiled it must be exported to the administrator workstation and imported on user workstations. You must also do this if the same diagram is to be used in several different environments.

To run export:

- Select **Diagram > Described Object > Export Writing Access Diagram**.

Import on user workstations is carried out in the normal way.

CUSTOMIZING WRITING ACCESS DIAGRAM DISPLAY

You can customize writing access diagram display:

- diagram structure representation
- display of persons connected to a writing access area

Customizing Diagram Structure Representation

You can customize representation of the structure of the writing access diagram using the drawing reorganization function.

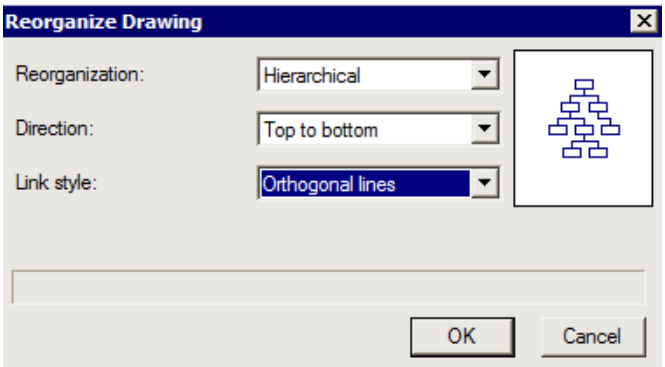
☺ *The automatic drawing reorganization functionality is automatically activated on loading a diagram that does not yet include a drawing.*

To modify organization of an existing drawing:

1. **From the** Administration tool, open the writing access diagram.

   ☛ *See "Opening the Writing Access Diagram", page 302.*

2. Select **Drawing > Reorganize Drawing**.
3. Select the desired reorganization mode, the direction and the style of links in the diagram.



☺ *The miniature image alongside the reorganization options gives you a view of each type of reorganization.*

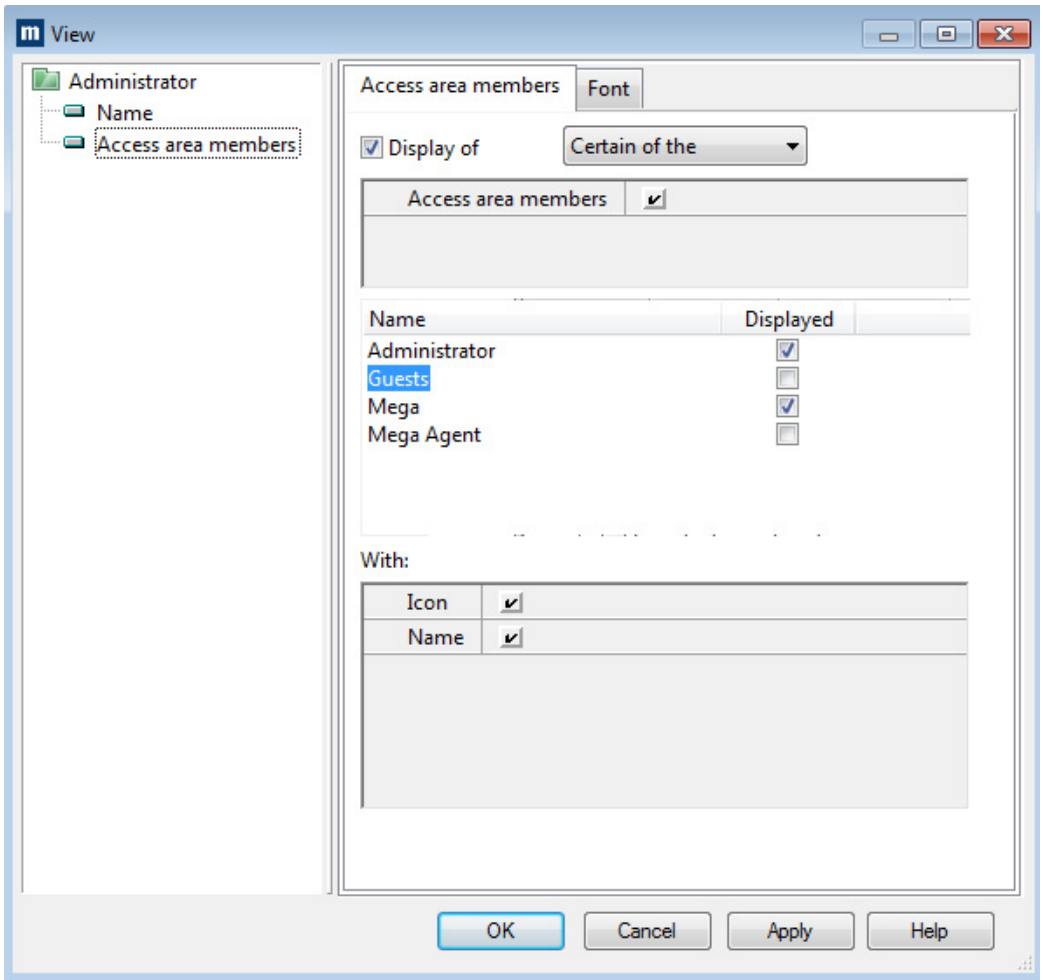
4. Click **OK** to apply the modifications.

Customizing Writing Access Area Display

You can show or hide persons, person groups, objects connected to a writing access area.

To define writing access area display:

1. From the **Administration** application, open the writing access diagram.
   ☛ *See "Opening the Writing Access Diagram", page 302.*
2. Right-click the writing access area concerned and select **Shapes and Details**.
   The **View** dialog box opens.
3. In the tree on the left, select **Access Area Members**.
4. In the pane on the right, select **Access Area Members**.
5. Select the **Display of** option, then click the arrow and select **Certain of the** access area members.
   ☛ *To display all or none of the access area members, select **All the** or **None of the**.*
6. Select the persons you want to see displayed.



7. Click **OK**.

9

MANAGING DATA READING ACCESS

The following points are covered here:

INTRODUCTION

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

The following points are detailed here:

The Need to Manage Sensitive Data

Certain modeling projects may be confidential or contain confidential or sensitive data (costs, risks, controls, etc.).

The **MEGA** administrator may therefore need to mask objects corresponding to confidential or sensitive data.

These objects must be visible only to authorized users.

To meet these requirements concerning data confidentiality, **MEGA** offers functionalities for implementing consistent and effective confidentiality policies.

General Concepts

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

📖 *A user is a person with a login.*

📖 *A person can belong to a group. A user group is a group of persons with a login.*

Each user or group of users is associated with a reading access area. It is the person or person group that carries the reading access area.

The reading access area to which the person or person group belongs determines the objects that the user or group of users can see. A user or user group can only see objects located in his/her own or lower confidentiality areas.

💣 **With definition of reading access areas, hidden objects are inaccessible. This concept differs from that of the filter, which hides occurrences of MetaClasses so as not to disturb the final view of the user, see "Managing UI Access (Permissions)", page 282.**

Activating Data Reading Access Management

When you activate reading access management, confidential data is visible only to authorized users. Before activating reading access management, **MEGA** recommends that you familiarize yourself with reading access management using **MEGA**.

> ☛ *For more details on confidential data, see "Confidential or Sensitive Object Behavior", page 347.*

To manage confidential or sensitive data , you must first activate data reading access area management.

To activate data reading access management:

1. From **MEGA Administration**, connect to the environment concerned.

   > ☛ *See "Connecting to an Environment", page 5.*

2. In the **User Management** folder, right-click **Data Reading Access** and select **Activate Management**.

   > **A message warns you that activation of reading access management is irreversible.**

3. Carefully read this warning message, then click **Yes** if you wish to activate data reading access management.

Consulting Environment Reading Access Information

When working in **MEGA** you can check:

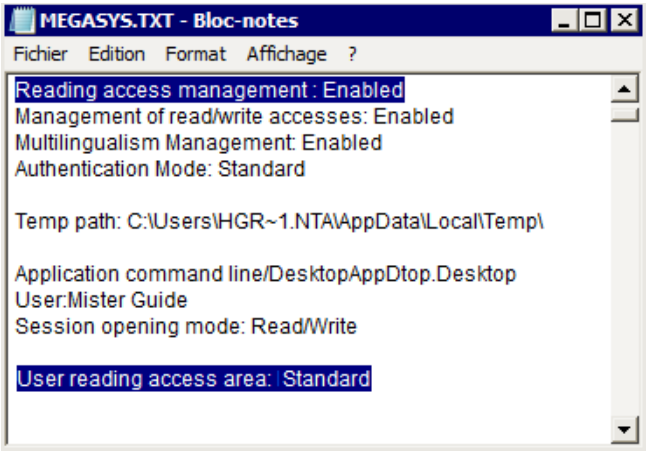
- if reading access management is activated in your environment or not.
- the reading access area to which the connected user belongs.

To consult reading access information of your current environment:

1. From the **MEGA** menu bar, select **Help > About MEGA**.
   The **About MEGA** dialog box appears.
2. Click **System Information**.
3. In the menu bar of the **System Properties** dialog box, select **System Info > Edit**.
   The Megasys.txt text file opens.

At the beginning of the file you can consult the properties of:

- ***Reading access management***
- ***Reading access area of the user***



Managing Reading Access in MEGA

You can set up and manage data reading access in **MEGA** in two ways:

Reading access area matrix method:

1. Create the different user reading access areas you require.
2. Distribute persons or person groups in user reading access areas.
3. Distribute objects in object reading access areas.
4. Associate user reading access areas with object reading access areas.

☛ *For more details, see "Reading Access Area Matrix", page 326.*

Reading access diagram method:

1. Define organization and hierarchy of the different reading access areas you require.
2. Create and organize these users in a reading access diagram.
3. Associate persons or person groups with different reading access areas. Objects created by users are then distributed in the user reading access area.

☛ *For more details, see "Reading Access Diagram", page 330.*

Compiling the Reading Access Diagram

Running reading access diagram compilation assures consistency of behavior of **MEGA** with declarations of the diagram.

If the diagram is not compiled, there is a risk that certain users will be able to see objects that are normally hidden.

To compile the reading access diagram:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **User Management** folder of the environment.
3. Right-click the user **Data Reading Access** folder and select **Compile**.
   On completion of compilation, a message indicates the result of the operation.

READING ACCESS AREA MATRIX

The reading access area matrix enables organization of user groups with object groups. Only a user with administrator profile connected to the maximum reading access area can configure reading access areas.

In the reading access area matrix, you can create two types of reading access areas:

- an **object reading access area**  , grouping only **MEGA** objects
- a **user reading access area**  , grouping only persons or person groups

> *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.*
>
> **To ensure coherence of the reading access diagram, if you begin management of reading access of your data from the reading access area matrix, you must continue to manage reading access from this matrix.**

You can create links between these two types of reading access area.

Accessing the Reading Access Area Matrix

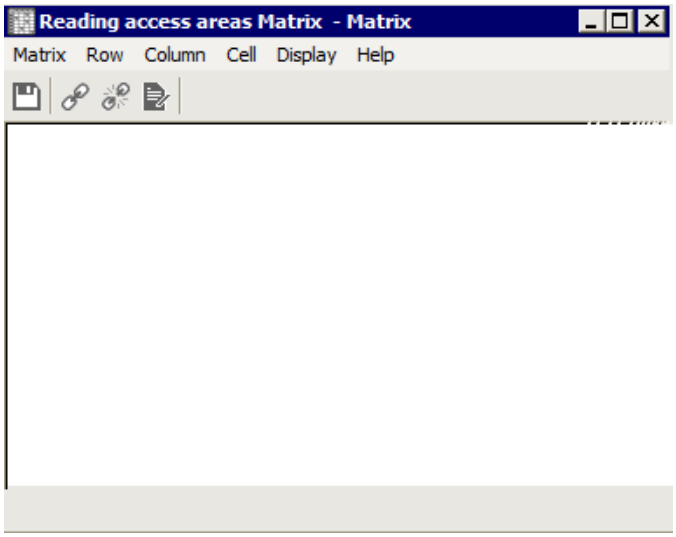
To access the reading access area matrix:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **User Management** folder.

3. Right-click the user **Data Reading Access** folder and select **Reading Access Matrix**.
   An empty reading access area matrix appears.



Adding an Object Reading Access Area

To add an object reading access area in the matrix:

1. Open the reading access area matrix.
   ☛ *See "Accessing the Reading Access Area Matrix", page 326.*
2. Select **Row > Create**.
3. In the dialog box that appears, enter the name of the object reading access area and click **Finish**.

Adding a User Reading Access Area

To add an user reading access area in the matrix:

1. Open the reading access area matrix.
   ☛ *See "Accessing the Reading Access Area Matrix", page 326.*
2. Select **Column > Create**.
3. In the dialog box that appears, enter the name of the user reading access area and click **Finish**.

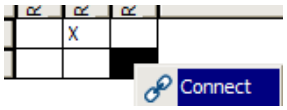
Associating User Reading Access Areas with Object Reading Access Areas

To associate a user reading access area with an object reading access area

1. Open the reading access area matrix.

   ☛ *See "Accessing the Reading Access Area Matrix", page 326.*

2. In the reading access area matrix, right-click the cell at the intersection of the user reading access area and the object reading access area and select **Connect**.



A cross represents the association between the two selected reading access areas. The corresponding links are automatically drawn in the reading access diagram.

If you begin management of reading access of your data from the reading access area matrix, you must continue management of reading access from this matrix. Do not manually modify links created automatically in the reading access diagram; you may invalidate the diagram.

☛ *For more details on the reading access diagram, see "Reading Access Diagram", page 330.*

Associating Users with User Reading Access Areas

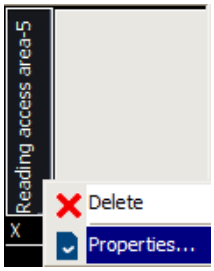
In the case of the reading access area matrix, to associate a user (or user group) with a reading access area:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **User Management** folder.
3. Right-click the user **Data Reading Access** folder and select **Reading Access Matrix**.
   The reading access area matrix appears.

4. Right-click the user reading access area concerned and select **Properties**.



The user reading access area properties dialog box appears.

5. In the **Persons** tab, click **Connect**.

> ☛ *If you want to create a new Person (or new person group) and associate it with the reading access area, click **New**.*

6. In the query tool, click the arrow in the first field and select **Person** (or **Person Group**).

> ☛ *If you want to select persons and person groups, select Access Area Member.*

7. (optional) In the second field, enter the character string to be queried.
8. Click **Find** .
9. In the query result list, select the person (or person group) required and click **Connect**.

> ☛ *Press the [CTRL] key to select several persons and/or person groups simultaneously.*

The user (or user group) you have connected appears in the list of users in the selected reading access area.

READING ACCESS DIAGRAM

The *reading access diagram* enables organization of the repository by sets of objects, unlike the writing access diagram which enables organization by work groups.

> 🕮 *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.*

The reading access diagram can be opened only by an Administrator profile user connected to the maximum reading access area.

> ☛ *The reading access diagram feature is accessible only if you have the **MEGA Supervisor** technical module.*
>
> 💣 **If you begin management of reading access of your data from the reading access area matrix, you must continue to manage reading access from this matrix. Do not manually modify links created automatically in the reading access diagram, you might invalidate the diagram.**
>
> 💣 **Warning: on exiting the reading access diagram, if a message indicates that the diagram is incorrect, the diagram is not compiled and reading access management does not operate. MEGA recommends that you correct the error that prevents diagram compilation.**

This section covers the following points:

Reading Access Diagram Operating

The reading access diagram implements reading access areas of **General** type. These areas can group both objects and persons and/or person groups.

Reading access areas are organized hierarchically. **MEGA** provides two extreme reading access areas:

- **Maximum Reading Access**, the highest reading access level.
- **Standard**, the lowest reading access level.

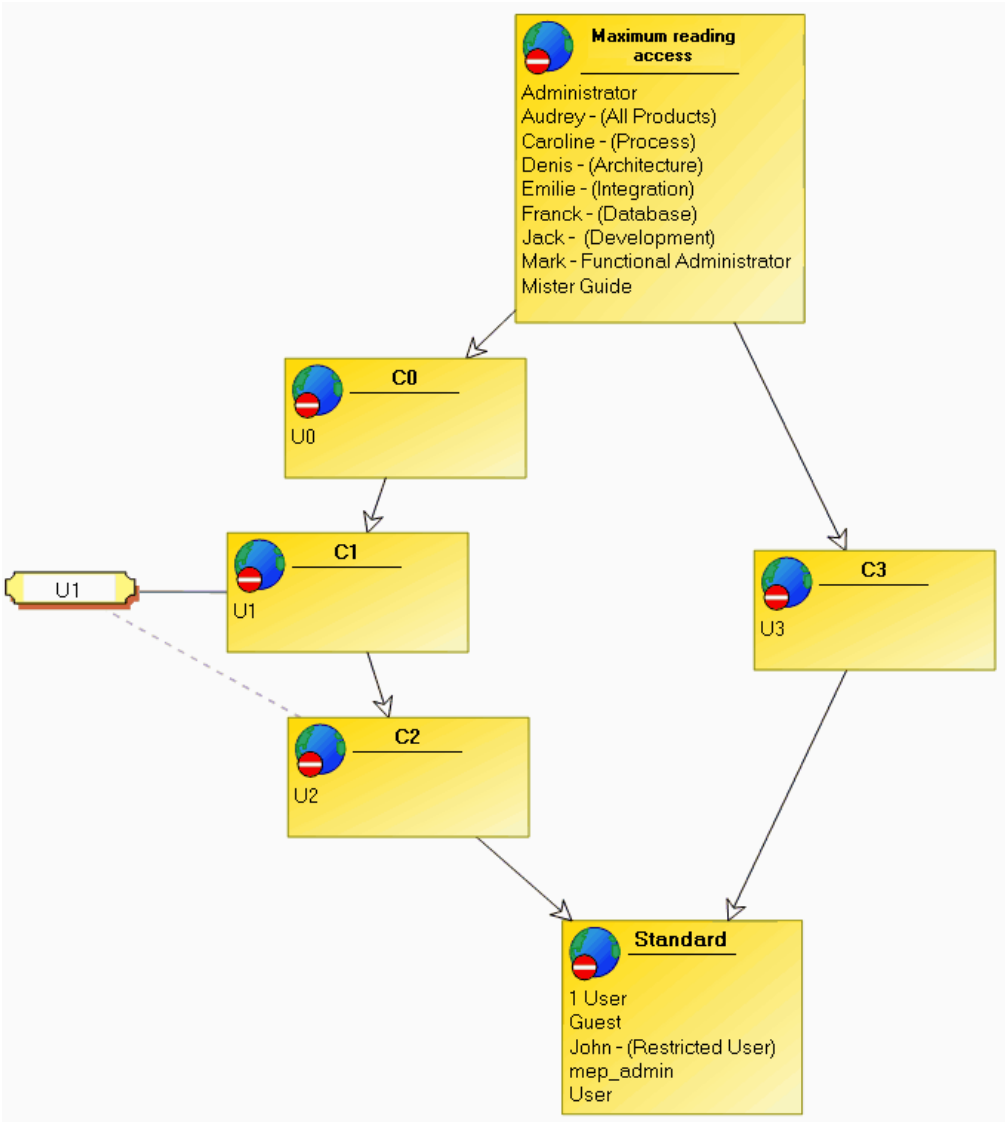
Each object belongs to a reading access area (**Standard** by default).

Each person or person group is connected to one of the reading access areas. The persons or person groups that are connected to:

- **Maximum reading access** sees all repository data.
- A created reading access area sees all data of this area, as well as that of lower level reading access areas.
- **Standard** sees only non-confidential data of the repository.

For example, a user U1 connected to a reading access area C1 sees all objects that belong to:

- his/her reading access area (C1)
- lower level reading access areas (C2 and Standard).



In the preceding reading access diagram, user U1:

- is connected to reading access area C1
- to a reading access area at creation C2.

When user U1 creates an occurrence of a MetaClass:

- if sensitive (high sensitivity), this belongs to reading access area C1.
- if non-sensitive (standard sensitivity), this belongs to reading access area C2.

> ☛ *For more details on MetaClass sensitivity, see "Managing MetaClass Sensitivity and Reading Access Areas", page 345.*

If a user does not have a reading access at creation, any occurrences of a non-sensitive MetaClass he/she creates belong to the standard reading access area.

However, Web sites and reports (MS Word) are always created at the reading access level of the user. This ensures confidentiality of the information they may contain.

Users connected to reading access area C3 cannot see objects belonging to reading access areas C0, C1, and C2, since area C3 does not belong to the same hierarchical branch as areas C0, C1, and C2.

Activating the reading access diagram

To be able to access the reading access diagram, you must first activate the reading access diagram option.

> ☛ *By default, only the reading access area matrix is accessible.*

To activate the reading access diagram option:

1. From **MEGA Administration**, connect to the environment concerned.
   > ☛ *See "Connecting to an Environment", page 5.*
2. Right-click the environment and select **Options > Modify**.
3. In the **Repository** group of options, select the **Activate the reading access diagram** option.
4. Click **OK**.
   The reading access diagram option is activated. The reading access diagram is accessible.

Prohibiting Reading Access Diagram Modification

By default, reading access diagram modification is authorized.

To prohibit reading access diagram modification:

1. From **MEGA Administration**, connect to the environment concerned.
   > ☛ *See "Connecting to an Environment", page 5.*
2. Right-click the environment and select **Options > Modify**.
3. In the **Repository** options group, for option **Authorize modification of writing access and reading access diagrams** select "Prohibit".
4. Click **OK**.
   Reading diagram modification is prohibited.

Opening the reading access diagram

See:

- "Opening the reading access diagram (Windows Front-End)", page 333
- "Opening the reading access diagram (Web Front-End)", page 334

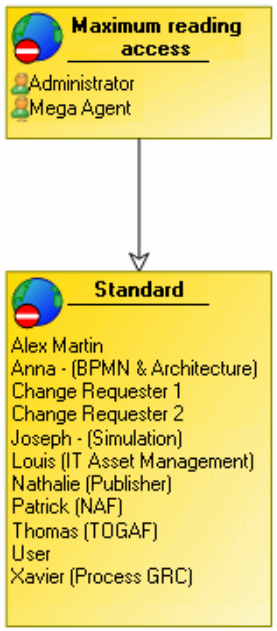
Opening the reading access diagram (Windows Front-End)

To access the reading access diagram:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **User Management** folder.
3. Right-click the **Data Reading Access** folder and select **Open Diagram**. The reading access diagram appears.



By default, the reading access diagram contains two reading access areas:

- **Maximum Reading Access** is the highest reading access area level. Users connected to this area can see all objects in the repository.
- **Standard** is the lowest reading access area level.

  ☛ *There can only be one maximum level and one minimum level (standard) reading access area in the diagram.*

Opening the reading access diagram (Web Front-End)

To open the writing access diagram:

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

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*

2. Select the **Persons by reading access area** or **Person groups by reading access area** sub-folder.
3. In the edit area, click **Diagram** .
   The diagram appears.

Organizing Reading Access Areas

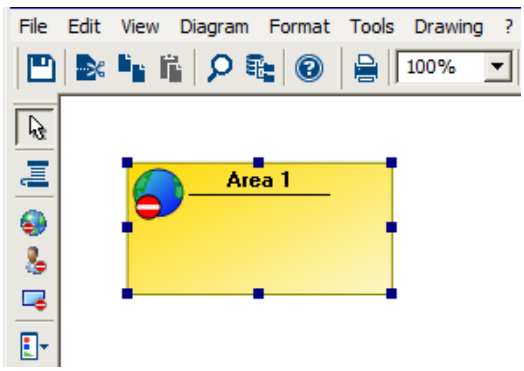
Creating reading access areas

To create a *reading access area* in the diagram:

1. Open the reading access diagram.

   ☛ *See "Opening the reading access diagram (Windows Front-End)", page 333.*

2. In the diagram insert toolbar, click **General Reading Access Area** , then click in the diagram.
3. In the creation wizard dialog box that appears, enter the name of the reading access area and click **Create**.
   The creation wizard allows you to modify the reading access area type if necessary.
4. Click **Finish**.
   The general reading access area appears in the diagram.



Connecting two reading access areas

Reading access areas must be hierarchically interlinked. Except for **Maximum Reading Access** and **Standard** reading access areas, each reading access area must be connected to a lower level area and a higher level area.

To connect two reading access areas:

1. Open the reading access diagram.

   ☛ *See "Opening the reading access diagram (Windows Front-End)", page 333.*

2. In the diagram insert toolbar, click **Link** and draw a link between the two reading access areas (from the higher level reading access area to the lower level reading access area).

Displaying reading access areas associated with a reading access area

To display object (or user) reading access areas associated with a reading access area:

1. Open the reading access diagram.

   ☛ *See "Opening the reading access diagram (Windows Front-End)", page 333.*

2. Open the properties dialog box of the reading access area in question.
3. Select the **Matching Object reading access areas** or **Matching User reading access areas**.
   The associated object reading access areas or user reading access areas are listed.

Adding a User in the Reading Access Diagram

You can add a person or person group in the reading access diagram.

Adding a person in the reading access diagram

To add a person in the reading access diagram:

1. Open the reading access diagram.

   ☛ *See "Opening the reading access diagram (Windows Front-End)", page 333.*

2. In the diagram insert toolbar, click **Person**, then click in the diagram.

   ☛ *If the **Person** icon is not present in the insert toolbar, add it via **View > Views and Details**.*

   The **Add Person** dialog box appears.
3. In the **Name** field, click the arrow to find the person then click **Connect**.

   ☛ *To add a new person, in the **Name** field, enter the name of the person then click **Create**. Also create the login of the person.*

Adding a person group in the reading access diagram

To add a person group in the reading access diagram:

1. Open the reading access diagram.

   ☛ *See "Opening the reading access diagram (Windows Front-End)", page 333.*

2. In the diagram insert toolbar, click **Person Group**  , then click in the diagram.

   ☛ *If the **Person Group** icon is not present in the insert toolbar, add it via **View > Views and Details**.*

   The **Add Person Group** dialog box appears.
3. In the **Name** field, click the arrow to find the person group then click **Connect**.

   ☛ *To add a new person group, in the **Name** field, enter the name of the person group then click **Create**. Also create the login of the person group.*

Connecting Users to Reading Access Areas

A user can:

- be connected to a ***reading access area***
  This area defines the view the user has of the repository and the objects the user can access.
- have a ***reading access area at creation***
  Occurrences created by the user belong to this reading access area at creation.

  ☛ *If a user does not have a reading access area at creation, the occurrences he/she creates will belong to the standard reading access area.*

Reading access area of the user

☛ *(Web Front-End) See "Connecting a Person to a Reading Access Area (Web Front-End)", page 73 and "Connecting a person group with access to a reading area (Web Front-End)", page 67.*

To connect a user to a reading access area:

1. Open the reading access diagram.

   ☛ *See "Opening the reading access diagram (Windows Front-End)", page 333.*
2. Right-click the reading access area concerned and select **Properties**.
3. Select the **Persons** tab and click **Connect**.

   ☛ *If you want to create a new user and associate him/her to a reading access area, select **New > Person**.*

   The access area member search dialog box appears.
4. In the first query field, select the type of access area member you wish to connect: **Person** (or **Person Group**).

   ☛ *If you want to connect persons and person groups, select Access Area Member.*
5. (optional) In the second query field, enter the character string to be queried.
6. Click the **Find**.
7. In the result list, select the person (press the [CTRL] key to select several) and click **Connect**.
   The user appears in the reading access area.

Reading access area at creation

You can assign a reading access area at creation to an existing user from:

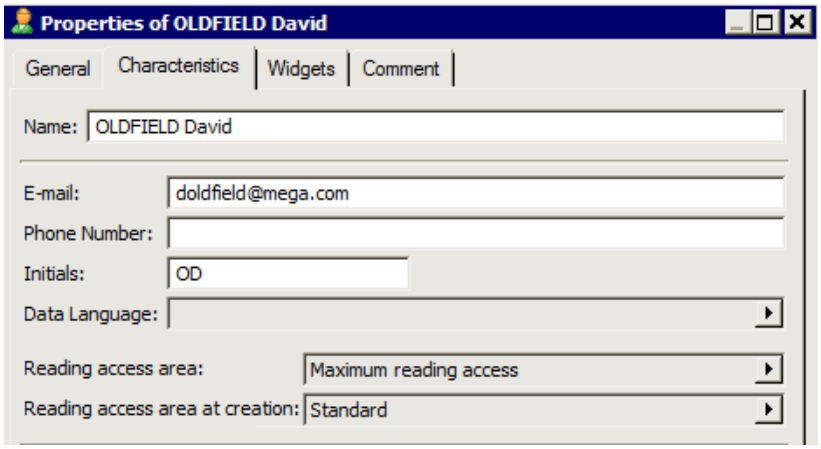
- the reading access diagram
- the **Properties** dialog box of the person

To assign a reading access area at creation to a user from the reading access diagram:

1. Place the user in the reading access diagram.
2. Connect the desired reading access area at creation to the person. This area must be at a level lower than or the same as the reading access area of the user.
   A dialog box asks you to select the type of link to be created: **Access area member** or **Access area member at creation**.
3. Select the link type **Access area at creation member**.
   This area is the reading access area at creation of the user.

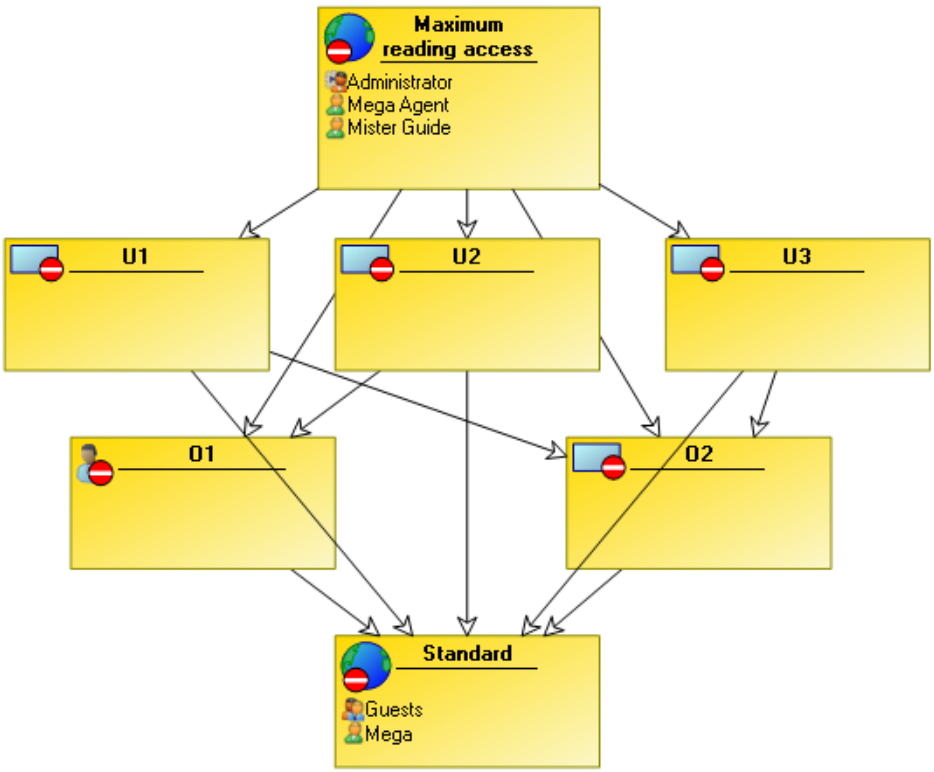
To assign a creation reading access area to a user from the user properties dialog box:

1. Open the **Properties** dialog box of the person and select the **Characteristics** tab, see *"Modifying User Properties", page 70*.
2. In the **Reading access area at creation** field, select the required value.



Consulting Reading Access Diagram Information:

At reading access diagram compilation, user and object are connected to the ***Maximum reading access*** reading access area and the ***Standard*** reading access area.



Open the user reading access area properties dialog box to consult:

- the list of persons connected to the area and to connect new users (**Persons** tab)
- the list of reading access areas for associated objects (**Matching Object Reading Access Areas** tab)

Open the object reading access area dialog box to consult:

- the list of user reading access areas associated with an object reading access area (**Matching User Reading Access Areas** tab)

Customizing Reading Access Area Display

By default, when you create a reading access area, all users belonging to this area are displayed in the diagram reading access area. You can decide to hide certain users in this reading access area.

To define users displayed in their reading access area:

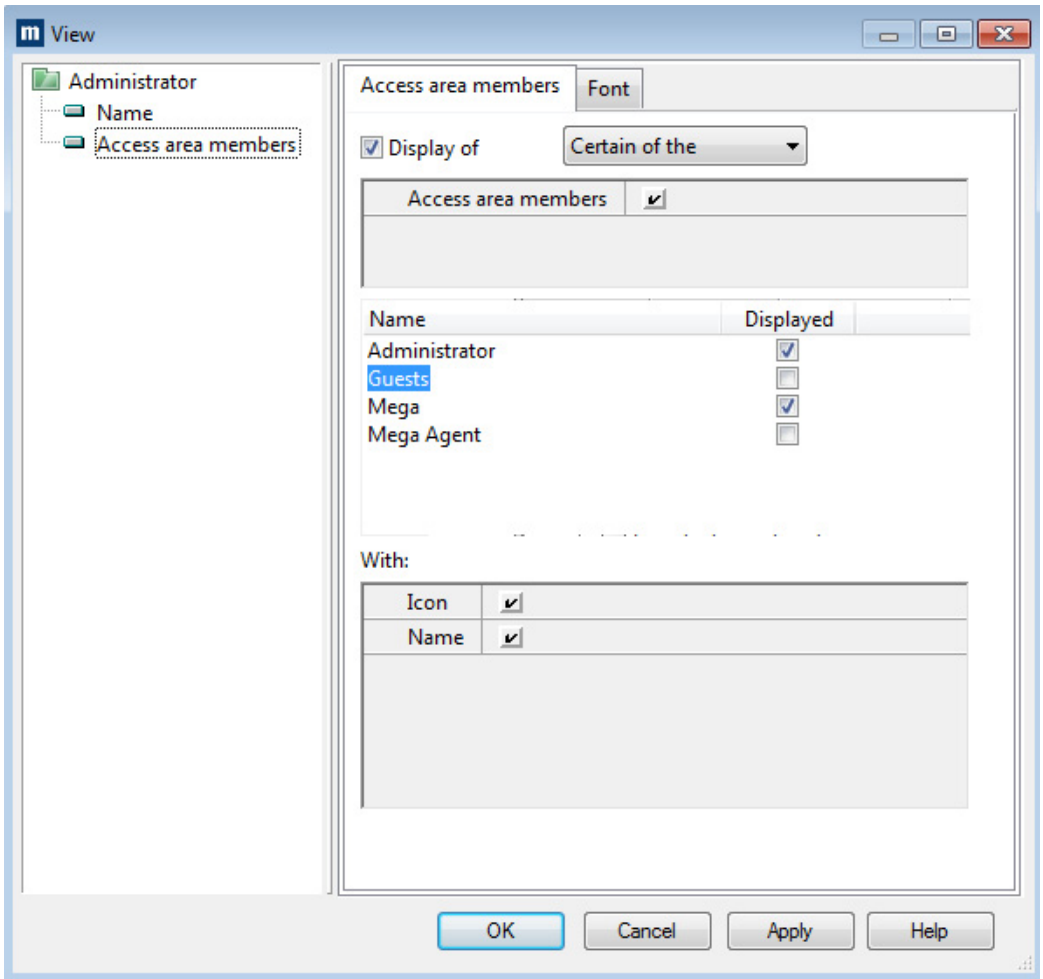
1. From **MEGA Administration**, open the reading access diagram.

   ☛ *See "Opening the reading access diagram (Windows Front-End)", page 333.*

2. Right-click the reading access area concerned and select **Shapes and Details**.
   The **View** dialog box opens.
3. In the tree on the left, select **Access Area Members**.
4. In the pane on the right, select **Access Area Members**.
5. Select the **Display of** option, then in its drop-down menu select **Certain of the** *Access area members*.

   ☛ *To display all or none of the access area members, select **All the** or **None of the**.*

6. Select the persons you want to see displayed.



7. Click **OK**.

CONFIGURING DATA READING ACCESS

In the **MEGA** desktop, the navigation window allows access to certain data reading access functions.

This section presents how to:

Associating Objects with Reading Access Areas

The **Administration** navigation window of the **MEGA** desktop allows access to general and object reading access areas.

> ☛ *To access content of the **Administration** navigation window, you must have **Advanced** or **Expert** metamodel access (see "Configuring metamodel access", page 77).*

The reading access areas tree is used to:

- connect objects to a given reading access area
- quickly propagate the reading access area to child objects

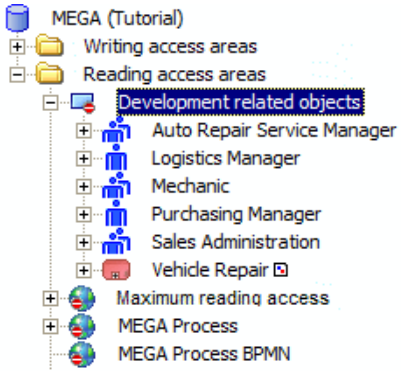
This tree simplifies management of propagation of reading access areas (see "Propagating a reading access area from MEGA", page 344). Its advantage compared with the classic propagation tool is that the propagation trace is kept thanks to the link.

Connecting objects to object reading access areas

To connect an object to an object reading access area:

1. In **MEGA**, open the **Administration** navigation window.
2. Expand the **Data Reading Access** folder.
3. Right-click the object reading access area concerned and select **Connect Object**.

4. In the query dialog box, find and select the desired objects and click **OK**. The objects are connected to the object reading access area and appear in the tree.



Disconnecting objects from reading access areas

To disconnect an object connected to a reading access area:

1. In **MEGA**, open the **Administration** navigation window.
2. Expand the folder of the reading access area concerned.
3. Right-click the object you want to disconnect and select **Disconnect**. The object disappears from the tree.

Displaying the list of objects associated with a reading access area

To display the list of objects associated with a reading access area:

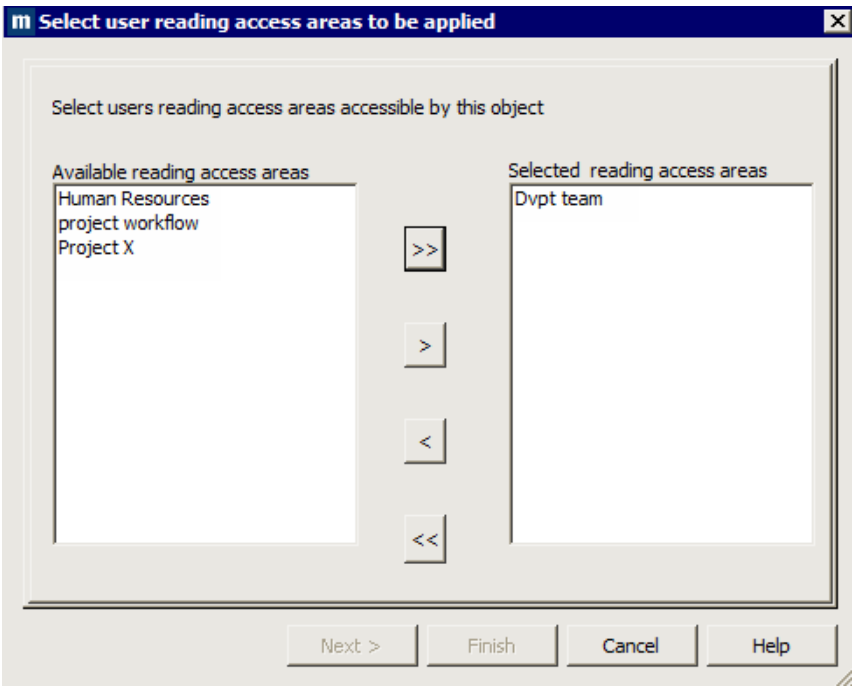
1. In **MEGA**, open the **Administration** navigation window.
2. Expand the **Data Reading Access** folder.
3. Right-click the reading access area concerned and select **Objects associated with reading access area**.
   A dialog box displays a list of these objects.

Associating user reading access areas with objects

To associate an object with one or several groups of users, proceed as follows:

1. From **MEGA**, select an object.
2. In the object properties dialog box, select the **General** tab, then the **Administration** subtab.
3. In the **Reading Access Area** drop-down list, click the arrow and select **Associate User Reading Access Areas**.

4. Using the arrows in the selection dialog box, move the user user reading access areas from available to selected, then click **Next**.



5. In the next dialog box, if an object reading access area corresponds to the user reading access areas, you are invited to validate this area, otherwise you must enter the name of a new user reading access area, which will be created corresponding to the previously selected user reading access areas.
6. Click **Finish**.

If you had to create a new object reading access area, this is automatically added in the reading access diagram and is connected to the corresponding user reading access area or areas, as well as to the ***Standard*** reading access area.

Propagating Reading Access Areas

A reading access area can be propagated to objects connected to a given object. You can propagate reading access areas from:

- **MEGA Administration**
- **MEGA**.

> ☛ *The propagation trace is kept when you propagate from the **MEGA** workspace.*

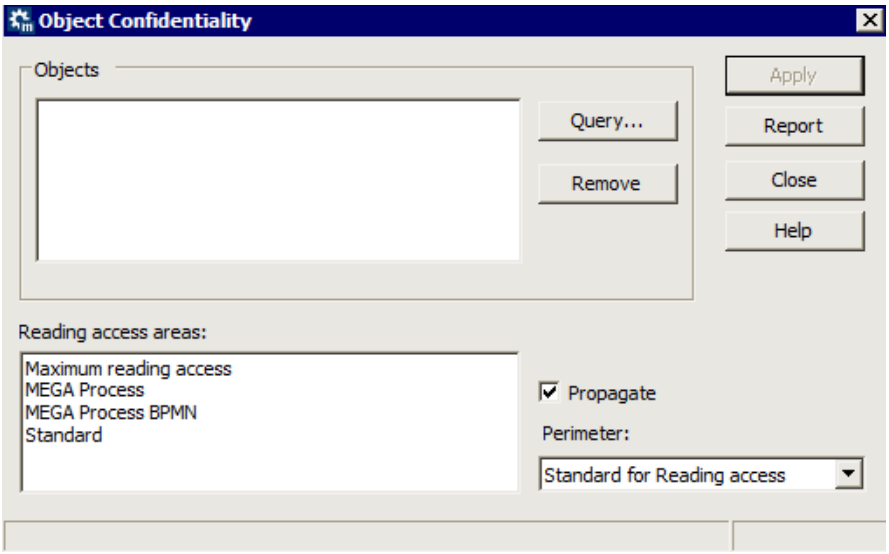
Propagating a reading access area from MEGA Administration

To propagate a reading access area:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **Repositories** folder.
3. Right-click the desired repository and select **Object Management > Object Confidentiality Setting**.



4. In the **Object Confidentiality** dialog box that opens, click **Query**.
5. Select the desired objects using the query tool, then click **OK**.
6. In the **Object Confidentiality** dialog box, in the **Reading Access Areas** frame , select the reading access area you want to apply to the selected objects.
7. (Optional) Select **Propagate** to propagate the reading access area to sub-objects.
8. Click **Apply**.

   ☛ *The operator used to propagate reading access areas is the "Standard for reading access" operator.*

Propagating a reading access area from MEGA

To propagate a reading access area:

1. In **MEGA**, open the **Administration** navigation window.
2. In the **Administration** navigation window, right-click the reading access area you wish to propagate and select **Propagation of reading access area to associated occurrences**.
   A dialog box may warn you of the presence of propagation conflicts.

   ☛ *Conflicts can arise if child objects are already connected to a different reading access area. You are informed that propagation stops*

at this child object (the physical link that connects the object to a reading access area is stronger than the reading access attribute value)

☛ *The operator used at reading access area propagation is the "Standard for reading access" operator.*

☛ *Alternatively, you can use the confidentiality area propagation tool via the menu **Tools > Manage > Object Confidentiality Setting**.*

Managing MetaClass Sensitivity and Reading Access Areas

☛ *The attribute enabling configuration of MetaClass sensitivity is accessible only if you have the **MEGA Supervisor** technical module.*

In the reading access management frame:

- a user is connected to a reading access area that defines all the objects he/she can see.

  ☛ *See "Connecting Users to Reading Access Areas", page 336.*

- an object type (MetaClass) is characterized by its sensitivity.

A MetaClass can be of sensitivity:

- **standard** (default value)
  Occurrences of the MetaClass created by a user belong to the user reading access at creation area or the Standard reading access area if the user does not have a reading access at creation area.
- **High**
  Occurrences of the MetaClass created by a user belong to the reading access area of the user that creates them.

  ☛ *To modify the sensitivity of a MetaClass, you must have rights to modify **MEGA** data. The option "Authorize MEGA Data Modification" must be activated at environment level, see "Managing Options", page 365.*

You can modify sensitivity value of the MetaClass.

☛ *See "Modifying MetaClass sensitivity", page 346.*

☛ *By default, a MetaClass is **Standard** sensitivity.*

Opening the MEGA MetaClasses reading access configuration dialog box

To open the **MEGA** MetaClasses reading access configuration dialog box:

1. From **MEGA Administration**, connect to the environment concerned.

   ☛ *See "Connecting to an Environment", page 5.*

2. Expand the **User Management** folder.
3. Right-click the **Data Reading Access** folder and select **Configure MEGA MetaClasses for reading access**.
   The **MEGA MetaClasses Reading Access Configuration** dialog box appears, listing the available **MetaClasses**.

   The icon alongside the name of each MetaClass indicates that default values:

   - have been modified
   - are retained.

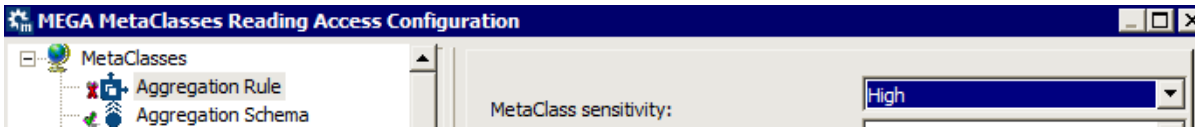
Modifying MetaClass sensitivity

To modify MetaClass sensitivity:

1. Open the **MEGA** MetaClasses reading access configuration dialog box.

   ☛ *See "Opening the MEGA MetaClasses reading access configuration dialog box", page 345.*

2. In the list of **MetaClasses**, select the desired MetaClass.
3. In the right pane, select the MetaClass sensitivity value:



☛ *A red cross alongside the name of the MetaClass indicates that at least one attribute of the MetaClass has no longer its default value.*

4. Click **OK**.

Modifications carried out may be canceled when your environment is updated. Remember to back up your extensions (metamodel and technical data).

Hiding confidential or sensitive objects in a diagram

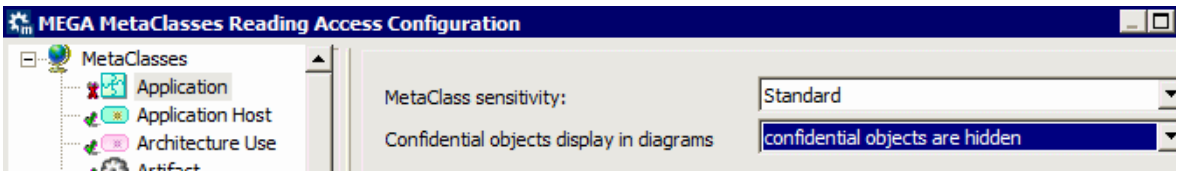
So as not to distort a diagram, confidential or sensitive objects are visible by default.

To hide confidential or sensitive objects in a diagram:

1. Open the **MEGA** MetaClasses reading access configuration dialog box.

   ☛ *See "Opening the MEGA MetaClasses reading access configuration dialog box", page 345.*

2. In the list of **MetaClasses**, select the desired object.
3. In the right pane, in the **Confidential objects display in diagrams** box, select "Confidential objects are hidden".



☛ *A red cross alongside the name of the MetaClass indicates that the MetaClass default value has been modified.*

4. Click **OK**.

☛ *These modifications are not taken into account in the metamodel until the metamodel is compiled. Compile the metamodel before closing*

*the **MEGA Administration** module, see "Compiling an Environment", page 231.*

Objects corresponding to this MetaClass will be hidden in the diagram.

☛ *When you select "Confidential objects are visible", objects corresponding to this MetaClass appear grayed in the diagram and you cannot access information relating to these objects.*

Modifications carried out may be canceled when your environment is updated. Remember to back up your extensions (metamodel and technical data).

Confidential or Sensitive Object Behavior

A confidential object is inaccessible to a user that does not have access to the corresponding reading access area.

It is as if the object did not exist, the object:

- does not appear in lists.
- is ignored in query results.
- does not appear in reports (MS Word) or Web sites.
- is not exported, duplicated, deleted or backed up, and its possible "children" (operations of a process, for example) are considered as orphans.
- only appears when another object is created with the same name or when a higher level object with a lower reading access level is deleted.
- cannot be modified.

☛ *Reading access management is not supported in **MEGA Database Builder**.*

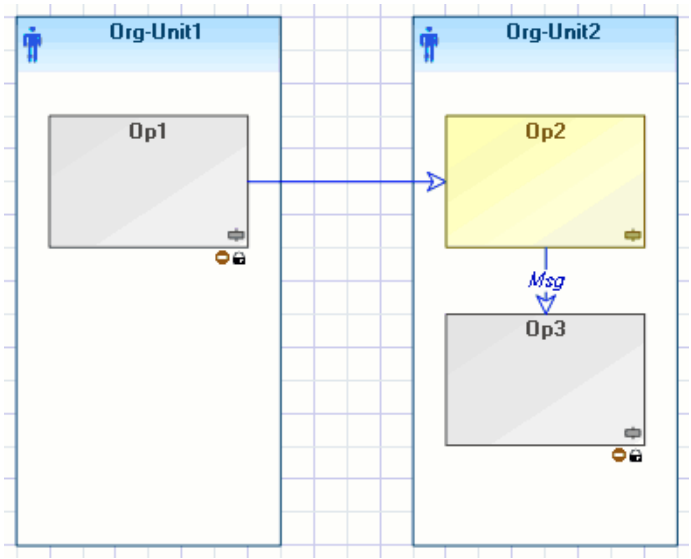
For more details on reading access areas, see "Managing Reading Access in MEGA", page 324.

Displaying a confidential or sensitive object in a diagram

By default, confidential or sensitive objects are visible in diagrams.

☛ *To hide confidential or sensitive objects, see "Hiding confidential or sensitive objects in a diagram", page 346.*

The name of a confidential or sensitive object is visible in the diagram, but its properties are not accessible. It appears grayed and an icon at bottom right indicates that the object is confidential or sensitive.



A confidential or sensitive object can only be resized and moved.

To hide MetaClass occurrences in diagrams:

1. In the **MEGA** menu bar, select **View > Navigation Windows > MetaStudio**.
2. Expand the **MetaClass** folder and its sub-folders.
3. Right-click the desired MetaClass and select **Properties**.
4. In the **Characteristics** tab (**Standard** subtab) for the **Confidential objects display in diagrams** property, select **Confidential objects are hidden**.
5. Click **OK**.
   The occurrences of the corresponding MetaClass are now hidden in diagrams.

   ☛ *You can also configure display of objects in diagrams via the reading access diagram, see "Hiding confidential or sensitive objects in a diagram", page 346.*

Export and Duplication

In the case of object export and duplication, if these operations have an impact on confidential objects, a warning message will ask you if you want to continue. If you do execute export or duplication, the confidential objects concerned will be neither copied nor exported.

Invisible objects (confidential) are not duplicated during object duplication. Only a message in the status bar indicates that the duplication result is incomplete.

Generation of reports (MS Word) and Web sites

When created, reports (MS Word) and Web sites are created with the reading access level of their creator (and not with the reading access level at creation)..

They are then always generated at their their reading access level.

A **Reading access area path** attribute exists on all reading access areas. If this attribute is specified, Web sites and reports (MS Word) are generated in this folder. Reports (MS Word) and Web sites are generated in this folder to facilitate reading access management of generated files by defining access rights to this generation folder. This task should be handled by the system administrator.

Confidential report (MS Word) and Web site generation paths can be defined in the properties dialog box of a reading access area.

To define this path:

1. In the reading access area properties dialog box, select the **Characteristics** tab.
2. In the **Reading access area path** field, specify the required path.
3. Click **OK**.

Macros

The principle of reading access management in macros is to carry out all calculations in **MEGA** and hide confidential or sensitive objects from users that do not have sufficient reading access area access rights to view them.

By default a macro is executed at user reading access level.

A macro can also be executed at its own reading access level.

If you execute a macro with a reading access level higher than the level of the current user, the methods.

- GetProp(xxx, "display") and GetFormatted return empty,
- GetProp("xxx") returns the value.

ExecuteGlobal and ***CreateObject*** ("Mega.Application") methods are prohibited in macros.

Other properties are accessible.

So that a macro can be executed with its reading access level:

1. In the macro properties dialog box, select the **Characteristics** tab.
2. In **_ExecutionOptions**, select the **Execution at Reading Access level** option.

Confidential or sensitive objects and namespaces

If an object with a namespace is not confidential or sensitive, but its parent is confidential or sensitive, the name of the latter will be masked in **MEGA**. It appears in **MEGA** as:

```
" ***::Operation 1 "
```

Modifying Reading Access Areas

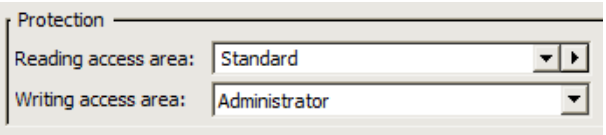
This section explains how to modify the reading access area area of an object or a user:

Modifying object reading access areas

From the properties dialog box of an object you can consult the reading access area to which it belongs.

To determine the reading access area of an object:

1. Right-click the object and select **Properties**.
2. In the object **Properties** dialog box, select the **General** tab, then the **Administration** subtab.
   In the **Protection** frame, you can consult and modify the **Reading access area**.



Modifying user reading access areas

You can modify a user reading access area from:

- the user management dialog box (**Reading access area** column of the person).

  ☛ *See "Modifying User Properties", page 70.*

  ☛ *The reading access diagram is compiled to take account of modifications.*

- Open the properties dialog box of the person.

  ☛ *See "Configuring a Person", page 56.*

  Warning: if you modify the reading access area in the user properties dialog box, you must recompile the reading access diagram so that the modification will be taken into account.

- the reading access diagram

  ☛ *See "Connecting Users to Reading Access Areas", page 336 or "Reading access area of the user", page 336.*

You can modify a user reading access area at creation from:

- Open the properties dialog box of the person.

  ☛ *See "Configuring a Person", page 56.*

  Warning: if you modify the reading access area in the user properties dialog box, you must recompile the reading access diagram so that the modification will be taken into account.

- the reading access diagram

  ☛ *See "Reading access area at creation", page 337.*

METACLASS CONFIDENTIALITY EXCEPTIONS

The following MetaClasses cannot be made confidential:

_Add-ins_data
_Add-ins_meta
_Brick
_Class
_ClassCommand
_Code Template
_Command
_Dispatch
_Executable
_MappingTypeItem
_MappingTypeItemProperty
_Object
_Operator
_Property
_Proposed_Table
_Resource
_StdFile
_Style
_TagAttributeDef
_TagAttributeDefValue
_TagDef
_Template
_Text
_Transaction
_TransactionData
_TransferredObject
_Type
_UML Reserved Word
Method author
MEGA Repository
ChangeItemData
ChangeItemDataTechnical
ChangeItemSystem
Generation kinematics
Component Template
DiagramTypeLink
DiagramTypeLinkStyle
DiagramTypeObject
DiagramTypeCollection
DiagramTypeField
DiagramTypeFormat
DiagramTypeParam
DiagramTypePath
DiagramTypePathPart
DiagramTypePopulating
DiagramTypeProperty
DiagramType
DiagramTypeView
Stem Codes Folder
Web Site Templates Folder
Analysis Templates Folder
Diagram Types Folder
HTML Formatter
Generality
Generator
Programming Language
Language
Animation Mask
Matrix Template

MetaAssociation
MetaAssociationEnd
MetaAssociationType
MetaAttribute
MetaAttributeGroup
MetaAttributeValue
Metaclass
MetaClassDiagramType
MetaCommand
MetaField
MetaList
MetaListType
MetaPattern
MetaPicture
MetaPropertyPage
MetaTest
MetaTree
MetaTreeBranch
MetaTreeNode
Method

Associative Object
Default Associative Object
Generic Object
System Generic Object
Analysis Parameter
Profile
Query Parameter
Generation rule
Modeling Rule
Modeling Regulation
Query
Web Site Template
SQL Clause Type
TaggedValue
Analysis Type
user
Descriptor Setting
DBMS Version
Writing access area
Reading access area

10

COMMAND FILE SYNTAX

The following points are covered here:

COMMAND FILE EXTENSIONS

> 🕮 *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).*

Command files can be obtained in two ways:

- By logical backup or by object export (.MGR): the *absolute identifiers* (IdAbs) of the imported objects are used and the authorization levels are kept.

  > 🕮 *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.*

- By logfile export (.MGL): the commands contain, in addition to the *absolute identifiers* (IdAbs) of objects, that of the user executing each command to check at import that the user had the necessary rights to execute this update.

Result of the import of these files is therefore different:

- ".MGR" corresponds to an image, complete or partial, of the repository at a given moment. It is therefore recommended that it be imported into an empty repository to rebuild this image.
- ".MGL" corresponds to commands to be applied to the repository to pass from initial state to final state.

At import, checks are performed automatically as a function of the file extension:

- For command files with the MGR extension, the absolute identifiers of the imported objects are used and the writing access levels are kept.
- For command files with the MGL extension (exported logfile or backup logfile), the absolute identifiers of the imported objects are used. Writing access levels are checked. The authorization levels are kept if the updates are consistent with the writing access diagram for the environment, otherwise they are rejected.

OBJECT NAMING RULES

Object naming will depend on the uniqueness rule applied to its name. This rule is important, since the name appears in command files.

An object has a unique name

An object must have a unique name throughout the repository.

```
For example, a report template (MS Word) has a name that
appears in command files.
```

A name is unique in a given context

Several objects can have the same name, but the name must be unique in a particular context: therefore it has a namespace.

```
For example, an operation of an organizational process: its
name must be unambiguous within the process, but several
different process operations can carry the same name.
```

For these objects, two names are presented to the user in the user interface:

Con-cept	Example	Comment
Name	Hire::Call candidate	Complete object name. Unique in the repository. Calculated from the local name and the name-space name (which can itself have a name-space). Here the operation "Call candidate" belongs to the "Hire" process.
Local name	Call candidate	Name of the object in its namespace. Unique in the namespace.

Two names are used in **MEGA** command language:

Concept	MetaAttribute	Example of value
Internal name of the object. It contains HexaIdabs of the object.	Name	14B8162B3F3A0347
Local name of the object and Hex-aIdabs of its namespace.	Generic Local Name	Call candidate [85ED06B63EC95B6F]

These build rules ensure respect of naming rules imposed by the repository:

- The name must be unique: the IdAbs is built to be so.
- The local name must be unique in its context: specify a uniqueness constraint on the GenericLocalName.

> ☛ *If the object is detached from its namespace, in the local name the indicated HexaIdAbs is then a string of 16 "0".*

Objects without name constraint

There is no name uniqueness constraint on certain objects such as messages: the same operation can send or receive several messages with the same name.

In this case, the object constitutes its own namespace.

Two names are used in **MEGA** command language:

Concept	MetaAttribute	Example of value
Internal "Name" of the object. It contains HexaIdabs of the object.	Name	14B8162B3F3A0347
Local name of the object and HexaIdabs of its namespace (itself).	Message Local Name	Convocation [14B8162B3F3A0347]

COMMANDS

Commands on objects

- .Create (creation of an object)
- .Update (modification of an object MetaAttribute)
- .Delete (deletion of an object)

Commands on links

- .Connect (creation of a link between two objects)
- .Disconnect (deletion of a link between two objects)
- .Change (modification of a link MetaAttribute)

Other Commands

- .Validate (triggers intermediate save on import)
- .Description (produces display in import dialog box)

Rules to be respected

Command files must comply with the following rules:

- A command line cannot contain more than 5000 characters.
- Object names are limited to:
  - 63 characters for object types without namespace.
  - 255 characters for object types with namespace (name or local name).
- Commands begin with a verb infinitive prefixed by ".".
- The "." of the command must be in the first column.
- Use a hyphen (-) at the end of a line to indicate that it continues on the next line.
- Comment lines are indicated by a hyphen (-) at the beginning of the line.
- Use double-quotes (") around values that contain spaces or characters other than letters or digits.

Remarks

- Certain objects are functionally invalid if one of their MetaAttributes is not entered or a link is not defined. For example, a diagram type object must be connected to another object by a descriptor type link. We say that the diagram describes this object.
- To exchange data between two **MEGA** environments, they must have identical metamodels and coherent user diagrams.

Commands as function of file type

Each command must consist of:

- a verb indicating the action to be carried out
- a list of parameters required to carry out this action (object types and names)
- a keyword ".CHK" followed by a list of the IdAbs of objects impacted by this command.

> ☛ *The fact of repeating the object name and IdAbs in the command enables its correct execution, even if the object has been renamed.*

The difference between the command of an ".MGR" file and the same command of an ".MGL" file is in the ".CHK":

- they have the same verb
- they have the same list of parameters
- the ".CHK" of MGL contains in addition in last position, the IdAbs of the user that issued the order.

> ☛ *A third file format (obsolete in this version) is ".MGE". In these files commands do not have a .CHK. The IdAbs are assigned as required. It is therefore not possible to process "namespaced" objects for which the namespace IdAbs cannot be assigned, since it forms part of their name.*

References to the metamodel

Each metamodel instance (MetaClass, MetaAttribute, …) can be prefixed by its IdAbs. This assures permanence of files despite renamings which may be carried out in the metamodel.

```
Example:
"~OsUiS9B5iiQ0[Operation]" is equivalent to "Operation".
```

BASIC SYNTAX

Creating an Object

Syntax	***.Create ."Object type""Object name" -*** ***.CHK "..."***
Example 1	.Create ."~IdAe93gyh020[Report template (MS Word)]" "Application documentation" - .CHK "w0e4VVXC)440e0SDsNpple00"
Example 2	.Create ."~OsUiS9B5iiQ0[Operation]" "14B8162B3F3A0347" - .CHK "GZB5hOXE)Sq0C30000mCpCpC"

In this command, the ".CHK" is the concatenation of the following IdAbs:

- IdAbs of the object
- IdAbs of object writing access
- In the case of the MGL, the IdAbs of the user that made this command.

Certain MetaAttributes, such as "Creation date" or "Creator" can only be updated at object creation. They must therefore be incorporated in this command.

Example:

```
Create ."~OsUiS9B5iiQ0[Operation]" "14B8162B3F3A0347" -
    .CHK "GZB5hOXE)Sq0C30000mCpCpC" -
    ."~510000000L00[Creation Date]"          "2003/08/13 10:42:51" -
    ."~(10000000v30[Creator]"                "OmNRasMwq400" -
    ."~520000000L40[Create Version]"         "25088"
```

The "Creator" and "Modifier" MetaAttributes contain the IdAbs of users that have created and modified the object. If they are not specified in the command, they automatically take the IdAbs of the user importing the file.

Similarly, "Link creation date" and Link modification date" are specified from the import date if they are absent.

Deleting an Object

Syntax	***.Delete ."Object type" "Object name" -*** ***.CHK "..."***
Example 1	.Delete ."~ldAe93gyh020[Report template (MS Word)]" "Application documentation" - .CHK "w0e4VVXC)440"
Example 2	.Delete ."~OsUiS9B5iiQ0[Operation]" "14B8162B3F3A0347" - .CHK "GZB5hOXE)Sq0"

In this command, the ".CHK" is the concatenation of the following IdAbs:

- IdAbs of the object
- In the case of the MGL, the IdAbs of the user that made this command.

Deletion of an object systematically results in:

- Loss of its attribute and text values.
- Deletion of all of the links around the object.

Modifying an Object

Syntax	***.Modify ."Object type" "Object name" -*** ***.CHK "..." -*** ***."metaattribute1" "Value1" -*** ***."metaattribute2" "Value2"***
Example 1	.Update ."~MrUiM9B5iyM0[Application]" "874B9C483D7828C6" - .CHK "PjqX8n9UzOCA" - ."~610000000P00[Modification Date]" "2010/09/07 10:26:30" - ."~b10000000L20[Modifier]" "xDqT)UdFwC10" - ."~2yUL4SsRp4B0[Application Code]" "GESTCAT11" - ."~ByUL4SsRpeB0[Operating Application Date]" "1995/10/04 23:00:00"
Example 2	.Update ."~gsUiU9B5iiR0[Organizational Process]" "0A496AAE407D1621" - .CHK "Vba2kgMV05Y5" - ."~pjRX1OOKne20[Process Frequency]" "Q""

In this command, the ".CHK" is the concatenation of the following IdAbs:

- IdAbs of the object
- In the case of the MGL, the IdAbs of the user that made this command.

The "Modification date" and "Modifier" MetaAttributes can be modified like standard MetaAttributes. If they are not specified in the command, they automatically take the file import date and the IdAbs of the user importing the file.

In the case of "Example 2" with a tabulated attribute, the value to be entered is the internal value (for process frequency this is "D" and not "Daily").

Modifying Text

Syntax	***.Modify ."Object type" "Object name" -*** ***.CHK "..." -*** ***."Text name" "Text format"*** ***Text value*** ***.***
Example 1	.Update ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" - .CHK "AH(tl0UJDDxA" - ."~f10000000b20[Comment]" "g3TCfAJnyq00" 00680SbnxCMPqRc5SN6bpSsvXS6DfCZ5dN38rPcLaN31cPcLaRc5iC35dUpOpRsPST7HkUsnY 00680C6PSRcPSN6nfQ6DcSt9XC7HbKqqWQ5CWR6nbR4GWVJjd2WrzQNPSQtTbP6vfTLmqN 35Z 00602Sc5mPbnaPbmmC39pRqCWPMrj87Hk86PlS71XOsbiQNHX86vlS5mn3N9X3NqA000A .

Text format	Value
ASCII text	0 000000000000
Binary text	1 000000000001
RTF text	"MRDYO5Oe(smC"
HTML text	"LQDYO58M6tmC"
ANSI text	"G3000000W10S"

In this command, the ".CHK" is the concatenation of the following IdAbs:

- IdAbs of the object
- In the case of the MGL, the IdAbs of the user that made this command.

In a command file, each line of text is limited to 74 characters.

End of the text marked by a line containing only one point (".") in the first column.

A semi-colon in the first column inserts a blank line (the rest of the line must be left blank).

> ☛ *When text is extracted, lines are divided after character 73 and a semicolon is inserted in position 74, indicating that the next line is to be concatenated with the previous one.*

Complementary indicators:

- Each text modification applies to its totality. It is not possible to add just one complement.
- The semicolon character (;) in first position inserts an blank line. To reinitialize a text, it is sufficient that the text value contains just a semicolon.
- The characters period and semicolon (.;) in first and second position create a line containing a period only.
- Two semicolon characters (;;) in first and second position create a line containing a semicolon only.
- Apostrophe (') and quotation marks (") are authorized as text values.
- The semicolon character (;) enables cutting of text lines exceeding 74 characters. The semicolon is therefore the last significant character in the line.

To reinitialize a text, it is sufficient that the text value contains just a semicolon.

```
Example:
Update ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" -
        .CHK "AH(tl0UJDDxA" -
        ."~f10000000b20[Comment]" "000000000000"
;
.
```

To delete a text, the text value should be left empty.

```
Example
Update ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" -
        .CHK "AH(tl0UJDDxA" -
        ."~f10000000b20[Comment]" "000000000000"
.
```

A reinitialized text contains nothing but it exists, while a deleted text no longer exists. For example the query *"Select Application where Comment null"* returns applications that have no comment, but not those that have a reinitialized comment.

Modifying a Name

Syntax	***.Modify ."Object type" "Object name" -*** ***.CHK "..." -*** ***."Name or Local name" "Value "***
Example 1	.Update ."~ldAe93gyh020[Report template (MS Word)]" "Report template (MS Word)-1" - .CHK "RJ(tBUUJD5(AV(WEIeZIDT4B" - ."~210000000900[Name]" "Report template (MS Word)-New"
Example 2	.Update ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" - .CHK "AH(tl0UJDDxA" - ."~g20000000f60[Generic Local name]" "Application-1[0000000000000000]"

Creating and Modifying an Object with a Single Command

At object creation, creation of a "modification" command by MetaAttributes to be specified is of no interest: MetaAttributes (non-textual) can be directly assigned by the create command.

Syntax	***.Create ."Object type" "Object name" -*** ***.CHK "..." -*** ***."metaattribute1" "Value1" -*** ***."metaattribute2" "Value2"***
Example 1	.Create ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" - .CHK "AH(tl0UJDDxAC30000mCpCpC" - ."~510000000L00[Creation Date]" "2011/02/05 11:41:35 PM" - ."~610000000P00[Modification Date]" "2011/02/06 12:31:38 AM" - ."~(10000000v30[Creator]" "V(WEIeZIDT4B" - ."~b10000000L20[Modifier]" "V(WEIeZIDT4B" - ."~520000000L40[Create Version]" "29248" - ."~620000000P40[Update Version]" "29248" - ."~)20000000z70[Confidentiality area identifier]" "sTlVwxdH3100" - ."~2yUL4SsRp4B0[Application Code]" "AA" - ."~KyUL4SsRpCC0[Version Number]" "12" - ."~ByUL4SsRpeB0[Operating Application Date]" "2011/02/11 11:00:00" - ."~)Sgoy)ygu020[Application Type]" "M" - ."~nOU8g8IMCb30[Converted Name Version]" "0" - ."~PYq45X2wBP92[Date of C&A Completion]" "2011/02/06 11:00:00" - ."~Ol8pdE(l8r(0[Deployment Date]" "2011/02/27 11:00:00" - ."~g20000000f60[Generic Local name]" "Application-1[0000000000000000]" - ."~PZq41c2wBXP2[Security Planning]" "Operational" - ."~a20000000H60[LanguageUpdateDate]" "2011/02/05 23:41:57"

Creating a Link Between Two Objects

Syntax	***.Connect ."Object type" "Object 1 name" ."MetaAssociationEnd" "Object 2 name" -*** ***.CHK "..."***
Example 1	.Connect ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" ."~mi54NLn-HzCj0[Application within Internal Architecture]" "DFE4F2274D4D2C43" - .CHK "AH(tl0UJDDxAbJ(td8VJDD4B" - ."~710000000T00[Link creation date]" "2011/02/06 00:58:15" - ."~810000000X00[Link modification date]" "2011/02/06 00:58:15" - ."~720000000T40[Link Creator]" "V(WEIeZIDT4B" - ."~920000000b40[Link Modifier]" "V(WEIeZIDT4B" - ."~410000000H00[Order]" "9999"

In this command, the ".CHK" is the concatenation of the following IdAbs:

- IdAbs of object 1
- IdAbs of object 2
- In the case of the MGL, the IdAbs of the user that made this command.

The "Order" MetaAttribute is optional. If present, the order is numeric on maximum four positions, otherwise the order is set by default to 9999.

The "Link creator" and "Link modifier" MetaAttributes contain the IdAbs of users that have created and modified the link. If they are not specified in the command, they automatically take the IdAbs of the user importing the file.

Similarly, "Link creation date" and Link modification date" are specified from the import date if they are absent.

> ☛ *If this link is used to build a namespace, it must be completed by modification of the local name of the namespaced object to maintain repository consistency.*

Similar to object creation, it is possible to specify link MetaAttributes (except texts) directly in this command, without passing via a modification command.

Modifying a Link

With the exception of its header, this command has the same syntax as the object modification command.

☛ *See "Modifying an Object", page 356.*

Syntax	***.Change ."Object type" "Object 1 name" ."MetaAssociationEnd" "Object 2 name" -*** ***.CHK "..." -*** ***."metaattribute 1" "Value 1" -*** ***."metaattribute 2" "Value 2" -*** ***."Text name" "Text format" -*** ***Text value*** ***.***
Example	.Change ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" ."~mi54NLnHzCj0[Application within Internal Architecture]" "DFE4F2274D4D2C43" - .CHK "AH(tl0UJDDxAbJ(td8VJDD4B" - ."~810000000X00[Link modification date]" "2011/02/06 1:22:26 AM" - ."~920000000b40[Link Modifier]" "V(WEIeZIDT4B" - ."~b20000000L60[LinkLanguageUpdateDate]" "2011/02/06 01:22:26" - ."~C3cm9FyluS20[Link Comment]" "g3TCfAJnyq00" 00680SbnxCMPqRc5SN6bpSsvXS6DfCZ5dN38rPcLaN31cPcLaRc5iC35dUpOpRsPST7HkUsnY 00680C6PSRcPSN6nfQ6DcSt9XC7HbKqqWQ5CWR6nbR4GWVJjd2WrzQNPSQtTbP6vfTLmqN35Z 00362Sc5mPbnaPbmmC39pR68WR69XS5nX3N9X3NqA000A .

In this command, the ".CHK" is the concatenation of the following IdAbs:

- IdAbs of object 1
- IdAbs of object 2
- In the case of the MGL, the IdAbs of the user that made this command.

The MetaAttributes “Link modification date”, and “Link modifier” can be modified just like standard MetaAttributes. If they are not specified in the command, they automatically take the file import date and the IdAbs of the user importing the file.

Deleting a Link

Syntax	***.Disconnect ."Object type" "Object name 1" ."MetaAssociationEnd 2" "Object name 2" -*** ***.CHK "..."***
Example	.Disconnect ."~MrUiM9B5iyM0[Application]" "DFE4E02F4D4D2BB3" ."~mi54NLnHzCj0[Application within Internal Architecture]" "DFE4F2274D4D2C43" - .CHK "AH(tl0UJDDxAbJ(td8VJDD4B"

In this command, the ".CHK" is the concatenation of the following IdAbs:

- IdAbs of object 1
- IdAbs of object 2
- In the case of the MGL, the IdAbs of the user that made this command.

Deletion of a link results in loss of link MetaAttributes values.

☛ *If this link is used to build a namespace, it must be completed by modification of the local name of the "namespaced" object to maintain repository consistency. Its namespace has become "[0000000000000000]".*

Managing Translations

For each language supported by MEGA, two MetaAttributes indicate the last modification date of translations in a language:

- "[LanguageUpdateDate (Language)]" for an object
- "[LinkLanguageUpdateDate (Language)]" for a link

These MetaAttributes are managed following the same rules as the"Modification date" and "Link modification date" MetaAttributes:

- They can be modified in the same way as standard MetaAttributes.
- If they are not specified in the command modifying a translation, they automatically take the file import date.

Validating Import

Syntax	***.Validate***

This command does not contain a .CHK and produces an intermediate save operation at import.

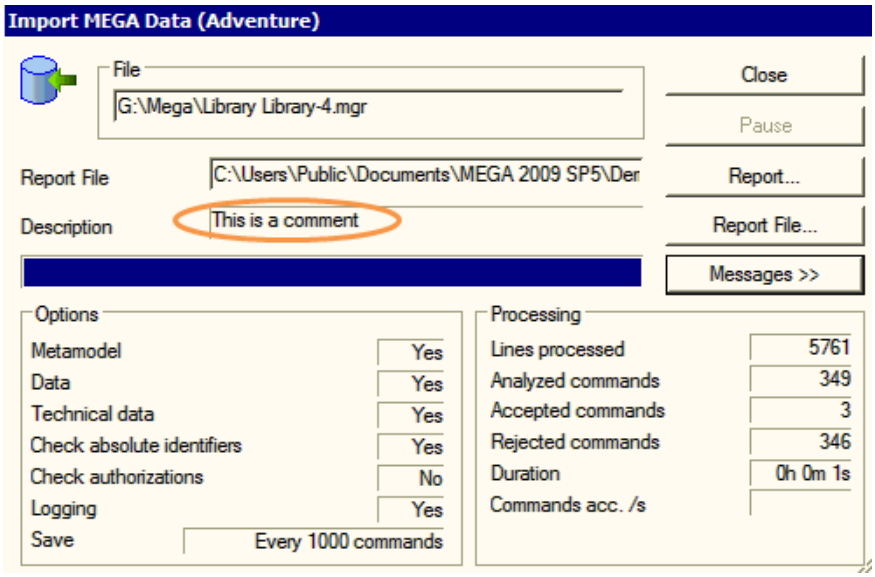
☛ *This command invalidates save operation selection made by the user interface. For example, to validate consistency of a command file, the user generally imports with "Save Never". Commands are then saved until the last ".Validate" of the file.*

Displaying a Comment in the Import Dialog Box

Syntax	***.Description 'Text'***
Example	.Description 'MetaClass: Acceptance Criteria'

This command does not contain a .CHK.

The text appears on the user interface at import.



Transforming an MGL File to MGR

☛ *See "Command file extensions", page 350.*

You do not need to transform an .mgl file to .mgr.

To obtain the same result, when importing an .mgl file:

- in the data import dialog box, in the **Checks** frame, clear the **Check Writing Accesses** check box.

Transforming an MGR File to MGL

☛ *See "Command file extensions", page 350.*

You do not need to transform an .mgr file to .mgl.

To obtain the same result, when importing an .mgr file:

- in the data import dialog box, in the **Filter** frame, select the **Reassign User** check box.
  Each command is then processed as if its CHK contained the IdAbs of the importing user. Writing access checks are carried out related to its rights.

  ☛ *At import in the CHK of an MGL command, the "Reassign User" check box also allows substitution of the IdAbs of the user by that of the person importing.*

11

MANAGING OPTIONS

This chapter presents the various tools and options used to configure and customize **MEGA**.

The following points are covered here:

OPTIONS OVERVIEW

MEGA options concern:

- site technical configuration.
- values proposed by default for each function of **MEGA**. These values can be modified by users on each workstation.
  This configuration is described in the guides covering each function.

MEGA options are accessible at several levels. **MEGA** functions can be configured at the following levels:

- site

  *The site is the location where **MEGA** is installed; it is the root of the application.*
- environment
- profile (which groups a configuration common to several users)
- user
- workstation

There is by default an inheritance mechanism between these different levels (excepting workstation level):

- the environment inherits options define at site level.
- the profile inherits options defined at environment level.
- the user inherits options defined at connection profile level.

Customizations made at user level are of highest priority, followed in order of priority by those made at profile, environment and site levels.

Having modified option values, it is recommended that you dispatch or save your work, close MEGA and then reopen it. Certain problems in refresh can occur if these precautions are not taken.

For detailed information on these options, see the context-sensitive help in the lower part of the window.

OPTION WINDOW PRESENTATION

The left pane of the window contains the various option groups. It comprises two parts:

- options available for the site, environment, profile, and user

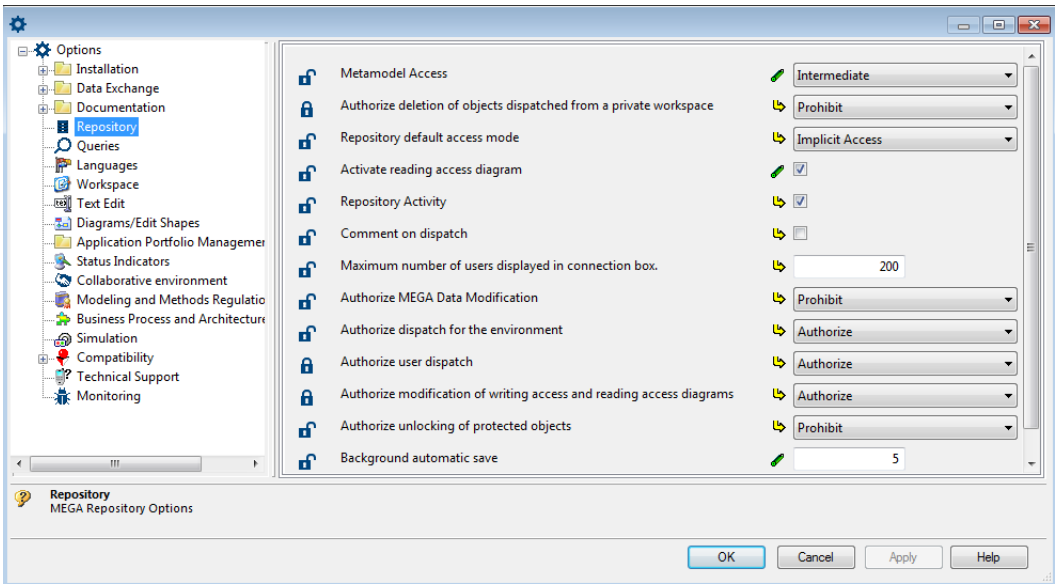
  ☛ *See "User options", page 375.*

- options specific to the workstation

  ☛ *See "Workstation Options", page 376.*

The right pane enables configuration of the various options corresponding to the group selected in the left pane.

☛ *Options vary depending on products you have available.*



For more details on an option:

❱ Click on the name of the option to display the context-sensitive help in the lower part of the window.

☛ *When the user has a private workspace in progress, you cannot modify its options from **MEGA Administration**.*

ACCESSING OPTIONS

Options Level

You can modify options at the following levels:

- site
  - ☛ *See "Modifying options at site level", page 368.*
- environment
  - ☛ *See "Modifying options at environment level", page 368.*
- profile
  - ☛ *See "Modifying options at profile level", page 369.*
- user
  - ☛ *See "Modifying options at user level", page 369.*
- workstation
  - ☛ *See "Modifying options at workstation level:", page 370.*

Modifying options at site level

To modify options at site level:

1. Start **MEGA Administration**.
   - ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*
2. In the navigation tree, right-click the site name and select **Options > Modify**.
   The site options window opens.

Modifying options at environment level

You can modify options at the environment level from the:

- **Administration** desktop (Web Front-End)
- **MEGA Administration** (Windows Front-End)

Web Front-End

To modify options at environment level from the **Administration** desktop:

1. Connect to the **MEGA Administration** desktop.
   - ☛ *See "Connecting to the Administration Desktop (Web Front-End)", page 7.*
2. In the edit area, click **Environment Options**.
   The environment options window opens.

Windows Front-End

To modify options at the environment level from **MEGA Administration** :

1. From **MEGA Administration**, connect to the desired environment.

   ☛ *See "Connecting to an Environment", page 5.*
2. Right-click the desired environment and select **Options > Modify**.
   The environment options window opens.

Modifying options at profile level

You can modify options at the profile level from:

- **Administration** desktop (Web Front-End)
- **MEGA Administration** (Windows Front-End)

Web Front-End

To modify options at the profile level from the **Administration** desktop:

1. Access the Profiles management pages.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. In the edit area, select the profile concerned.
3. Click **Options**.
   The profile options window opens.

Windows Front-End

To modify options at profile level from **MEGA Administration**:

1. From **MEGA Administration**, connect to the desired environment.

   ☛ *See "Connecting to an Environment", page 5.*
2. Open the manage profiles dialog box.

   ☛ *See "Opening the profile management window (Windows Front-End)", page 41 or "Opening the business roles and profiles management window (Windows Front-End)", page 41.*
3. In the **Profile** tab , right-click the profile and select **Options**.
   The profile options window opens.

Modifying options at user level

You can modify user options with the:

- **Administration** desktop (Web Front-End)
- **MEGA Administration** (Windows Front-End)
- **MEGA** (Windows Front-End)

Web Front-End

To modify options at the user level from the **Administration** desktop:

1. Access the user management page.

   ☛ *See "Accessing the User Management Pages (Web Front-End)", page 31.*
2. Select a **Persons** sub-folder.
3. In the edit area, select the person concerned.

4. Click **Options**.
   The person's options window opens.

Windows Front-End

To modify the options of a user with **MEGA Administration**:

1. Connect to the desired environment.
   ☛ *See "Connecting to an Environment", page 5.*
2. Open the user management Dialog Box.
   ☛ *See "Opening the user management window (Windows Front-End)", page 40.*
3. Select the **Persons** tab.
4. Right-click the desired person and select **Options**.
   The user options window opens.

To modify user options from **MEGA**:

1. Connect to **MEGA**.
2. In the menu bar, select **Tools > Options**.
   The user options window opens.

Modifying options at workstation level:

To modify options at workstation level:

1. Start **MEGA Administration**.
   ☛ *See "Connecting to MEGA Administration (Windows Front-End)", page 4.*
2. Right-click **Workstation** and select **Options**.
   The workstation options window opens.

Each option can take several values.

Option Inheritance

An option inherits a value defined at a higher level:

- A user inherits options defined at the connection profile level.
- A profile inherits options defined at the environment level.
- An environment inherits options defined at the site level.

The icon located opposite the option indicates the inheritance, or not, from the higher level:

- **Default value** indicates the inheritance from the higher level.
- **Modified value** indicates that the inherited option value has been modified. The value is no longer inherited from the higher level.

To specify that an option does not inherit the value defined at higher level:

1. Open the options page.
   ☛ *See "Options Level", page 368.*
2. Click **Default value**.
   The icon changes in **Modified value**.

Checking Option Modifications

You can prohibit modification of any option at a level lower than your current level.

```
Example: if you open options of the environment, you can
prohibit modification of all options at user level.
```

Prohibiting modification of a lower level option

To prohibit modification of a lower level option:

1. Access the options.

   ☛ *See "Options Level", page 368.*

2. Click  icon located opposite the option concerned.

   The padlock closes  : option modification by a user is now prohibited from **MEGA**.

Unlocking the modification of a lower level option

To unlock modification of a lower level option:

1. Access the options.

   ☛ *See "Options Level", page 368.*

2. Click the closed padlock icon.
   The padlock opens: modification of the option is again possible.

Reinitializing Option Values

You can reinitialize the values for:

- an option
- an option group

Reinitializing the values of an option

To reinitialize the value of an option:

1. Access the options.

   ☛ *See "Options Level", page 368.*

2. Click:

   - (Web Front-End) **Reinitialize** 
   - (Windows Front-End) **Modified Value**  , the icon changes to **Default Value** 

   The value of the option is reinitialized.

Reinitializing the values of an option group (Windows Front-End)

To reinitialize values of an option group with **MEGA Administration**:

1. Access the options.

   ☛ *See "Options Level", page 368.*

2. In the options tree, right-click the option group and select **Reinitialization**.
   All the options in the group selected are reset to their default values.

GENERATING THE LIST OF OPTIONS (WINDOWS FRONT-END)

You can generate a report that lists all options classified by group, with their comments.

To generate the list of options:

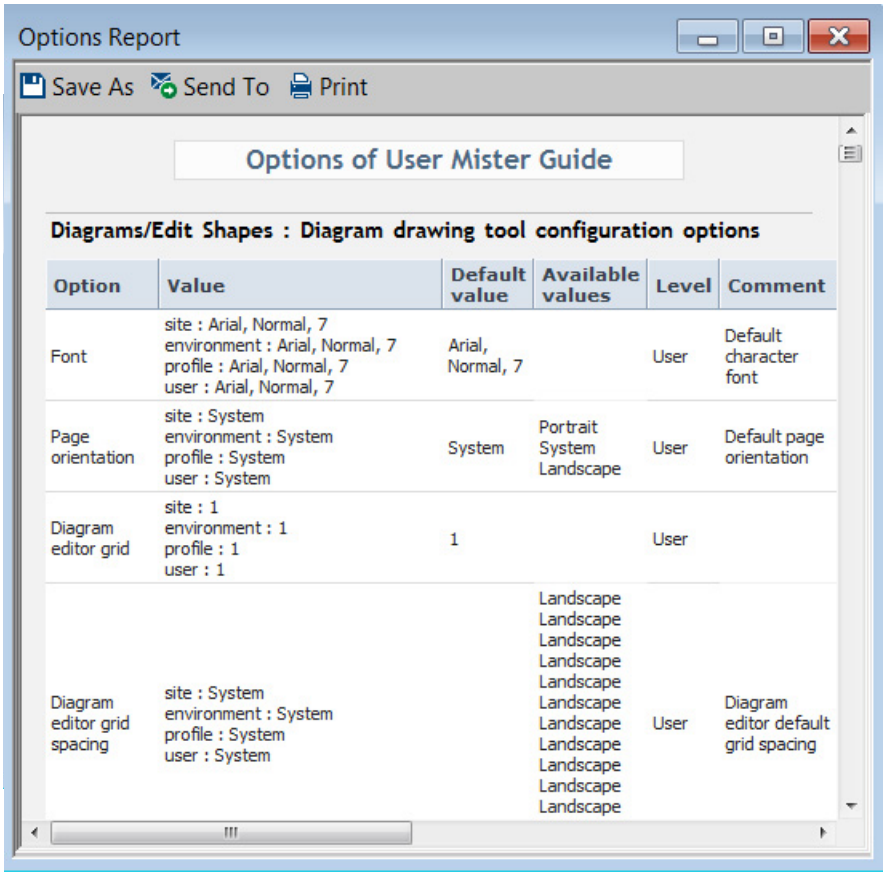
1. Open the options dialog box of the user.

   ☛ *See "Modifying options at user level", page 369.*

2. Right-click **Options** and select **Report**.
   Report generation may take some time.

It contains:

- the names of available options
- the values available for each option
- the default value
- a comment explaining the option use context
- the option level:
  - user
  - environment
  - site



To save this report in .html format:

- Click **Save As** and select *.htm format.

AVAILABLE OPTION GROUPS

User options

☛ *At user configuration level, certain options are grayed. They can be defined only for an environment or site and not for a user.*

Note that repository and modeling options contain important information for the functional administrator.

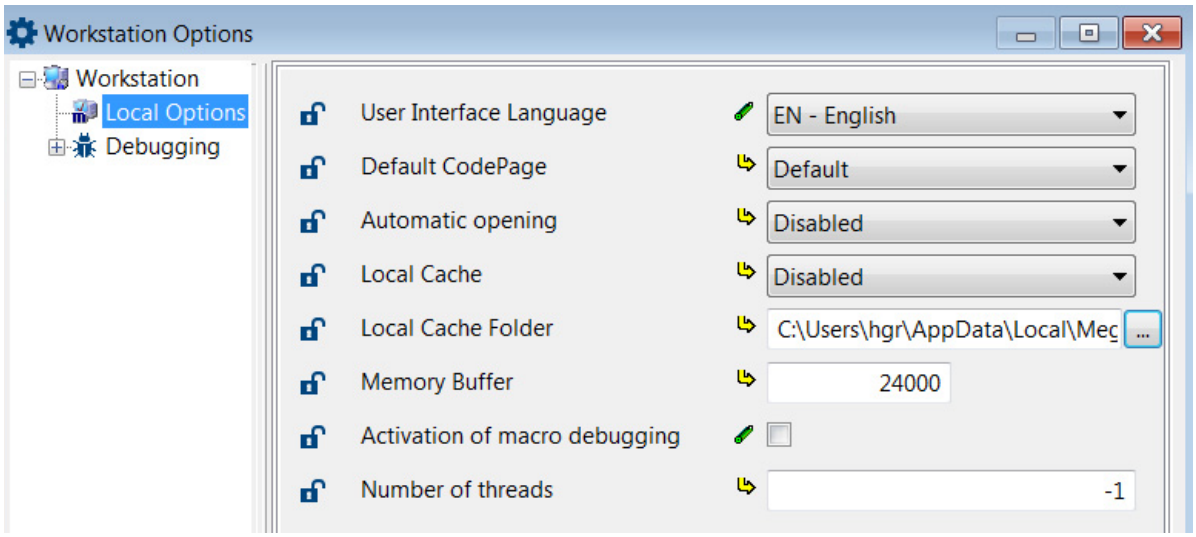
- **Installation**
  Options linked to installation: licenses, **MEGA Advisor**, information on the company, Web application (options linked to the **MEGA** user workspace (Web Front-End)
- **Data Exchange**
  Options linked to import/export, exchanges with third party tools.
- **Documentation**
  Options linked to documentation generated by **MEGA** (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
- **Workspace**
  Options linked to the user workspace of **MEGA** (Windows Front-End). They enable display of a certain number of functions or not, as well as management of user inactivity or not.
- **Editing Text**
  Options concerning RTF format comment entry
- **Diagrams/Edit Shapes**
  Options of drawing tool configuration (diagrams and shapes editor)
- **Status indicators**
  Options concerning display of indicators available in workspace and diagrams
- **Collaborative Environment**
  Options available with **HOPEX Collaboration Manager**
- **Mapping Editor**
  Options linked to the mapping editor, a tool enabling alignment of data models (essentially with **MEGA 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 level of use of **MEGA Simulation**
- **Compatibility**
  Options of compatibility concerning diagrams and obsolete functionalities
- **Technical Support**
  Options concerning access to Technical Support
- **Monitoring**
  Option used to supervise data access

Workstation Options

The local options group contains information specific to the workstation.

☛ *This information is stored in file "MEGAWKS.INI".*



MANAGING LANGUAGES

The following points are detailed here:

Changing User Interface (Windows Front-End) Language

You can change interface language of a **MEGA** user (Windows Front-End).

> ☛ *To modify the language of Web applications, see "Managing Languages in Web Applications", page 379*

To change the (Windows Front-End) user interface language

1. With **MEGA Administration** in the **MEGA** tree, right-click **Workstation** and select **Options**.
2. In the **Workstation** tree, select **Local Options**.
3. In the right pane, modify the value of the **User Interface Language** option.
4. Click **OK**.
   The change is effective at next restart of **MEGA (Windows Front-End)**.

Defining the Data Languages Available for a User

You can also select the languages available in **MEGA** and in which you can enter data.

> ☛ *See "Installing Additional Languages", page 378.*

So that a **MEGA** workstation can be used in multilingual mode, multilingual mode must be authorized for the site.

> ☛ *When you duplicate an object, it must be in the repository language so that translations in the various languages will be correctly transferred to the duplicates.*
>
> *To determine the language of your repository, consult repository properties.*
>
> ☛ *For more information on the use of languages, see the **MEGA Common Features** guide, "**MEGA** in a Multilingual Context" section.*

To define the data languages available for a user:

1. With **MEGA Administration**, access the options management window.
   - ☛ *See "Modifying options at environment level", page 368.*
   - ☛ *See "Modifying options at profile level", page 369.*
   - ☛ *See "Modifying options at user level", page 369.*
2. In the options tree, select **Languages**.
3. In the right pane, select the languages available for the interface.
4. Click **OK**.

Changing User Data Language (Windows Front-End)

The user can change his/her own data language.

- ☛ *To change user data language in Web applications, see "Specifying Data Language for a User or User Group (Web Front-End)", page 135.*

To modify the data language from **MEGA (Windows Front-End)**:

1. Connect to **MEGA (Windows Front-End)**.
2. In the menu bar, select **Tools > Languages**.
3. Select the data language.
   - ☛ *Translated data appears in the selected language.*
   - ☛ *To install additional languages, see "Installing Additional Languages", page 378:*

Installing Additional Languages

To install additional languages in **MEGA**:

1. From **MEGA Administration**, connect to the desired environment.
   - ☛ *See "Connecting to an Environment", page 5.*
2. Right-click the environment (or site) and select **Metamodel > Install Additional Languages**.
3. The dialog box **Install Additional Languages** opens.
4. Select the languages you wish to have available in **MEGA**, and click **OK**. A window indicates progress of import of the corresponding libraries.

   The additional languages are accessible from the **Tools > Language** menu of the **MEGA** desktop.

Defining the Language of e-mails in Workflows

To define the language of e-mails in workflows:

1. Access the options management window.
   - ☛ *See "Modifying options at environment level", page 368.*
2. In the options tree, expand the **Installation** folder and select **Workflows**.

3. In the right pane, in option **Language for sending mails**, select the language to be defined in e-mails.
4. Click **OK**.

Managing Languages in Web Applications

You can modify:

- the interface language in Web applications, see:
  - "Modifying the interface language in Web applications at environment level", page 379.
  - "Modifying the interface language in Web applications at user level", page 379
- the data language in Web applications, see "Modifying the data language in Web applications at environment level", page 379.

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 interface language from his/her desktop, see "Modifying the interface language in Web applications at user level", page 379.*

To define the interface language in Web applications:

1. Access the environment options management window.

   ☛ *See "Modifying options at environment level", page 368.*
2. In the options tree, expand the **Installation** folder and select **Web Application**.
3. In the right pane, modify the value of the **GUI language** via the drop-down menu.

Modifying the interface language in Web applications at user level

From his/her **MEGA** desktop, the user can change his/her interface language.

To modify data language from the **MEGA** desktop (Web Front-End):

1. From your **MEGA** desktop (Web Front-End), in the **Miscellaneous** toolbar, select **My Account > Options**.
2. Expand the **Installation** folder and select **Web Application**.
3. In the right pane, modify the value of the **GUI language** via the drop-down menu.

   ☛ *You must disconnect for this modification to be taken into account.*

Modifying the data language in Web applications at environment level

The data language is the language with which the user connects by default the first time. If the user changes data language in the interface, this is kept for the next connection.

By default, the data language is defined in the environment options.

If necessary you can define the data language for each user.

☛ *See "Specifying Data Language for a User or User Group (Web Front-End)", page 135.*

The data language defined at user level takes priority over the language defined in the environment options.

To modify the data language at environment level:

1. Access the environment options management window.

☛ *See "Modifying options at environment level", page 368.*

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.

FREQUENTLY ASKED QUESTIONS (FAQ)

The following points are covered here:

COMMON OPERATIONS

How do I copy a repository from one environment to another?

Standard procedure: make a logical backup of the repository, then carry out a logical restore of the backup in an empty repository of the target environment.

For GBMS environments you can copy repository files (EMA, EMB, EMS, EMV) in a folder carrying the repository name, then create a reference for the repository in the second environment, but only if the metamodel is exactly the same in both environments.

Can I create a reference for an environment in another site?

No, the functional rule is that a reference for a MEGA environment should only be referenced in an installation (site).

Can I delete a user?

Yes, you can delete a user. See "Deleting Users", page 74.

> **When you delete a user from the repository, all actions linked with this user are lost.**

To delete a user but retain its actions, modify user repository access mode to **Inactive user** (see "Modifying User Properties", page 70). The user no longer appears in the connection dialog box, but its actions are kept.

> *Note that you cannot delete the "Administrator" user, or the "Administrator" writing access.*

Can I delete a writing access area?

Yes, you can delete a writing access area.

> **When you delete a writing access area, the objects that were attached to it pass implicitly to "Administrator" writing access level.**

MEGA recommends that before deletion, you modify the writing access of objects attached to the writing access area.

RECURRENT MESSAGES

Abnormal operation when refreshing a private workspace

Symptom: Message stating "Could not refresh your private workspace".

Reason: Rejects occurred when importing private workspace updates into the reference repository.

Solution:

1. Examine the reject file Rmmjj.MGL (eg: MGLR07150000.MGL) in the user work repository (<repository>\USER\<user code>).
2. Identify and process causes of rejects (see "Rejects When Dispatching", page 193).
3. Delete reject files that are no longer needed.

> ☛ *For as long as reject files are not deleted, a warning persists when connecting to MEGA.*

Environment version

Symptom: Message "Your environment and site are not of the same version" when opening an environment from the MEGA administration console" (or "Your environment and site are not of the same version. Your environment requires updating. Refer to documentation for how to carry out this action").

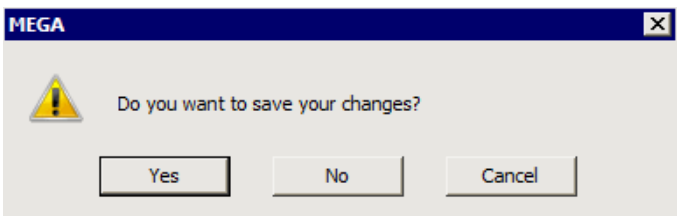
- Click **OK**.
  Another window appears displaying a second message: "Your environment requires an update for compatibility with your version of **MEGA**". Do you wish to run this procedure now? ".

Reason: It is possible that the environment has not been created, or is not at the same version level as the site referencing it: an update is therefore proposed:

- if you have a physical backup of environment data, accept modification by clicking **Yes**.
- If this is not the case, refuse the modification by clicking **No** to exit the MEGA data administration console. Then execute physical backup of data.

"Later" option not proposed at disconnect

Symptom: When you exit **MEGA**, the dialog box that appears does not propose the "Later" option to save your modifications.



Reason:

- You are not connected to **MEGA (Windows Front-End)** and the license used does not have technical module **MEGA Lan**.

  You prevent other users from dispatching their private workspaces.

- You are connected to **MEGA (Web Front-End)**, in a public workspace.

PRODUCT CODES

Access your list of available products

To view the products to which you have access:

1. Start **MEGA Administration**.
2. In the menu bar, select **Help > About MEGA**.
3. Click **System Information**.
4. With the drop-down menu, select **Available components**.
   All the products for which you have a license are listed as well as their associated code.

Products: product code, availability, and storage type

The following table presents for each product or solution:

- its associated code
- its availability:
  - Web Front-End: available only through a Web browser
  - Windows Front-End: available only through Windows Front-End
  - Multi Front-End: available through Windows Front-End and through a Web browser

  *: ANW license is required for its availability through a Web browser
- its storage type required

Product	Code	Availability	Storage
HOPEX Business Architecture	BAM	Web Front-End	RDBMS recommended
HOPEX Collaboration Manager	HTK	multi Front-End	RDBMS
HOPEX Regulatory Compliance	MCM	Web Front-End	RDBMS
HOPEX ERM	ERMW	Web Front-End	RDBMS
HOPEX Explorer	HEXP2	Web Front-End	RDBMS
HOPEX Internal Audit	MIAW	Web Front-End	RDBMS
HOPEX Internal Control	ICM	Web Front-End	RDBMS
HOPEX IT Risk Management	ITGRC	Web Front-End	RDBMS
HOPEX Productivity Pack	HPP	Web Front-End	RDBMS
MEGA SolMan	SAP	multi Front-End*	N/A

Product	Code	Availability	Storage
HOPEX Studio	MTS2	Windows Front-End	RDBMS recommended
MEGA Architecture	ARC	multi Front-End*	N/A
MEGA Assessment	MASSW	Web Front-End	RDBMS
MEGA Business Strategy	MBS	multi Front-End*	N/A
MEGA Database Builder	DBB	Windows Front-End	N/A
MEGA Information Architecture	INFA	Web Front-End	RDBMS
MEGA Internal Audit offline	MIA	multi Front-End*	N/A
MEGA IT Portfolio Management	APM	Web Front-End	RDBMS
MEGA Lan	LAN	N/A	N/A
MEGA Portfolio & Planning	MPP	multi Front-End*	N/A
MEGA Process BPMN Edition	PMN	multi Front-End*	N/A
MEGA Requirement Tracker	MDS	Windows Front-End	N/A
MEGA Service Design	SDE	multi Front-End*	N/A
MEGA Simulation BPMN Edition	PMS	Windows Front-End	N/A
MEGA Suite for NAF	NAF	multi Front-End*	N/A
MEGA for TOGAF	TOG	multi Front-End*	N/A
MEGA Supervisor	SUP	multi Front-End	RDBMS recommended
MEGA System Blueprint	ITD	Windows Front-End	N/A
Read-only Mode	ROM	N/A	N/A
Repository Storage (ORACLE)	RSO	N/A	N/A
Repository Storage (SQL Server)	RSQ	N/A	N/A
Web Front-End Control	ANW	N/A	N/A

GLOSSARY

absolute 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.

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 making backups of 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 **MEGA Administration** desktop (Web Front-End) is the Web version of the **Administration** (Windows Front-End) application accessible via an internet browser.

administrator The administrator is a person who has administration rights to manage sites, environments, repositories and users. In addition to Administrator (who cannot be deleted) and MEGA users, created at installation, you can grant administration rights to other users.

attribute See *Characteristic*.

backup A physical backup (GBMS only) consists of copying the files of a repository from their original location to another.

backup logfile The backup logfile is an additional file stored outside the repository or private workspace. It ensures that the changes made to the repository or private workspace can be recovered even if the repository files become corrupted. Creation of this file is requested in the configuration of each repository (including the system repository). It is created when the first update is made in a private workspace or repository.

business role A business role defines a function of a person in a business sense. A person can have several business roles. Business roles are only considered when the "Management of assignment of business roles to persons" option is activated (default mode) A profile can be associated with a business role. Assigning a person a business role with which a profile is associated indirectly assigns this profile to this person. 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).

comparison You can compare objects in two repositories, creating a file that will modify objects in one repository to make these equivalent to objects in the other repository (with the **MEGA Supervisor** technical module or **HOPEX Collaboration Manager**). This comparison also allows you to list the differences between the contents of the two different objects.

compilation Compilation is carried out after migration or customization. Compilation checks configuration of the environment concerned. When completed, processing for all users of this environment is speeded up. Metamodel compilation includes in parallel translation in the current language. You can also translate the metamodel into another language.

consolidation Consolidation groups the updates from stand-alone workstations or remote sites (with Lan) and merges them in a reference site. After dispatch of the private workspaces of each of the users, the repository log is exported and reinitialized. The logfiles are imported into the reference repository, then this is recopied on each of the user sites.

descriptor 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 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 via menu **File > Discard** or at disconnection.

dispatch Dispatching your work allows the other users to see the changes you have made to the repository. They will see these when they open a new workspace, either by dispatching, refreshing or discarding their work in progress

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

external reference — An external reference enables association of an object with a document from a source outside **MEGA**. This can relate to regulations concerning safety or the environment, legal text, etc. Location of this document can be indicated as a file path or Web page address via its URL (Universal Resource Locator).

functionality — A functionality is a means proposed by the software to execute certain actions (for example: the shapes editor and the descriptor editor are functionalities proposed as standard).

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

group — Descriptors, which are available with the **HOPEX Studio** technical module, comprise a tree of several successive groups. Each group concerns one object, and defines the query or link used to access this object from the preceding object. You can connect texts and other groups to a group. Users can define the order in which groups and texts are processed.

import — 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 **MEGA** 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.

link orientation

The two objects connected by a link do not normally have symmetrical roles. For example, to connect an operation to an organizational process with the **MEGA Supervisor** technical module, you must be authorized to modify the organizational process, since this action will modify its behavior. This action will not however modify the operation. You do not need authorization to modify the operation to create this link. The organizational process is said to be major for this link, the operation is minor. This characteristic is used by administration tools for object export, protection, object comparison and querying isolated objects.

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.

log

Logs 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 log 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.

log export

Export of a log creates a command file from the log 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.

major

The major object in the link is the one whose nature changes with the presence or absence of the link. For example a process, defined as a succession of operations, is modified if you remove an operation. The process is then major for the link. If the objects are protected, you must have the correct authorization for modifying the major object in order to create or delete the link.

matrix A matrix is a table comprising rows and columns containing objects from the repository. Matrices show the relationships between two sets of objects and allow you to create or delete links without having to open the diagrams themselves. For example, you can build a matrix showing the messages sent by the different org-units in a project.

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.

minor The minor object in a link is the one whose nature is not modified or only slightly modified by presence or absence of this link. For example, removing an operation from a process does not change characteristics of this operation. Therefore the process is minor in the link.

model A model is a formal structure which represents the organization of a company, or its information system. In another sense, a model can be a template for reproducing objects with similar characteristics. This is the case for report templates (MS Word) and matrix models.

object An object is an entity with an identity and clearly defined boundaries, of which status and behavior are encapsulated. In a **MEGA** 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 **MEGA 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 electronic mail address.

A person can access **MEGA** once the administrator assigns him/her a login and a business role (or profile).

The list of persons can for example come from an LDAP server.

Person group

A Person Group groups persons in a group. These persons share the same connection characteristics.

perspective

A perspective is associated with each **MEGA Advisor** user when accessing the portal. It corresponds to user centers of interest and enables adaptation of the content of pages displayed. The user can change perspective depending on the information he/she wants to consult.

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 tools, and how he/she sees and can do it. 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 (**MEGA 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.

reflexive link

A reflexive link is a link between two objects of the same type, for example: the link between projects that allows you to define sub-projects.

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.

reorganization

Reorganizing a repository consists of executing a logical backup of the repository, reinitializing it and reimporting the logical backup (without log).

report (MS Word)

Reports (MS Word) managed by **MEGA** 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

See *repository*.

repository

A repository is a storage location where MEGA manages objects, links, and inter-repository links.

The main part is managed by a database system (GBMS, SQL Server, or Oracle). The remainder is in a directory tree (content of Business Document versions, backup logfiles, locks.

The different users in the environment can access the repositories connected to it.

repository log

The repository log stores all the updates of users working in a repository. It is reinitialized at repository reorganization, or by selecting **Repository Log > Manage Repository and Object Log** in the repository pop-up menu. This log is stored in the .EMB file of the repository.

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 **MEGA**. 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.

setting

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 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.

site

A site groups together everything that is shared by all **MEGA** users on the same local network: the programs, standard configuration files, online help files, standard shapes, workstation installation programs, and version upgrade programs. The site is installed on a local network resource or on each workstation if you are working without a network connection.

snapshot

See *repository snapshot*

style

A style is a particular format applied to a paragraph of text in a word processor. Styles allow you to systematically apply formats such as fonts, margins, indents, etc. Several styles are available for report (MS Word) configuration. These styles have the M- prefix and are based on the M-Normal style that is similar to the Word Normal style. Note that the M-Normal style text is in blue. All these styles are contained in the Megastyl.dot style sheet.

SystDb

SystDb is a particular repository containing the metamodel and technical data (descriptors, Web site templates, queries, etc.). The metamodel and technical data are common to all repositories in the same environment. Definition of users and their rights are stored in this repository, essential for operation of the software.

system repository

See *SystDb*.

text

You can associate text with each object found when browsing object descriptors (**HOPEX 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.

trace file

The trace file (Megaerr*.txt) is accessible via menu **?** or from the **MEGA Server Supervisor** tool (available in the **Utilities** folder). It traces all problems and errors encountered on the workstation. Technical support may ask you to check this file.

user

A user is a person (or person group) with a login.

A user is authorized to access certain functions of the product and certain repositories. Each user has a specific desktop in each database, and can connect to this desktop from any workstation in a given environment.

The code associated with the user is used to generate file names as well as a specific work folder for the user.

By default at installation, Administrator persons (Login: System) and Mega (Login: Mega) enable administration of repositories and creation of new users.

work folder

Each user has a work directory in each repository that he/she uses. This directory is located in sub-directory User\XXX of the repository (XXX represents the user code).

workstation

A workstation is defined for each computer connected to the environment. A workstation contains programs and a configuration file that allow you to use **MEGA** on that machine.

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 **MEGA Supervisor** technical module.

writing access diagram

The writing access diagram is available if you have the **MEGA 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.

Technical Articles (EN)

Sommaire

Description of MEGA Data Exchange XML Format

This technical article presents detailed explanation on various tags used in MEGA XML data exchange files.

INTRODUCTION

MEGA allows you to import and export data in a standard XML exchange format.

Data contained in MEGA data XML documents can be described in the form of commands as for MGR, MGL or MGE documents. It can also be described in Content mode. Content mode now allows processing of sets of objects independently, free of any context (see Content exchange: <Content> tag, Content Mode, Hierarchical link in content mode).

Importing an XML document in a MEGA repository means executing or creating the commands it contains in this repository.

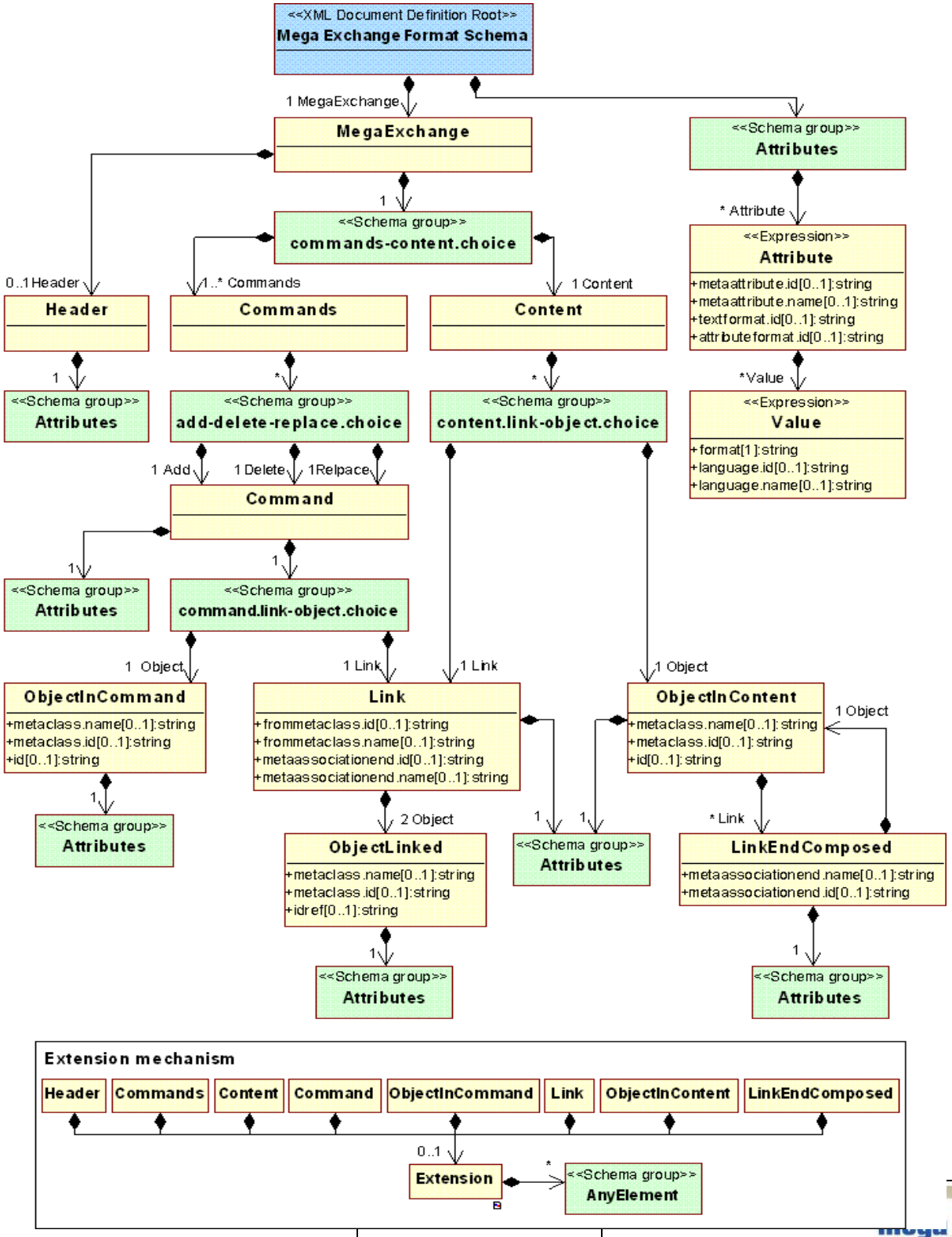
Exporting MEGA (objects, command) consists of dispatching this data in XML standard format. MEGA data exchange XML documents can also be created by software external to MEGA with a view to integrating the data they contain in a MEGA repository. Finally, they can be created manually.

You will find the XSD schema (“xmlmega.xsd”) of MEGA data exchange XML files in the MEGA installation "system" directory.

An XSLT style sheet is also provided in the MEGA installation "system" directory, which presents MEGA data exchange XML documents. This style sheet is provided only as an example.

Note: References to documentation concerning the following are given in the glossary: MEGA metamodel, XML language, importing a data file, exporting a data file.

FORMAT XML SCHEMA MODEL



Description

TAGS IN BRIEF

<MegaExchange>

This is the root element of the document. It contains all other tags.

(See Logical structure)

<Header>

This tag describes the characteristics of the document itself. We find here for example the exchange format version, the document creation date, the default exchange language, etc.

(See Logical structure)

<Attribute>

An <Attribute> tag enables expression of a command characteristic in an Add>, <Delete> or <Replace> tag, of an object in an <Object> tag, of a link in a <Link> tag, or of the exchange document itself in the <Header> tag.

(See Description of attribute values)

<Value>

This tag contains an attribute value. It appears only in <Attribute> tags. It serves to express a value in a particular format when this value can be expressed in several possible formats in an <Attribute> tag (for example, "internal" or "display" format).

(See Attribute value format)

<Commands>

This tag appears at root element level and enables expression of a set of commands.

(See Command exchange: <Commands> tag)

<Content>

This tag appears at root element level and enables inventory of a set of objects and links.

(See Content exchange: <Content> tag)

<Object>

An <Object> tag contains the description of an object: it is characterized by its type (MetaClass) and its attribute values. It can serve to describe or identify an object, for example an object to be connected at creation of a link.

(See Object Descriptions)

<Link>

A <Link> tag contains the description of a link: its type (MetaClass of the object to be connected and MetaAssociationEnd by which the second object is connected), identifications of the two objects to be connected and the link attribute values.

(See Link description)

<Add>

The <Add> tag is used in the <Commands> tag. It enables representation of an object or link creation command. Content is either an <Object> tag describing the object to be created, or a <Link> tag describing the link to be created.

(See Command exchange: <Commands> tag, Command Mode)

<Delete>

The <Delete> tag is used in the <Commands> tag. It enables representation of an object or link deletion command. Content is either an <Object> tag describing the object to be deleted, or a <Link> tag describing the link to be deleted.

(See Command exchange: <Commands> tag, Command Mode)

<Replace>

The <Replace> tag is used in the <Commands> tag. It enables representation of an object or link update command. Content is either an <Object> tag describing the object to be modified, or a <Link> tag describing the link to be modified.

(See Command exchange: <Commands> tag, Command Mode)

<Extension>

Various tags can contain the <Extension> tag.. When it is present in an element, this tag enables addition of supplementary information to the element (for example, addition of information concerning reasons for command reject). This information can be taken into account in a particular way according to tools used.

FORMAT IN DETAIL

In the remainder of this document, MEGA data exchange XML format will be referred to as "MEGA XML".

MEGA data exchange XML document structure

Physical structure

Like all XML documents, MEGA XML documents must start with XML declaration:

<?xml version="1.0"?>.

Encoding can be specified using the "encoding" attribute.

<?xml version="1.0" encoding="ISO-8859-1"?>

MEGA XML documents should be expressed in a code supported by the applications used to process them. For example, before importing a MEGA XML document it should be confirmed that MEGA can handle documents in the encoding proposed. MEGA import, like any XML analyzer, can basically handle input of Unicode encodings: UTF-8, UTF-16 little endian and big endian and ASCII. Other encodings such as ISO Latin1 FR can be used.

Note: see XML specifications for values to be specified for the "encoding" attribute (ref. Extensible Markup Language (XML) 1.0: http://www.w3.org/TR/2004/REC-xml-20040204/), and MEGA documentation to determine supported encodings.

Note: values that can be specified for the "encoding" attribute to identify the different encodings:

- "ISO-8859-1" corresponds to ISO Latin-1 FR encoding
- "UTF-8" corresponds to Unicode encoding on one or several bytes per character
- "UTF-16" corresponds to Unicode encoding on a multiple of two bytes per character

Logical structure

Like all XML documents, MEGA XML documents can have only one root tag, its name being *<MegaExchange>*.

A MEGA XML document firstly contains information relating to the document itself, such as the document creation date, the format version used or the attribute value expression language. This information is described in a *<Header>* tag.

In addition, information exchanged must be expressed either in a *<Commands>* tag, or in a *<Content>* tag

Example 1 : MEGA data exchange XML document structure

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="format_version">Mega Xml Format Version
0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged data -->
    <Add>
      <Object metaclass.name="Procedure" id="1">
        <Attribute metaattribute.name="Name">Procedure-1</Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

Exchanged data description modes

Data exchanged via MEGA XML documents can be described in two modes:

- Either as a series of commands to be processed one after the other.
- Or as a repository content or sub-content, in other words as a set of objects.

Command exchange: <Commands> tag

Command series data expression mode is by use of the *<Commands>* tag.

It is this tag that contains command description tags in XML. The order of command description tags within the *<Commands>* tag is significant. It corresponds to the order in which commands must be processed by the

MEGA XML document analysis tools. In fact, a command may not be validated unless preceding commands have been processed.

For example, if a command for creation of a link between two objects appears before the command for creation of one (or both) of the objects themselves, the link creation command is not valid from a logical viewpoint.

Example 2 : Command exchange

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Procedure" id="1">
        <Attribute metaattribute.name="Name">Procedure-1</Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

Content exchange: <Content> tag

Content description mode uses the *<Content>* tag. This tag contains a collection of objects and links.

These objects and links should be interpreted as independent data free of any context: they are not connected to a particular repository and do not require any other data in order to be significant (except for the metamodel describing them).

Data of an XML exchange document using description mode produces creation commands (creation of described objects and links) when the document is imported.

Order of appearance of tags describing data contained in the *<Content>* tag is significant. It corresponds to the order in which data must be processed by the MEGA XML document analysis tools.

If a link between two objects appears before one (or both) of the objects themselves, the link description is not valid from a logical viewpoint.

Example 3 : Content description mode data exchange

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.name="Procedure" id="1">
      <Attribute metaattribute.name="Name">Procedure-1</Attribute>
    </Object>
  </Content>
</MegaExchange>
```

In content description mode, we can explicitly show the hierarchical view of exchanged data structure. In fact, tags describing objects can themselves contain other tags describing contained objects from a logical viewpoint (for example a procedure containing operations).

This hierarchical description is valid only in content description mode.

Example 4 : <Object> tag containing an <Object> tag

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.name="Procedure" id="1">
      <Attribute metaattribute.name="Name">Procedure-1</Attribute>
      <!-- hierarchical link use  -->
      <Link metaassociationend.name="Contained operation">
        <!-- contained object -->
        <Object metaclass.name="Operation" id="2">
```

```
            <Attribute metaattribute.name="Name">Procedure-1</Attribute>
          </Object>
        </Link>
      </Object>
    </Content>
  </MegaExchange>
```

Commands description: <Add>, <Delete>, <Replace> tags

Command tags can be used only in command mode. These tags are contained in the *<Commands>* tag explained in the chapter Command exchange: <Commands> tag.

The three available commands are:

- Creation command represented by an *<Add> tag.*
- Deletion command represented by a *<Delete> tag.*
- Modification command represented by a *<Replace> tag.*

Each of these three commands can be applied to an object or to a link: a tag representing a command can contain one tag only: *<Object>* or *<Link>*.

In command mode, *<Object>* tags cannot directly or indirectly contain other *<Object> tags.* : The hierarchical aspect of exchanged data logical structure cannot be represented by the hierarchical aspect of XML when data is exchanged in command mode.

Example 5 : Object and link creation commands

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Class">
        <Attribute metaattribute.name="UML ClassName (Français)">Ma classe</Attribute>
      </Object>
```

```
    </Add>
    <Add>
      <Link frommetaclass.name="Package" metaassociationend.name="Contained class ">
        <Object metaclass.name="Package">
          <Attribute metaattribute.name="Name">My package</Attribute>
        </Object>
        <Object metaclass.name="Class">
          <Attribute metaattribute.name="Name">My org-unit</Attribute>
        </Object>
        <Attribute metaattribute.name="Order">9999</Attribute>
      </Link>
    </Add>
  </Commands>
</MegaExchange>
```

Object Descriptions

Objects are described by the *<Object> tag*..

The MetaClass of the object is identified by the name or MEGA absolute identifier (idabs in hexadecimal) of the MetaClass. The name of the MetaClass is specified by the value of the *"metaclass.name"* attribute of the *<Object> tag*, the idabs of the MetaClass is specified by the value of the *"metaclass.id"* attribute of the *<Object> tag*.

In addition, the objects themselves must be identified when we wish to make reference to them in the exchange document (see Object identification mechanisms).

Example 6 : Object metaclass identification by metaclass name

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.name="Procedure">
        <Attribute metaattribute.name="Name">Procedure-1</Attribute>
    </Object>
  </Content>
```

```
</MegaExchange>
```

Example 7 : Object metaclass identification by metaclass idabs

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.id="B1EDB25E2C1401BB">
      <Attribute metaattribute.name="Name">Procedure-1</Attribute>
    </Object>
  </Content>
</MegaExchange>
```

Command Mode

In commands description mode, an object is described in an *<Add>*, *<Delete>* or *<Replace>* tag, depending on whether we wish to create, delete or modify the object.

In this case, the *<Object>* tag describing the object can if necessary contain an *<Extension>* tag containing information not allowed for by MEGA XML format. It also contains *<Attribute>* tags specifying attribute values characterizing this object, these tags following the *<Extension>* tag if this is present.

Example 8 : Object creation command by attribute specification

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Procedure" id="1">
        <Attribute metaattribute.name="Name">Procedure-1</Attribute>
```

```
        <Attribute metaattribute.name="Type-Procedure">General</Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

An object described in a deletion command must make reference to an existing object recognized by the tool analyzing the MEGA XML document. The object description must therefore specify the value of its MEGA absolute identifier (object "_idabs" attribute) in an *<Attribute> tag*.

Example 9 : Object deletion command

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Delete>
      <Object metaclass.name="Procedure">
        <!-- object identifier attribute -->
        <Attribute metaattribute.name="_IdAbs">MnJgyaAJ0100</Attribute>
      </Object>
    </Delete>
  </Commands>
</MegaExchange>
```

An object described in a modification command must make reference to an existing object recognized by the tool analyzing the MEGA XML document. The object description must therefore specify the value of its MEGA absolute identifier (object "_idabs" attribute) in an *<Attribute> tag*. In addition to the *<Attribute>* tag specifying the MEGA absolute identifier value, we find *<Attribute>* tags giving the values of attributes to be changed for the object concerned.

Example 10 : Object modification command

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Replace>
      <Object metaclass.name="Procedure">
        <!-- object identifier attribute -->
        <Attribute metaattribute.name="_IdAbs">MnJgyaAJ0100</Attribute>
        <!-- modified attribute -->
        <Attribute metaattribute.name="Code-Procedure">XYZ</Attribute>
      </Object>
    </Delete>
  </Commands>
</MegaExchange>
```

Content Mode

In content description mode, *<Object>* tags describing objects are contained in the *<Content> tag*.

The *<Object>* tag describing the object can if necessary contain an *<Extension>* tag containing information not allowed for by MEGA XML format. It also contains *<Attribute>* tags specifying attribute values characterizing this object. These tags follow the *<Extension>* tag if this is present.

In addition, in content description mode, objects can be described as containing other objects. The *<Object>* tag can therefore indirectly contain other *<Object>* tags describing contained objects (see Hierarchical link in content mode).

The same considerations apply to *<Object>* tags representing contained objects, which can themselves contain *<Object> tags*.

Example 11 : Object description in content mode

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
```

```
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.name="Procedure" id="1">
      <Attribute metaattribute.name="Name">Procedure-1</Attribute>
    </Object>
  </Content>
</MegaExchange>
```

Object identification mechanisms

We need to make reference to objects internal or external to the document within the framework of:

- An object modification command
- An object modification command
- The link between one object and another

We distinguish objects described in the document from those not described in the document but which are the object of a command:

- Objects internal to the document: these are described in the document and can be referenced in the document via use of *"id"* and *"idref"* attributes of the *<Object> tag*.
- Objects external to the document: these are not described in the document but can be the target of a command. These should be recognized by the tool processing the document and are identified by the "_idabs" attribute of the object.

Object identification therefore uses either an identifier internal to the document or a MEGA absolute identifier.

Identification internal to the document is by use of the *"id"* attribute of the *<Object>* tag. The value of the *"id"* attribute must be unique throughout the document with no other constraint on form; it is an ID type attribute (ID type is defined in XML1.0 specifications). Reference to a document object is by using the *"idref"* attribute of the *<Object>* tag, which must therefore have the same value as the *"id"* attribute of the *<Object>* tag representing the referenced object. For example, within the framework of a link, the *<Object>* tags referencing linked objects can each have an *"idref"* attribute.

External identification is by definition of an *<Attribute>* tag defining the value of its MEGA absolute identifier (object "_idabs" attribute). Objects can be created with an "_idabs" attribute by use of the *<Attribute>* tag (see Description of attribute values). Similarly, *<Object>* tags referencing objects, as in the *<Delete>*, *<Replace>* or *<Link>* tags, can identify objects by their MEGA absolute identifier, and in this case they contain an *<Attribute>* tag specifying the value of the object "_idabs" attribute.

Example 12 : Identification by <Object> tag id attribute

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.name="Procedure" id="1">
      <Attribute metaattribute.name="Name">Procedure-1</Attribute>
    </Object>
    <Object metaclass.name="Procedure" id="2">
      <Attribute metaattribute.name="Name">Procedure-2</Attribute>
    </Object>
    <Link frommetaclass.name="Procedure" metassociationend.name="Next procedure">
      <Object metaclass.name="Procedure" idref="1"/>
      <Object metaclass.name="Procedure" idref="2"/>
    </Link>
  </Content>
</MegaExchange>
```

Example 13 : Identification by idabs

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
```

```
      <Object metaclass.name="Procedure">
        <Attribute metaattribute.name="Name">Procedure-1</Attribute>
        <!-- object identifier attribute -->
        <Attribute metaattribute.name="_IdAbs">MnJgyaAJ0100</Attribute>
      </Object>
    </Add>
    <Delete>
      <Object metaclass.name="Procedure">
        <!-- object identifier attribute -->
        <Attribute metaattribute.name="_IdAbs">MnJgyaAJ0100</Attribute>
      </Object>
    </Delete>
  </Commands>
</MegaExchange>
```

Link description

Links are described by the *<Link> tag.*.

The MetaAssociation of the link is identified by the name or MEGA absolute identifier (idabs in hexadecimal form) of the MetaAssociationEnd by which the objects are connected.

The name of the MetaAssociationEnd is specified by the value of the *"metaassociationend.name"* attribute of the *<Link>* tag.

The idabs of the MetaAssociationEnd is specified by the value of the *"metaassociationend.id"* attribute of the *<Link>* tag.

One of the attributes *"metaassociationend.name"* or *"metaassociationend.id"* must be present to identify the link. Both can be present simultaneously.

Hierarchical link in content mode

In content mode, a link can be represented hierarchically. The *<Object>* tag representing the first object therefore contains a *<Link>* tag which itself contains the *<Object>* tag describing the connected object.

The *<Link>* tag serves to specify the MetaAssociationEnd by which the second object is connected. To do this, we must therefore specify the *"metaassociationend.name"* attribute or the *"metaassociationend.id"* attribute.

In addition, the *<Link>* tag can contain *<Attribute>* tags describing link attribute values. These *<Attribute>* tags are placed before the *<Object>* tag.

Example 14 : Hierarchical ink description in content mode

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.name="Procedure" id="1">
      <Attribute metaattribute.name="Name">Procedure-1</Attribute>
      <!-- hierarchical link use  -->
      <Link metaassociationend.name="Contained operation">
        <!-- link attributes -->
        <Attribute metaattribute.name="Order">1</Attribute>
        <!-- contained object -->
        <Object metaclass.name="Operation" id="2">
          <Attribute metaattribute.name="Name">Procedure-1</Attribute>
        </Object>
      </Link>
    </Object>
  </Content>
</MegaExchange>
```

Other links

Links that are not hierarchical links can be used in both command mode command tags (<*Add*>, <*Delete*>, <*Replace*>) and in the content mode <*Content*> tag. These links make reference to two connected objects describing but not referencing these objects. The connected objects can be external to the document.

A link between two objects is described by the MetaAssociationEnd by which the second object is connected to the first. To do this, the <*Link*> tag representing the link contains either the MetaAssociationEnd idabs value in hexadecimal form in the *"metaassociationend.id"* attribute, or the MetaAssociationEnd name value in the *"metaassociationend.name"* attribute. In the latter case, the MetaClass of origin of the MetaAssociationEnd must be specified, ie. the MetaClass of the first object. This is done via the *"frommetaclass.id"* or *"frommetaclass.name"* attributes of the <*Link*> tag, specifying either the MetaClass idabs in hexadecimal form or the MetaClass name.

In addition, the *<Link>* tag contains two *<Object>* tags that reference the two connected objects. Each of these has a *"metaclass.id"* attribute specifying either the MetaClass idabs in hexadecimal form, or a *"metaclass.name"* attribute specifying its name. The object is referenced either by specifying the *"idref"* attribute value of the *<Object>* tag in the *<Link>* tag, which should be equal to the *"id"* attribute value of the *<Object>* tag describing the object referenced in the document, or by adding an *<Attribute>* tag specifying the "_idabs" attribute value of the referenced object, which in this case can be an object not described in the document.

Finally, the *<Link>* tag can contain *<Attribute>* tags describing link attribute values. These *<Attribute>* tags are placed after the two *<Object>* tags.

Example 15 : Description of a link between two objects of the document: use of "idref" attribute

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Content>
    <!-- exchanged data -->
    <Object metaclass.name="Package" id="1">
      <Attribute metaattribute.name="Name">Package-1</Attribute>
    </Object>
    <Object metaclass.name="Package" id="2">
      <Attribute metaattribute.name="Name">Package-2</Attribute>
    </Object>
    <Link frommetaclass.name="Package" metaassociationend.name="Referenced package">
      <!-- link source object -->
      <Object metaclass.name="Package" idref="1"/>
      <!-- link destination object -->
      <Object metaclass.name="Package" idref="2"/>
      <!-- link attributes -->
      <Attribute metaattribute.name="Order">9999</Attribute>
    </Link>
  </Content>
</MegaExchange>
```

Example 16 : Description of a link between two objects by idabs

```
<?xml version="1.0" encoding="ISO-8859-1"?>
```

```
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Link frommetaclass.name="Package" metaassociationend.name="Referenced package">
        <!-- link source object -->
        <Object metaclass.name="Package">
          <Attribute metaattribute.name="_idabs">ODiTpSNApa10</Attribute>
        </Object>
        <!-- link destination object -->
        <Object metaclass.name="Package">
          <Attribute metaattribute.name="_idabs">dCyP0ZtmxSA8</Attribute>
        </Object>
        <!-- link attributes -->
        <Attribute metaattribute.name="Order">9999</Attribute>
      </Link>
    </Add>
  </Commands>
</MegaExchange>
```

Description of attribute values

Attribute values are specified in *<Attribute>* tags. The following tags can contain attribute values: *<Header>*, *<Link>*, *<Object>*, *<Add>*, *<Delete>*, *<Replace>*.

In an *<Attribute>* tag, the valuated characteristic is identified by the *"metaattribute.name"* attribute, which determines its name, or by the *"metaattribute.id"* attribute, which determines its idabs in hexadecimal form.

The value is directly contained in the *<Attribute>* tag..

Example 17 : Description of an attribute value

```
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
```

```
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Package">
        <!-- object attributes -->
        <Attribute metaattribute.name="_idabs">ODiTpSNApa10</Attribute>
        <Attribute metaattribute.name="nom">Packagee-1</Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

Attribute value format

Direct values in *<Attribute>* tags are expressed in the format specified by the *<Attribute>* tag representing the *"default_format"* attribute of the *<Header>* tag.

If this attribute is not specified, default format is left to the tool analyzing the document.

Example 18 : Attribute value default format

```
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
    <Attribute metaattribute.name="default_format">internal</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Package">
        <!-- object attributes -->
        <Attribute metaattribute.name="_idabs">ODiTpSNApa10</Attribute>
        <Attribute metaattribute.name="nom">Packagee-1</Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

The *<Attribute>* tag enables attribute value specification in several formats. The different forms that the attribute value can take are each contained in a *<Value>* tag, the format being specified by the *<Value>* tag *"format"* attribute.

Example 19 : Attribute value expressed in several formats

```
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="xmg_version">XMG version 0.1</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Application">
        <!-- object attributes -->
        <Attribute metaattribute.name="_idabs">ODiTpSNApa10</Attribute>
        <Attribute metaattribute.name="name">Application-1</Attribute>
        <Attribute metaattribute.name="MMI">
          <Value format="internal">W</Value>
          <Value format="display">Windowed</Value>
        </Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

Translatable attributes and attribute value expression language

In the MEGA repository, for a given translatable attribute, there are as many attributes as there are languages into which the attribute is translatable. For example, for the "Name" attribute there are corresponding "Name (English)","Name (French)", "Name (Dutch)", etc. attributes.

In a MEGA XML document, the *"language.id"* and "language.name" attributes of the *<Value>* tag enable specification of the language in which the attribute value is expressed.

Translatable attributes are therefore identified by the name or absolute identifier of the root attribute using the *"metaattribute.name"* and *"metaattribute.id"* attributes of the *<Attribute>* tag, and the language in which the value is expressed using the *"language.name"* and *"language.id"* attributes.

For value expression language to be specified, at least one of the two attributes *"language.name"* or *"language.id"* must be present in the *<Value>* tag.

When neither the *"language.name"* nor the *"language.id"* attribute is present, the value is expressed in the language specified by the *<Attribute>* tag representing the *"model_default_language"* attribute of the *<Header>* tag.

Example 20 : Attribute value expressed in default language

```
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="model_default_language"> Français</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Application">
        <!-- object attributes -->
        <Attribute metaattribute.name="_idabs">ODiTpSNApa10</Attribute>
        <Attribute metaattribute.name="name">Application-1</Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

Example 21 : Attribute value expressed in several languages

```
<MegaExchange>
  <Header>
    <!-- document information -->
    <Attribute metaattribute.name="model_default_language"> Français</Attribute>
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Application">
        <!-- object attributes -->
        <Attribute metaattribute.name="_idabs">ODiTpSNApa10</Attribute>
        <Attribute metaattribute.name="name">
          <Value>Invoicing</Value>
          <Value language.name="English">Invoicing</Value>
        </Attribute>
```

```
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

MEGA XML format extensions

MEGA XML format includes an extension mechanism enabling addition of information to different format tags.

A format extension is created by use of the *<Extension>* tag. The extension tag can contain any information expressed in XML.

Information contained in the *<Extension>* tag is not part of the format. It cannot be taken into account by a tool using MEGA XML format.

The following tags can contain an extension tag: *<Header>*, *<Link>*, *<Object>*, *<Add>*, *<Delete>*, *<Replace>*.

Example of use of the *<Extension>* tag by MEGA

The *<Extension>* tag is used by the MEGA import function which creates a report of commands analyzed at import. The report contains commands analyzed in MEGA XML format indicating if they have been accepted, rejected or contain warnings. Therefore each MEGA XML format command in the report can contain an *<Error>* tag or *<Warning>* tags in the *<Extension>* tag of the command concerned. These tags enable appreciation of the import result, but are not to be taken into account in another context.

Example 22 : Use of the *<Extension>* tag by MEGA

```
<MegaExchange>
  <Header>
    <!-- document information -->
  </Header>
  <Commands>
    <!-- exchanged commands -->
    <Add>
      <Object metaclass.name="Application">
        <Extension>
          <Error code="XXXXXXXX">There is no « metaattribute » with « color » value as
« name »<Error>
        </Extension>
        <!-- object attributes -->
        <Attribute metaattribute.name="_idabs">ODiTpSNApa10</Attribute>
        <Attribute metaattribute.name="name">Invoicing</Attribute>
```

```
        <Attribute metaattribute.name="color">blue</Attribute>
      </Object>
    </Add>
  </Commands>
</MegaExchange>
```

Attributes of MEGA XML documents used by MEGA

A MEGA XML document exported from a MEGA repository contains a certain number of attributes that describe general elements relating to the document itself. These are described in this section.

Document attributes are located in the *<Header>* tag of the document.

Example 23 : Document attributes

```
<?xml version="1.0" encoding="UTF-8"?>
<MegaExchange>
  <Header>
    <Attribute metaattribute.id="27C729AE3F4E004A"
metaattribute.name="exchange_format_version">
      <Value format="internal">000100</Value>
      <Value format="display">MEGA XML version 0.1</Value>
    </Attribute>
    <Attribute metaattribute.id="27C729AE3F4E0050" metaattribute.name="mega_version">
      <Value format="internal">25856</Value>
      <Value format="display">MEGA Version 2005 Pre release</Value>
    </Attribute>
    <!-- ... -->
  </Header>
  <Commands>
    <!-- ... -->
  </Commands>
</MegaExchange>
```

Document attributes list

- exchange_format_version : this attribute indicates the version of MEGA XML exchange format.
- mega_version : this attribute indicates the version of MEGA used at export.
- metamodel_language : this attribute specifies the language used to identify types in the attributes of *"metaclass.name"*, *"metaattribute.name"*, *"metaassociationend.name"* tags.

- model_default_language : this attribute specifies the default language used for translatable attribute values of objects and links when the language has not been specified by *"language.name"* or *"language.id"* attributes of the <*Value*> tag.

- author : the value of the *author* attribute identifies the user that executed export.

- source_database : the value of the *source_database* attribute identifies the repository from which export was executed.

- creation_date : specifies MEGA XML document creation date.

GLOSSARY

XML attribute:

An XML attribute is unstructured text data contained in an XML tag.

Example: <attribute tag="value"/>

MEGA object attribute:

Object characteristics are called attributes. For a given object, attributes can take a value of which the type is defined for the attribute.

XML tag:

XML tags are syntax elements that structure XML documents. They mark opening and closing of XML document data definition.

Example: <tag>…</tag>

MEGA command:

The various actions possible that modify a MEGA repository are called commands. In particular these include creation, deletion and modification of objects and links.

XML element :

An XML element is structured data comprising an opening tag, attributes of this tag, a closing tag and text data and tags contained between opening and closing tags.

Example: <attribute tag="value">text<sub-tag/></tag>

File export

MEGA repository data can be exported in a file. From a MEGA repository we can export : objects (exported data describing exported objects), transactions (exported data describing transaction commands) or the complete repository (exported data describing all repository objects, this procedure also being known as logical backup). The various export functions are described in the "MEGA Help" CHM file and in the "MEGA Administration" PDF user guide in the following sections: "Administration > Managing Transactions > Managing Updates > Exporting the Transaction Logfile", "Administration > Managing Objects > Exporting MEGA objects", "Administration > Managing Repositories > Reorganizing a Repository > Logical Backup of a Repository".

MEGA APIs enable file export using Automation interfaces. Data export and logical backup functions using API are covered in the "MEGA Help" CHM file in the section "API > API - Reference Guide > Administration > MEGA Database" and in the "MEGA API" PDF user guide in the similarly named section.

IdAbs

Absolute identifier of data stored in the MEGA repository, idabs is generally represented in hexadecimal or base 64 form. The idabs is for example an object attribute (attribute "_idabs").

File import

Importing an XML document in a MEGA repository means executing or creating the commands it contains in this repository. MEGA can import files of type MGR, MGL, MGE and MEGA XML. The import function is covered in the "MEGA Help" CHM file in the section "Administration > Managing Repositories > Reorganizing a Repository > Updating a Repository (Importing)" and in the "MEGA Administration" PDF user guide in the similarly named section.

MEGA APIs enable file import using Automation interfaces. The API import function is covered in the "MEGA Help" CHM file in the section "API > API - Reference Guide > Administration > MEGA Database" and in the "MEGA API" PDF user guide in the similarly named section.

MEGA links :

For a given repository object, links enable definition of connected repository objects.

MEGA MetaAssociation :

This term indicates relationships existing between repository object types. MetaAssociations define repository links.

MEGA MetaClass :

This term indicates object types stored in the repository. MetaClasses define repository objects.

MEGA metamodel :

This comprises all MetaClasses and MetaAssociations defining objects that can be created and handled in the MEGA repository. The MEGA metamodel is covered in the "MEGA Help" CHM file in section "Metamodel and Glossaries > Metamodel".

MEGA object

Data stored in a MEGA repository are called repository objects. An object comprises attributes and can be connected to other repository objects. In addition, every object is identified uniquely by an attribute called the MEGA absolute identifier or idabs.

MEGA XML

Common name for MEGA data exchange XML format.

XML

Extendable tag language (eXtensible Markup Language), XML is a metalanguage describing languages of tagged hierarchical structure. XML specifications provide syntax basics of XML languages (ref. Extensible Markup Language (XML) 1.0: http://www.w3.org/TR/2004/REC-xml-20040204/).

HOPEX – Securing the platform

The goal of this document is to give detailed instructions as to how to secure the Hopex platform.

Activating SSL on the website

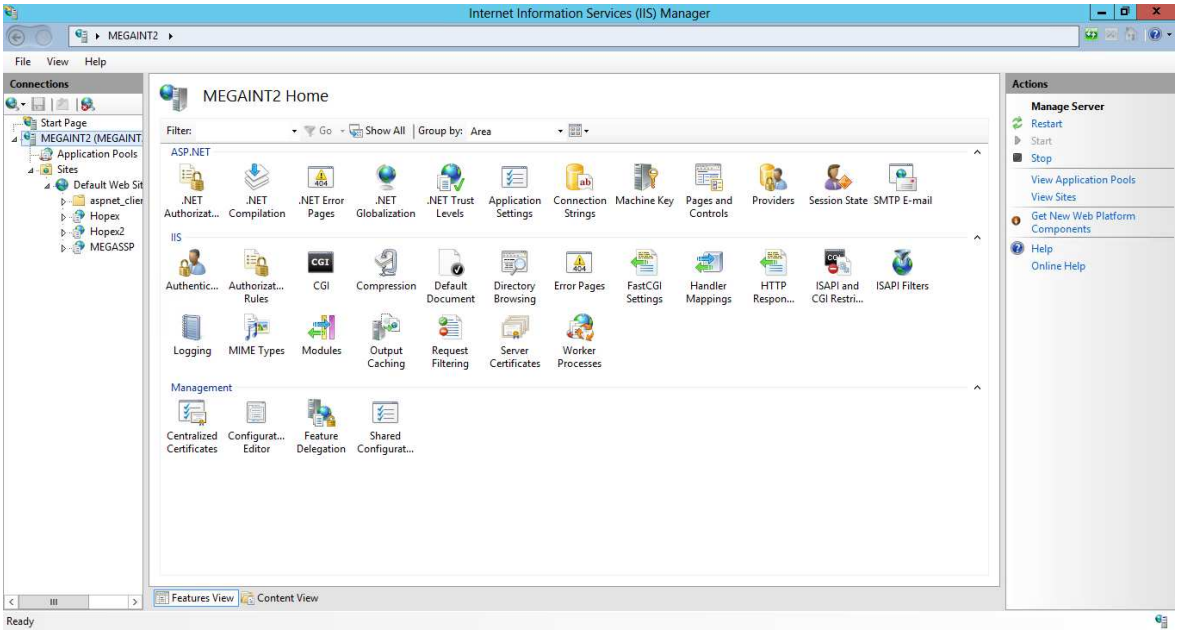
In order to encrypt the information sent between the users' workstation and the web server, the first step is to activate the SSL on the Hopex website.

The minimum level of certificate that is recommended is a certificate signed by a trusted third party. If internally, a root certificate exists and allows the applications to generate their own certificate, it is also a possibility.

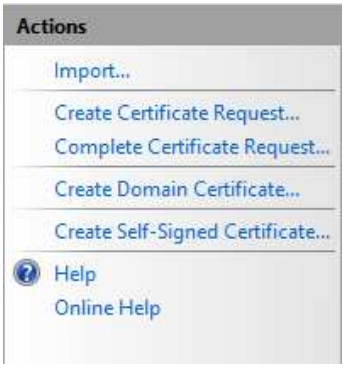
When you obtained that certificate, the steps to import it on your website are multiple. You will find hereafter one way to do it, and make sure that your website will be attainable only through HTTPS.

The following step-by-step procedure was done on a Windows Server 2012, with IIS 8.0. You need to adapt it based on your OS version.

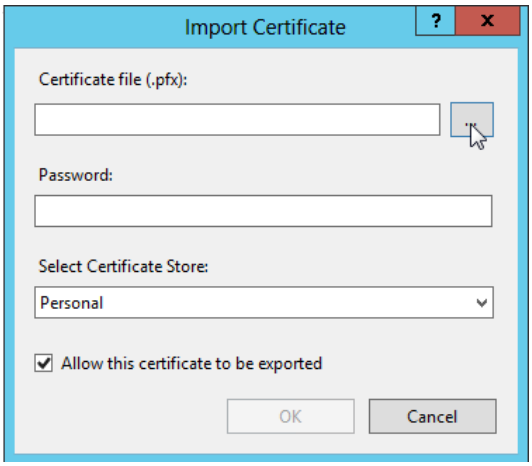
1. The first step is to copy the certificate on your server.
2. Next, open the "Internet Information Services (IIS) Manager" through the Administrative Tools of the server.
3. Go to the root of IIS :



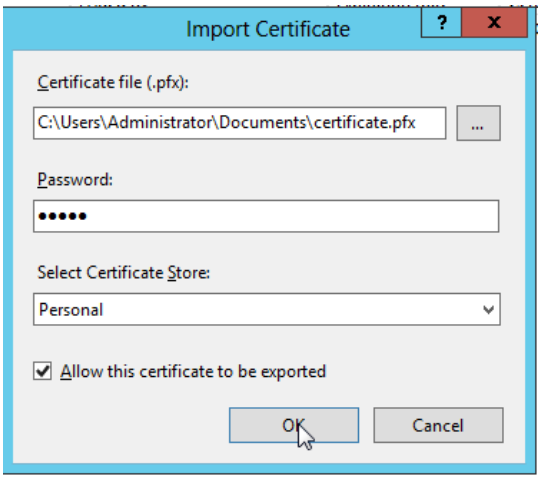
4. Double-click on « Server Certificates ».
5. Once this feature is opened, on the right pane, click on the « Import » link :



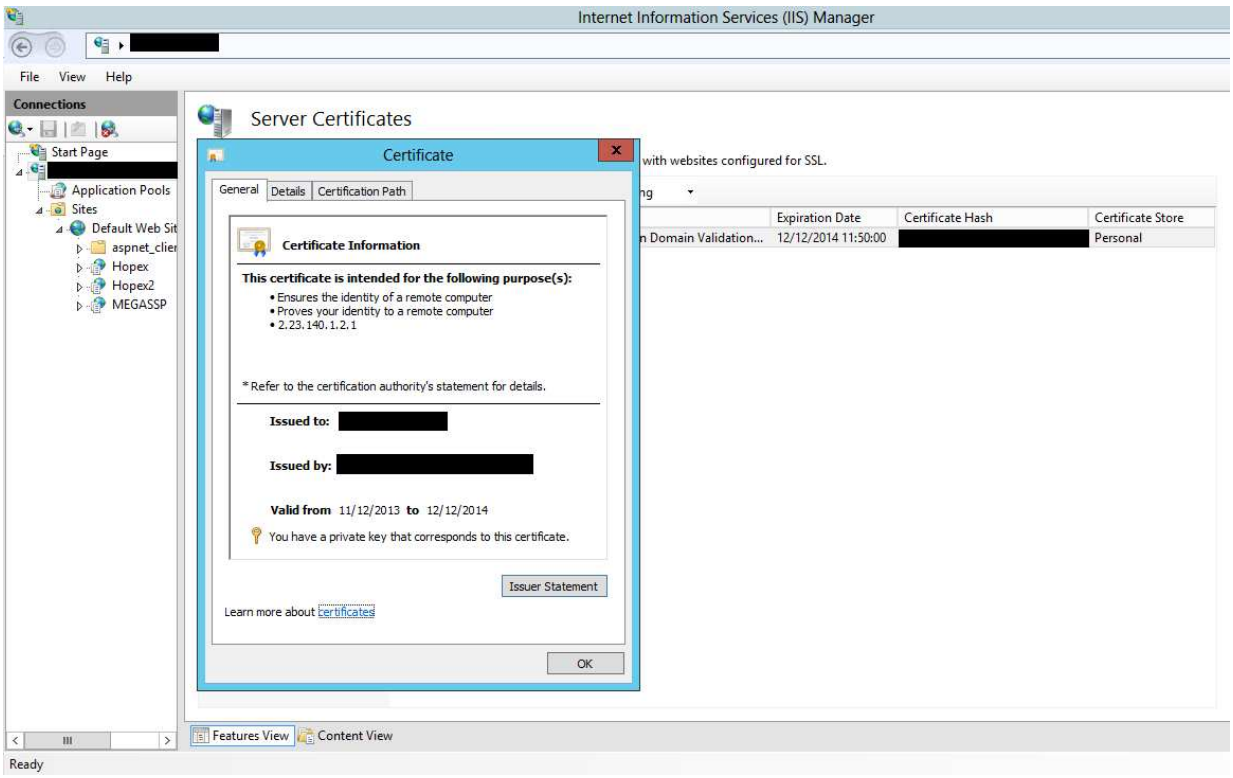
6. Click the button where the cursor is located, in order to look for the certificate :



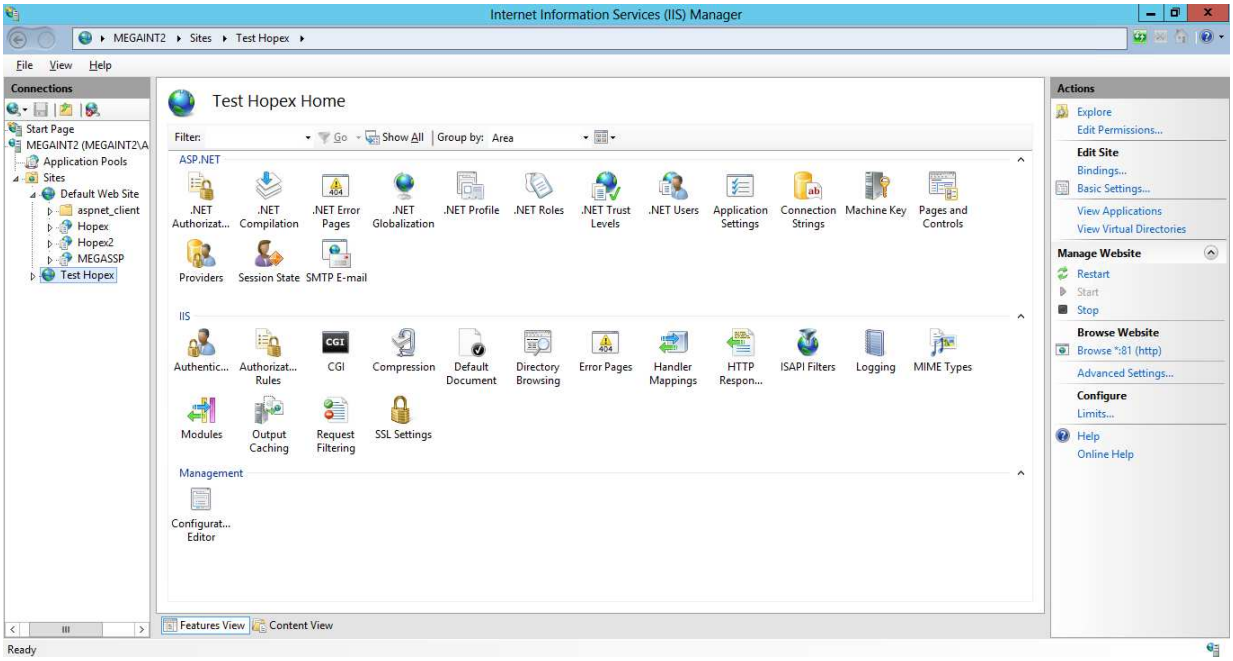
7. Select the certificate. Provide a password if necessary, and click « OK » to import the certificate :



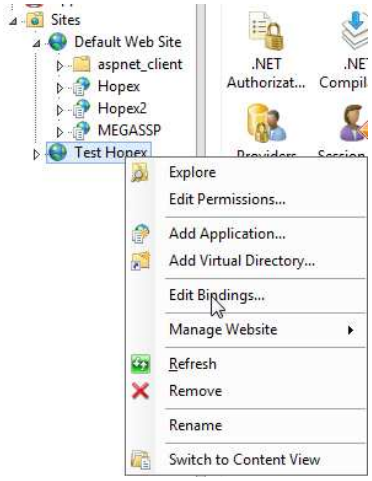
A new line will appear in the “Server Certificates” window. You can have a look at the imported certificate by double-clicking on the certificate :



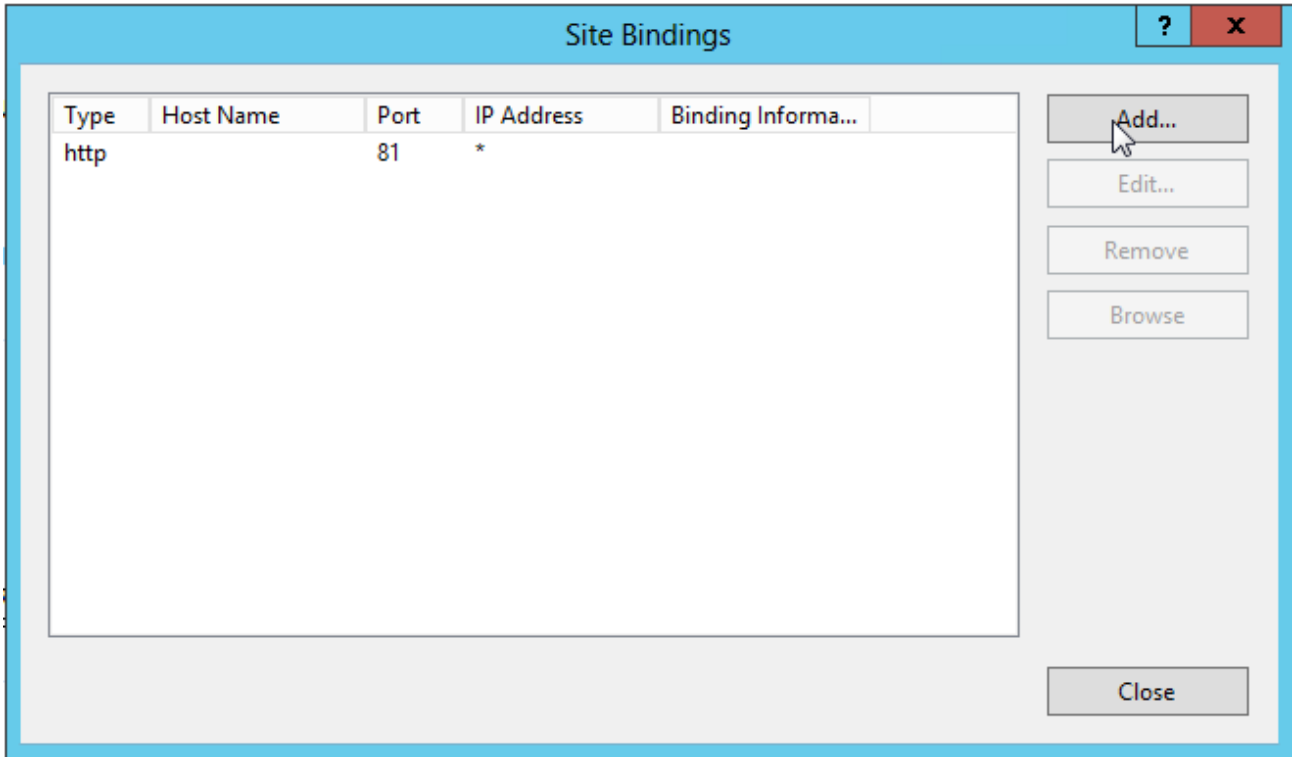
8. Locate the website where you want to create an HTTPS binding with the newly imported certificate. In this example, it is done on the "Test Hopex" website. Click the website to see its features.



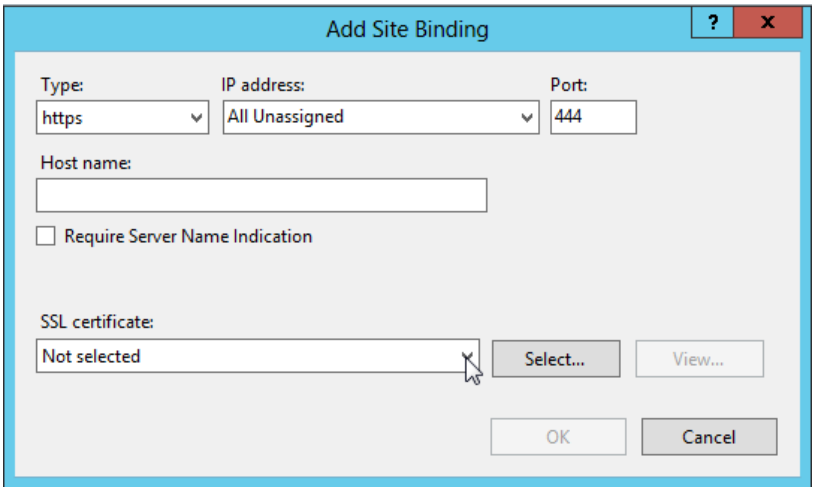
9. Right-click the website and select **Edit Bindings**.



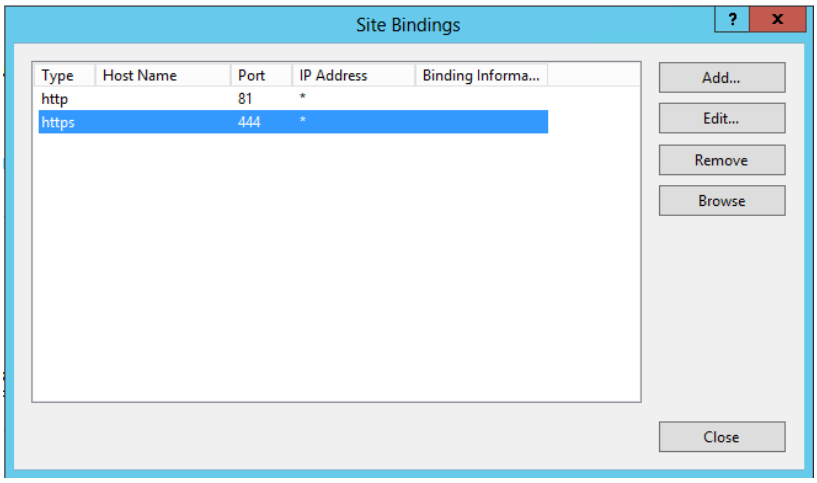
10. Add a new binding, for HTTPS, on a specific port (in this example, as the port 443 is already used, we will choose 444). Use the default port 443 whenever possible, as it permits you quite easily to make the URL of the website user-friendly :



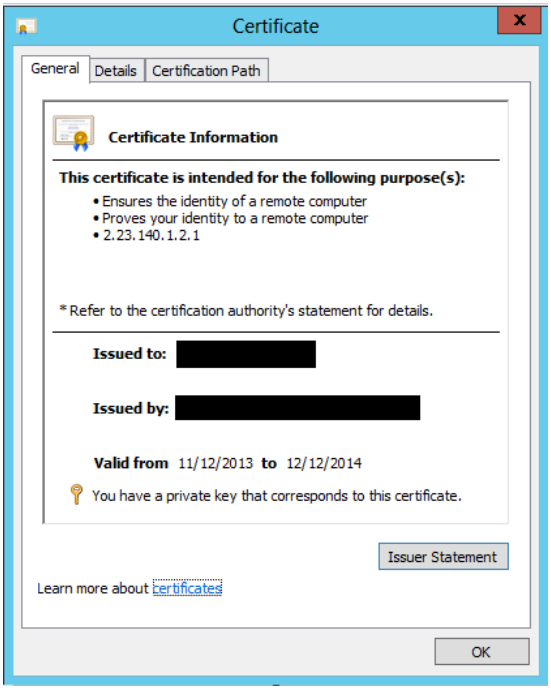
11. Use the dropdown list to select your certificate and click **OK**.



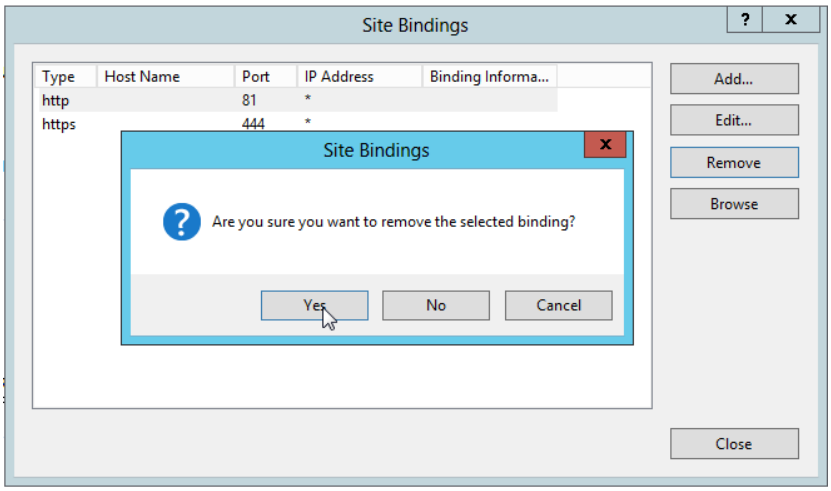
12. You see that a new binding exists. You can click **Close**.



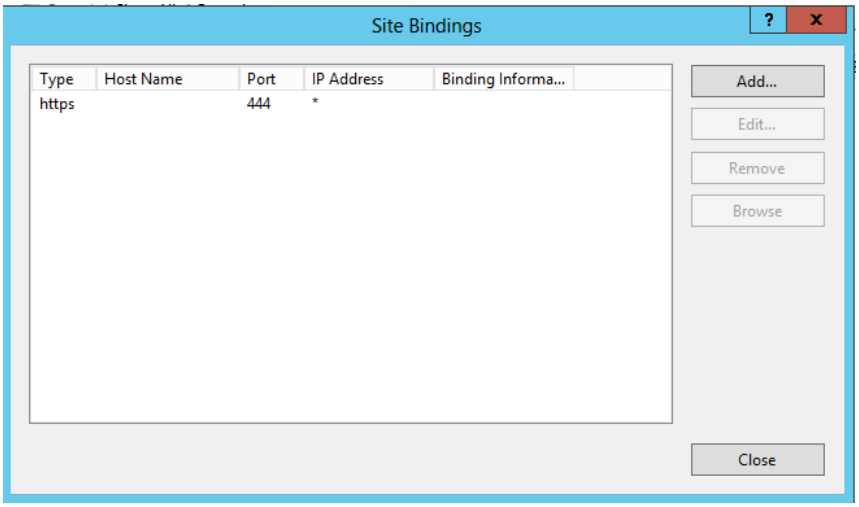
13. Install the application. Choose the appropriate website (here “test hopex”), and let the installation completes.
14. Whenever a URL is requested in the installation steps, make sure that you provide the HTTPS link, with possibly the port number, and that the address is relevant with the “Issued To” parameter when you open the certificate. Otherwise, you will receive some error messages in the application :



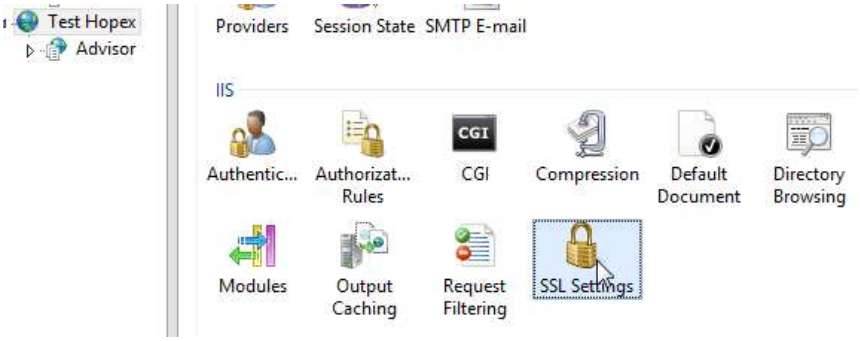
15. Once this is done, go back to IIS to force the use of SSL for your website. To do that, start by going back to the previous window to edit the bindings.
16. Select the "http" binding, and click **Remove**.



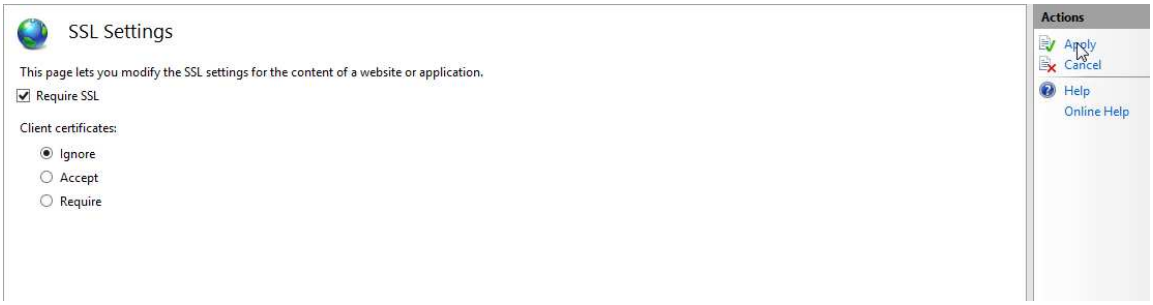
17. Check that only the https binding remains, and click **Close**.



18. Select your website, and open the « SSL Settings » feature :



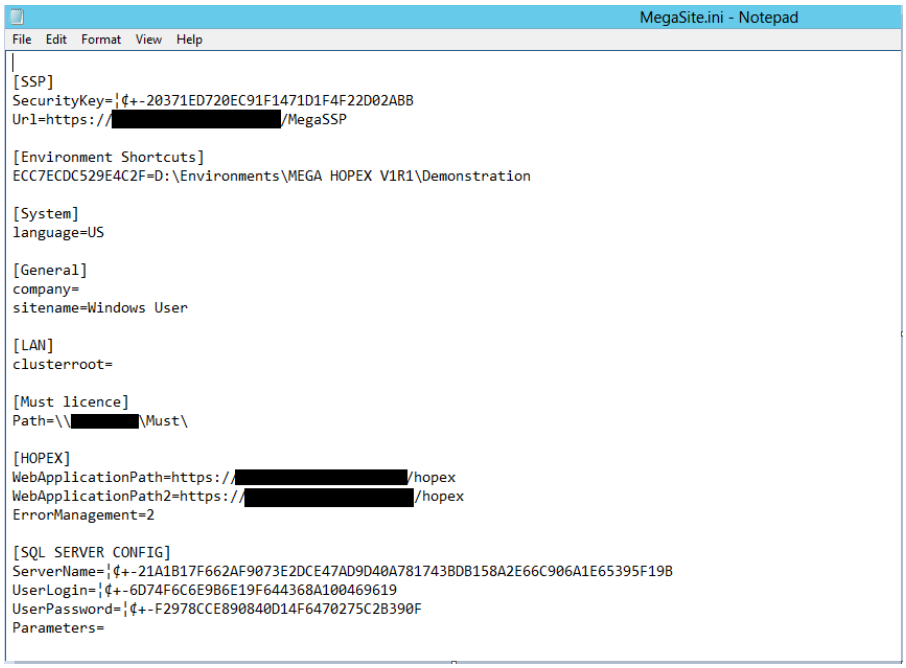
19. Click « Require SSL » and apply :



20. Install the Hopex Web front-end application on your server.

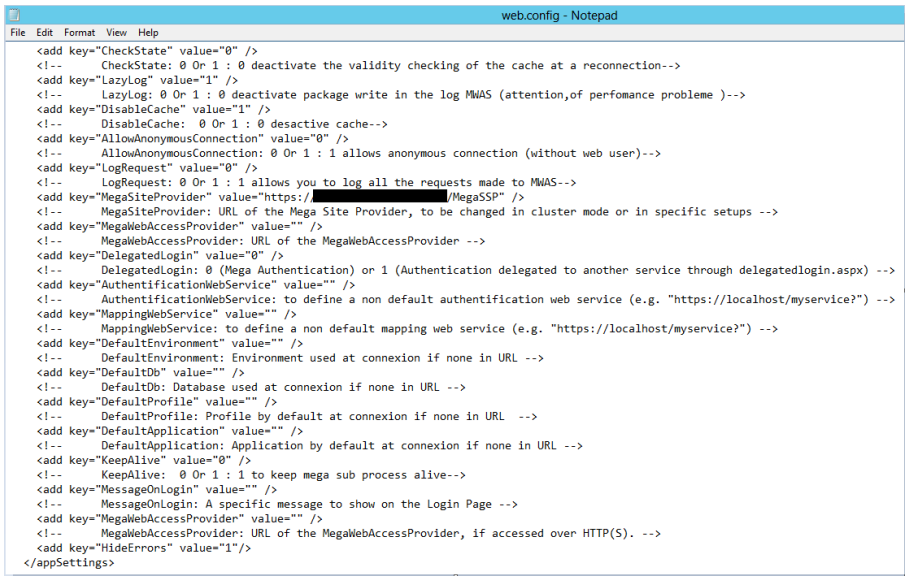
21. Last step, after the installation, is to check that the configuration files of the application all contain the proper URL. You can also install the application without SSL, and then decide to activate it. In that second scenario, you need to update the following files. If you installed with SSL activated, you just need to check the configuration with the next steps. Two locations contain such strings: the *web.config* file of the "Hopex" web application, and the *MegaSite.ini* in the "Cfg" folder of the installation folder of the application :

a. In the MegaSite.ini file, the URL, WebApplicationPath, and WebApplicationPath2 parameters need to reflect that use :

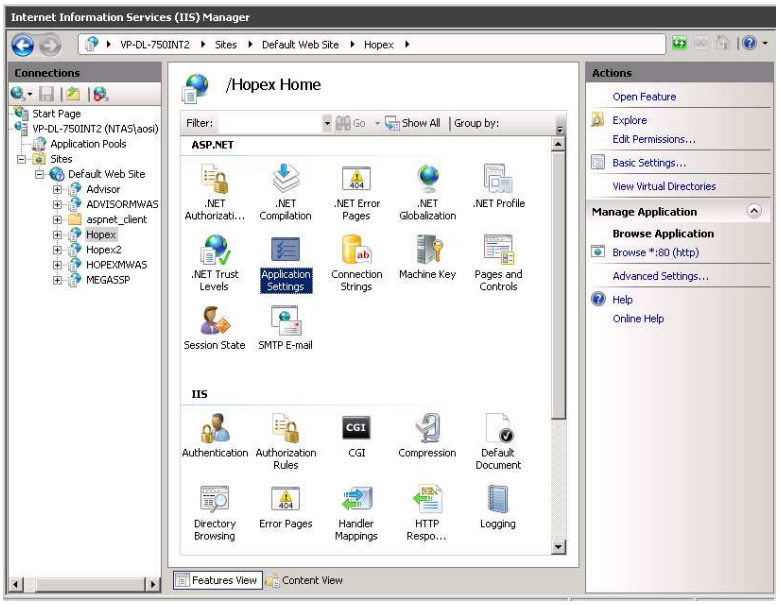


b. Application settings of the Hopex web application (two techniques), the parameters MegaSiteProvider, and MegaWebAccessProvider, also need to be switched to HTTPS with the proper port :

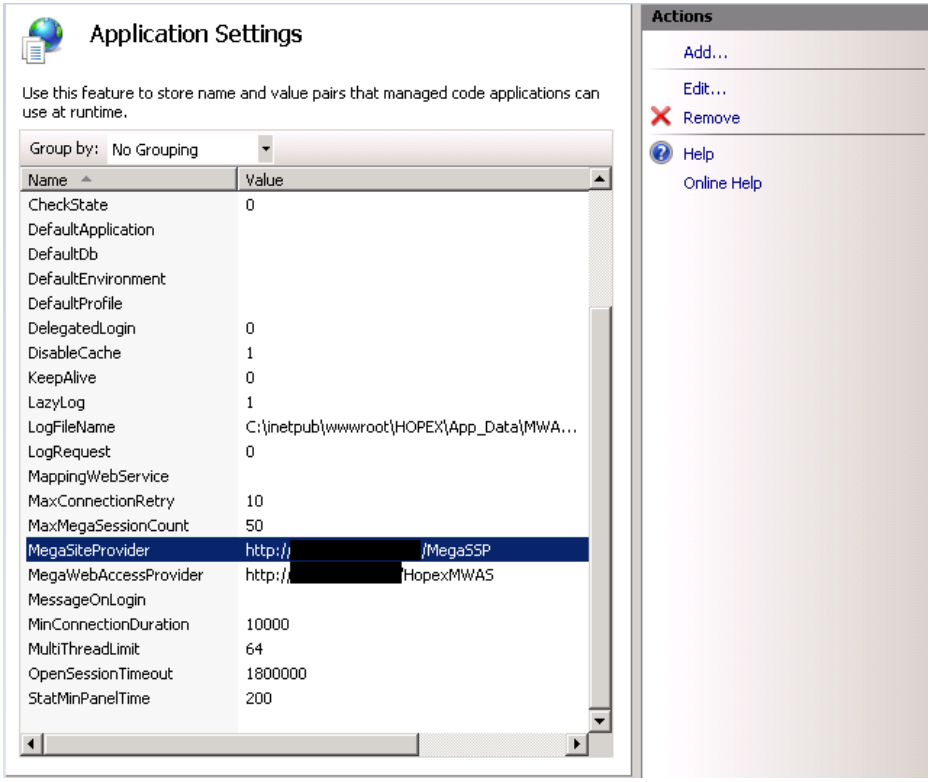
i. In the web.congif file :



ii. Through the « Application settings » feature in IIS :



You can select a line and click the **Edit** link on the right pane to update a URL :



Disabling SSL v2

On Windows Server 2008 R2 and Windows Server 2012, the SSL V2 and V3 are activated by default. As there are known vulnerabilities with SSL V2, and since we use it when securing the access to the website, an additional task would be to disable that V2 protocol, to keep only SSL V3 active.

The steps are :

1. Through the Startup menu, go to "Run" and type :

   regedit.exe

2. Browse through the registry until you reach the following key :

   HKey_Local_Machine\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 2.0

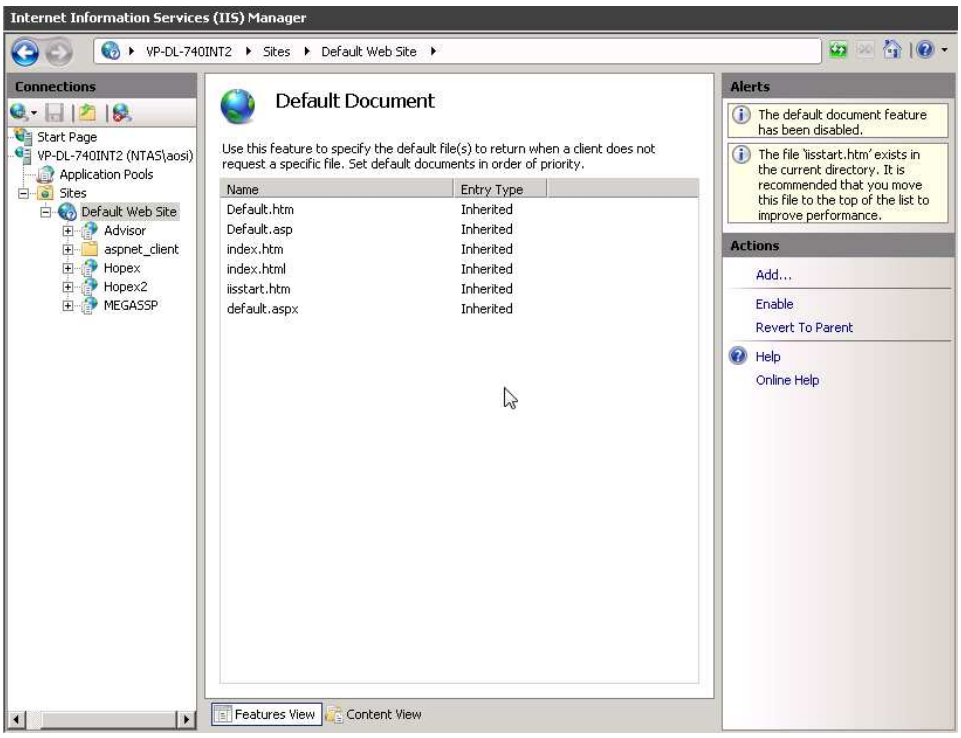
3. In the "SSL 2.0" key, create a new one, of type DWORD (32 bit) with the following details :
   a. Name : Enabled
   b. Value : 0
4. Close the registry and restart the server to take it into account.

Remove the default install page in IIS

After the application is installed, you can disable the "Default Document" feature for the website on which the application is deployed.

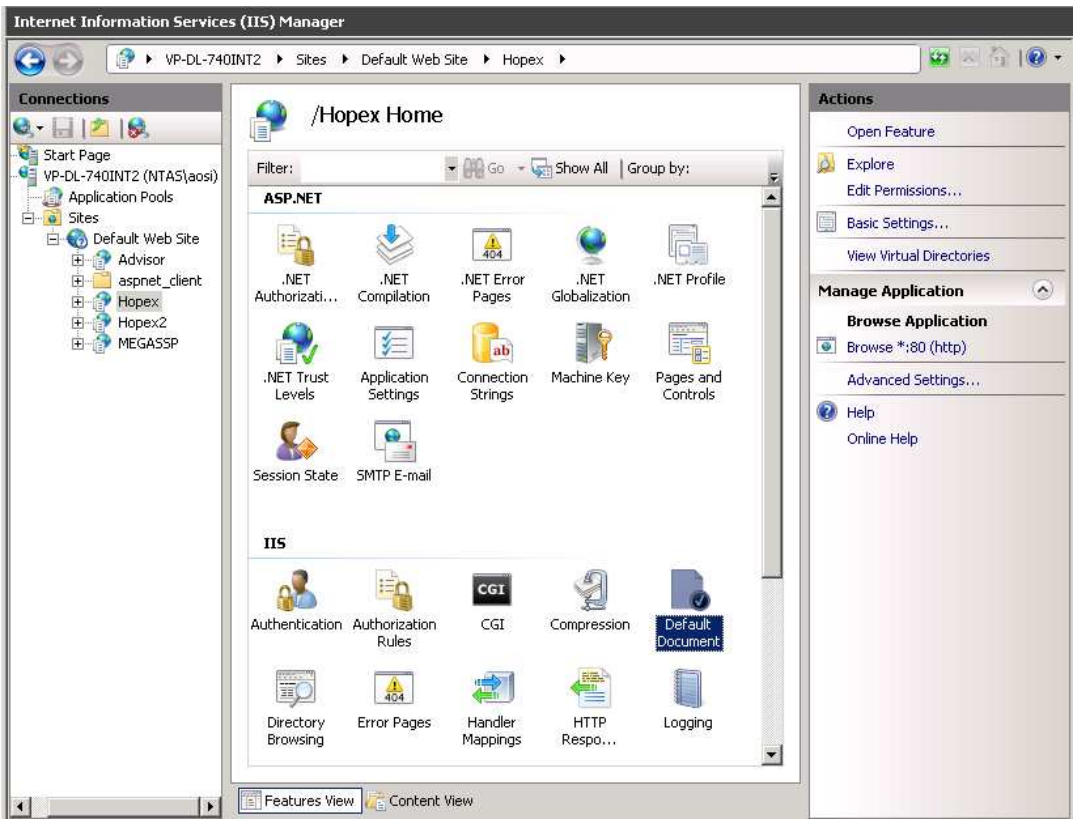
To do that :

1. Open the IIS Manager console.
2. Locate the website where the Hopex and/or Advisor web application is installed.
3. On the website, double-click **Default Document** to open this feature.
4. In the "Actions" pane on the right, click **Disable**. You should have this kind of screen after it is done :

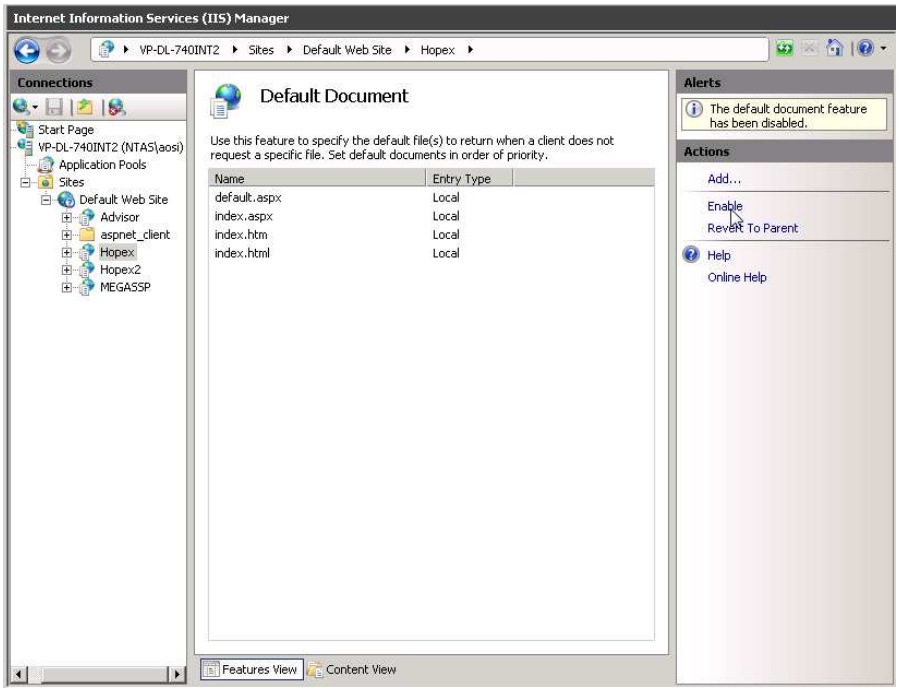


5. Make sure that the « Default Document » feature is enabled for the Hopex/Hopex2/Advisor web applications. Since it was disabled at the root level, you will have to :

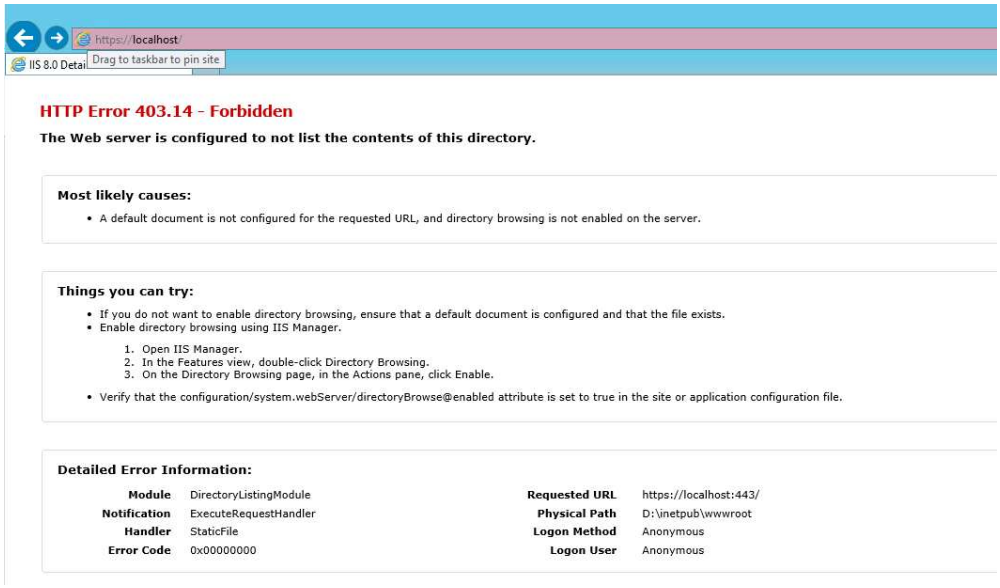
    a. Select each web application (here Hopex), and open the "Default Document" feature :

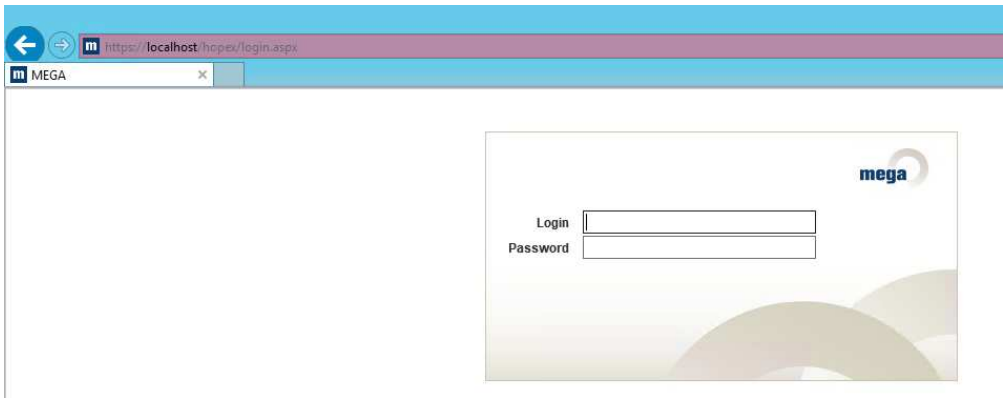


b. Click **Enable**.



c. This way, the URL https://servername won't reply, whereas the URL https://servername/hopex will redirect the users to the login page of Mega :



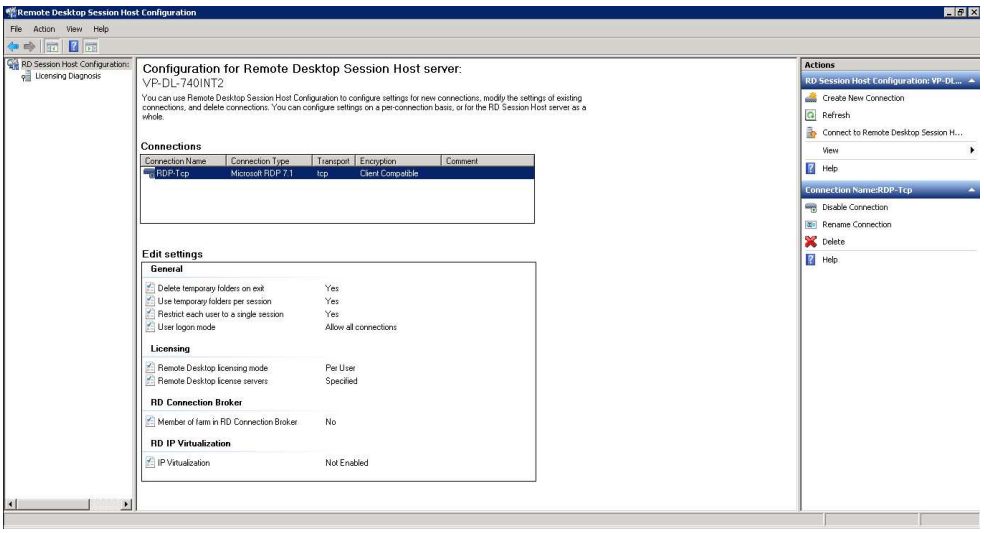


Securing the RDP access (Terminal Services)

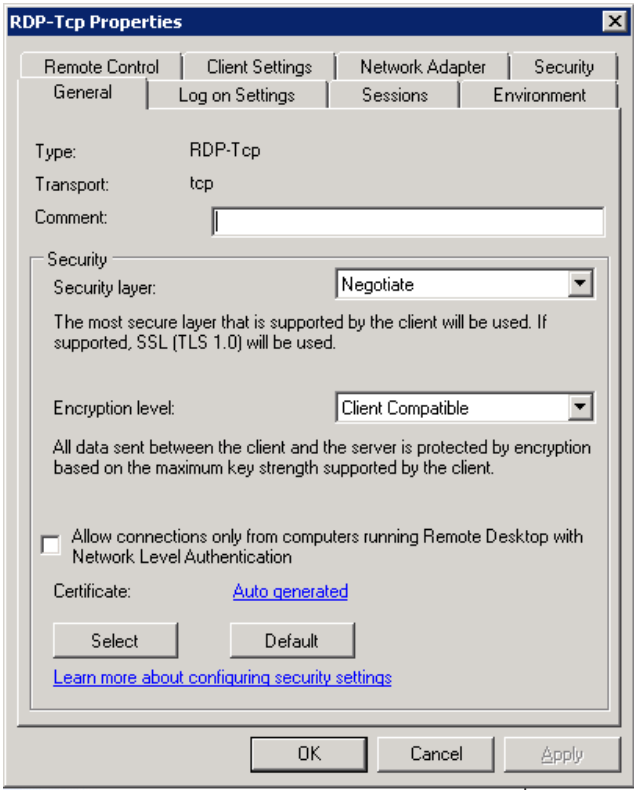
On a server hosted on a Windows 2008 R2 Operating System, you can secure the RDP layer by changing the security layer and the encryption layer of the Remote Desktop Protocol.

To do that:

1. Firstly, you have to open **Remote Desktop Session Host Configuration** the by clicking on "Start", point to "Administrative Tools", point to "Remote Desktop Services", and then click "Remote Desktop Session Host Configuration".

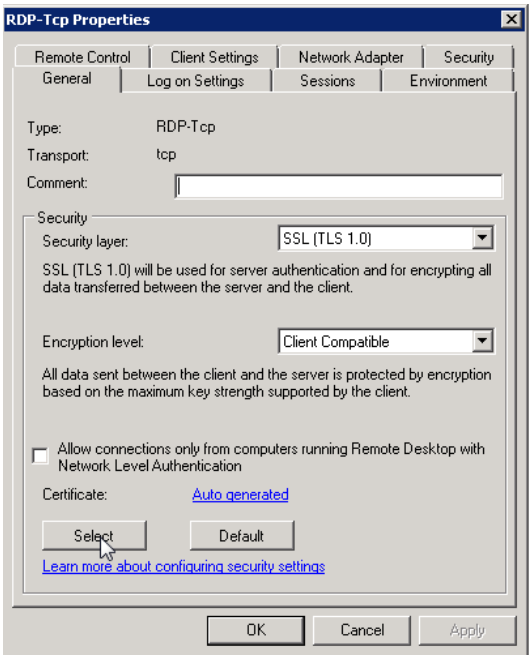


2. In the "Connections" section, do a right-lick on the "RDP-tcp" entry, and select "Properties" :

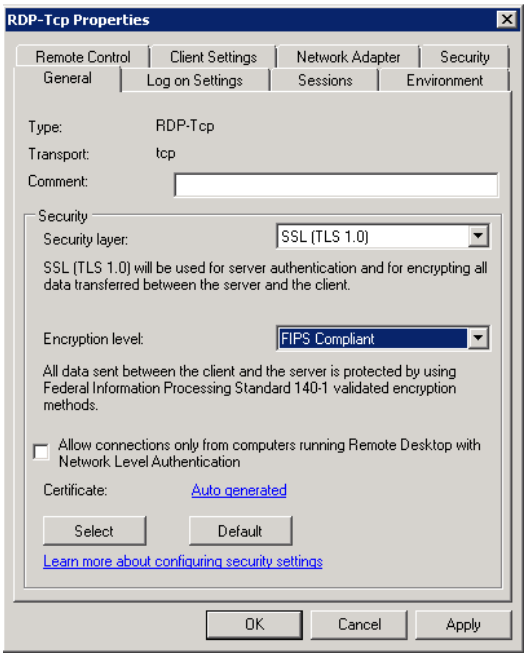


3. In the "General tab", as shown above, you can see the two security parameters that can be modified.

4. Change the "Security Layer" option to "SSL (TLS 1.0)". Be aware that you will need to have a specific certificate installed on your server to switch to that level. The "Select" button allows you to browse your installe certificates and choose the proper one:



5. Then, modify the « Encryption level » option and upgrade it to at least "High", and possibly "FIPS Compliant" :



6. Click **OK** to validate this modification and exit the configuration tool.

There are also numerous ways of securing the RDP protocol, whether it is using the Remote Desktop Gateway, filtering by IP address and user, etc.

Configuring the firewall

To avoid letting some unwanted users connect to the server or retrieve information from the server, some actions can/need to be taken on the firewall:

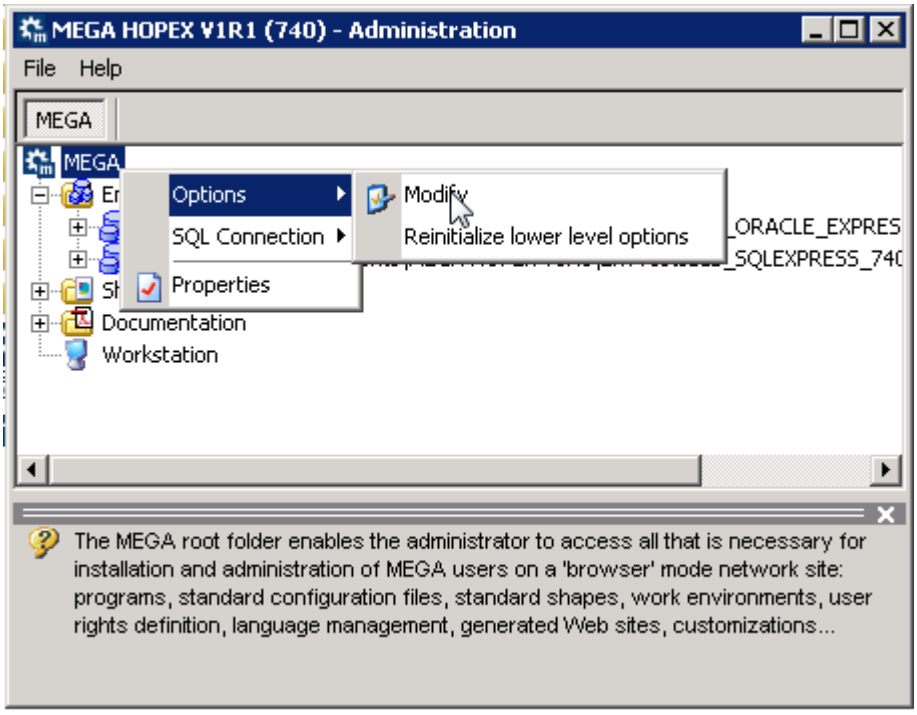
- If possible, restrict the access to port 3389 (RDP) to only the valid IP addresses of the System Administration, Application Administrators, and maybe the users that need to launch the Desktop client of Mega through Terminal Services.
- Restrict external access to all SMB services and ports, including TCP and UDP 135, TCP and UDP 139, and TCP and UDP 445.
- Regarding the ICMP protocol, block the following type of requests: ICMP timestamp requests (13), and ICMP timestamp replies (14).
- Limit the number of opened ports on the server to the least amount possible. Globally the server needs to be accessed through RDP, the SSL port needs to be opened, the SMB port also, and the communication port to the database server. All other ports need to be assessed in order to check that those are relevant.

Note that the following two sections are normally already configured by default with Hopex V1R2-V1R3. You can check those, and tune up the second section depending on the timeout you want to put in place.

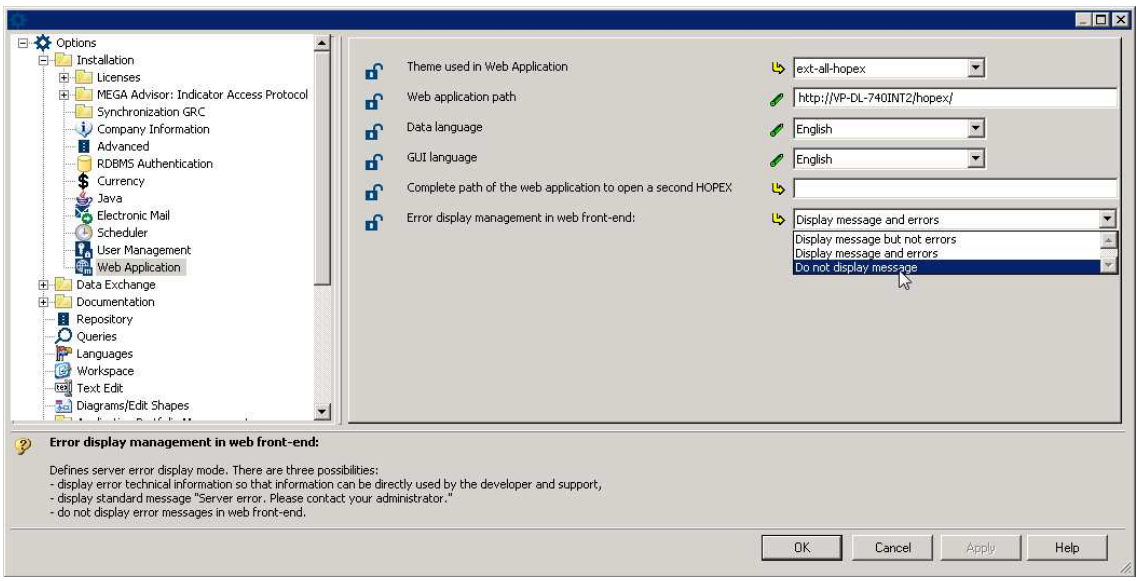
Hiding the error details

To prevent the end users from seeing the error details and get knowledge about how the application is written, some actions can be taken to hide those:

1. Open the Administration module of Mega on the web server (Administration.exe, in the installation module of Mega).
2. Open the options at the root level:



3. Go to “Installation”, and then “Web Application”, and change the option “Error display management in web front-end” to “Do not display message”:



4. Close the options and the Administration module.

5. Locate the web.config file of the “Hopex” web application (by default in “C:\inetpub\wwwroot\HOPEX”), and edit it.

6. Add the following key in the file :

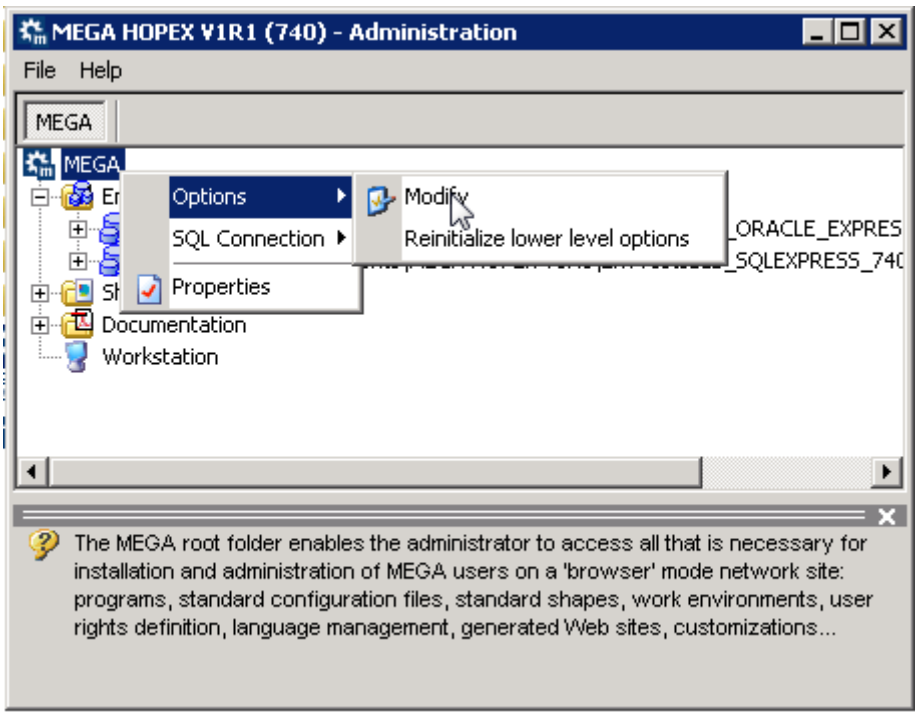
```
<add key="HideErrors" value="1"/>
```

Activating the automatic logoff

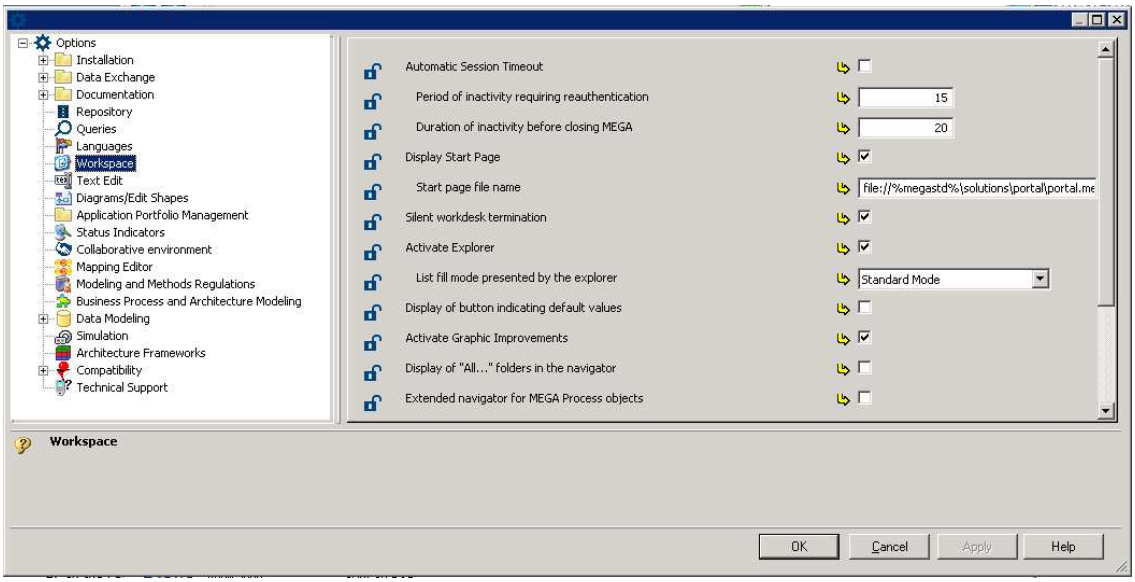
You can activate an automatic logoff of the users after a certain time of inactivity. To do so:

1. Open the Administration module of Mega on the web server (Administration.exe, in the installation module of Mega).

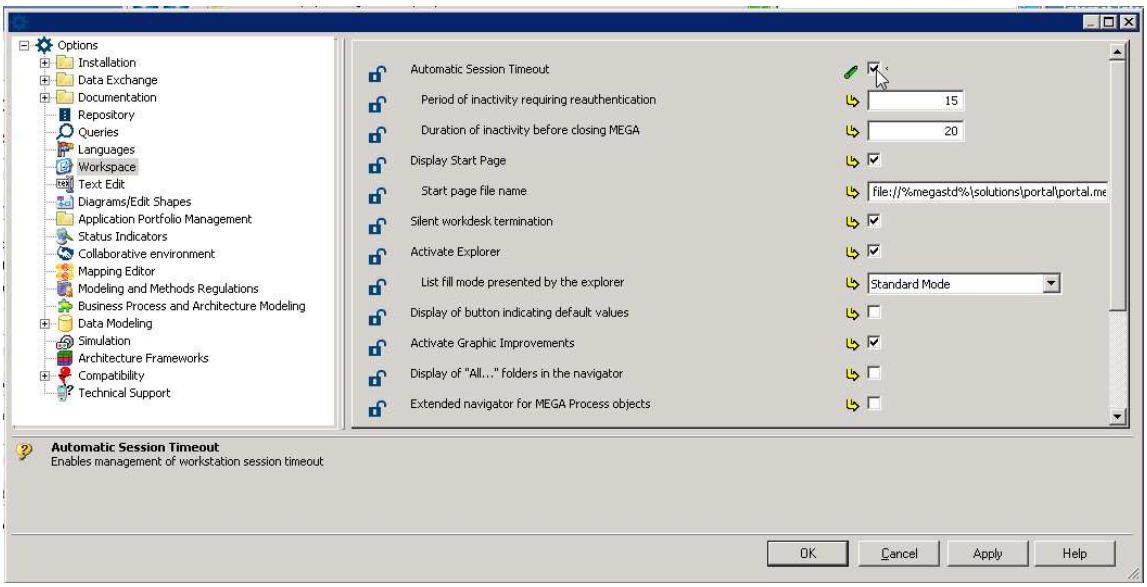
2. Open the options at the root level:



3. Go to "Workspace":



4. Check the box "Automatic Session Timeout", and tune up the parameters "Period of inactivity requiring authentication"and "Duration of inactivity before closing MEGA" to the wanted values (by default, in minutes, they are set to 15 and 20, respectively) :



5. Click **OK**, and close the Administration module.
6. Restart the application to validate this whole configuration.

Web connection overloading and configuration MEGA HOPEX 1.0 EN

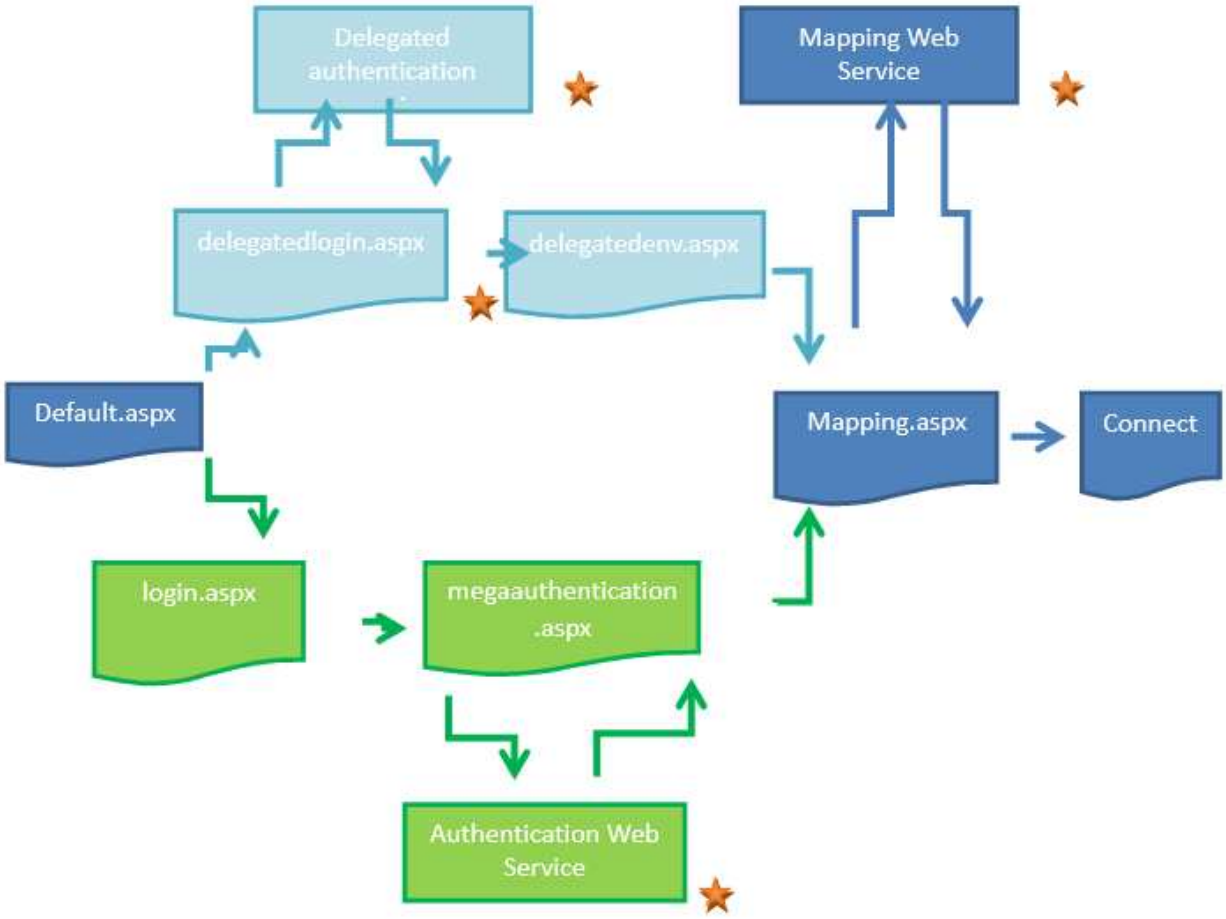
This technical article describes how to overload and configure web connection. This includes:

- the authentication and mapping services: this enables using non standard algorithms to authenticate or map users, or even to use centralized authentication, enabling Single Sign On scenarios.

- timeout and preload configuration: this enables improvements in first connection response times

AUTHENTICATION AND MAPPING PRINCIPLES

The authentication and mapping process is as follows:



The ★ sign denotes components whose overloading is explained in this document.

The administration of standard authentication and mapping (as provided by the standard web services) is explained in the product documentation.

> You should never modify any of the files provided except as noted in this document. Any other modification would be unsupported and could be erased by any patch or update.

OVERLOADING THE AUTHENTICATION WEB SERVICE

Defining the web service to call

By default, authentication is provided by a Mega Web service. The web service to call can be changed by editing the following entry in the Web.Config file:

```
<add key="AuthentificationWebService" value=""/>
```

If the entry is not present or its value is empty, the default service is used. If you wish to use your own service, you should provide its URL here. For example:

```
<add key="AuthentificationWebService"
value="https://myservices.example.com/mywebservice.myextension"/>
```

> As this service receives the password typed by the end user, use of the HTTPS (HTTP over SSL/TLS) protocol is highly recommended, especially if the service is not on the same machine or network as the Mega IIS Web server.

Web service interface to implement

The web service is called using POST with a JSON in the body of the request and should send a JSON back.

The calling JSON has the following format:

```
{"WebUserName":"sUser","WebUserPwd":"sPasswd","Environment":"sEnv","AuthToken":"sAuthToken",
"ContextHash":"sContextHash"}
```

- WebUserName: the login that was entered by the user
- WebUSerPwd: the password that was entered by the user
- Environment: the environment path or Id
- AuthToken: a token if the user was previously authenticated and did not re-enter its passoword and name
- ContextHash: a context hash identifying the computer from which the connection has been received

The response JSON must have the following format:

```
{"Error":"sError","IsAuthenticated":"bIsAuthenticated","AuthenticatedWebUser":"sAuthenticate
dWebUser","AuthenticatedLogin":"sAuthenticatedLogin","PassdIsExpired":false,"AuthToken":"sAu
thToken"}
```

- Error: an error message if IsAuthenticated is false
- IsAuthenticated: is the person authenticated?
- AuthenticatedWebUSer: the Person that was found
- AuthenticatedLogin: the Login that was found
- PasswdIsExpired: has the password expired? If yes, a password modification will be requested
- AuthToken: a token that can be used to re-authenticate without login/password.

OVERLOADING THE MAPPING WEB SERVICE

Defining the web service to call

By default, mapping is provided by a Mega Web service. The web service to call can be changed by editing the following entry in the Web.Config file:

```
<add key="MappingWebService" value=""/>
```

If the entry is not present or its value is empty, the default service is used. If you wish to use your own service, you should provide its URL here. For example:

```
<add key="MappingWebService"
value="https://myservices.example.com/mywebservice.myextension"/>
```

> Use of the HTTPS (HTTP over SSL/TLS) protocol is recommended, especially if the service is not on the same machine or network as the Mega IIS Web server.

Web service interface to implement

The web service is called using POST with a JSON in the body of the request and should send a JSON back.

The calling JSON has the following format:

```
{"WebUserName":"sMegaWebUser","Environment":"sEnv","isSSO":bIsSSO,"SSOPersonInformations":"s
SSOPersonInformations"}
```

- WebUserName: the login that was entered by the user
- Environment: the environment path, or Id.
- isSSO: do we come from a centralized auth service?
- SSOPersonInformations: if isSSO is true, describes extra informations on the person

The response JSON must have the following format:

```
{"Error":"sError","Person":"sPersonId","PersonGroup":"sPersonGroupId","Login":"sLogin"}
```

- Error: an error message, if no Person or PersonGroup was found
- Person: IdAbs of the mapped Person
- PersonGroup: IdAbs of the mapped PersonGroup
- Login: Login of the Person or PersonGroup

DELEGATING AUTHENTICATION TO A CENTRALIZED AUTHENTICATION SERVICE (SSO)

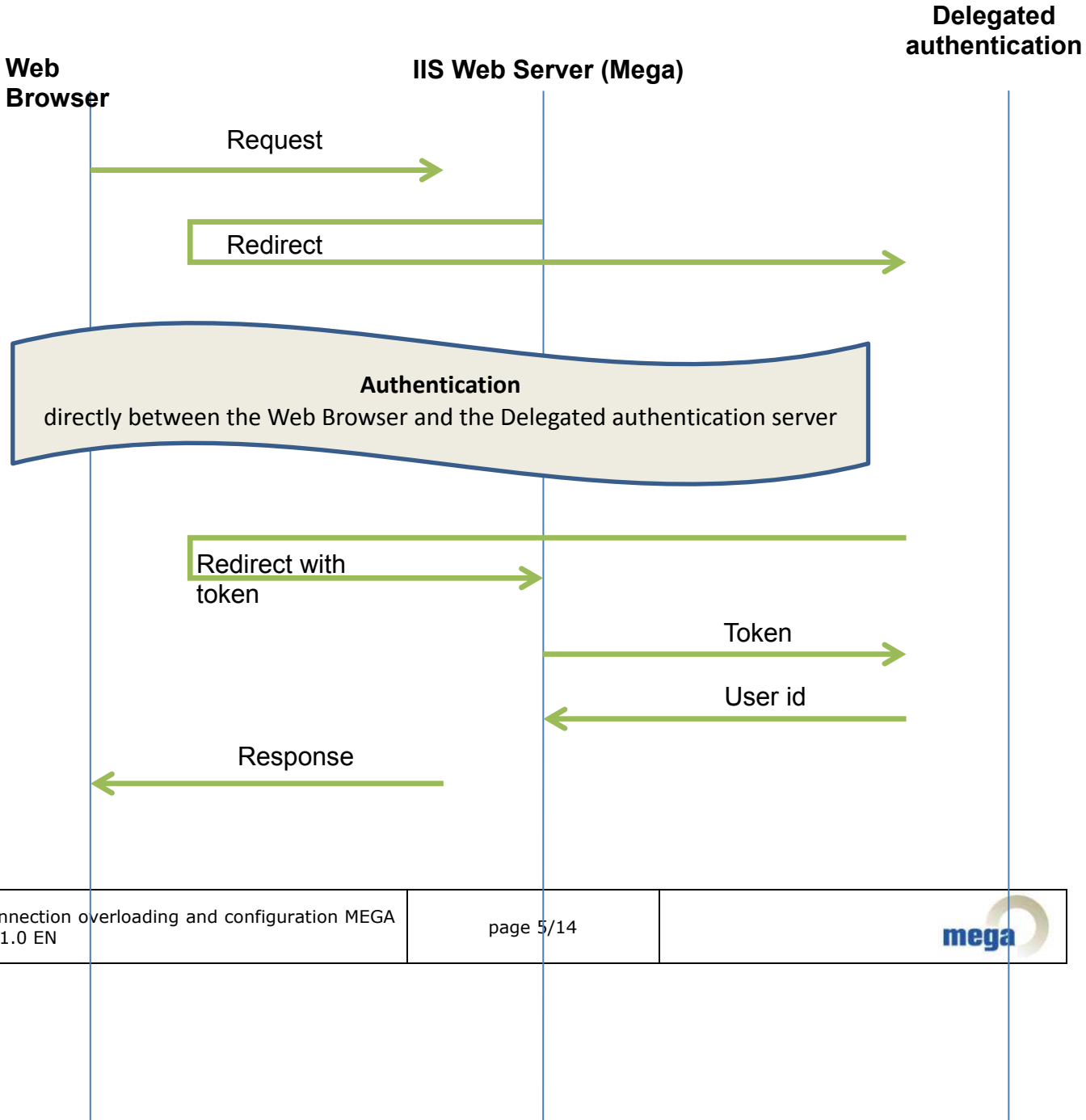
Delegated authentication principle

Delegated authentication means that the authentication of users is not handled by Mega but by a central authentication server shared between applications in your organization.

Many delegated authentication servers (e.g. ADFS, CAS, etc.) and protocols (e.g. SAML, WS-Federation, CAS, OpenID, etc.) exist and can be interfaced to the Mega web application by writing your own delegated authentication handler page.

Such a mechanism allows the setup of Single Sign-On (SSO) scenarios.

The general principle of delegated authentication is as follows:



Activating delegated authentication

Delegated authentication is activated in the Web.Config file of the web application. This file can also be modified through IIS Administration.

The following means that delegated authentication is disabled:

```
<add key="DelegatedLogin" value="0"/>
```

To enable it, replace this line with:

```
<add key="DelegatedLogin" value="1"/>
```

This configuration means that authentication will be handled by delegatedlogin.aspx rather than login.aspx.

The next step is to personalize delegatedlogin.aspx.cs to handle your delegated authentication protocol and server.

Delegated authentication samples

A few delegated authentication samples are delivered in the samples directory of the web application. These can serve as a starting point for writing your own delegatedlogin.aspx.cs file.

The following samples are available:

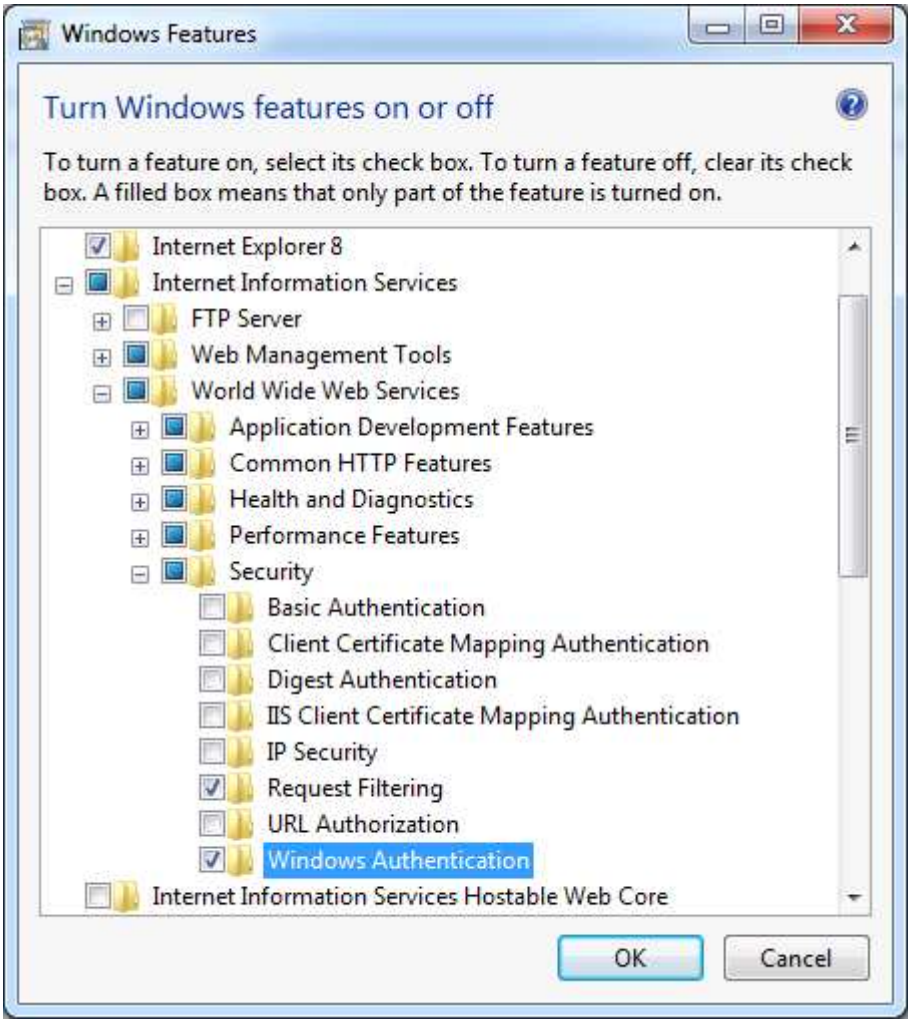
- delegatedlogin_cas.aspx.cs : delegated login using the CAS protocol
- delegatedlogin_passtrough.aspx.cs : pass-through login (no authentication)
- delegatedlogin_windows.aspx.cs : authentication using .Net Windows authentication

To use them, duplicate the chosen sample in the main directory of the web application and edit it. Do not forget to reference it in the delegatedlogin.aspx file.

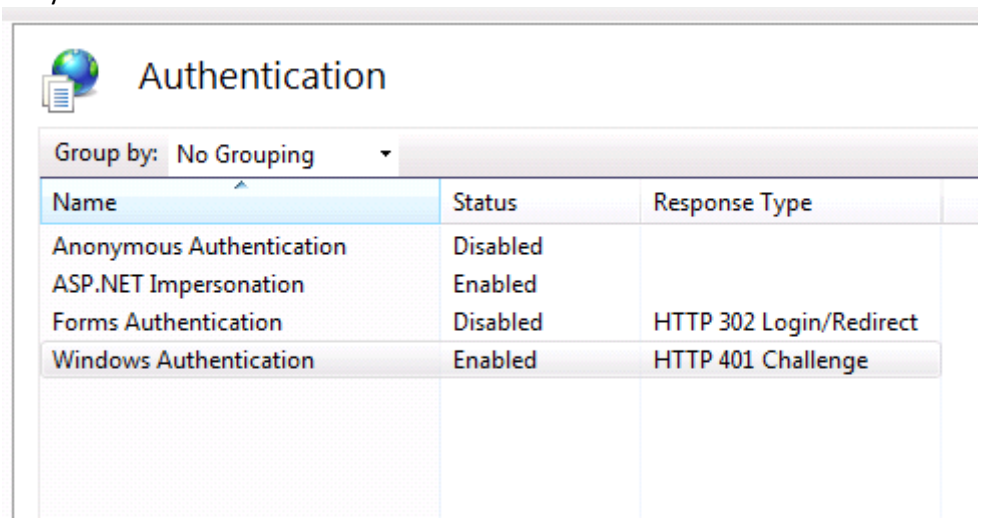
Windows .Net authentication

This authentication type requires extra configuration:

a) Add the “Windows Authentication” functionality to Windows Features (from Control Panel) :



b) Enable Windows Authentication for the site where Mega is installed in IIS, and disable anonymous authentication :



c) Add Windows authentication in the Web.config file, by replacing “None” by “Windows” :
<authentication mode="Windows" />

Writing your own delegated authentication service

Your delegatedlogin.aspx.cs must be written in C# .Net 4.0 and must provide at least the following services:

- When authentication is successful:
  - Set the session variable "AuthenticatedWebUser" with the name of the authenticated user
  - Redirect the browser to the delegatedenv.aspx page
- When delegated authentication fails:
  - Handle the error, for example by redirecting to the Mega login page, or by presenting the error directly to the end user

Here is a sample minimum implementation:

```
public partial class delegatedlogin : System.Web.UI.Page
{
  protected void Page_Load(object sender, EventArgs e)
  {
    …
    if (isAuthenticated)
    {
      Session["AuthenticatedWebUser"] = sMyAuthenticatedUser;
      Response.Redirect("delegatedenv.aspx");
    }
    else
    {
      Session["Error"] = "Delegated login failed";
      Response.Redirect("login.aspx");
    }
  }
}
```

You can also decide to provide more information to Mega about the user that is logging in. This information will be used to create the corresponding Person object in Mega. In order to do this, you can use the following code:

```
Dictionary<string, string> PersonInformations = new Dictionary<string, string>();
PersonInformations["idAbsOfTheAttribute1ToFillInOnPerson"] = "ValueOfTheAttribute1";
PersonInformations["idAbsOfTheAttribute2ToFillInOnPerson"] = "ValueOfTheAttribute2";
Session["PersonInformations"] = PersonInformations;
```

This allows you to give values to the attributes of your choice on the Person that will be created. It therefore only applies to the first connection of a given user. On subsequent connections, it will be ignored.

IMPROVING MEGA ADVISOR FIRST CONNECTION RESPONSE TIME

At the first Advisor connection, four processes are launched. By default, these processes are stopped, without requests, after 20 minutes of idle time.

The time spent to launch these processes slow down the connection to Advisor. To optimize the first connection time to the application you can configure IIS and the application to preload required processes and prevent them to stop.

To start with MEGA Advisor in optimized conditions, you must:

- Configure IIS and application timeout, the time with no activity before stopping mgwmwas.
- Configure Advisor to preload the Mega Sub Process needed for each mega profiles.
- Plan the preload using Windows Scheduler.

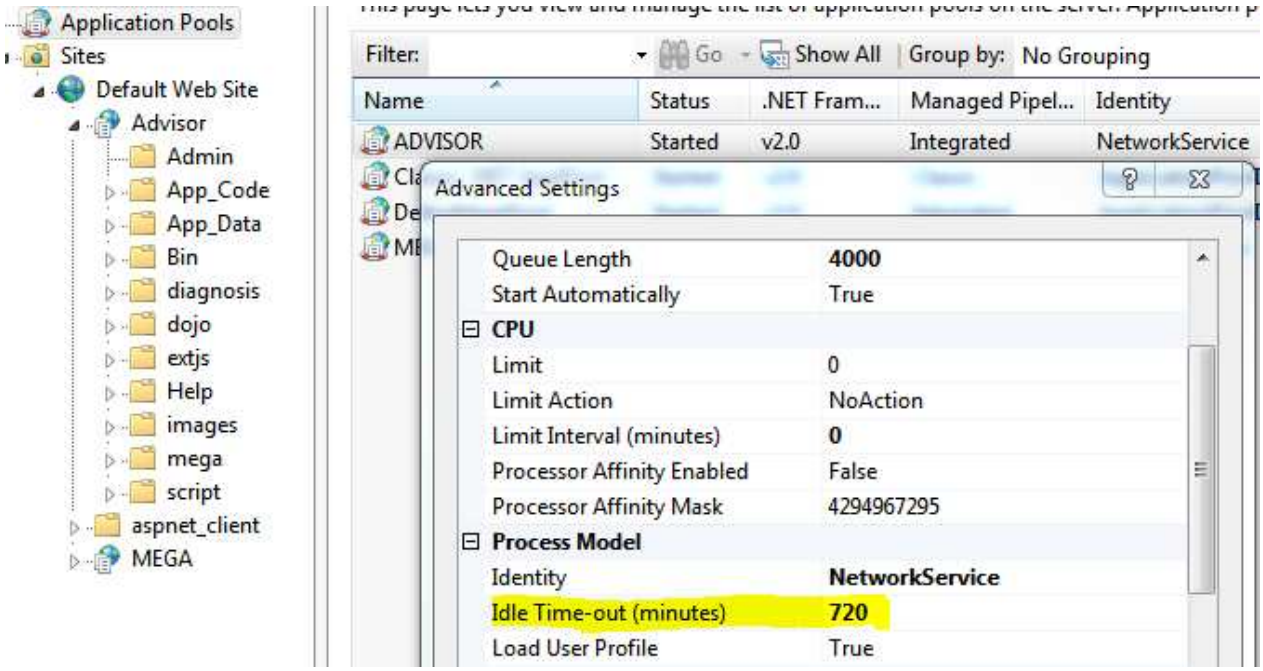
Timeout configuration

The default timeout configuration is 20 minutes. To prevent the mgwmwas process to shut down during a day, modify the default timeout to 12 or 24 hours.

Configuring IIS Application Pool timeout

From IIS:

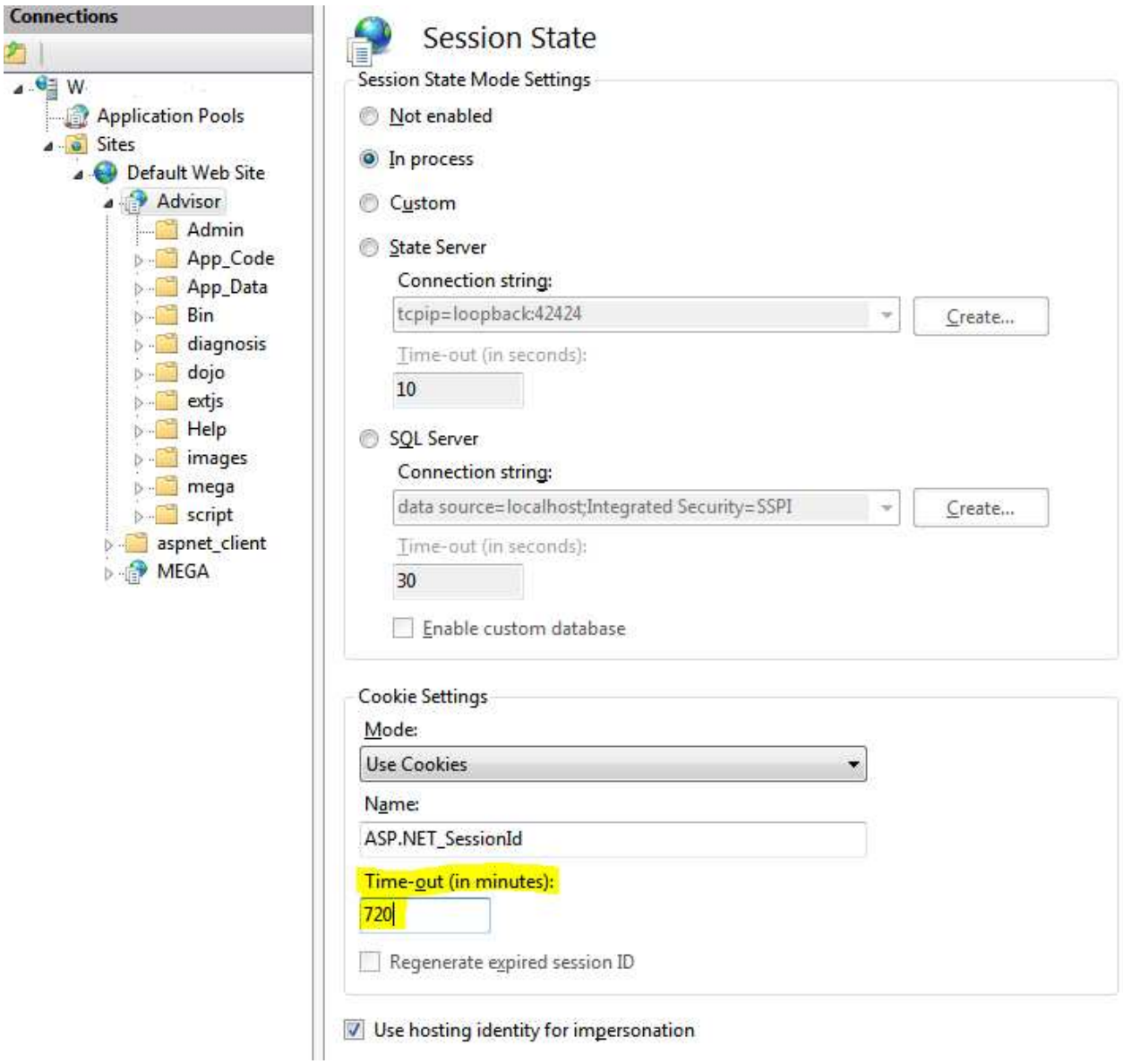
1. In the left pane, from the tree view select **Application Pools**.
2. In the right pane, right-click **ADVISOR** application and select **Advanced Settings**.
3. From the **Advanced Settings** window, in the **Process Model** part, modify the **Idle Time-out (minutes)** value.



Configuring Advisor ASP.NET Session State timeout

From IIS:

1. From the left pane, expend the **Sites** tree view and select the **Advisor** Application.
2. In the right pane, open the ASP.NET **Session State** feature.
3. Modify the **Time-out (in minutes)** value.
4. In the **Actions** pane, click **Apply** to validate your modifications



Configuring Advisor session timeout

From the root folder of the Advisor deployment path:

- In the Web.Config file, update the OpenSessionTimeout value.
  This value is given in milliseconds.

```
   <add key="OpenSessionTimeout" value="43200000"/>
   <!--      OpenSessionTimeout: Session Timeout in ms. Default value 1800000 (20 Mn)
-->
```

Values in the Web.config file can also be configured through IIS Application Settings

Preload profiles configuration

Configuring the KeepAlive value

By default a Mega Profile remains connected, and its associate Mega Sub Process alive, even when the last user using the profile has gone. The configuration parameter that controls this behavior is located in the Web.Config file.

- Make sure you have the following line in your Web.Config file:

```
<add key="KeepAlive" value="1"/>
<!--      KeepAlive:  0 Or 1 : 1 to keep mega sub process alive-->
```

Configuring the Preload profiles

Configuring the preload profiles consists of code instructions to open session for a user for each profile to preload and instructions to discard each preloaded environments.

1. From the **App_Code** folder, open the **preload.cs** file.
2. Modify the **Preload** method according to the following model:

<environment Path> must be replaced by the environment path with duplicate backslash.

```
  static public bool PreLoad(MEGAWebAccessLib.MegaWebAccess pMWA , settings
pSettings , int nLevel, bool bDiscarding)
    {
bool bPreloading = true;
if (bDiscarding && (nLevel == 1))
{
  pMWA.Discard(1, "<environment_1 path>");
  …
  pMWA.Discard(1, "<environment_n path>");
}
string[] sDiagramArray = new string[<nd - number of diagram type to
preload>];
----
sDiagramArray[0] = "<hexaidabs of a diagram for the first diagram type>";
…
sDiagramArray[<nd-1>] = "<hexaidabs of a diagram for the last diagram type>";

switch (nLevel)
```

```
{
  case 1:
                    PreLoadProfil(pMWA, pSettings,
"<LANGID>",
"<Environment Path with double backslash ie:
C:\\Users\\Public\\Documents\\MEGA 2009 SP4\\Demonstration>",
"<Base Name>",
"<APPID>",
"<DESKID>",
"<PERSONID>",
"<LOGINID>",
"<PROFILID>",
sDiagramArray);


…
  case <n>:
                    PreLoadProfil(pMWA, pSettings,
"<LANGID>",
"<Environment Path with double backslash ie:
C:\\Users\\Public\\Documents\\MEGA 2009 SP4\\Demonstration>",
"<Base Name>",
"<APPID>",
"<DESKID>",
"<PERSONID>",
"<LOGINID>",
"<PROFILID>",
sDiagramArray);
  break;
  default:
bPreloading = false;
  break;
}

return bPreloading;
}
```

Administration page

The administration page in the admin folder calls the Preload method when resetting cache with false for bDiscarding. Then only the selected environment will be discarded.

Otherwise to start the preload call the administration page with preload parameter set to 1 (see Preload planning p. 14).

Preload planning

You can plan the preload to have profiles loaded before the first user connection.

From the Windows Scheduler:

1. Create a new task.
2. Configure the trigger.

   Ex.: everyday at 6 AM.
3. Configure the action:

   a. Select **Start a program**.

   b. In the **Parameters** pane, **Browse** the mwsr.exe program (located in the Utilities\MEGA ldap folder).

   c. In the argument field set URL of the administration page with preload parameter set to 1, for instance :

```
"http://localhost/Advisor/admin/default.aspx?preload=1"
```

The preload start discarding environment which reset cache.

RDBMS Environment Duplication (EN)

Sommaire

RDBMS environment duplication - 1 - Oracle

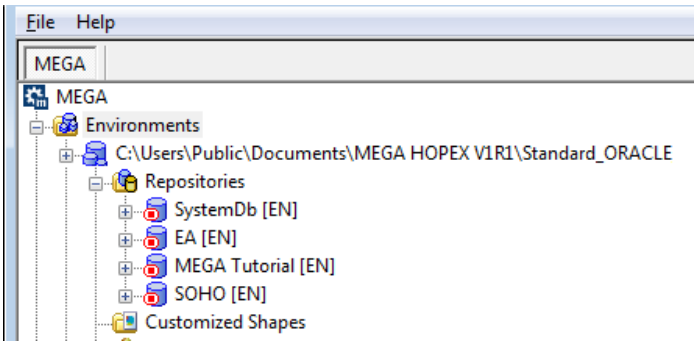
GENERALITIES

This document purpose is to explain the way of duplicating MEGA data that are stored in an Oracle RDBMS and how to use this data to create a duplicate MEGA environment that will point on this duplicated data.

It is important to have **no end user activity** on the MEGA environment while the export procedure is carried out **to avoid inconsistency** in the exported data.

You can go through the whole document to carry out the entire scenario. You can also jump directly to the Oracle data import section if you already have the Oracle dump files containing the SCHEMAs hosting the MEGA environment data.

MEGA recommends using a different Oracle SCHEMA for each MEGA repository. For example, if you have to deal with a MEGA environment like this one



It would mean that there are 4 SCHEMAs involved (also 1 for the SystemDb). It is technically possible to have every repository hosted in the same SCHEMA but **not recommended.**

For the following scenario, a local installation of Oracle will be used for exporting and importing data. The service name of this instance is EDE2.

Oracle supported versions

Refer to "*Web Front-End Architecture Overview*" or "*Windows Front-End Architecture Overview*" guides to find out the Oracle supported versions of your version.

Oracle tools used

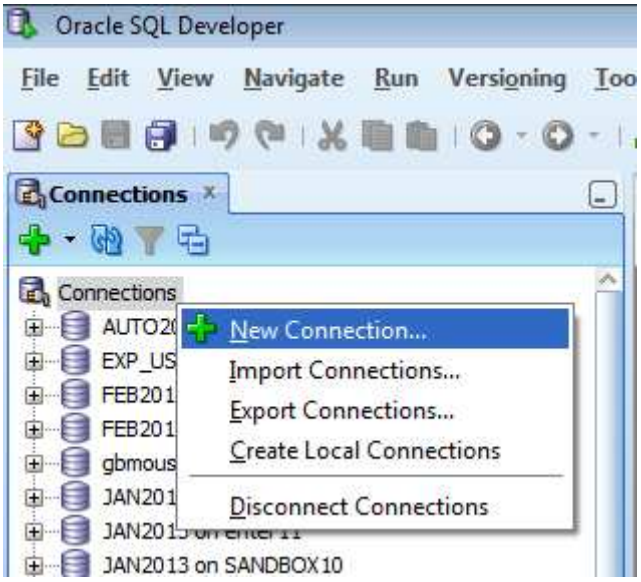
The Oracle tools that will be used are:

- Oracle SQL Developer, a free graphical tool that can be used for Oracle administration tasks. See Oracle documentation for details.
- Oracle Data Pump to export and import the physical Oracle data. There are different Data Pump components but you will be using only the command-line clients **expdp** and **impdp**. See Oracle documentation for details.

USING ORACLE SQL DEVELOPER

Oracle SQL Developer can be downloaded for free from the Oracle web site, on the Oracle software download page.

Using SQL Developer, the first thing to do is to set up a connection to be able to browse the content of the database for the SCHEMA that hosts MEGA data.



Reminder:

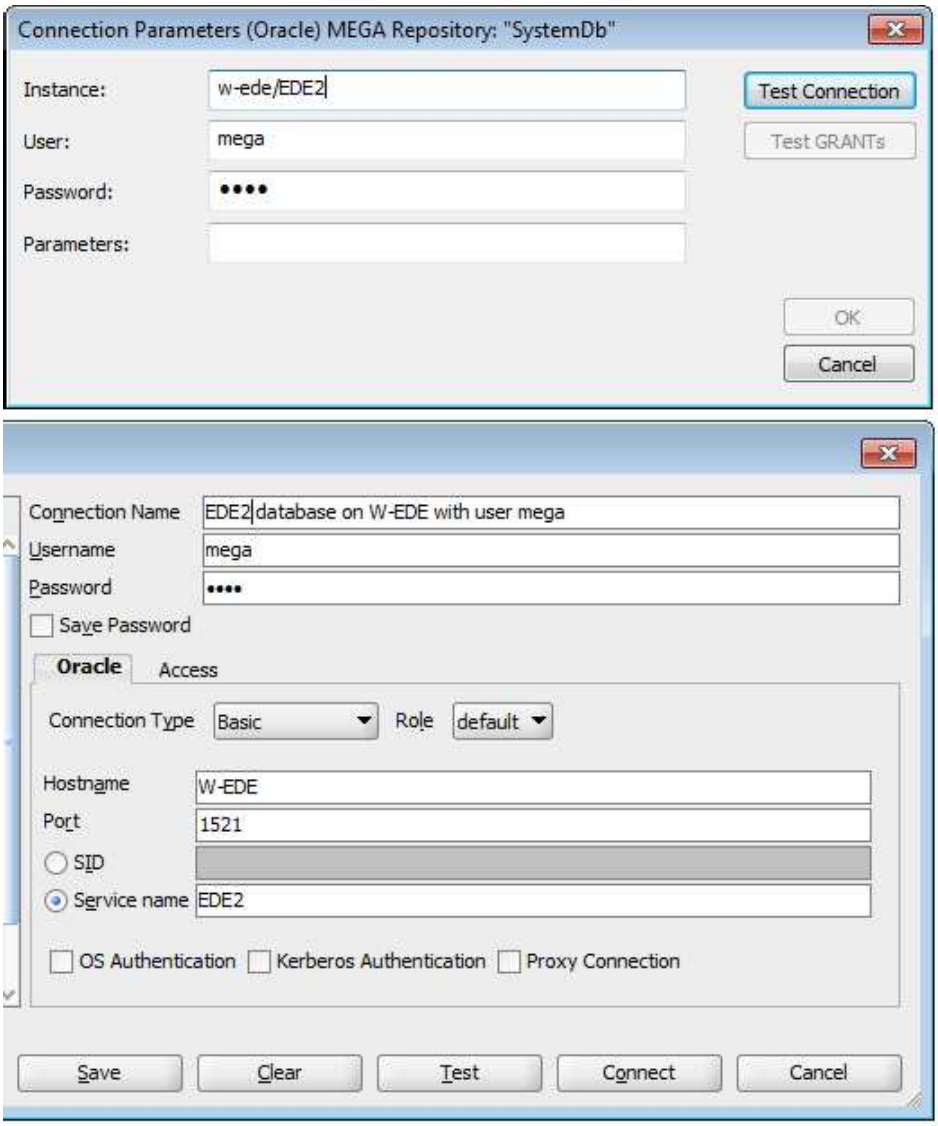
Note that the concepts of Oracle USER and Oracle SCHEMA are very similar but not exactly the same. Refer to Oracle documentation to clarify this point but here is what really needs to be understood:

> A **schema** is a collection of logical structures of data, or schema objects. A schema is owned by a database user and has the same name as that user. Each user owns a single schema.

Fill in the connection parameters according to MEGA Administration settings

Note that you have to enter a port number. Port number 1521 is the default one. If another port was used, you would see it in the connection parameters that were entered in MEGA.

For example: w-ede:1234/EDE2

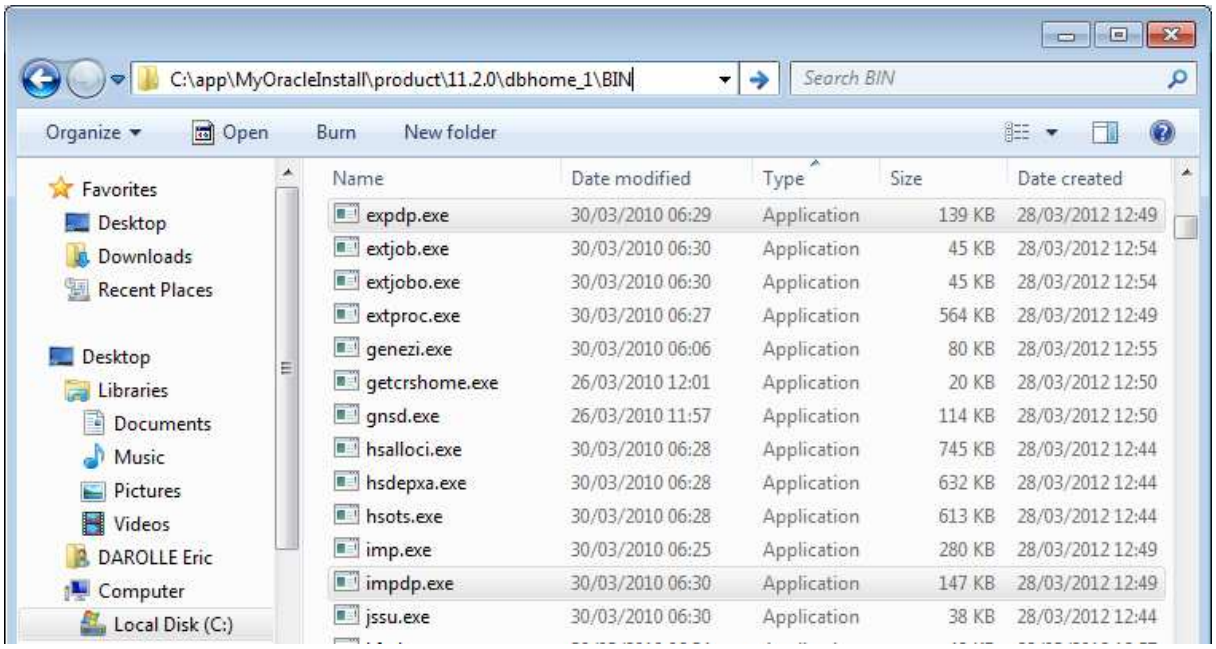


In this example, the connection parameters in MEGA were entered using a method called **EASY CONNECT NAMING**. They could also be entered in another form, using the **CONNECT DESCRIPTOR** method. This method is discussed further in this document.

THE ORACLE DATA EXPORT WITH EXPDP

The **expdp** client is a program that uses the Data Pump API. It is invoked by using the **expdp** command. See Oracle documentation for the parameters that are available in the export's command-line mode.

The **expdp** client can be found there for a typical Oracle installation on a Windows operation system.



Location of the Data Pump utilities

Prerequisites for using expdp utility

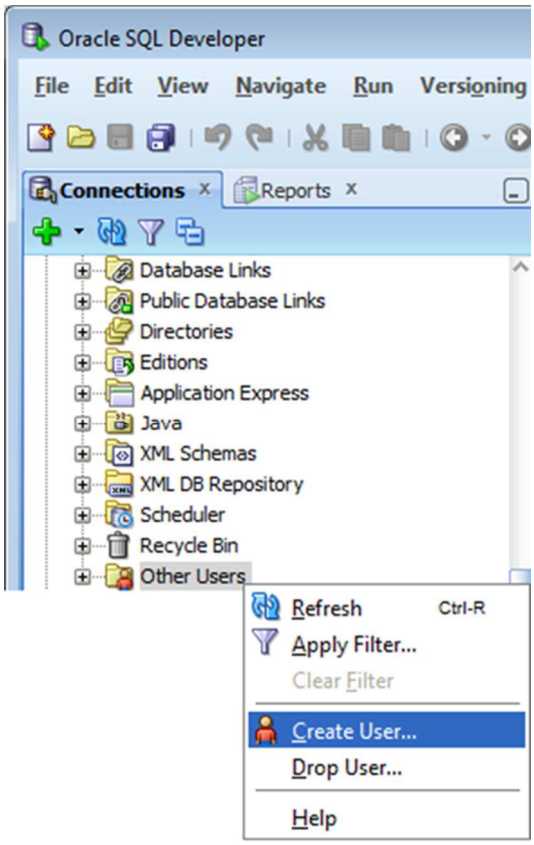
No one must be connected to MEGA when the export starts as it could lead in a set of **inconsistent data**.

Prerequisites to use the Data Pump export, you need to correctly configure the following Oracle Objects:

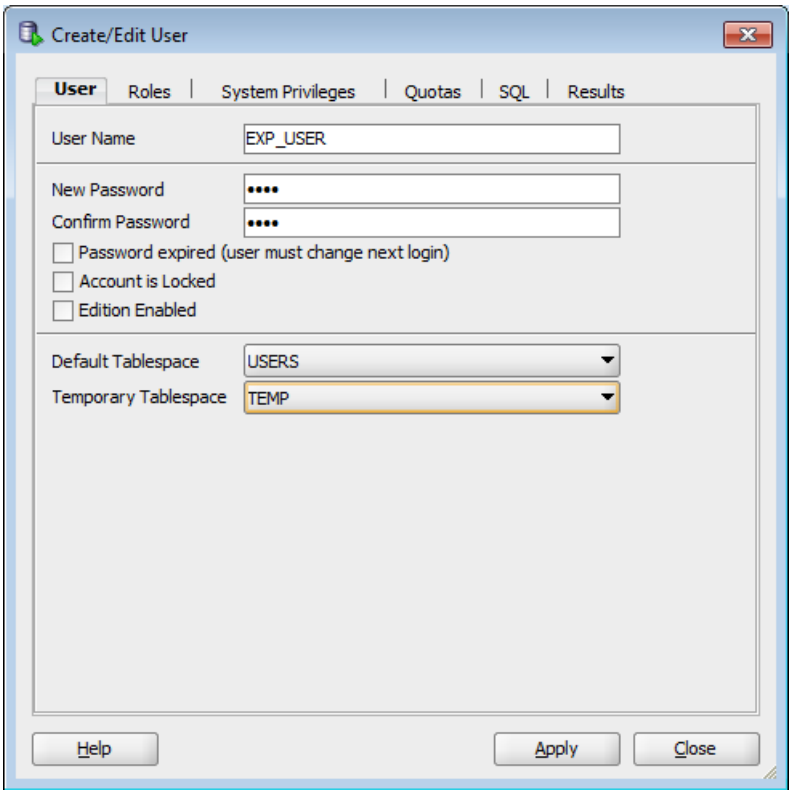
- an Oracle USER that has the rights to use Data Pump
- an Oracle DIRECTORY object that maps to a folder that will be used for putting the dump files.

Oracle USER configuration

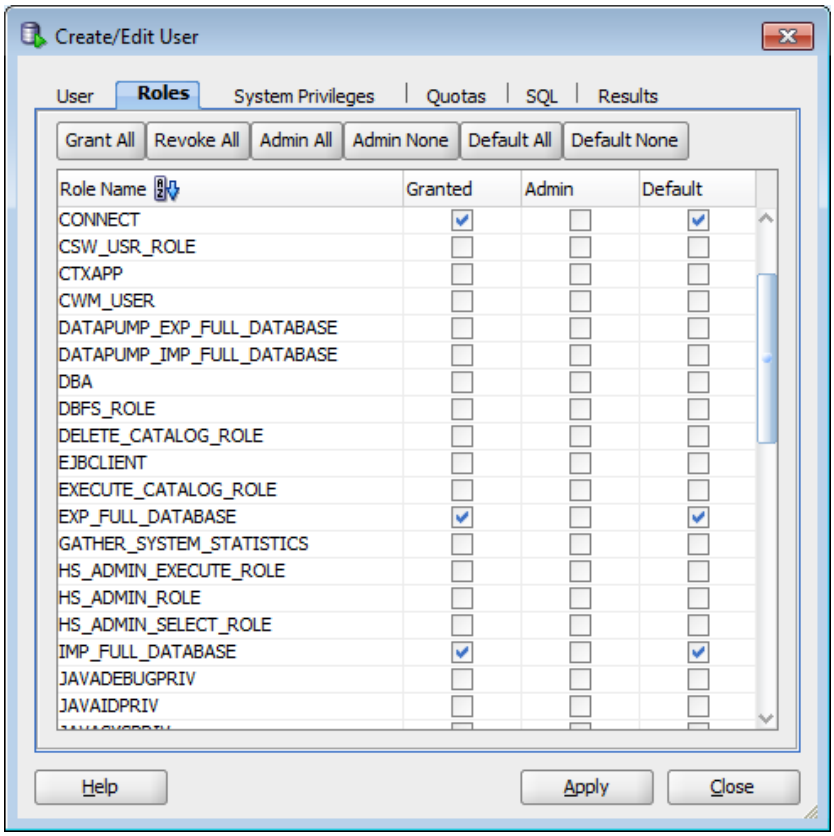
1. Launch Oracle SQL developer (other tools might be used) and connect to the Oracle database that hosts the original data to be duplicated with the USER SYSTEM (or any other USER that has the right to create USERs and to GRANT rights to these USERs).
2. From Oracle SQL developer, create an Oracle USER for exporting the data.



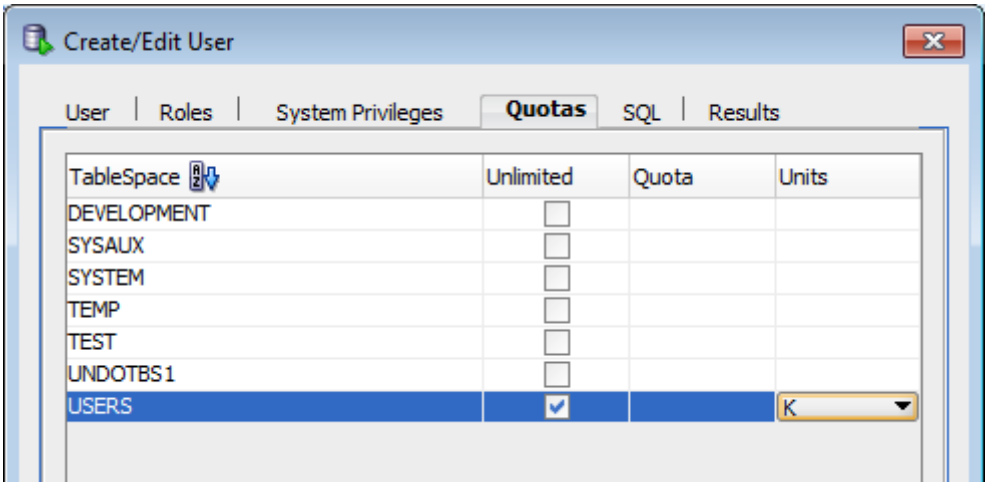
3. In the **User** tab, name the user: EXP_USER.



4. In the **Roles** tab, select **Granted** for the following roles:
   - CONNECT
   - EXP_FULL_DATABASE
   - IMP_FULL_DATABASE



5. In the **Quotas** tab, Quotas must be assigned on the tablespace hosting the data.



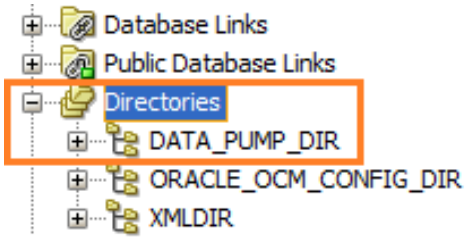
The resulting SQL script:

```
-- USER SQL
CREATE USER EXP_USER IDENTIFIED BY EXP_PWD
DEFAULT TABLESPACE "USERS"
TEMPORARY TABLESPACE "TEMP";
ACCOUNT UNLOCK;

-- ROLES
GRANT "CONNECT" TO EXP_USER ;
GRANT "DATAPUMP_IMP_FULL_DATABASE" TO EXP_USER ;
GRANT "DATAPUMP_EXP_FULL_DATABASE" TO EXP_USER ;

-- SYSTEM PRIVILEGES
GRANT CREATE ANY DIRECTORY TO EXP_USER ;

-- QUOTAS
ALTER USER EXP_USER QUOTA UNLIMITED ON USERS;
```

Note: there is an extra SYSTEM PRIVILEGE **CREATE ANY DIRECTORY** that was not mentioned before. It is not compulsory but nice to have if you want this user-to-be-created to be able to create DIRECTORIES for receiving the generated files.

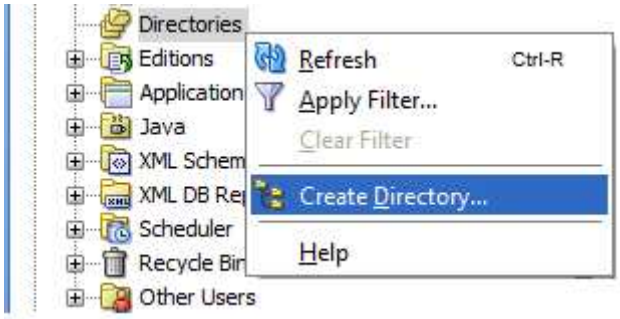
Oracle DIRECTORY object configuration

There is already a default DIRECTORY object in Oracle for using Data Pump with. It is called DATA_PUMP_DIR.

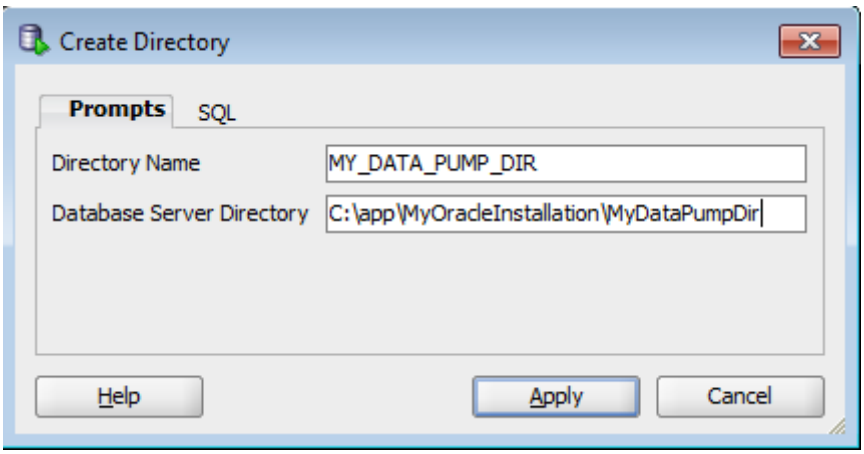


Since it could be mapped to a folder where writing is not allowed (for instance in a secured production environment), let us see how to create a new one where we are sure to be able to write and for which we know for sure that the remaining space available will be enough.

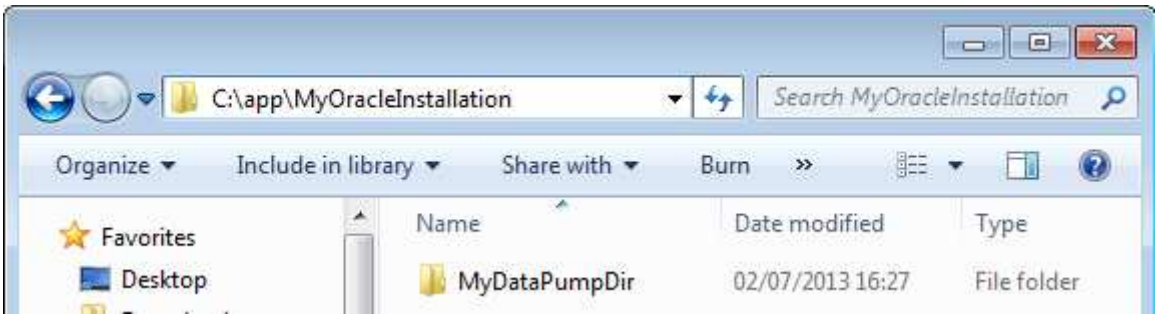
1. In Oracle SQL developer, with the same connection used to create the Oracle USER, right-click **Directories** node and select **Create Directory**.



2. Enter a name for the DIRECTORY object to be created (for example: MY_DATA_PUMP_DIR).
3. Enter the path to the actual folder for mapping the DIRECTORY created (for example: C:\app\MyOracleInstallation\MyDataPumpDir).



Make sure that this folder is writable in your context.


C:\app\MyOracleInstallation
Search MyOracleInstallation
Organize
Include in library
Share with
Burn
Favorites
Desktop
Name
Date modified
Type
MyDataPumpDir
02/07/2013 16:27
File folder

Initiating the export

This section describes how to launch the expdp export utility to create the dump files for each SCHEMA to duplicate each MEGA repository's data.

> **Note from Oracle documentation:**
> Do not invoke Export as SYSDBA, except at the request of Oracle technical support. SYSDBA is used internally and has specialized functions; its behavior is not the same as for general users.

expdp parameters explained

Here are the command and the parameters to use:

expdp

invokes the Data Pump export utility

user_name/user_password@address_of_Oracle_database_instance

specifies the Oracle USER that launches the export

must be followed by the USER's password

USER name and password are followed by the @ symbol and the Oracle database instance to export from. It could be seen as the "address" of the database or the way to identify it. There are more than one type of variables that can follow the @ symbol but we will show the example with one type only: a **CONNECT DESCRIPTOR** (since it is the one that will always be usable). See Oracle documentation for more details on CONNECT DESCRIPTORS.

The CONNECT DESCRIPTOR is of the following format:

(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP) (HOST = <DB server Id>) (PORT = <listener port number>)) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = <Oracle instance name>)))

DIRECTORY=

Specified the Oracle DIRECTORY object's name that will be the container of the dump file and the log file.

DUMPFILE=

The name of the resulting dump file. The dump file contains the data exported.

LOGFILE=

The name of the file that will log the actions that occur during the export.

SCHEMAS=

The name of the Oracle SCHEMAS to be exported. In our example the dump file will contain the data of only one SCHEMA.

Since a SCHEMA is supposed to match a MEGA repository (if MEGA recommendations have been followed), we will have as many dump files as the number of MEGA repositories in our environment (the SystemDb also counts for one repository).

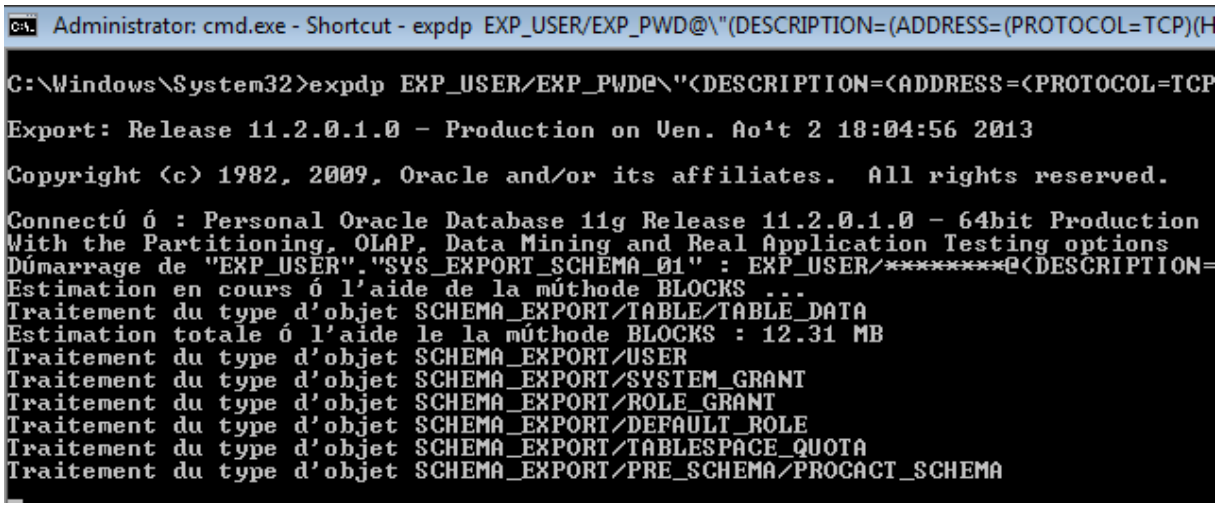
The actual export

MEGA recommends using one SCHEMA for hosting only one MEGA repository. This is for making Oracle administration tasks much easier. If, for any reason, this cannot be achieved, and many MEGA repositories are hosted in the same Oracle SCHEMA, a slightly different approach is to be used (see User data repositories export section).

SystemDb repository export

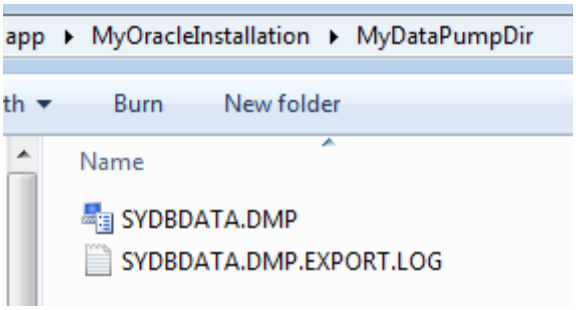
Here is the command used in our example, starting with the export of the SCHEMA used for the **SystemDb** repository. In this example the SCHEMA is named MEGASYSDB:

```
expdp EXP_USER/EXP_PWD@\"(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
(HOST = W-EDE) (PORT=1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = EDE2)))\" DIRECTORY = MY_DATA_PUMP_DIR DUMPFILE =
SYDBDATA.DMP LOGFILE = SYDBDATA.DMP.EXPORT.LOG SCHEMAS = MEGASYSDB
```



The export starts

Once it is done the data and log files are created in the directory.



User data repositories export

Now we will take care of the export for the SCHEMA(s) hosting the data corresponding to the User data repositories. To do this, refer to the export technique that has just been described. Only change the names for the files (dump and log) and use the correct corresponding SCHEMA.

Let us see how the command would look like the MEGA repositories hosting the MEGA User data (i.e. repository **Adventure** of the environment **Demonstration**). In this example the SCHEMA is named MEGADATA1:

Here is the command used (same as before with changes highlighted):

```
expdp EXP_USER/EXP_PWD@\"(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
(HOST = W-EDE) (PORT=1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = EDE2)))\" DIRECTORY = MY_DATA_PUMP_DIR DUMPFILE =
MEGADATA1.DMP LOGFILE = MEGADATA1.DMP.EXPORT.LOG SCHEMAS = MEGADATA1
```

Repeat the operation **for each MEGA repository**.

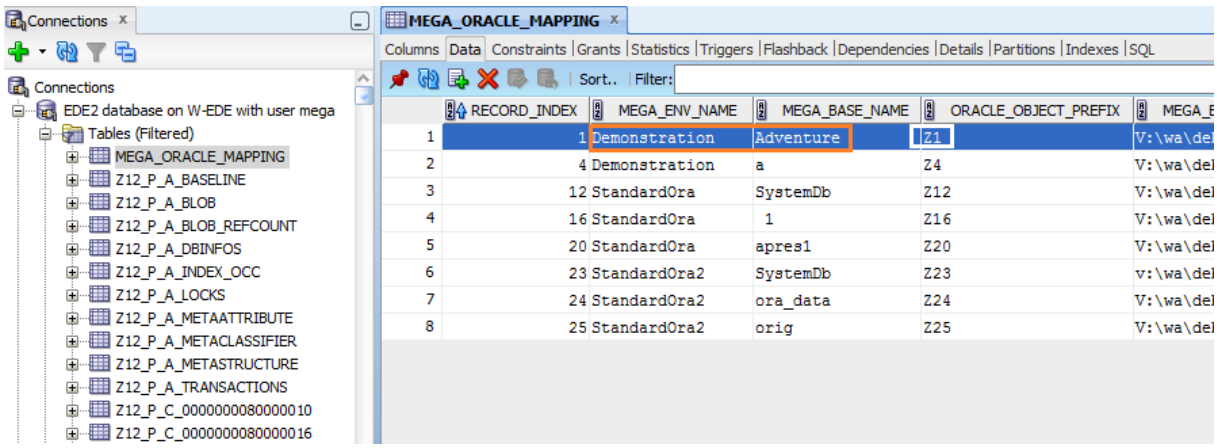
Special case (not recommended): many repositories for one SCHEMA

1. In that case, identify the repository to be exported.
2. Change the expdp command so that it filters only the tables corresponding to the repository to be exported.

Identifying the set of data corresponding to the MEGA repository

1. In SQL Developer, browse the SCHEMA of the original data.
2. Look for the table called MEGA_ORACLE_MAPPING.
3. Select the table name.
4. In the right pane select the **Data** tab.

   Here, we are interested in the value of ORACLE_OBJECT_PREFIX for the row where MEGA_ENV_NAME is **Demonstration** and MEGA_BASE_NAME is **Adventure**.



RECORD_INDEX	MEGA_ENV_NAME	MEGA_BASE_NAME	ORACLE_OBJECT_PREFIX
1	Demonstration	Adventure	Z1

The value is 'Z1'.

Filtering the export to include only that specific repository data

To filter the export so that it contains only the data of the **Adventure** repository, you need to provide the Data Pump export utility with something that says:

"In my export file, I want only the tables starting with 'Z1' ". To do that, you need to add the following instruction at the end of the command:

```
[INCLUDE=TABLE:]
```

Because the prefix used for the tables for the Adventure repository starts with 'Z1', it means that the tables we are interested in really start with 'Z1_'.

The underscore character ('_') is a special character in SQL queries for Oracle meaning "any character". So when you ask the export utility to export tables starting with 'Z1_', it will understand tables starting with 'Z1'. So table which names start with 'Z12' will also be exported…

➔ There is a work around: the ESCAPE clause. With this clause, you can tell Oracle that a special character (here you will use '!') will be used to make Oracle interpret the '_' literally, rather than as a special pattern matching character.

Here is the command that could be used:

```
expdp EXP_USER/EXP_PWD@\"(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
(HOST = W-EDE) (PORT=1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = EDE2)))\" DIRECTORY = MY_DATA_PUMP_DIR DUMPFILE =
MEGADATA1.DMP LOGFILE = MEGADATA1.DMP.EXPORT.LOG SCHEMAS = MEGADATA1
INCLUDE = TABLE:\"LIKE 'Z1!_%' ESCAPE '!'\"
```

The set of data **wouldn't be complete** if you forget to include the table **MEGA_ORACLE_MAPPING** during export. This needs not to be taken care of when exporting a full SCHEMA in the situation of a one to one SCHEMA – MEGA repository.

To include the MEGA_ORACLE_MAPPING table in the exported file, you need to change the way of filtering as the [INCLUDE=TABLE:] clause cannot handle the OR operator.

You could use a filtering query:

```
expdp EXP_USER/EXP_PWD@\"(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
(HOST = W-EDE) (PORT=1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = EDE2)))\" DIRECTORY = MY_DATA_PUMP_DIR DUMPFILE =
MEGADATA1.DMP LOGFILE = MEGADATA1.DMP.EXPORT.LOG SCHEMAS = MEGADATA1
INCLUDE = TABLE:"IN (SELECT TABLE_NAME FROM ALL_TABLES WHERE
TABLE_NAME='MEGA_ORACLE_MAPPING' OR TABLE_NAME LIKE 'Z1!_%' ESCAPE
'!')"
```

There is still a problem with this last expdp command. It will not work as it is because of all the special characters that need to be escaped in that string:

```
"IN (SELECT TABLE_NAME FROM ALL_TABLES WHERE TABLE_NAME =
'MEGA_ORACLE_MAPPING' OR TABLE_NAME LIKE 'Z1!_%' ESCAPE '!')"
```

to make it possible for the operating system's command prompt to pass a meaningful string to the expdp utility.

It is getting too complicated.

At that point you can use an expdp special feature that allows you to pass parameters in an easier way: the [PARFILE=] parameter. It is used to point to a file that contains all the parameters to pass to the expdp command.

It is used like this:

```
expdp EXP_USER/EXP_PWD@\"(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
(HOST = W-EDE) (PORT=1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = EDE2)))\" PARFILE = "C:\parm.txt"
```

having the parm.txt file containing:

```
DIRECTORY = MY_DATA_PUMP_DIR

DUMPFILE = MEGADATA1.DMP

LOGFILE = MEGADATA1.DMP.EXPORT.LOG

SCHEMAS = MEGADATA1

INCLUDE = TABLE:"IN (SELECT TABLE_NAME FROM ALL_TABLES WHERE
TABLE_NAME='MEGA_ORACLE_MAPPING' OR TABLE_NAME LIKE 'Z1!_%' ESCAPE
'!')"
```

Initiating the import

Now that the data is in a "transportable format" (i.e. dump files), we will take care of recreating a set of duplicated data based on it.

Since we saw in the export part of this document how to restrict the data contained in the dump file to contain only what is needed, we will assume that the Oracle dump files to be imported need no filtering.

Location of the target Oracle database

In many cases, the import phase will not take place in the same Oracle environment as the one used for the export.

Let us consider the scenario in which nothing is the same in the source and the target Oracle environments:

- The machine hosting the Oracle database is different.
- The Oracle service_name is not the same.
- The data pump DIRECTORY will not be the same.
- The SCHEMA in which the exported data are to be put in has a different name.
- The TABLESPACE of the source SCHEMA and the target SCHEMA have different names. We have not gone through the TABLESPACE concept yet, but we will explain it further.
- The Oracle USER that will be used for importing is not the same (here the User will be called IMP_USER). The GRANTS needed are very similar to the ones needed for exporting with expdp. See Oracle USER configuration section.

impdp parameters explained

The impdp utility is symmetric to the expdp utility. So for example, let us see a quick example of how an import command would look like (changes are highlighted):

```
impdp IMP_USER/IMP_PWD@\"(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
(HOST = W-EDE) (PORT=1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = EDE2)))\" DIRECTORY = DATA_PUMP_DIR DUMPFILE =
MEGADATA1.DMP LOGFILE = MEGADATA1.DMP.IMPORT.LOG SCHEMAS = MEGADATA1
```

Let us see the impdp specific parameters that can be used when the SCHEMA and the TABLESPACE are not the same.

Let us say that the origin SCHEMA is called **MEGADATA1** and the one available in the target Oracle environment is called **MEGAUSER**.

Also, the origin TABLESPACE is called **MEGA_TABLESPACE** and the TABLESPACE in the target Oracle environment is called **MEGAUSER_TBLSPC**.

REMAP_SCHEMA=

Used to tell Oracle that during the import, it should put the data extracted from **MEGADATA1** and put it into **MEGAUSER**

Example: REMAP_SCHEMA=source_schema:target_schema

REMAP_SCHEMA=MEGADATA1:MEGAUSER

See Oracle documentation for more details

REMAP_TABLESPACE=

Used to tell Oracle that during the import, it should put the data extracted from **MEGADATA1** that was in the TABLESPACE **MEGA_TABLESPACE** and put it into **MEGAUSER**'s TABLESPACE **MEGAUSER_TBLSPC.**

Example: REMAP_TABLESPACE=source_tablespace:target_tablespace

REMAP_TABLESPACE=MEGA_TABLESPACE:MEGAUSER_TBLSPC

See Oracle documentation for more details

Here is the command used (for a host called OHX03 and a service_name called PROD12)

```
impdp IMP_USER/IMP_PWD@\"(DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)
(HOST = OHX03) (PORT=1521)) (CONNECT_DATA = (SERVER = DEDICATED)
(SERVICE_NAME = PROD12)))\" DIRECTORY = DATA_PUMP_DIR DUMPFILE =
MEGADATA1.DMP LOGFILE = MEGADATA1.DMP.IMPORT.LOG SCHEMAS = MEGADATA1
REMAP_SCHEMA= MEGADATA1:MEGAUSER REMAP_TABLESPACE= MEGA_TABLESPACE:
MEGAUSER_TBLSPC
```

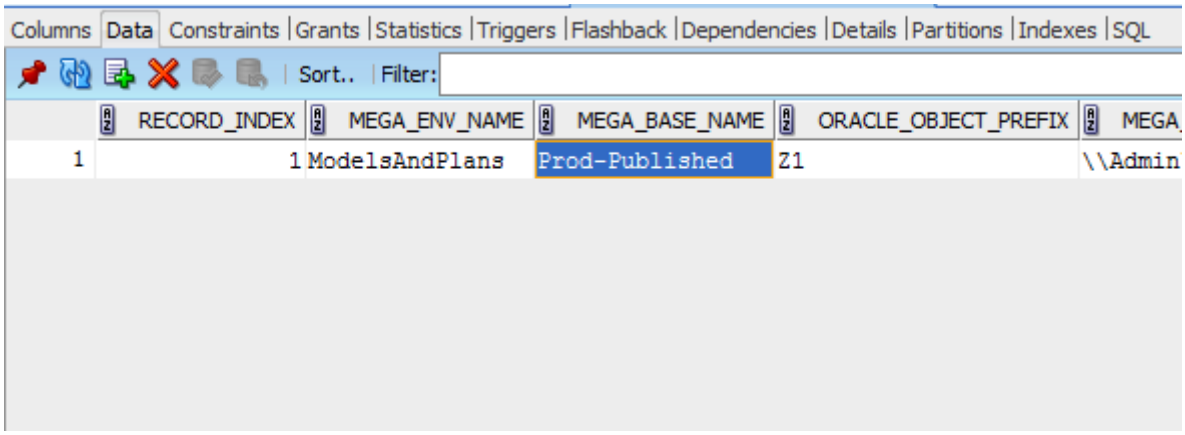
When duplicating a repository in an environment – Expert mode

This section is only if you are very confident about your Mega and RDBMS skills, since you have to modify data directly in some tables of your schema.

In case you want, within an environment, to duplicate a specific repository, you need to tweak the data manually in two tables of your restored schema.

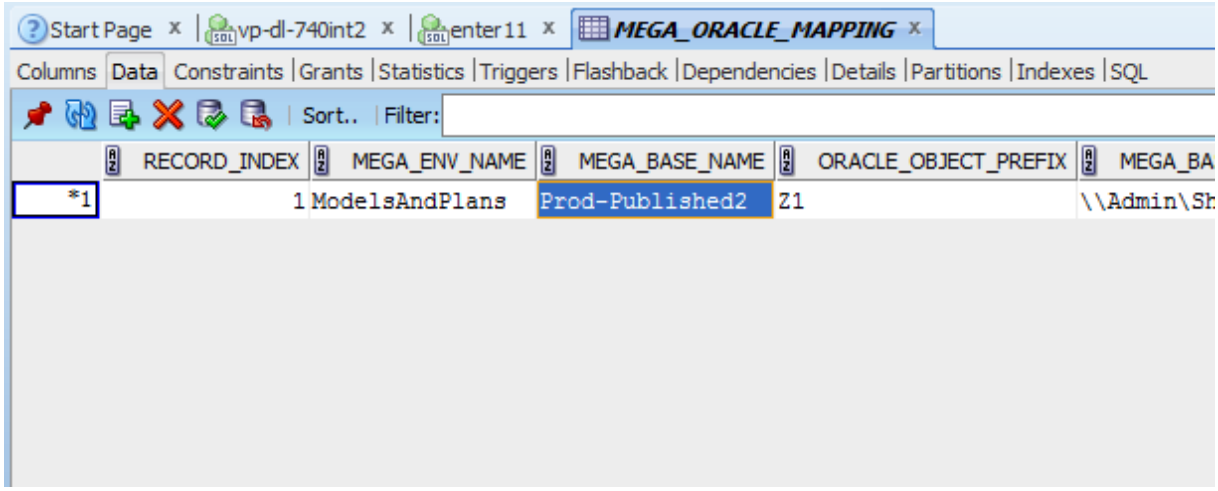
Proceed as follows:

1. Using for example SQL Developer, locate the "MEGA_ORACLE_MAPPING" table of your schema, and the line of your repository:

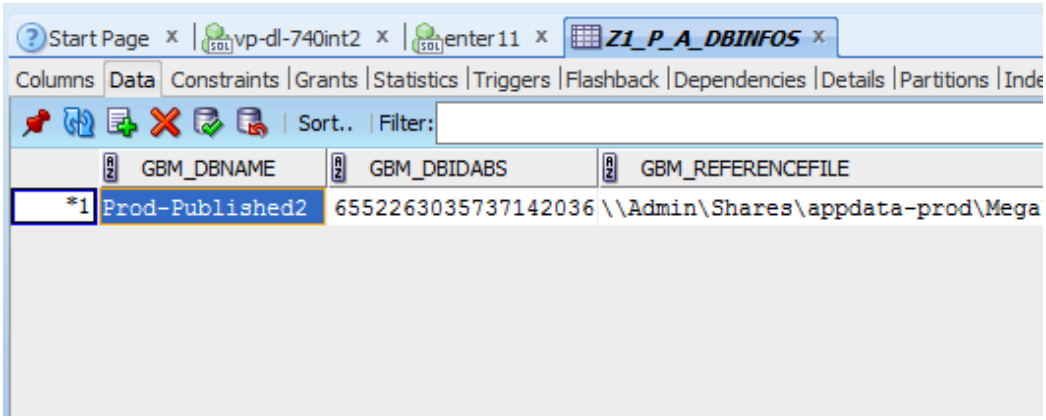


2. In the **MEGA_BASE_NAME** field of that line, enter the name of your duplicate, i.e. how you want it to appear in your environment.

   (for example here: "Prod-Published2")

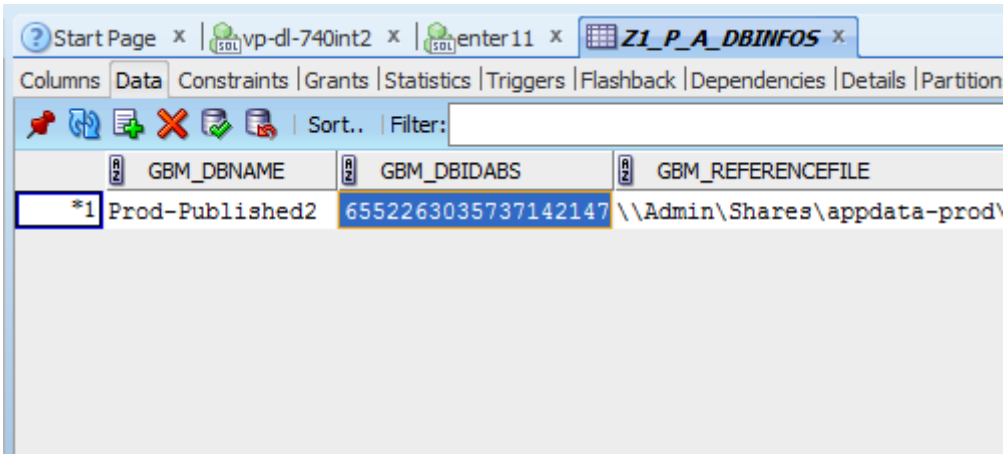


3. Commit the change and close the table.
4. Go to table that ends with "*_P_A_DBINFOS", '*' being the prefix of your repository (in this example, the prefix is "Z1", as shown in the previous screenshots), and locate the line of your repository.
5. In **GBM_DBNAME** field enter the same name as before (for example here: "Prod-Published2").



6. In **GBM_DBIDABS** field, which is the unique identifier of the repository within your environment, modify its value, and make sure that it is unique for all other repositories, so you need to check in all schemas.

   Make sure that when you change one or two characters, it will create a string that is not used by any other (for example here, we modified the last 3 digits from "036" to "147").



7. Commit your updates and close the table.

RDBMS Environment Duplication - 1 - SQL Server

The goal of this document is to give detailed instructions as to how duplicating a MEGA environment when it is hosted on an **SQL Server RDBMS**.

We will take the hypothesis that the new databases of the duplicated environment are hosted on a separate SQL Server instance. This way, it gives the appropriate details in case you move data from one server to another.

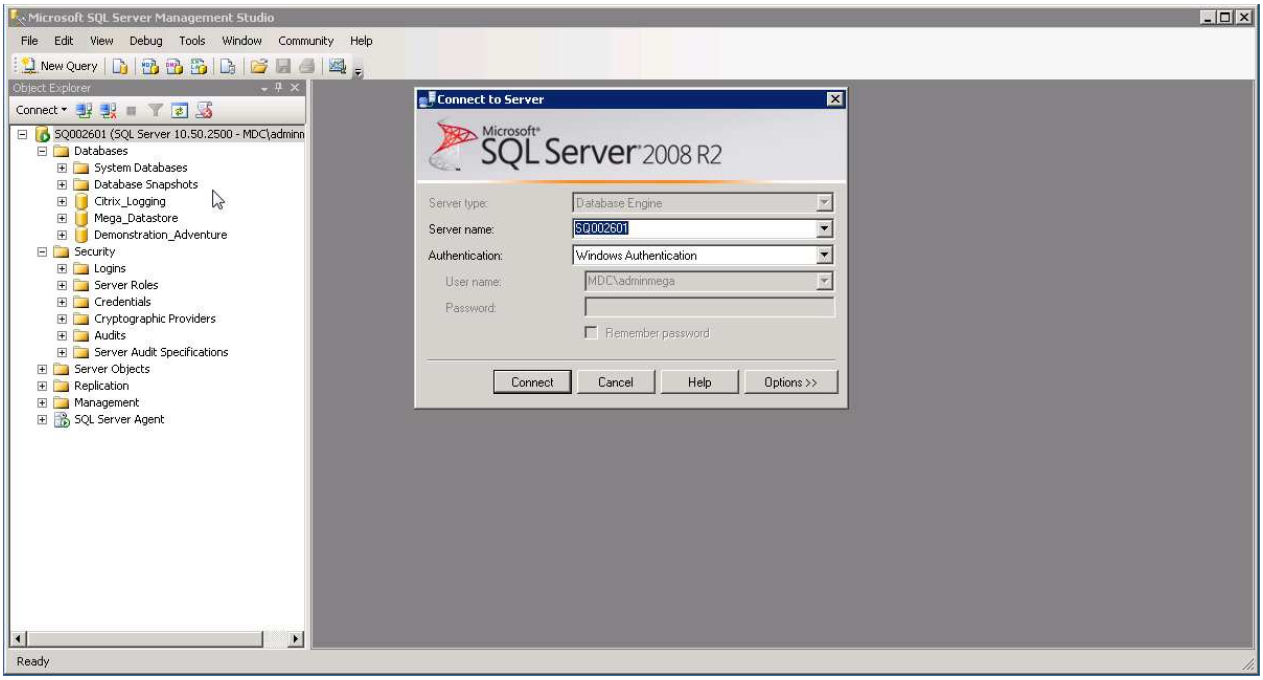
PREREQUISITES

The SQL Server account

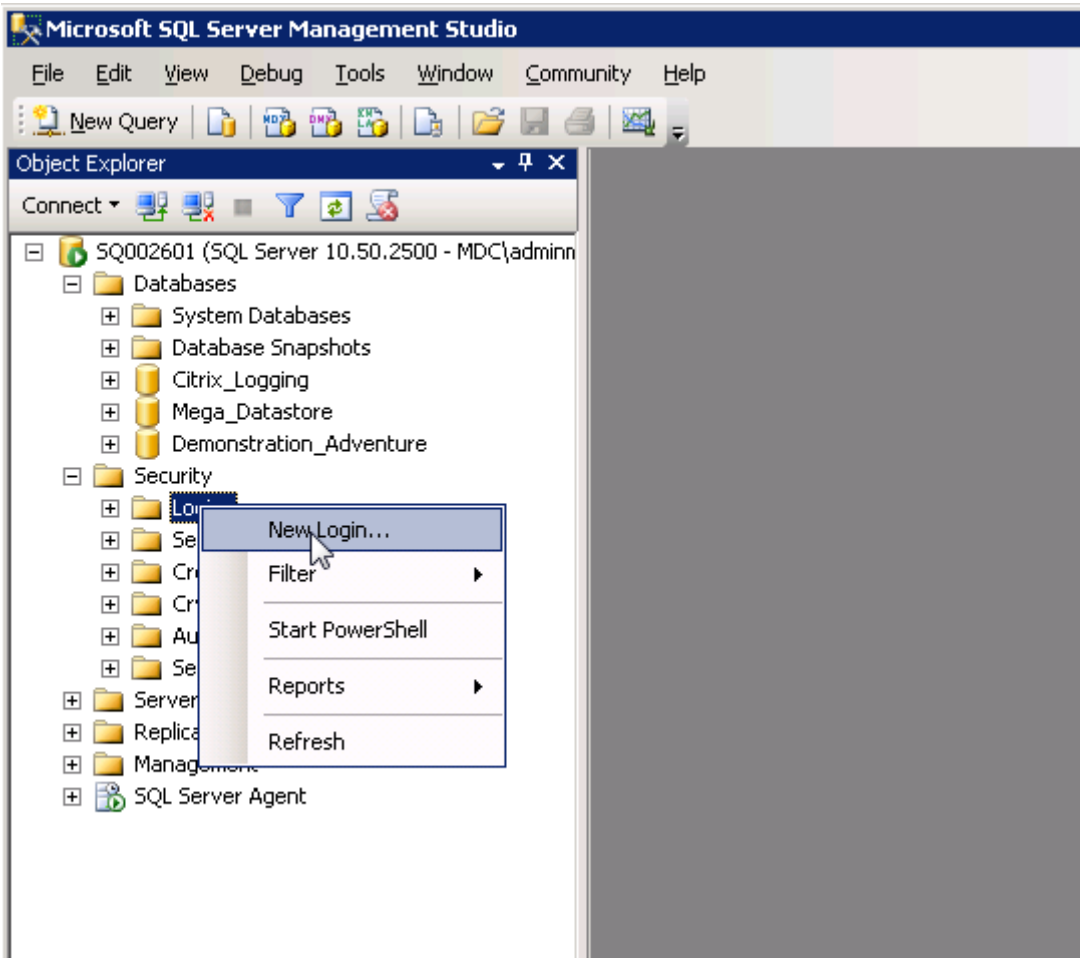
Before you start, you have to make sure that, where the duplicated databases are going to be hosted, you have a user with the proper rights, either:

- you are given the sysadmin right (the super admin) on the instance, and you perform those actions yourself, or
- you have to ask the DBA to create it and grant it.

1. Launch the "Microsoft SQL Server Management Studio" tool.
2. Connect to the SQL Server instance with the user having the sysadmin right.
3. If your Windows account is the one having the sysadmin right, stay in « Windows Authentication » mode. Otherwise, switch to "SQL Server Authentication", and provide the username and password. The field "Server Name" is the name of the instance.



4. In the left pane, expand **Security** file.
5. Right-click **Logins** and select **New Login**.

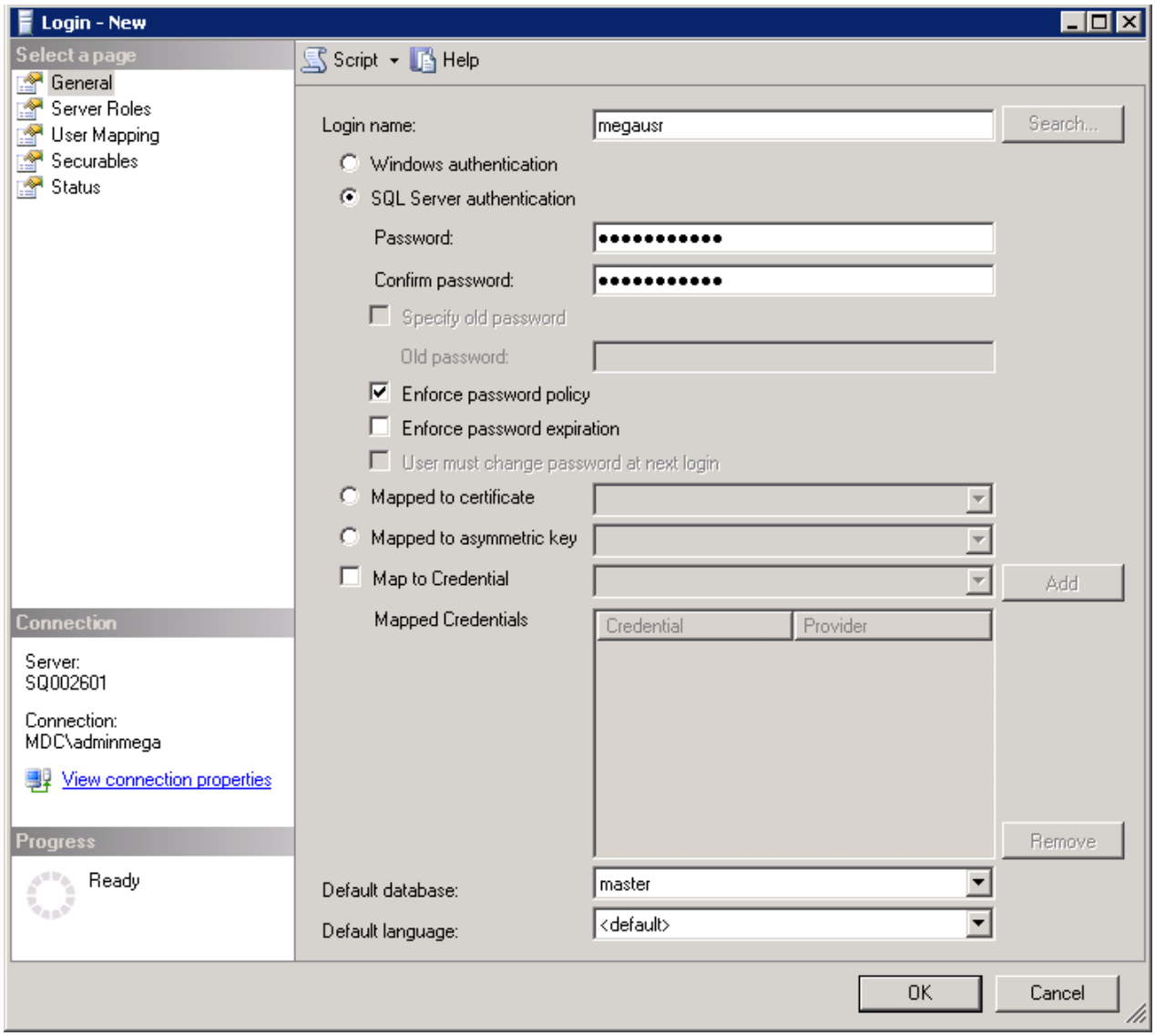


The **Login - New** window appears and displays and the **General** page.

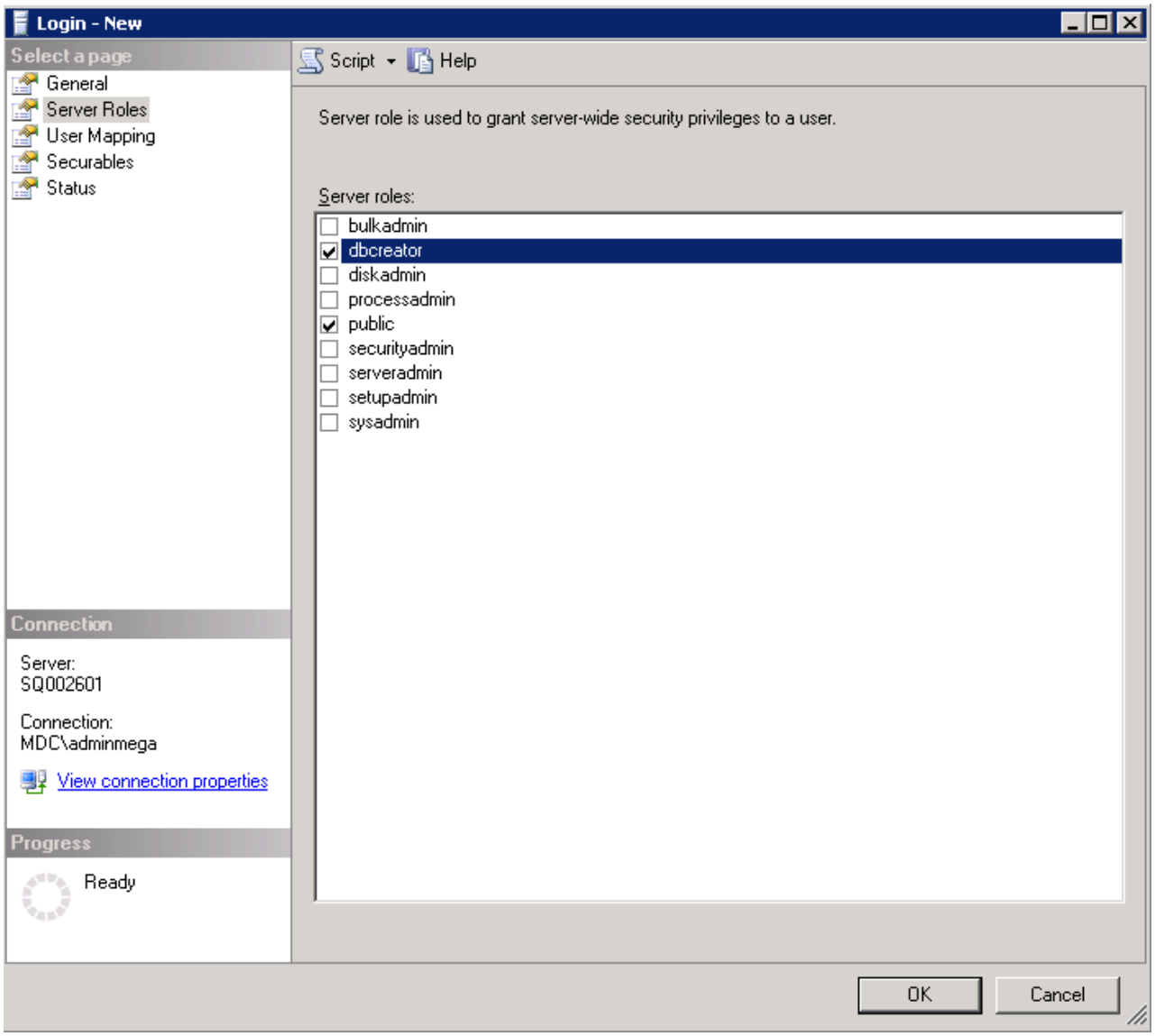
6. In the right pane:
   a. In the field **Login name** enter the login, for exemaple « megausr ».
   b. Select **SQL Server authentication** mode.
   c. In the field **Password**, enter a password that complies with security requirements, for example :

      `Mega2k8!usr`

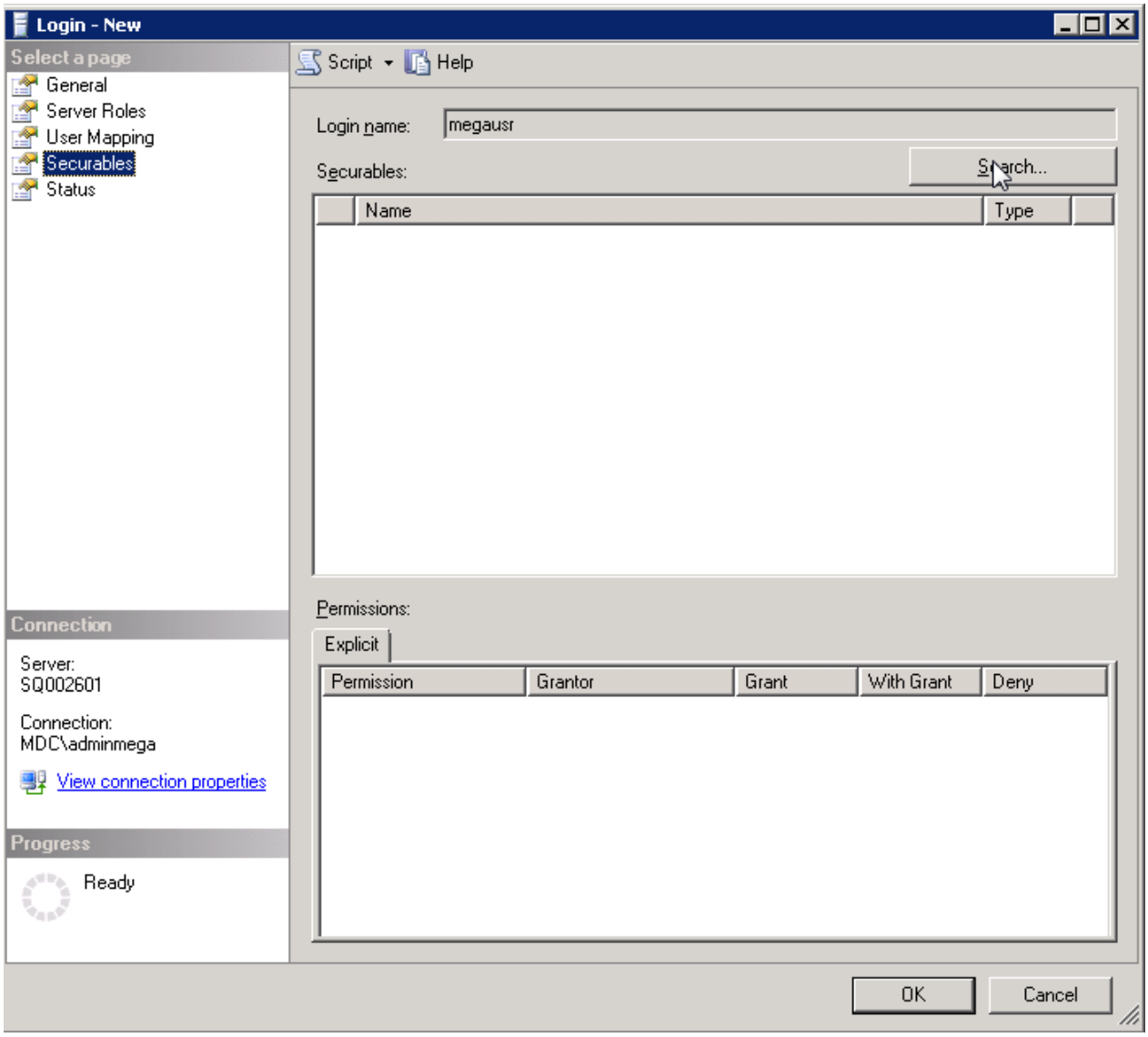
7. Unselect **Enforce password expiration** and User must change password at next login.



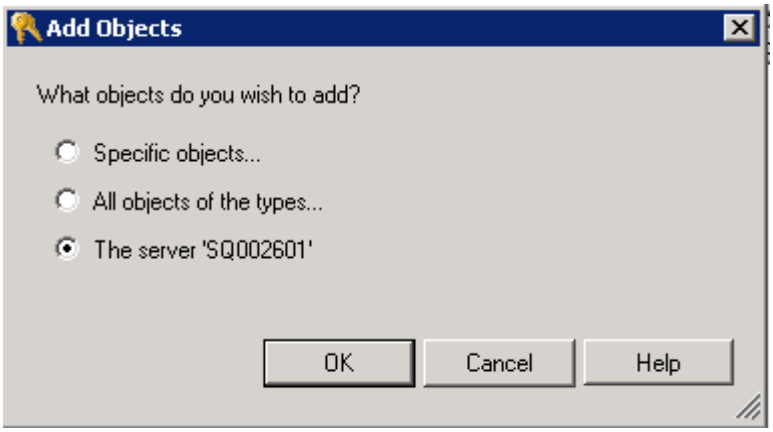
8. In the **Select a page** pane, select **Server Roles**.
9. In the right pane select **dbcreator**.



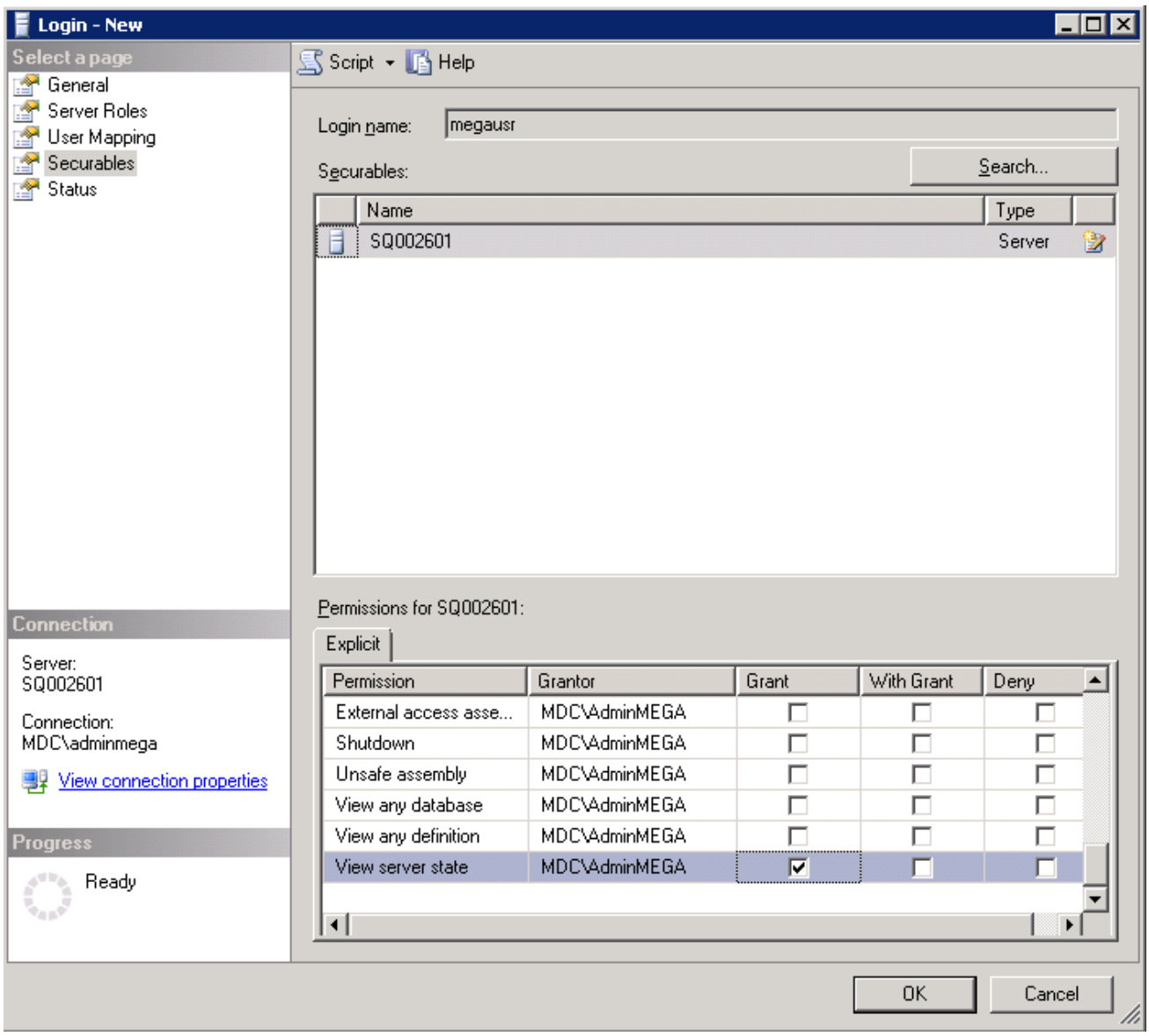
10. In the **Select a page** pane, select **Securables**.
11. In the right pane, click **Search**.



12. Select the instance to browser for its objects. Here we were on instance SQL002601 :



13. Click **OK**.
14. In the **Explicit** tab, for the **View Server state** permission select « Grant ».



15. Click **OK** to create the user.

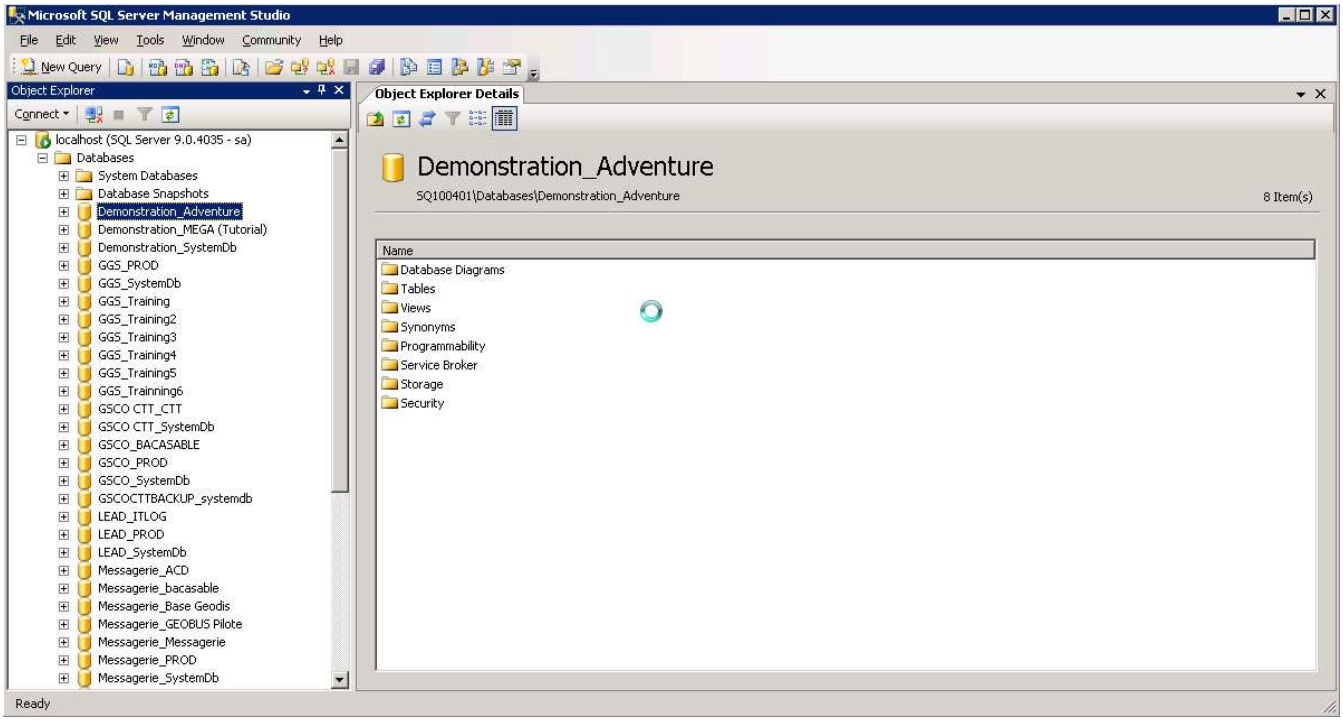
Backup and file transfer

1. Connect to the server hosting the source database.

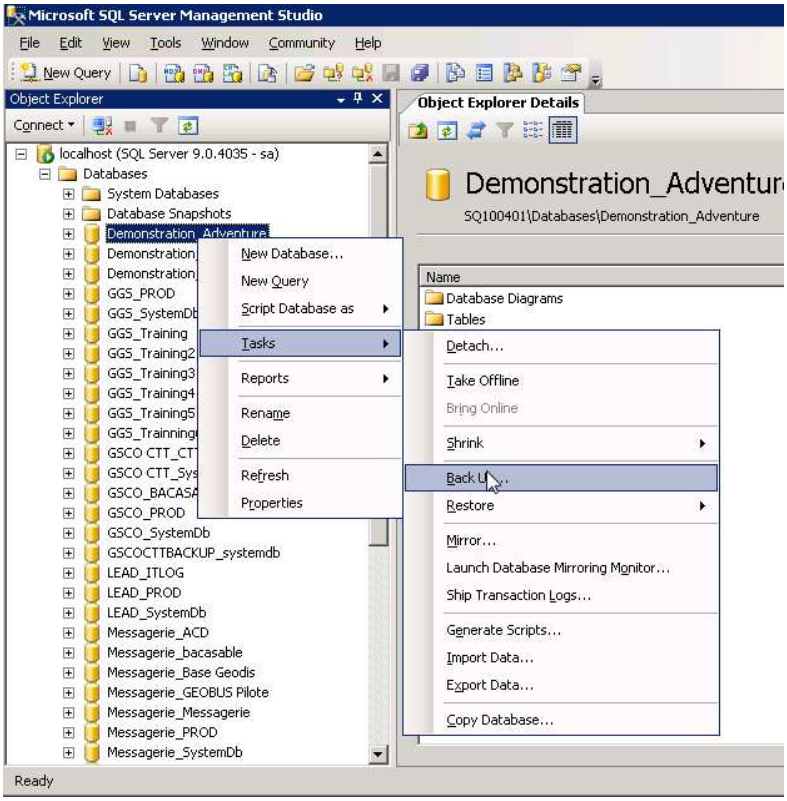
   Example: SQ100401.

2. Launch **Microsoft SQL Server Management Studio**.

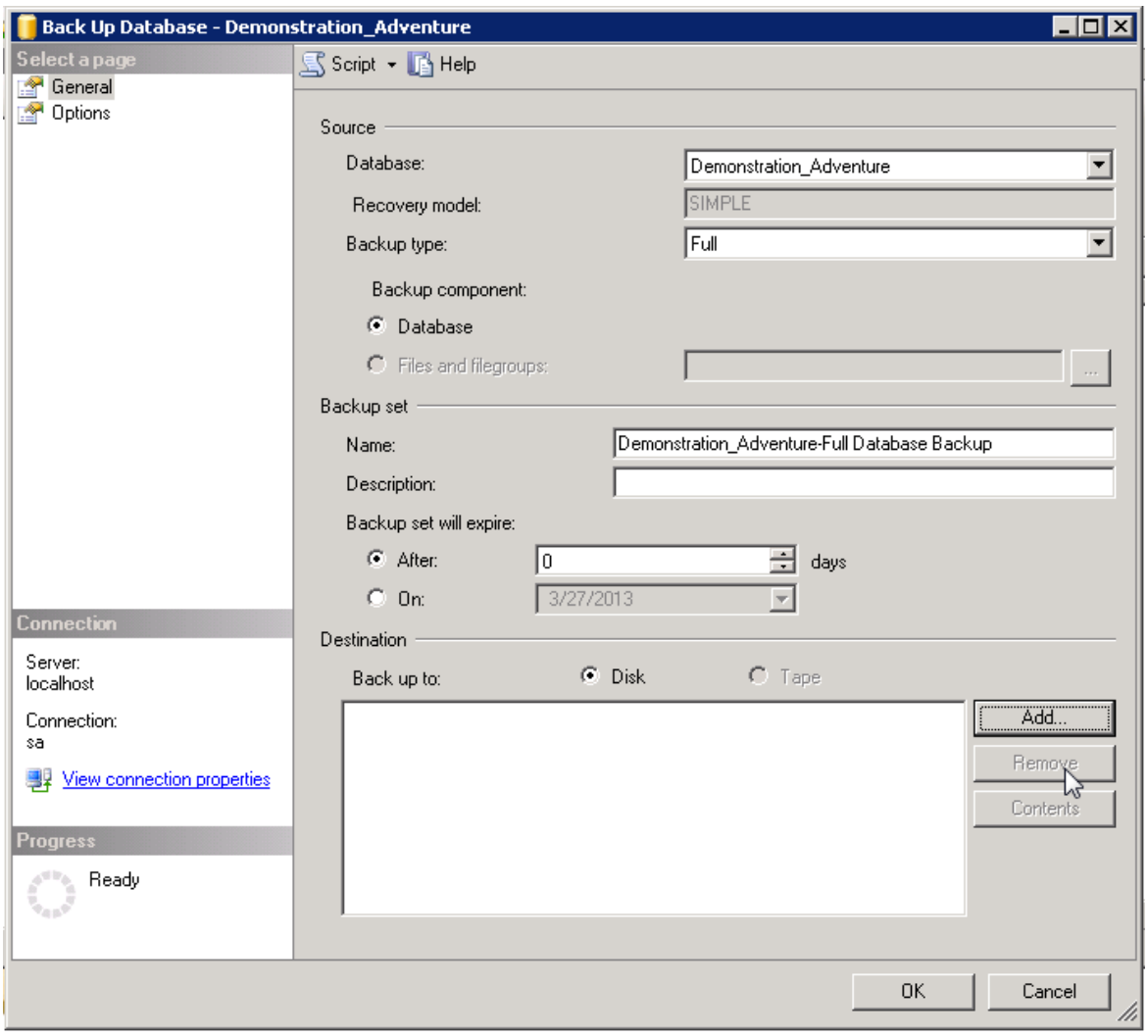
   If possible, connect with a Windows user that will have been granted sysadmin rights on the instance. Otherwise, you might encounter issues when creating the backup file to a specific location, or later, when you need to restore the database on the target instance.



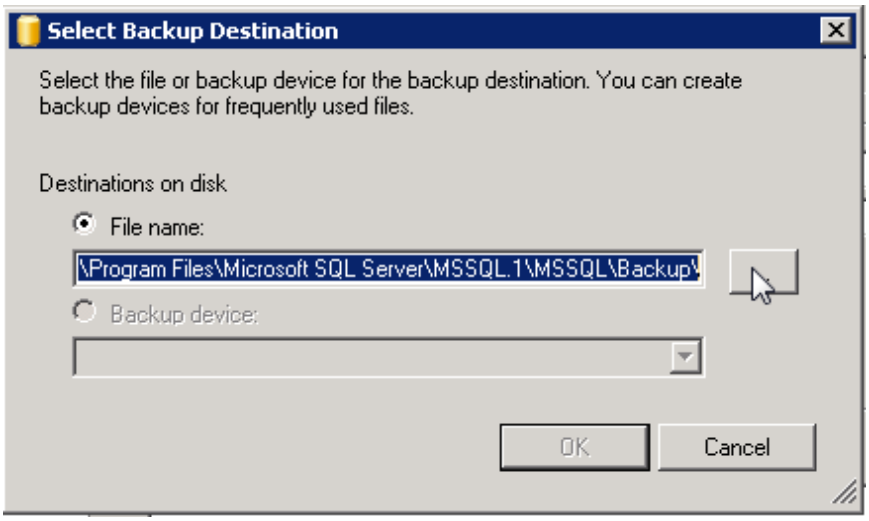
3. To make a backup of the source database (for example, Demonstration_Adventure), right-click the database and select **Tasks > Back Up**.



The **Back Up Database** window appears.

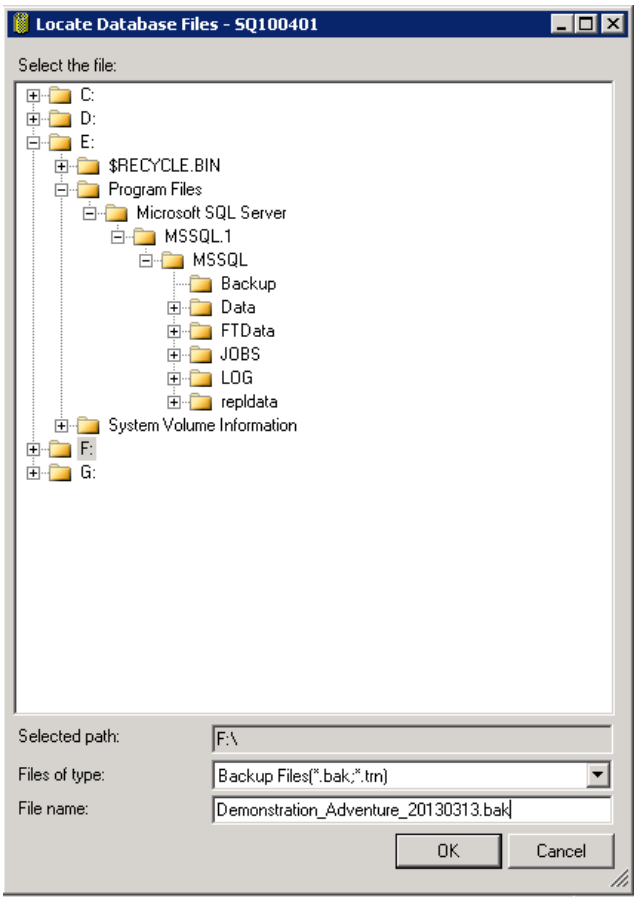


4. In the right pane, in the **Destination** pane, make sure that the destination list is empty. If it isn't, select each line and click **Remove**. Once it is empty, click **Add**.
5. In the **Select BackUp Destination**, click ....

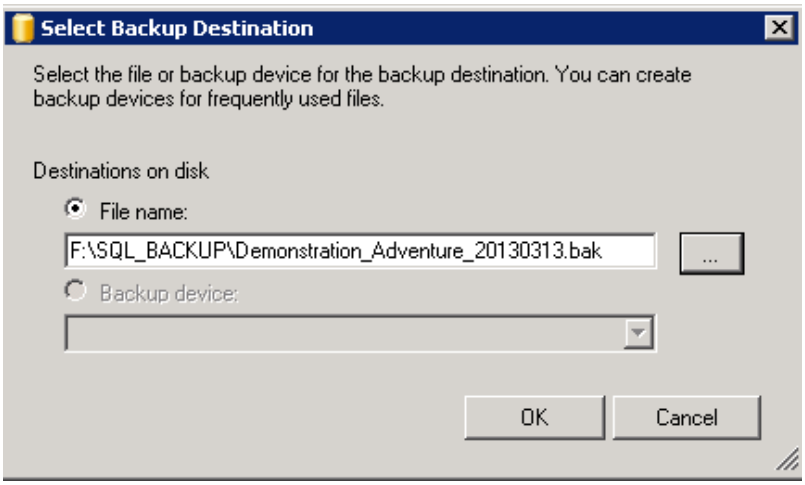


6. Choose a location where you know that the user you authenticated with, has rights to write on. In this example in « F:\SQL_BACKUP » of the F drive, and give the name of the backup file to create (here Demonstration_Adventure_20130313.bak).

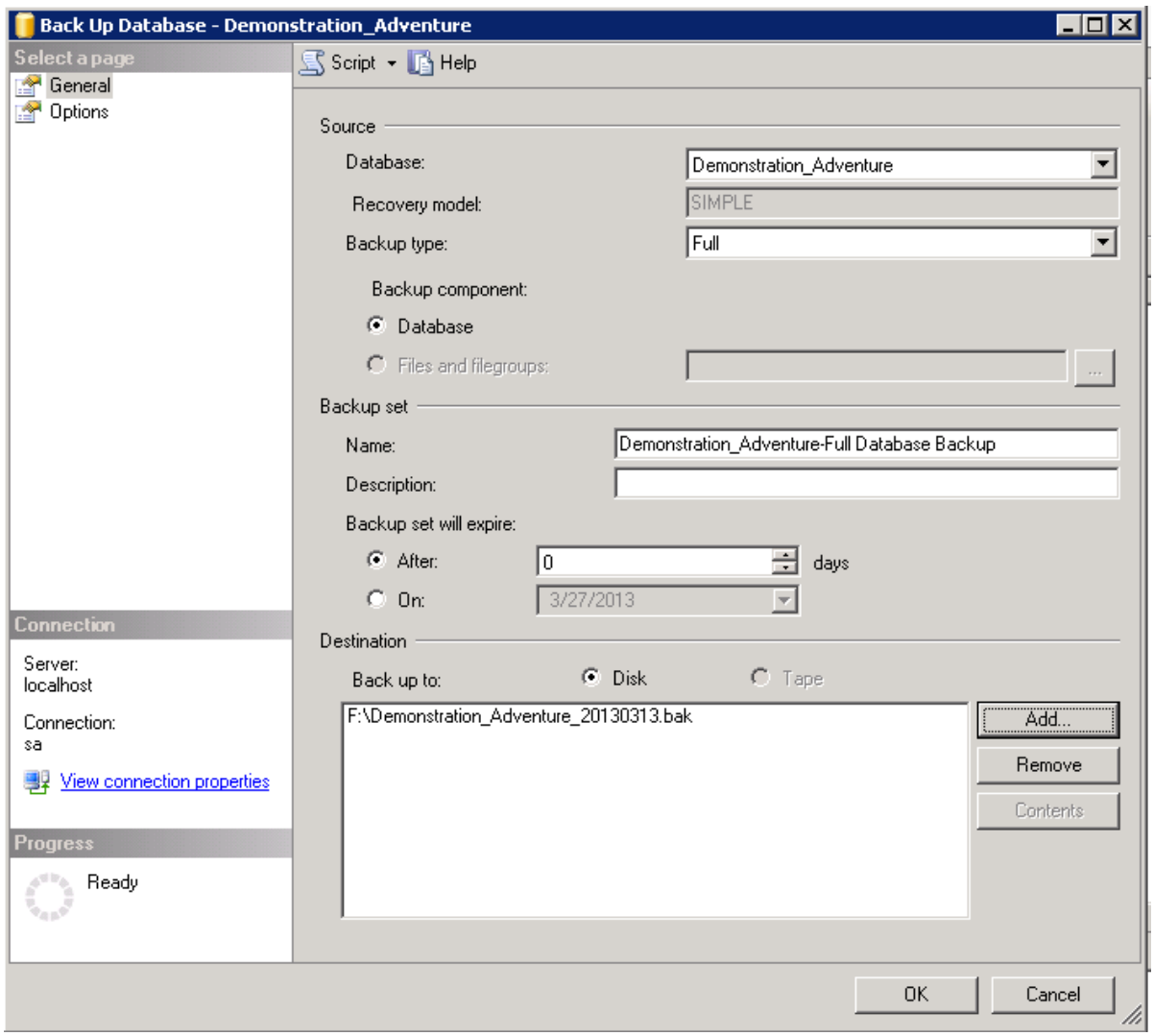
Please note that the known format of a full backup in SQL Server is **.BAK** files. You have to explicitely put it in the file name, otherwise it will not have any format.



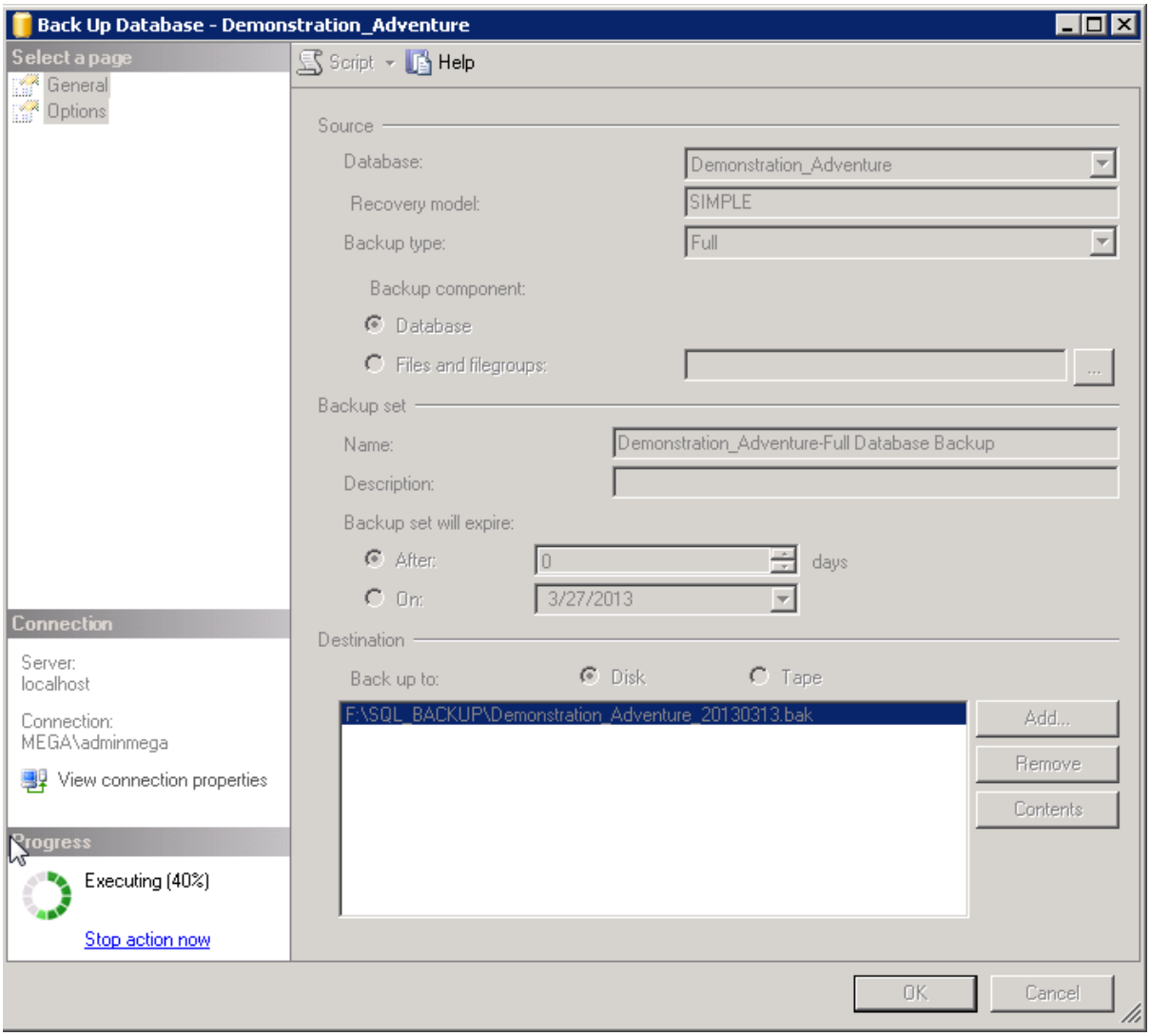
7. Click **OK**.



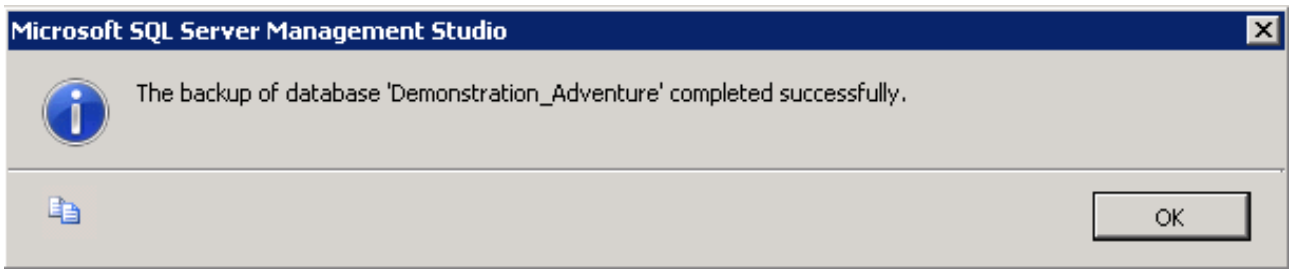
8. Click **OK**.



9. Click **OK** and check the progress of the restore by looking at the left-bottom section of this window (here, we are 40% done with the restore).



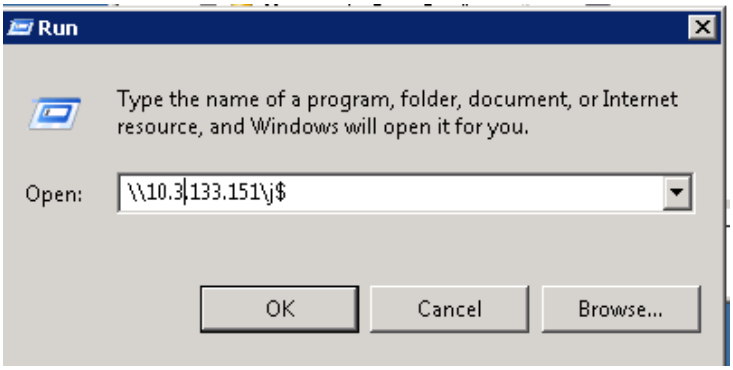
10. Check that the database was fully restored, and click **OK**.



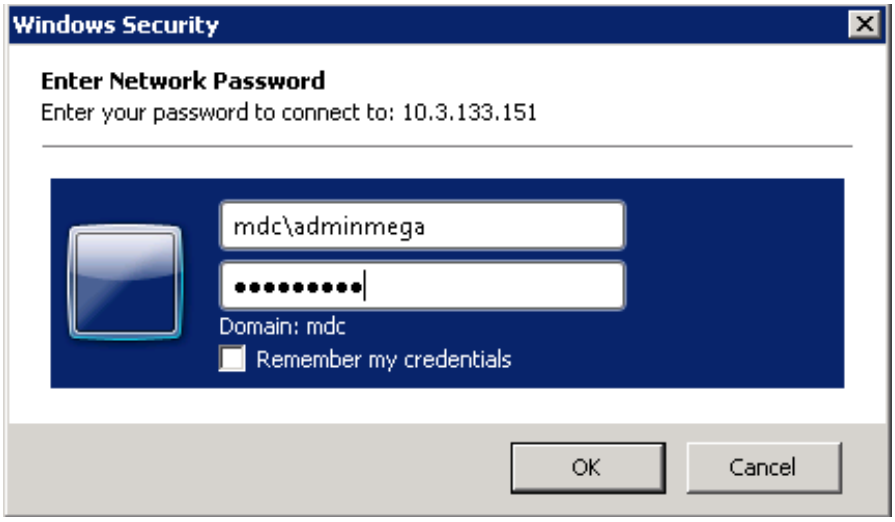
11. Transfer the backup file created on the SQL Server server, to the target server (for example, here it is SQL002601).

In this example, the drive hosting the databases on the target instance, as well as the daily backups, is the J drive.

We used its IP address instead of its name, as we were working over two different domains, that did not see each other.

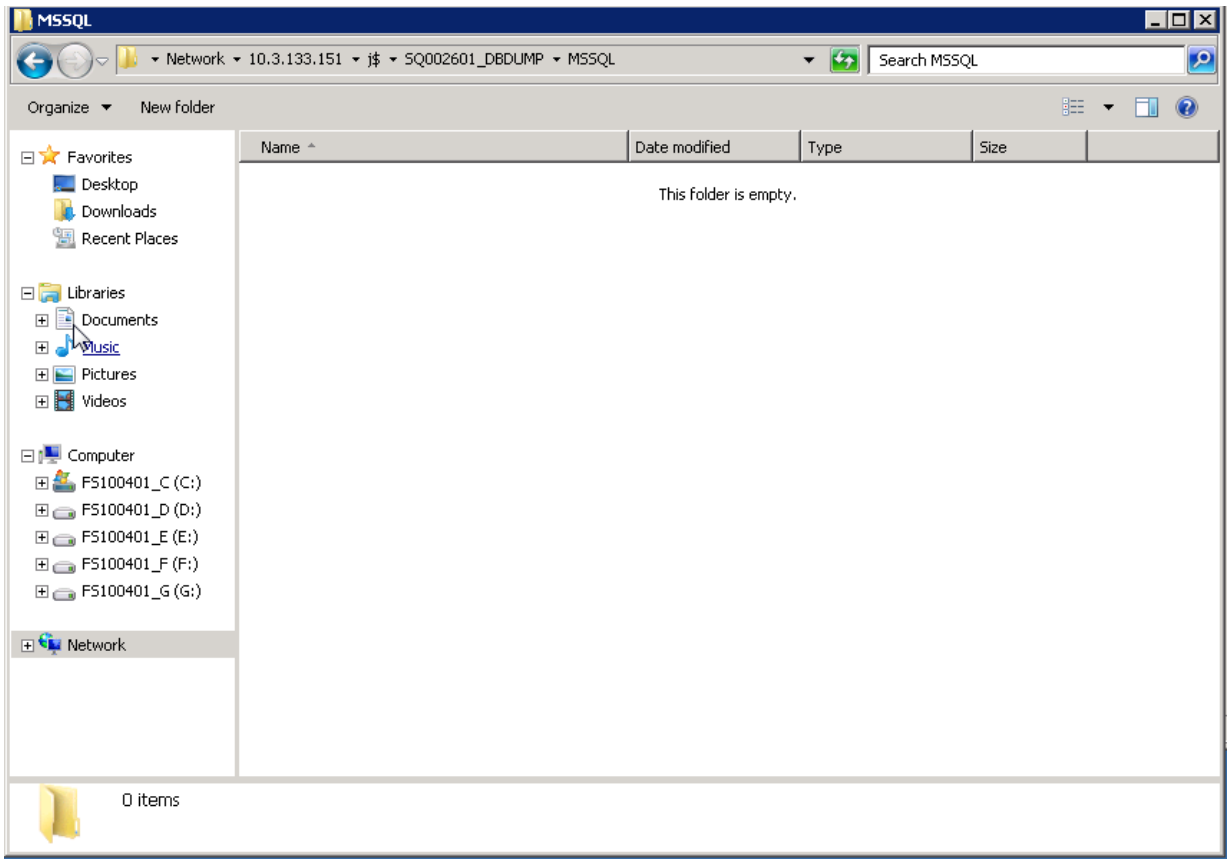


This is also the reason why we had to authenticate with another user.

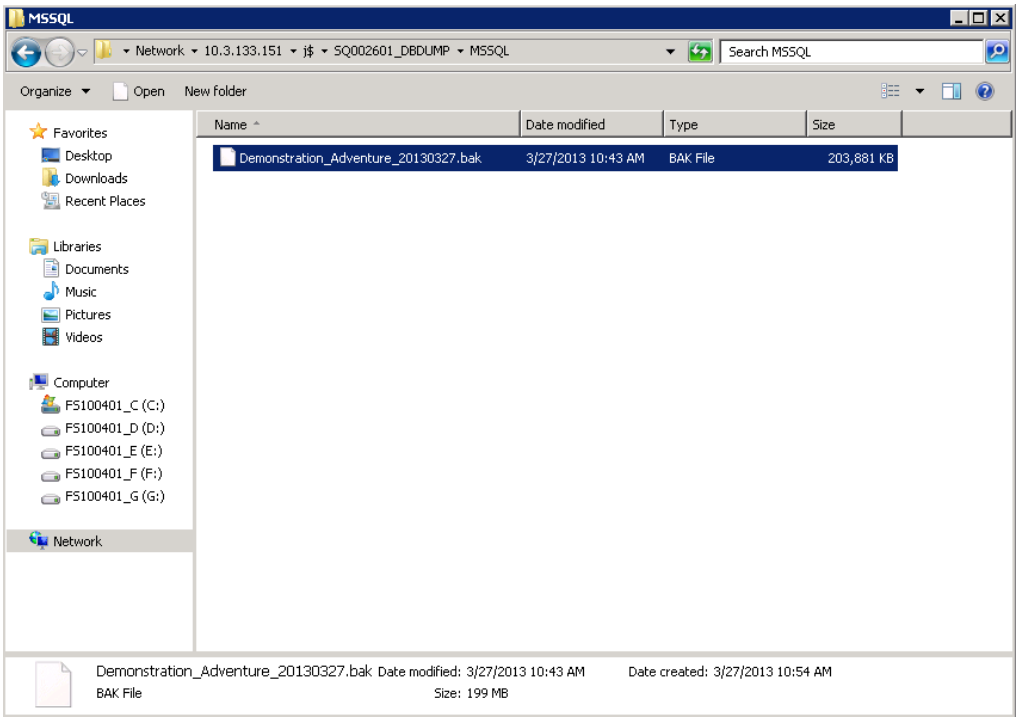


12. Go to the subfolder hosting the daily backups.

    (for example: « SQ002601_DBDUMP\MSSQL » on the J drive)

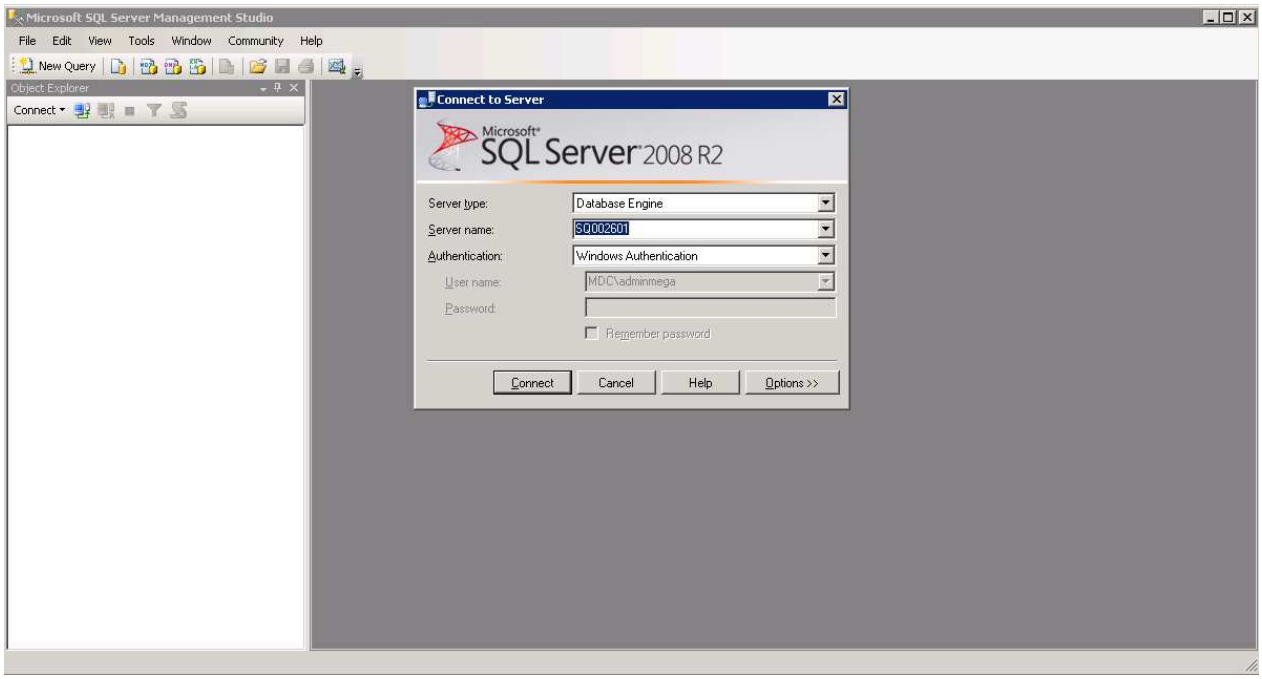


13. Copy the file from the source folder to this one.

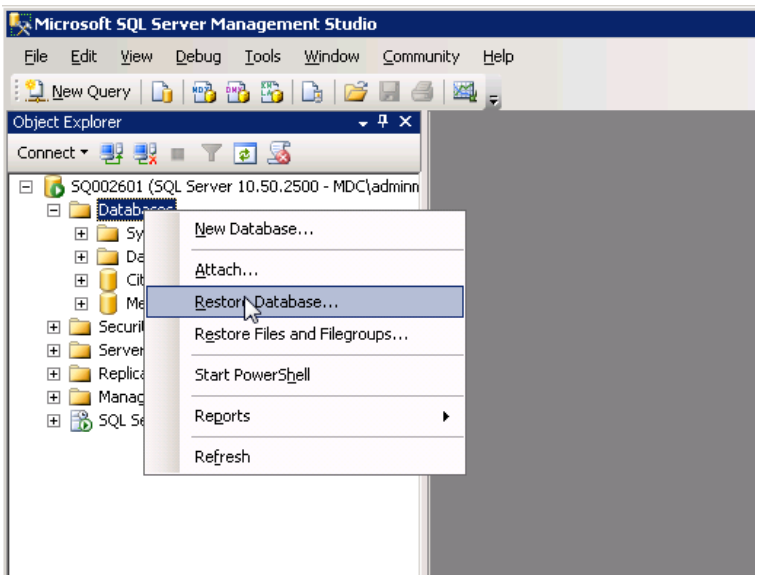


Restore

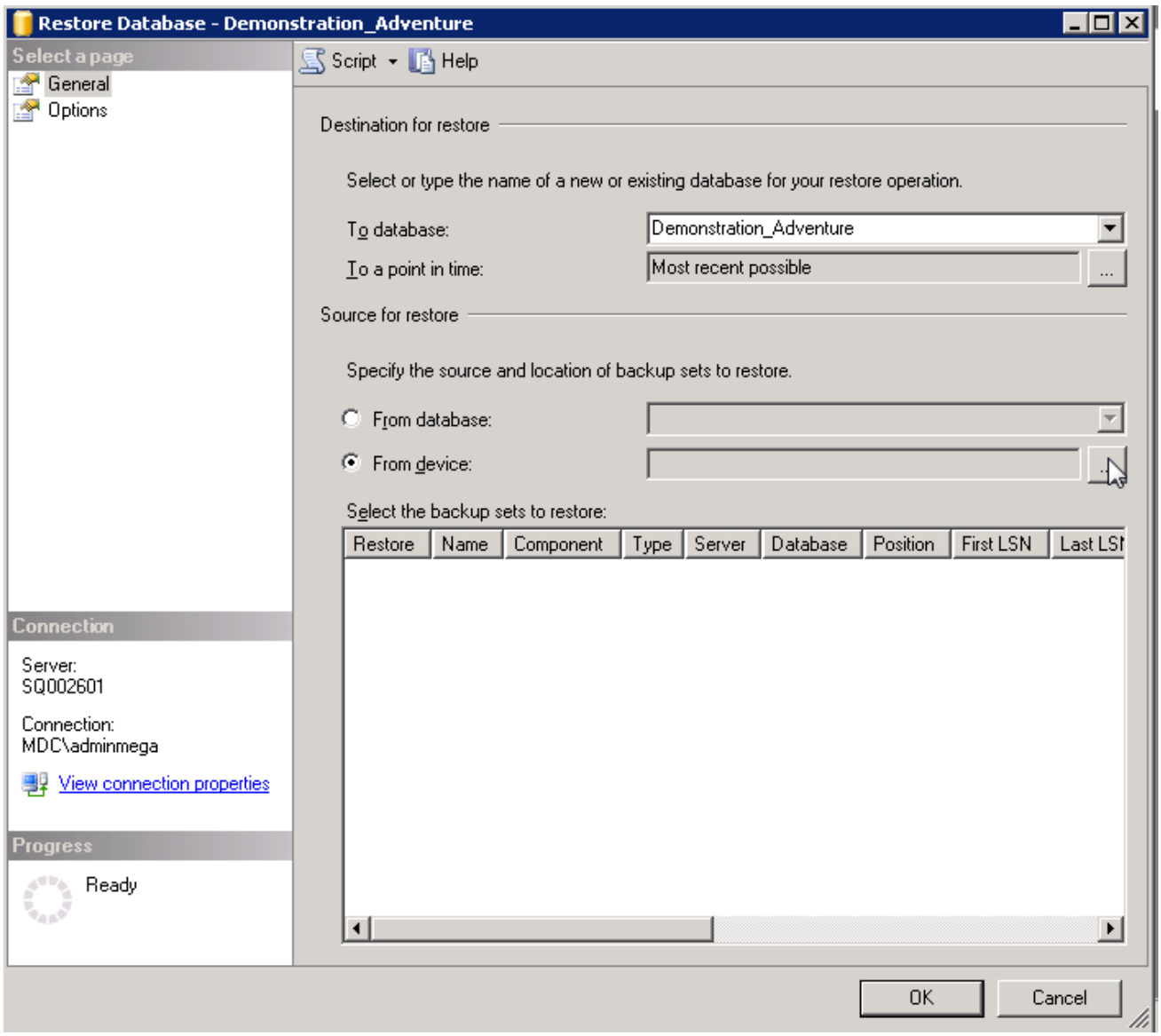
1. Connect to the target SQL Server server (example: SQL002601).
2. Launch the Management Studio, and connect to the instance using, if possible, a Windows account that is both sysadmin, and has access rights to the folder where the backup file was copied (example: mdc\adminmega).



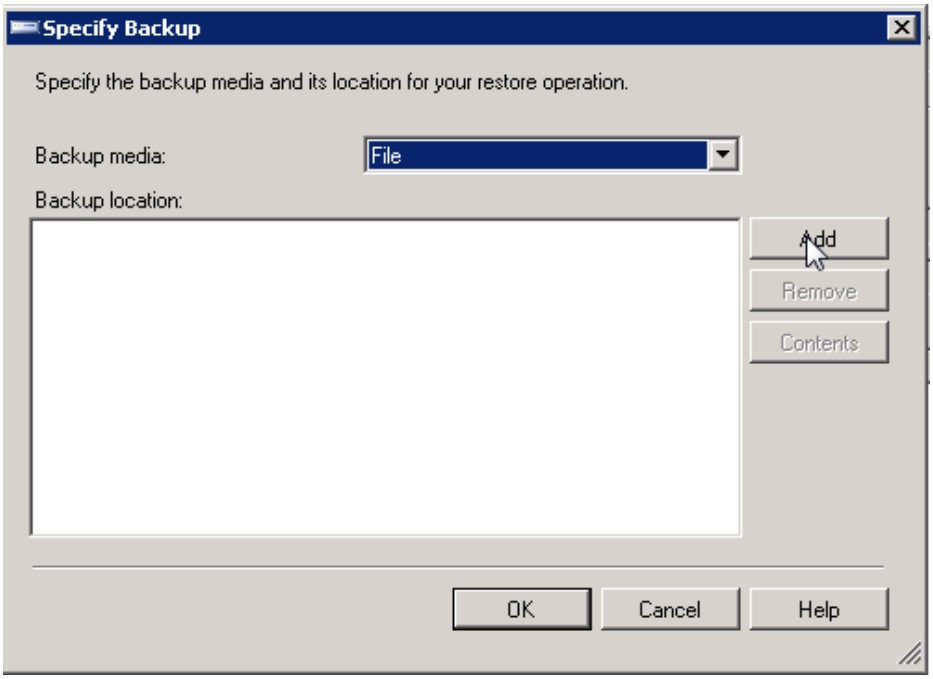
3. Right-click **Databases**, and select **Restore Database**.



4. From the **General** page, in the **Destination for restore** pane, in the **To database** field, provide the name of the database that will be created (example: Demonstration_Adventure).
5. In the **Source for restore** pane, select **From Device** option and click ....


Restore Database - Demonstration_Adventure
Select a page
General
Options
Script
Help
Destination for restore
Select or type the name of a new or existing database for your restore operation.
To database:
Demonstration_Adventure
To a point in time:
Most recent possible
Source for restore
Specify the source and location of backup sets to restore.
From database:
From device:
Select the backup sets to restore:
Restore
Name
Component
Type
Server
Database
Position
First LSN
Last LSN
Connection
Server:
SQ002601
Connection:
MDC\adminmega
View connection properties
Progress
Ready
OK
Cancel

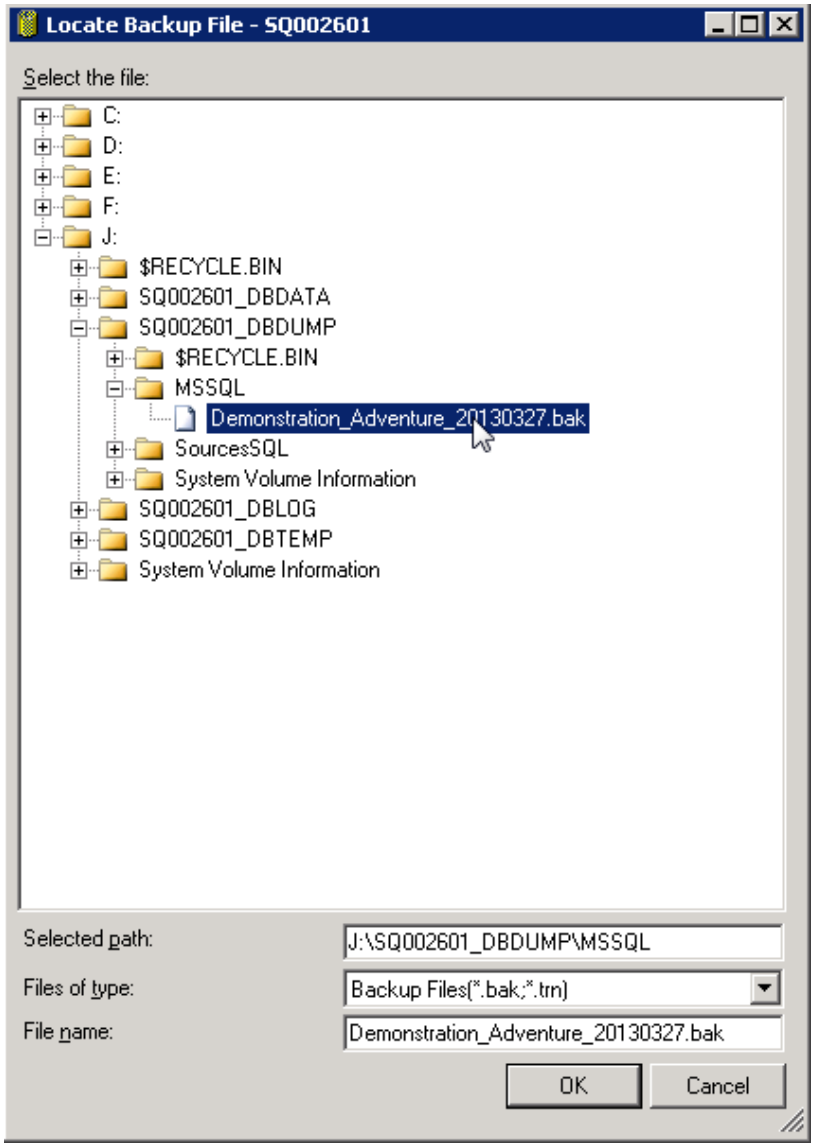
6. Click **Add**.



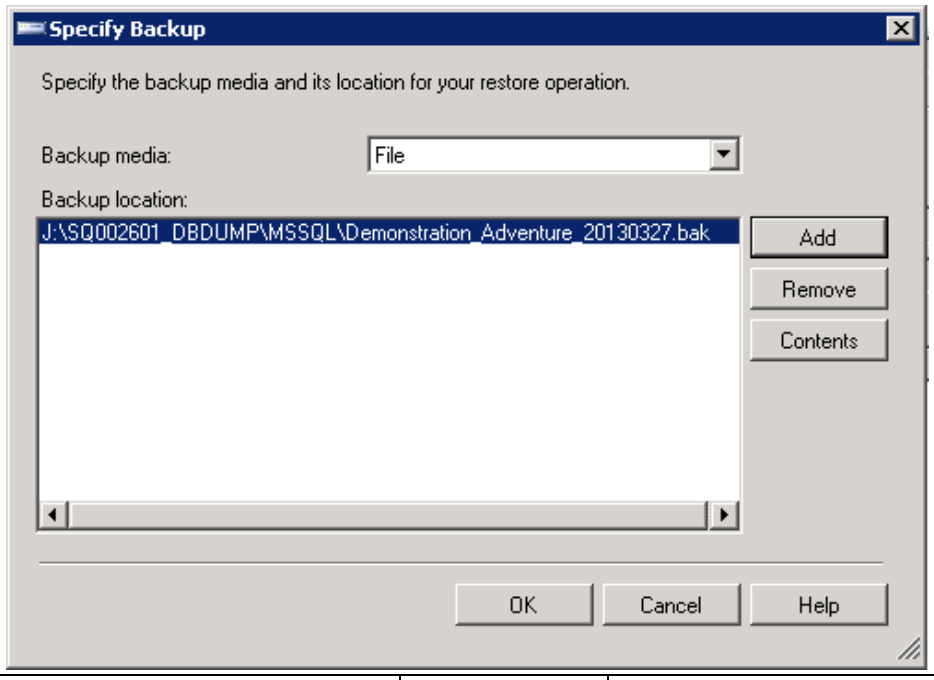
7. Check that we are correctly put in the folder « J:\SQ002601_DBDUMP\MSSQL».

   Otherwise, browse the folders to get to it. Then, click the .bak file that you just copied on the server (for example: « Demonstration_Adventure_20130327.bak »).

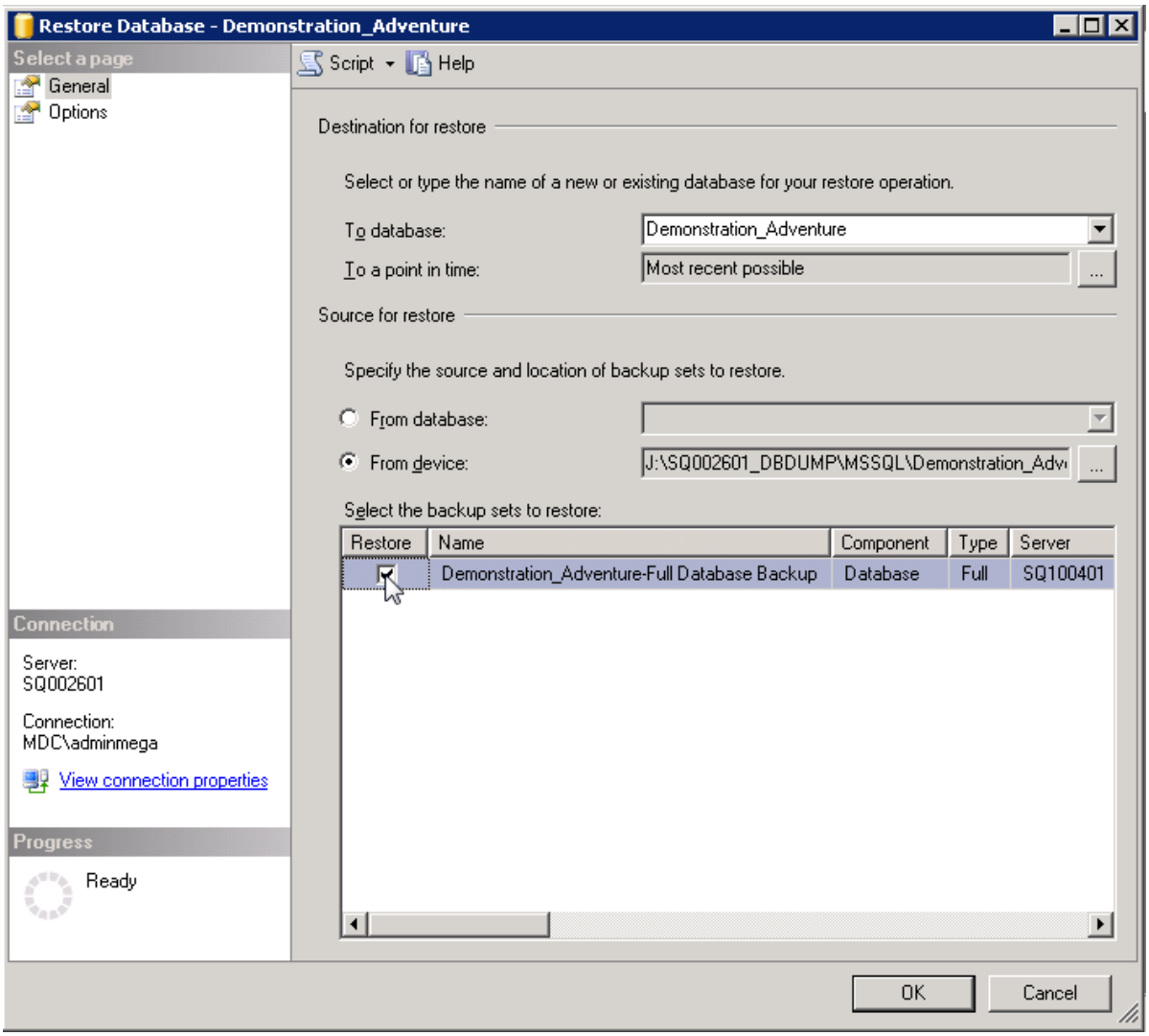
   Check that the « File Name » field is correctly filled, and click **OK**.


Locate Backup File - SQ002601
Select the file:
C:
D:
E:
F:
J:
$RECYCLE.BIN
SQ002601_DBDATA
SQ002601_DBDUMP
$RECYCLE.BIN
MSSQL
Demonstration_Adventure_20130327.bak
SourcesSQL
System Volume Information
SQ002601_DBLOG
SQ002601_DBTEMP
System Volume Information
Selected path:
J:\SQ002601_DBDUMP\MSSQL
Files of type:
Backup Files(*.bak;*.trn)
File name:
Demonstration_Adventure_20130327.bak
OK
Cancel

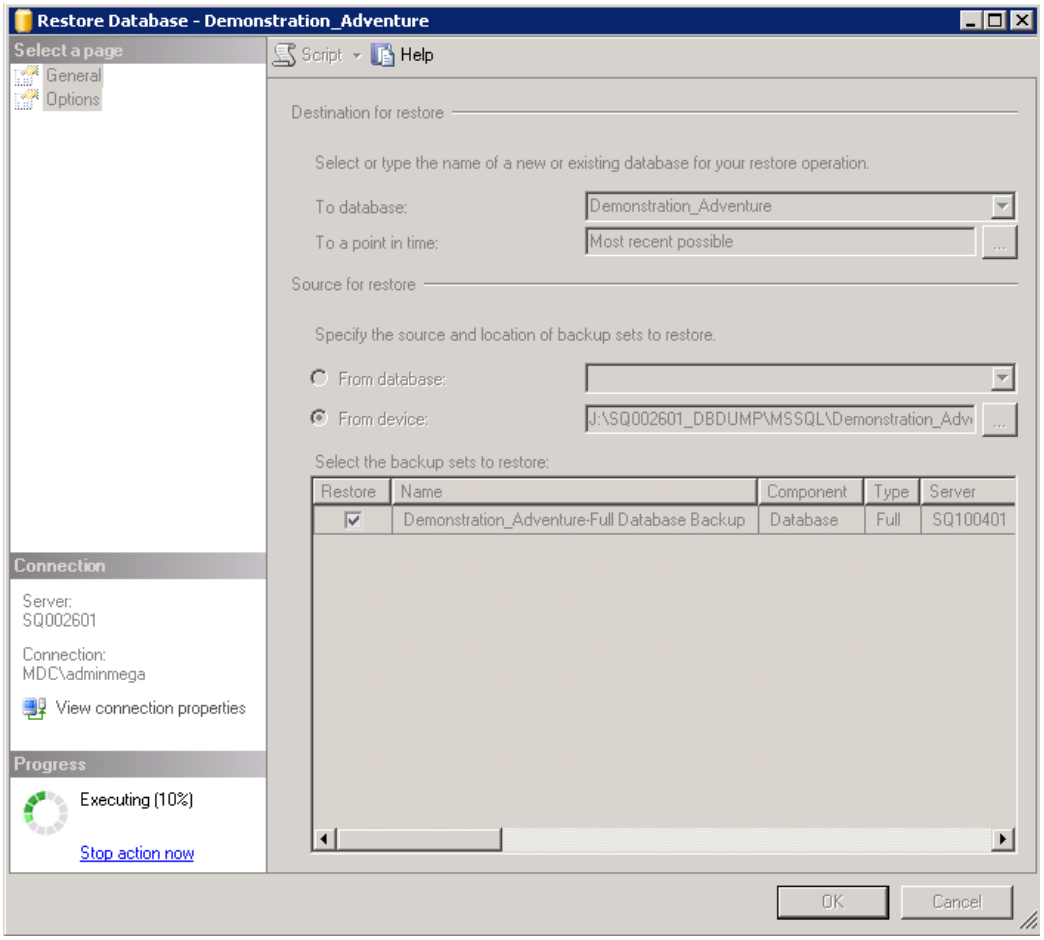
8. Click **OK**.


Specify Backup
Specify the backup media and its location for your restore operation.
Backup media:
File
Backup location:
J:\SQ002601_DBDUMP\MSSQL\Demonstration_Adventure_20130327.bak
Add
Remove
Contents
OK
Cancel
Help

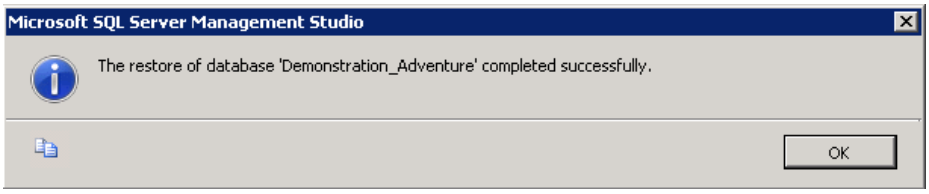
9. In the **Source for restore** pane, in the **Select the backup sets to restore** table select **Restore** at the beginning of the line.



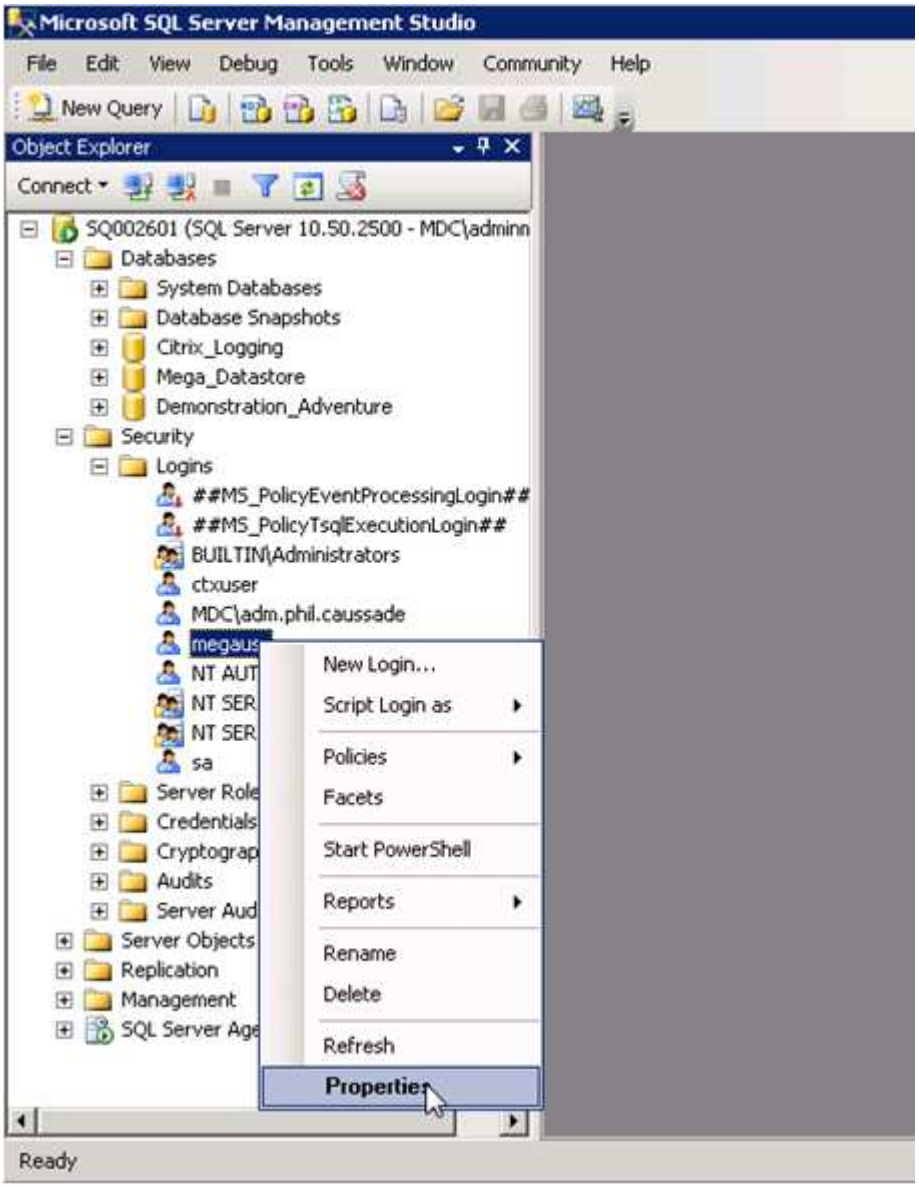
10. click **OK**.



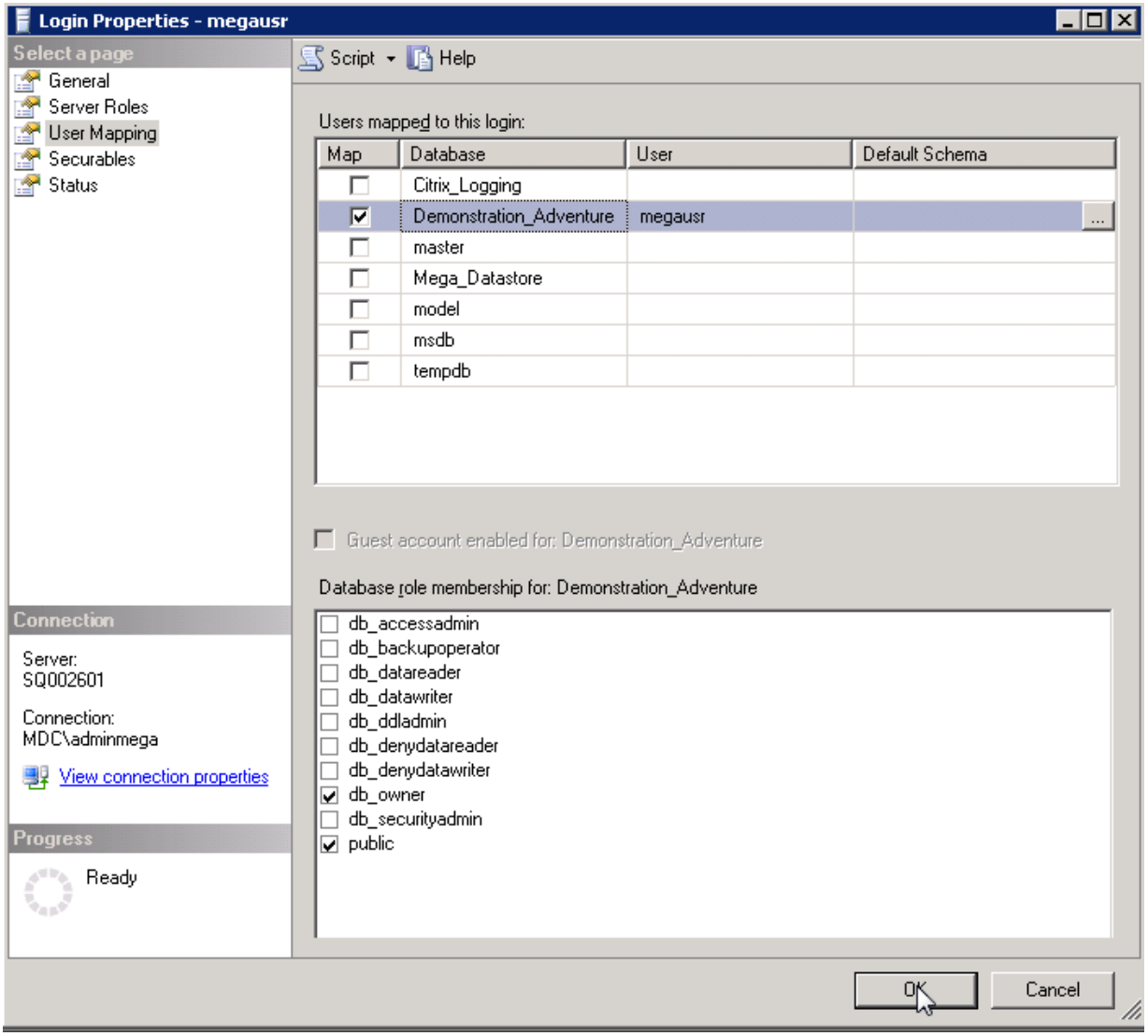
11. Once the restore completed successfully, click **OK**.



12. In ManagementStudio, expand **Security** folder, and **Logins** folder.
13. Right-click the account that you will use to connect the application to SQL Server (for example: login « megausr ») and select **Properties**.



14. In the **Login Properties - <login>** window, select **User Mapping** page, and select the **Map** corresponding to the database lin you just restored.
15. In the **Database role membering for: <database name>** pane, select « db_owner ».
16. Click **OK**.



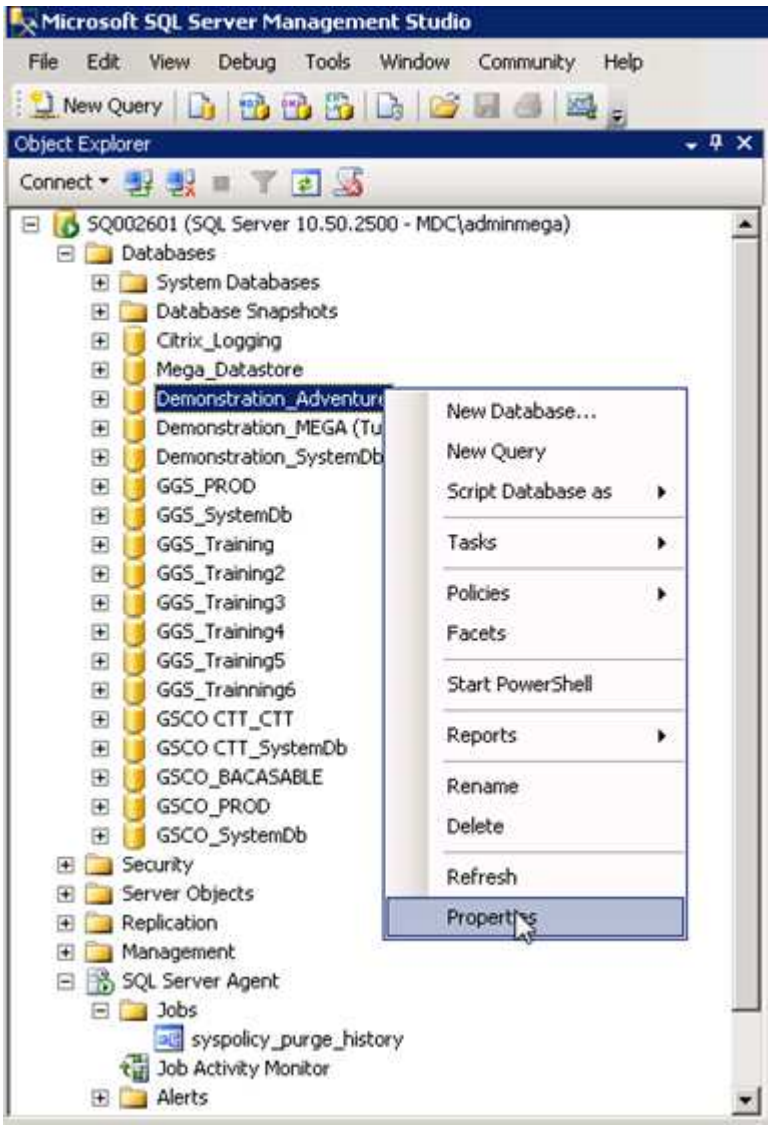
IF you moved from a version of SQL Server to a more recent one, you have to upgrade the compatibility level of your database.

> In this example, the source database came from an SQL Server 2005 instance, and was restore on an SQL Server 2008 instance.

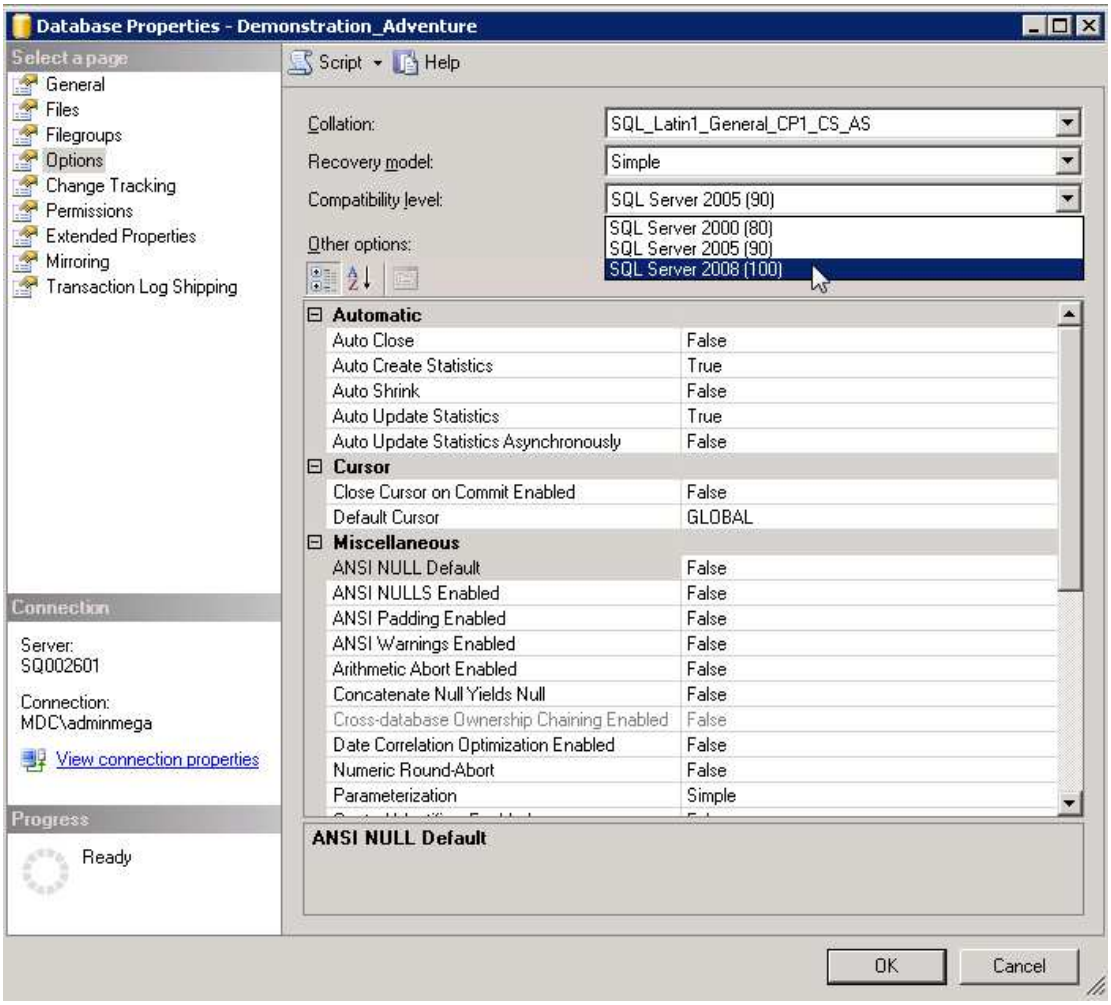
If you stay on the same version, go directly to the next section.

To upgrade:

1. Right-click the database and select **Properties**.



2. Select the **Options** page, in the **Compatibility level** drop down list select the appropriate version (for example « SQL Server 2008 (100) »).


Database Properties - Demonstration_Adventure
Select a page
General
Files
Filegroups
Options
Change Tracking
Permissions
Extended Properties
Mirroring
Transaction Log Shipping
Script
Help
Collation:
SQL_Latin1_General_CP1_CS_AS
Recovery model:
Simple
Compatibility level:
SQL Server 2005 (90)
SQL Server 2000 (80)
SQL Server 2005 (90)
SQL Server 2008 (100)
Other options:
Automatic
Auto Close
False
Auto Create Statistics
True
Auto Shrink
False
Auto Update Statistics
True
Auto Update Statistics Asynchronously
False
Cursor
Close Cursor on Commit Enabled
False
Default Cursor
GLOBAL
Miscellaneous
ANSI NULL Default
False
ANSI NULLS Enabled
False
ANSI Padding Enabled
False
ANSI Warnings Enabled
False
Arithmetic Abort Enabled
False
Concatenate Null Yields Null
False
Cross-database Ownership Chaining Enabled
False
Date Correlation Optimization Enabled
False
Numeric Round-Abort
False
Parameterization
Simple
ANSI NULL Default
Connection
Server:
SQ002601
Connection:
MDC\adminmega
View connection properties
Progress
Ready
OK
Cancel

3. Click **OK**.

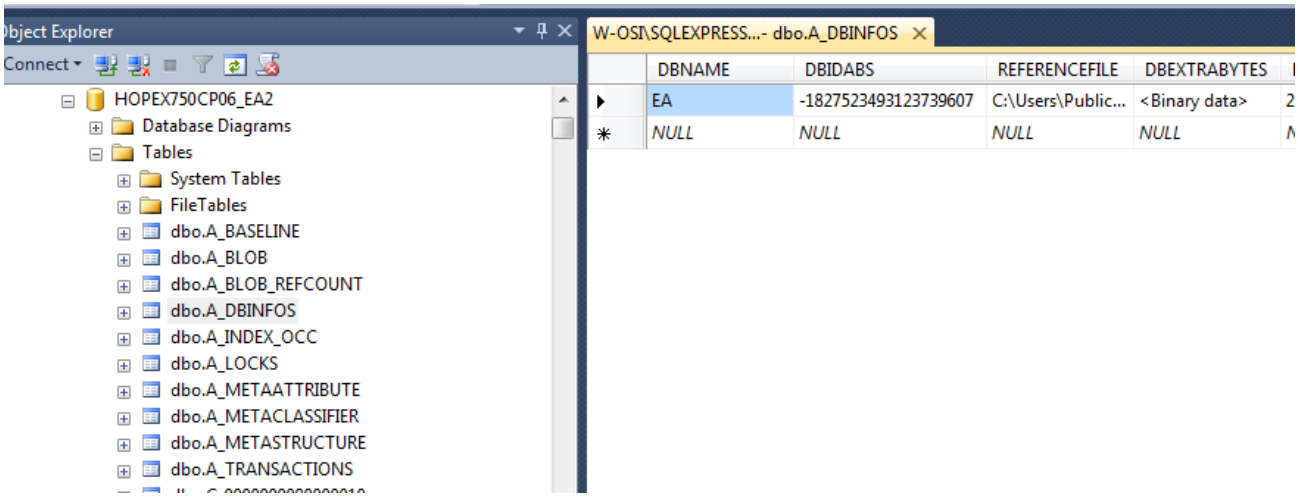
When duplicating a repository in an environment – Expert mode

This section is only if you are very confident about your Mega and RDBMS skills, since you have to modify data directly in some tables of your database.

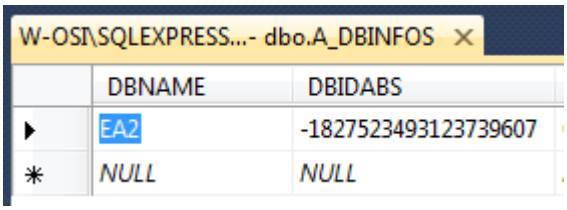
In case you want, within an environment, duplicate a specific repository, you need to tweak the data manually in two tables of your restored database.

For example: you want to duplicate repository "EA" to have a repository "EA2" in the environment "HOPEX750CP06".

1. You have restored database EA twice, in databases "HOPEX750CP06_EA" and "HOPEX750CP06_EA2".
2. Using SQL Server Management Studio, open database "HOPEX750CP06_EA2", and edit the table "dbo.A_DBINFOS":

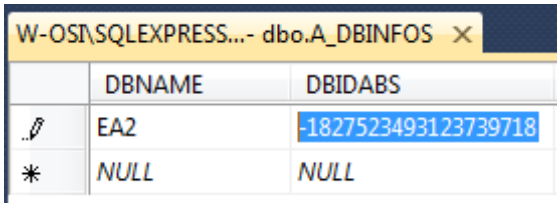


3. Modify the **DBNAME** field of that line, to enter the name of your duplicate, i.e. how you want it to appear in your environment (for example: here, "EA2").



4. Modify the **DBIDABS** field that is the unique identifier of the repository within your environment.

   You need to change its value, and make sure that it is unique for all other repositories, so you need to check in all schemas. Make sure that when you change one or two characters, it will create a string that is not used by any other (for example: here, we modified the last 3 digits from " 607" to "718").



5. Save your updates and close the table.

RDBMS Environment Duplication - 2 - Post Processing Tasks

INTRODUCTION

This document describes the tasks you need to cary out after duplicating the MEGA data that were stored in an SQL Server or an Oracle database.

You need to have gone through one of the following document first, depending on the RDBMS target:

- *RDBMS Environment Duplication - 1 - Oracle*

or

- *RDBMS Environment Duplication - 1 - SQL Server*

The first part details what to do to reattach to the set of duplicated data from MEGA point of view.

As all is not stored inside the RDBMS, this document details what you need to copy from the original MEGA environment to the new MEGA environment pointing at the duplicate RDBMS data.

Since the tasks that need to be carried out are almost exactly the same, this document does not differentiate between Oracle and SQL Server except for a few examples: the difference is highlighted in that case.

Create/Attach an environment in Mega

Creating an environment

To create an environment:

1. Connect to **MEGA Administration**.
2. In the navigation tree, right-click **Environments** and select **New**.
3. Enter the **Name** of the new environment.

   The environment name must respect Windows folder naming constraints.

   For SQL Server: It is the beginning of the name of the system database. It should be called <environment>_SystemDb, where <environment is the string that you put in the Mega admin tool. In this example, the environment is called "GGS".

   For Oracle: the environment name can be found in the MEGA_ORACLE_MAPPING table that can be found in the Oracle SCHEMA corresponding to the SystemDb of the environment. It will show in the MEGA_ENV_NAME column. See p.15 of "RDBMS environment duplication - 1 – Oracle" for more details.
4. (Optional) Location of the environment is specified by default; you can modify it if necessary using the **Browse** button.

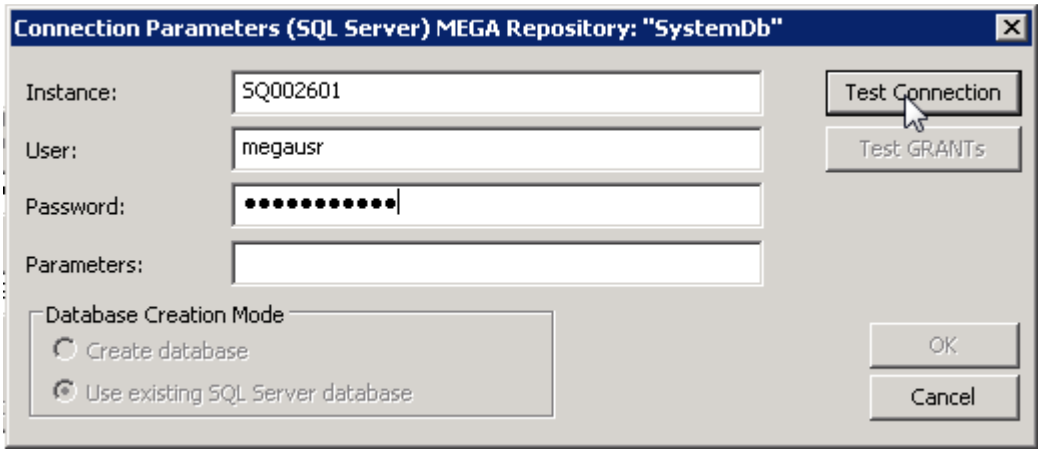
   In this example, we created a share on the server hosting the SQL Server instance, that will host the environment files, and that is called \\sq002601\EnvironnementsMega.
5. Select an RDBMS repository server type for the new environment: SQL Server or Oracle.
6. Select **Restore** which allows to connect to an existing MEGA formatted set of data on an instance,
7. Click **OK**.
8. Enter the connection parameters for the **Instance**.

   Do not enter anything in the **Parameters** field.

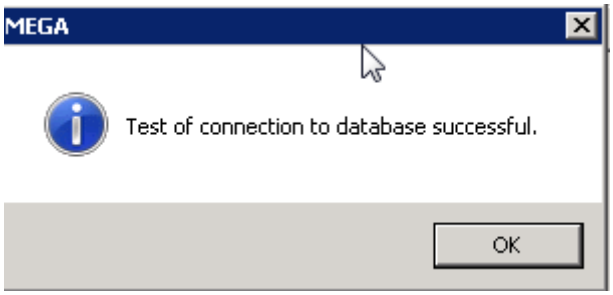
   Note:

   The syntax for a named instance on **SQL Server** is : server_name\instance_name. In this example, the instance is the default one, without a specific name. That is why we only provide the name of the server where the instance is running.

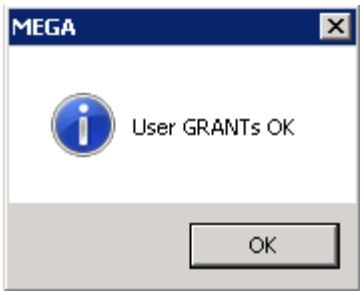
   For **Oracle**, the backslash needs to be replaced with a forwardslash server_name/instance_name.



9. Click **Test Connection**.

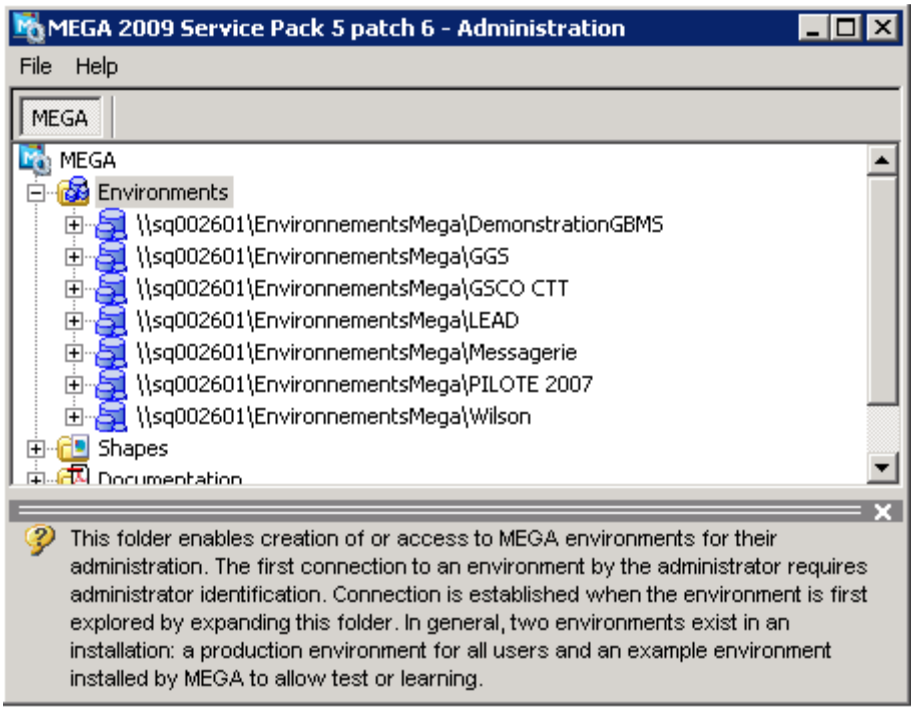


10. Click **Test GRANTS**.



11. Click **OK**.

    A popup indicating that the environment was successfully created appears, and the new environment is displayed in the list (for example here « \\sql002601\EnvironmentsMega\GGS).



Attaching the working database(s) to the environment

Once your environment is created, you still have to attach the working database(s) to this environment.

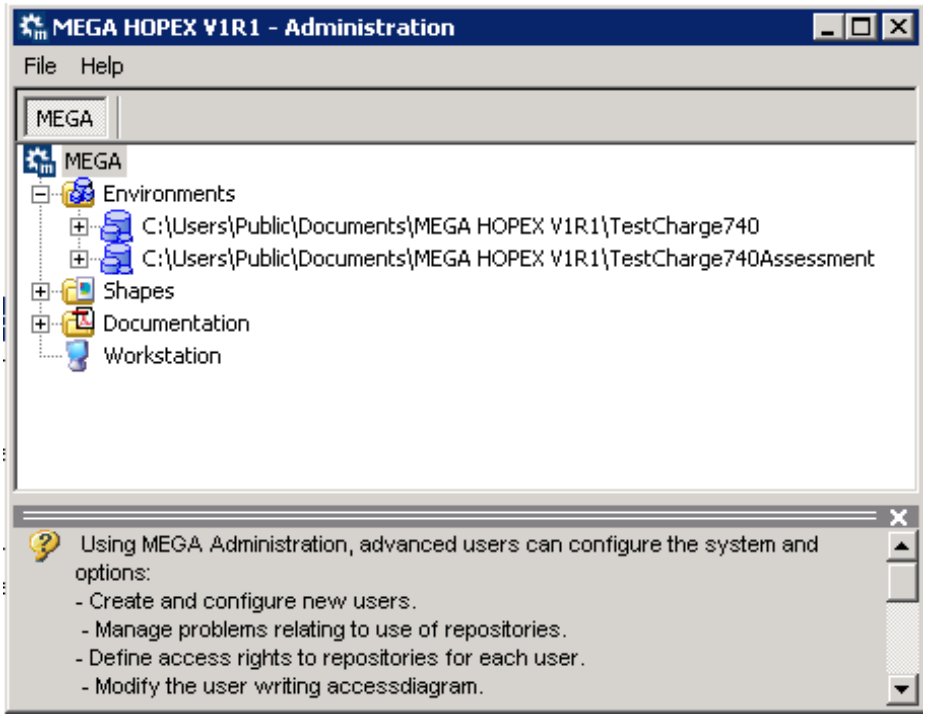
In **Repositories** you only have the SystemDb.

Now you have to connect to the environment, and add the Mega repositories. The first time you connect, you receive warning message(s) telling you that database "X" ("X" being the name of the repository that existed in the source environment, and most likely one of the repositories you are trying to attach) is not referenced.

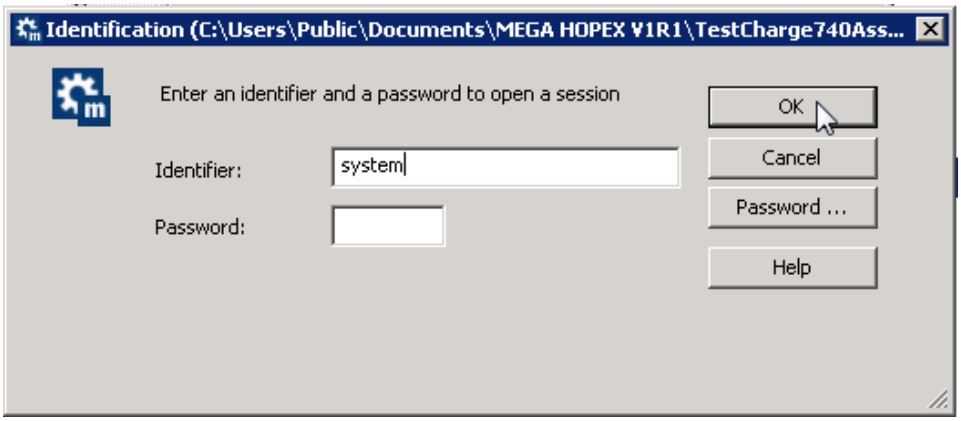
This is because the SystemDb database contains some information about the working repositories. You can discard this warning, and continue.

To attach a database, previously restored in SQL Server Management Studio:

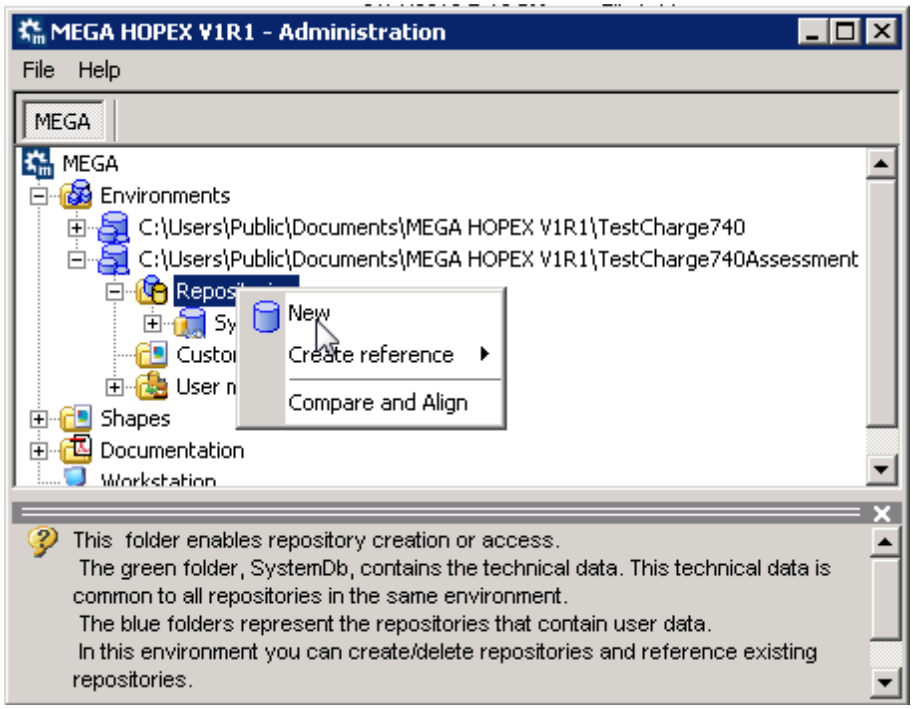
1. Connect to **MEGA Administration**.



2. Connect to the environment concerned (for example with **System** user).



3. Right-click **Repositories** and select **New**.

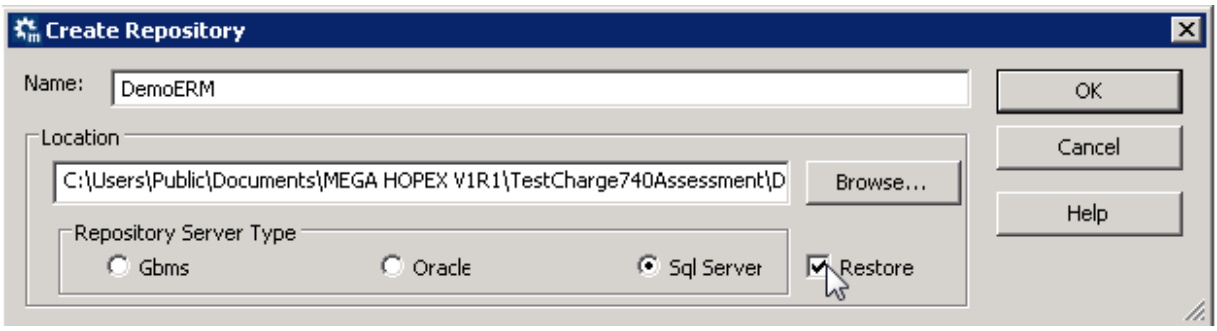


4. Enter the Name of the Repository (in this example erver rmati

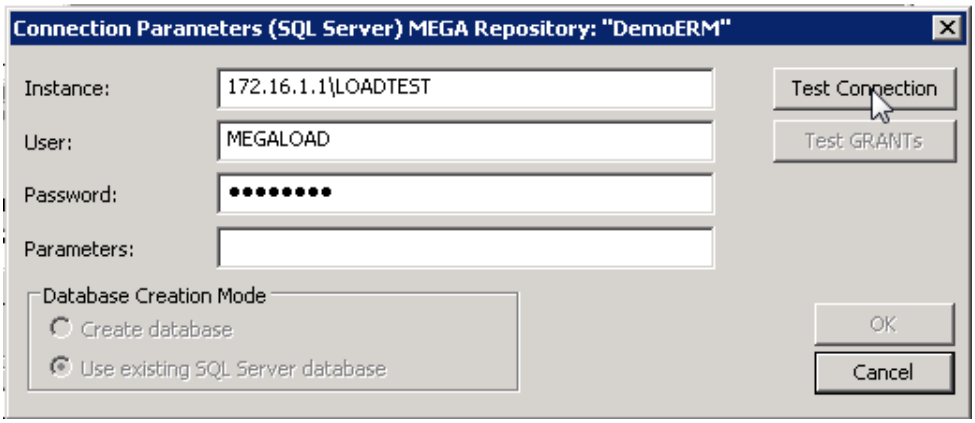
   In **SQL Server**, you should have a database called this example erver rmat_DemoERM" existing, with the native SQL Server user db_owner of the database.

   In **Oracle**, you need to know which SCHEMA is "CHEMA is to know ser dbase called this example erver rmation about the working repositories. You can discard this warning, and continue.

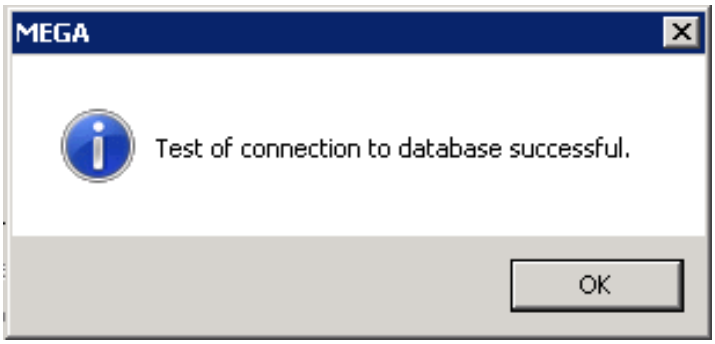
5. In the **Repository Server Type** pane, select **SQL Server** or **Oracle**.
6. Select **Restore**.



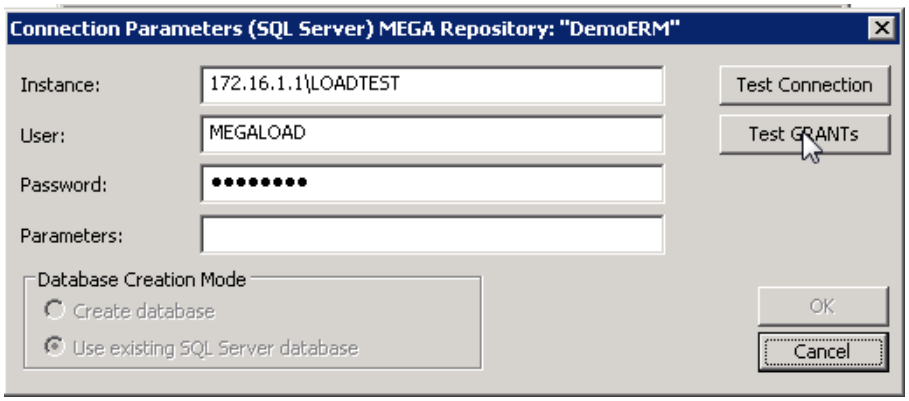
7. Click **OK**.
8. The connection parameters are already set. Check that they are correct.

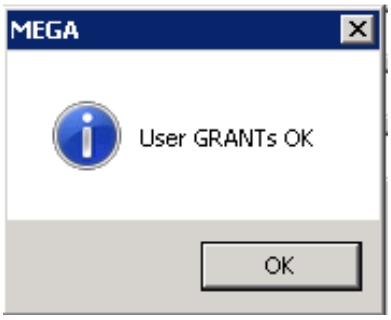


9. Click **Test Connection**.

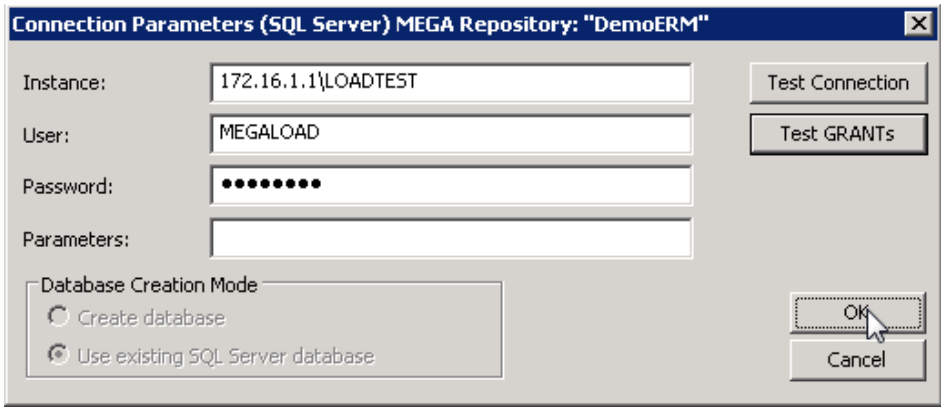


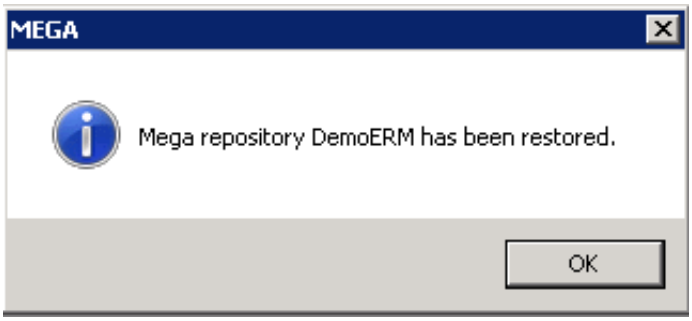
10. Click **Test GRANTs**.



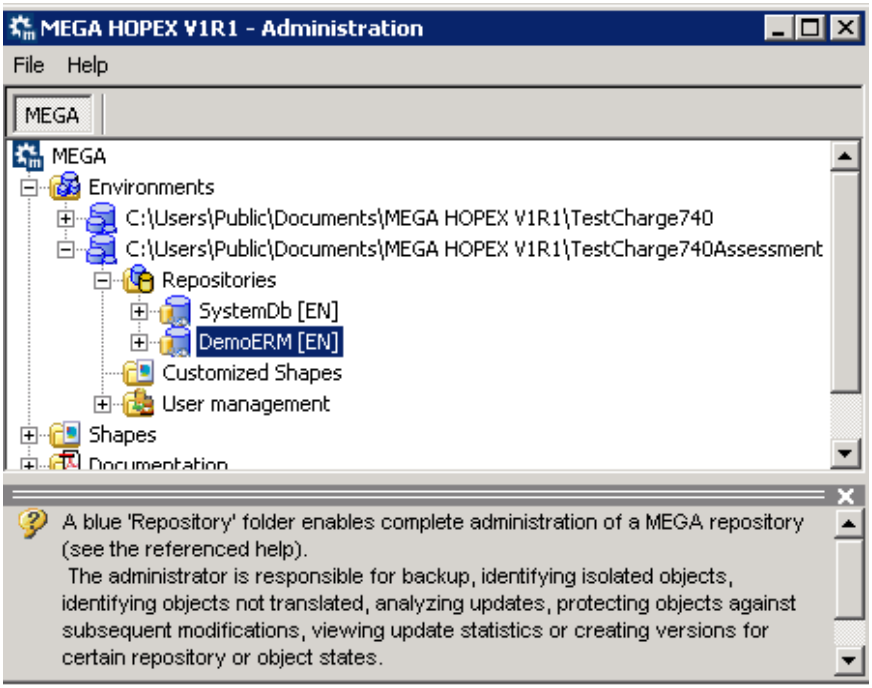


11. Click **OK** to create the repository.





The "DemoERM" repository appears in the **Repositories** list



When duplicating a repository

In case you are also creating a clone of an existing repository within your environment, you made preliminary steps while restoring either your databases (in SQL Server), or schemas (in Oracle).

Since this is done, you just have to perform again the Attaching the working database(s) to the environment procedure, and adapt it to give the name of your duplicated repository.

In the above example, you have "DemoERM". So we assume that you have also a database for the clone of the repository that would be called "DemoERM2" for instance.

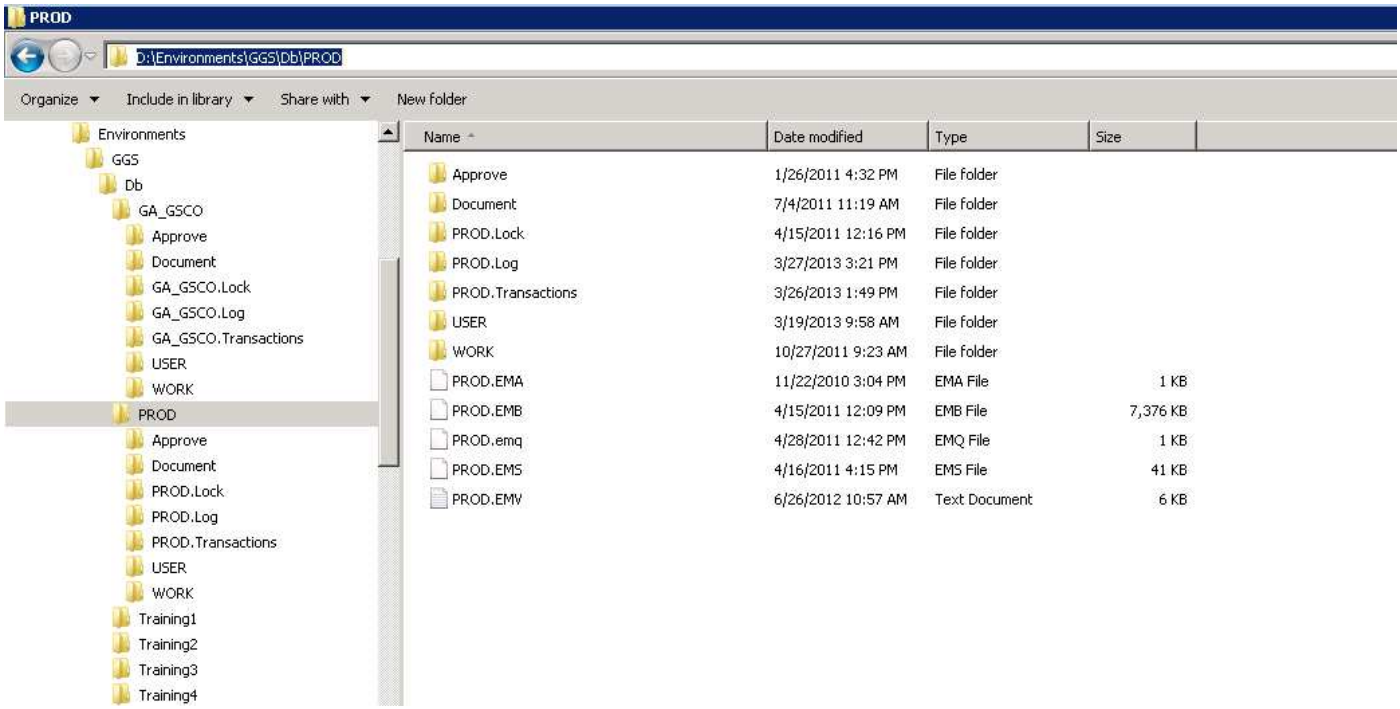
The same actions should allow you to add this copy in your environment, without any impact on the "DemoERM" repository.

Copy the documents from source to target

You have to copy the documents from source to target for each repository.

The Word/RTF documents

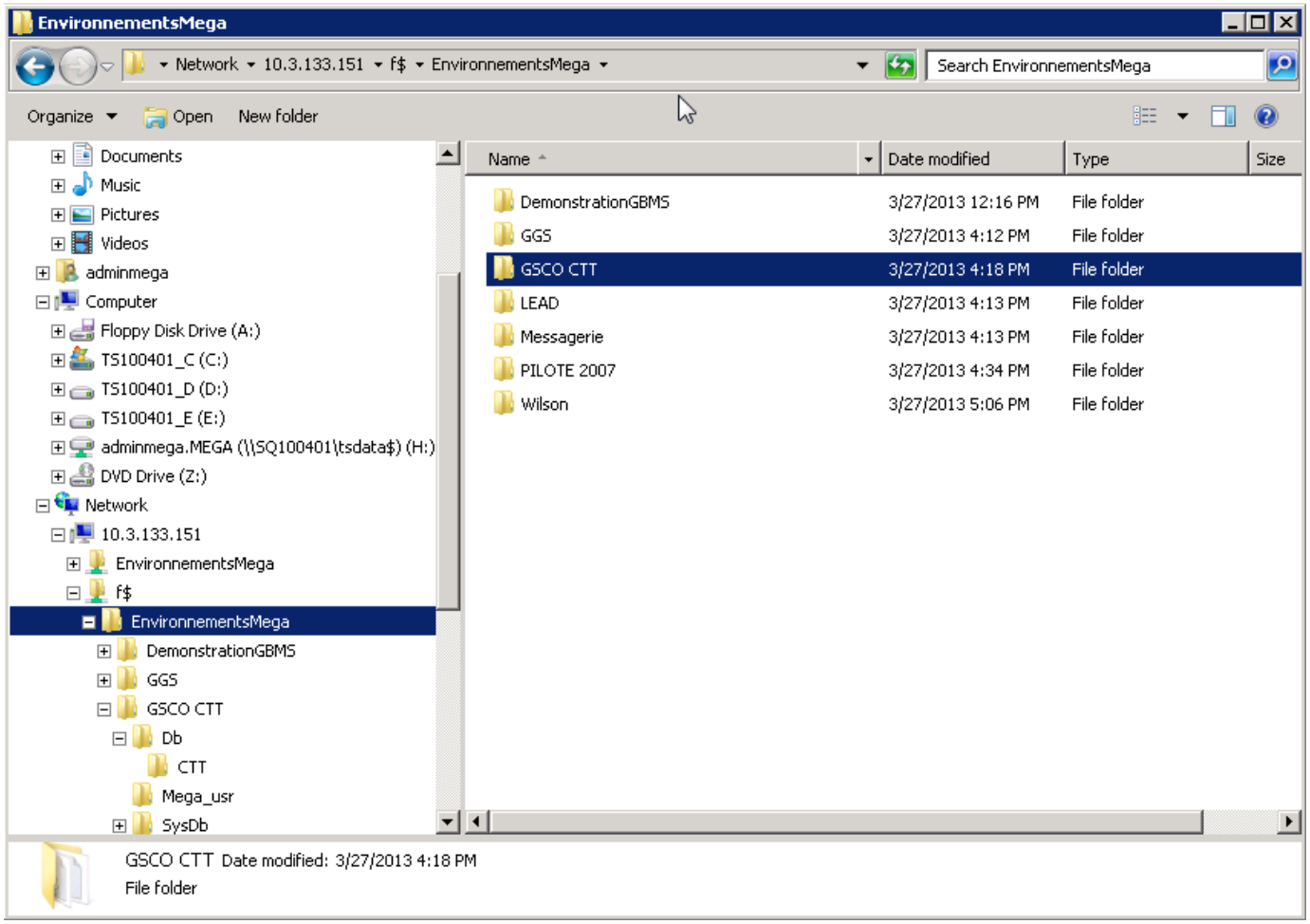
1. Connect to the source server.
2. Go to the folder hosting the environment (for example environment "GSCO CTT").
3. Go to the **Db** folder, and in the sub-folder of each repository you migrated (in this example « D:\Environments\GGS\Db\PROD » contains the data of the repository called "CTFTM_OLD").



4. From the source server, open an explorer on the target server, in the same folder.

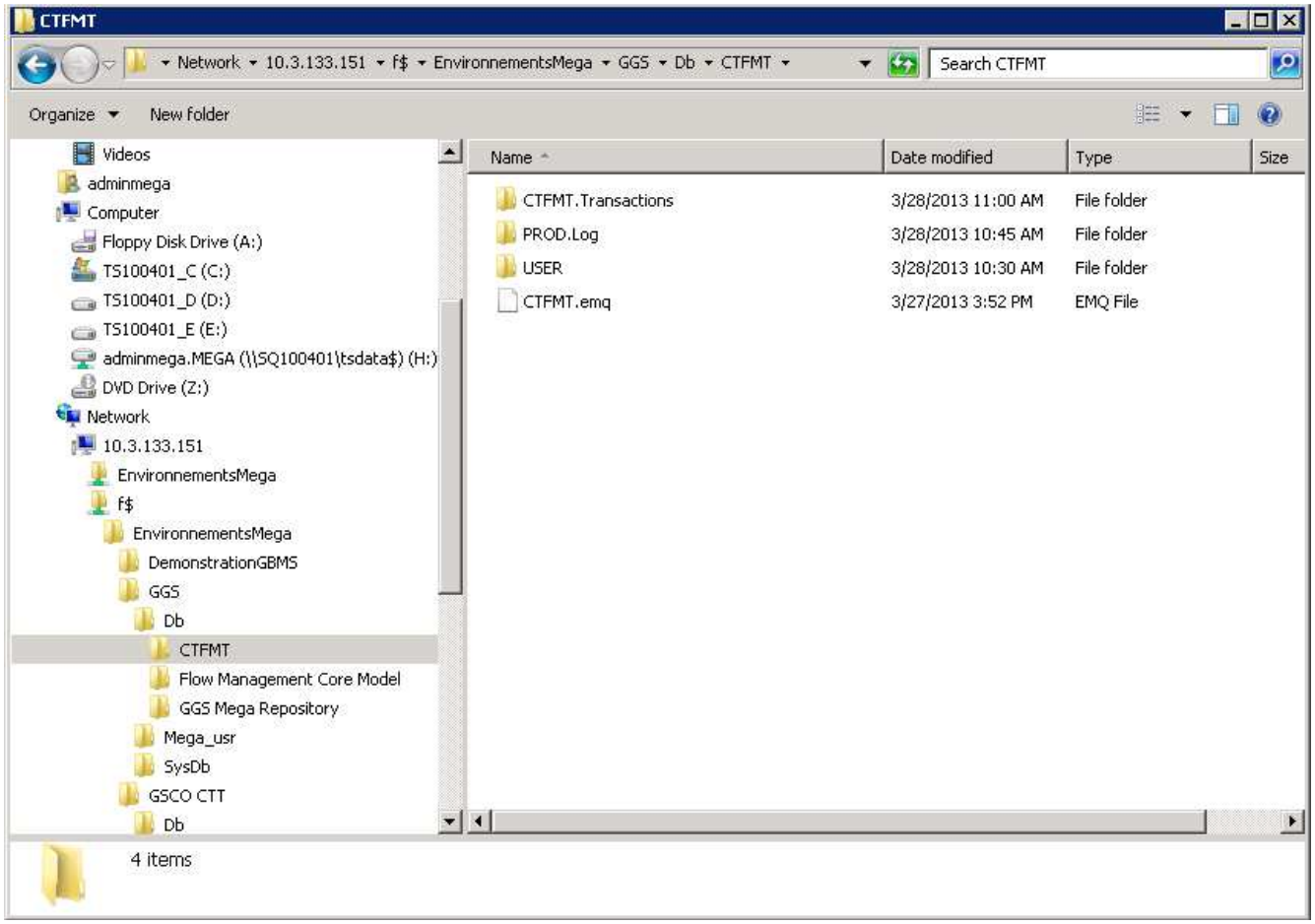
   In this example, the environments on the target server are hosted on the server with 10.3.133.151 IP address, and on that server the environments are located on the F drive in the "EnvironnementsMega" folder, so that the syntax is:

   \\10.3.133.151\f$\EnvironnementsMega\

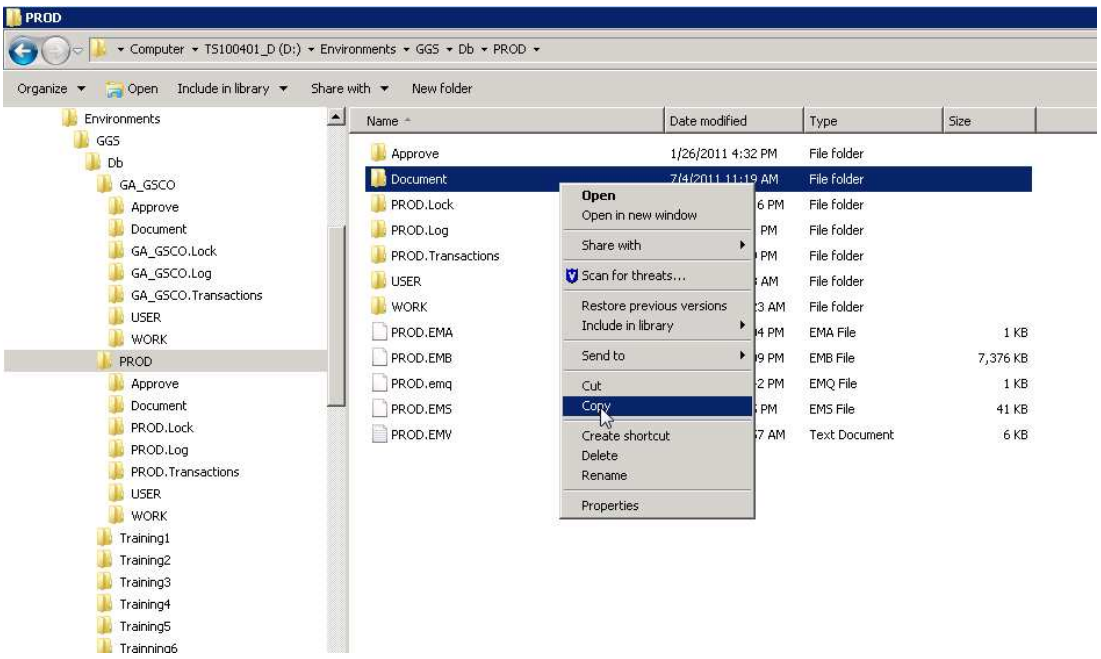


5. Go to the same sub-folder « …\GGS\Db\CTFMT ».

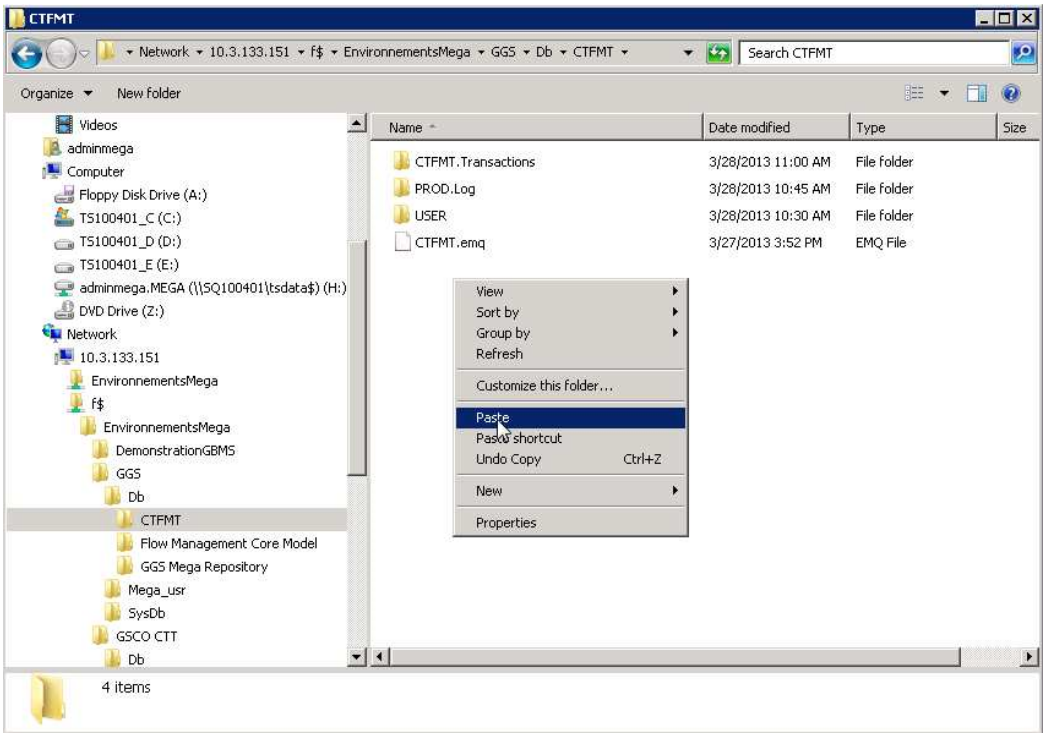
   Note: If you are wondering why it is not the same environment name and the same repository name, that is because in this example, this repository was taken from one environment to another, with a rename.



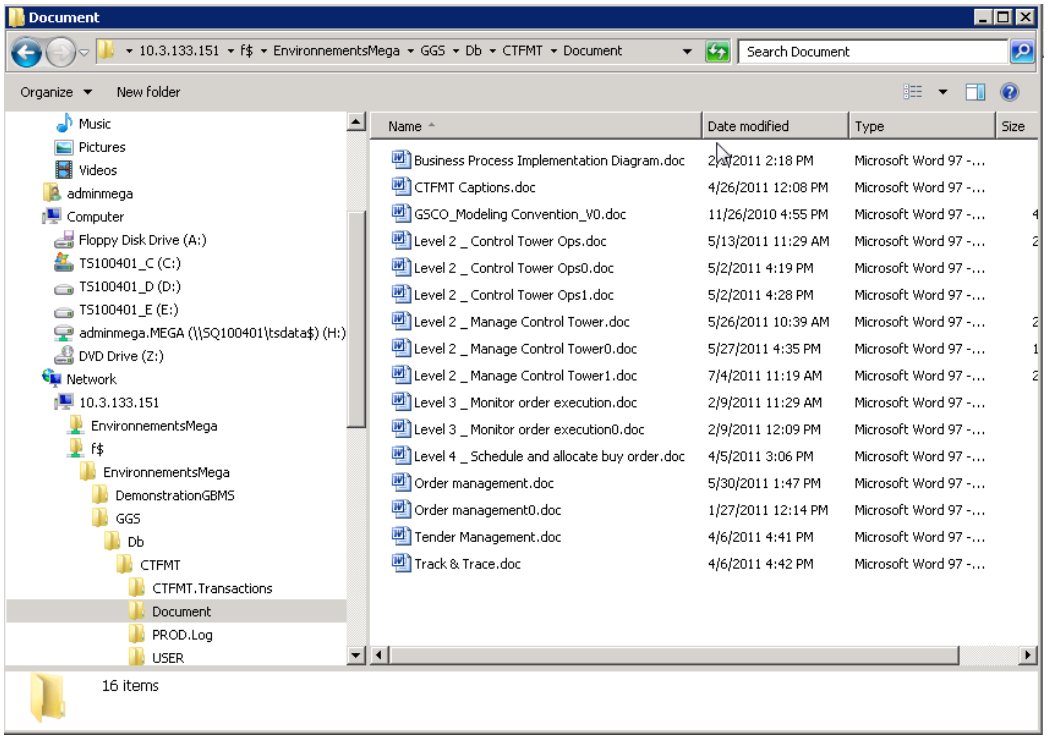
6. Right-click the **Document** folder from the source and select **Copy**.



7. Paste it on the target (future Production).



8. Check that the documents are all in the target folder.



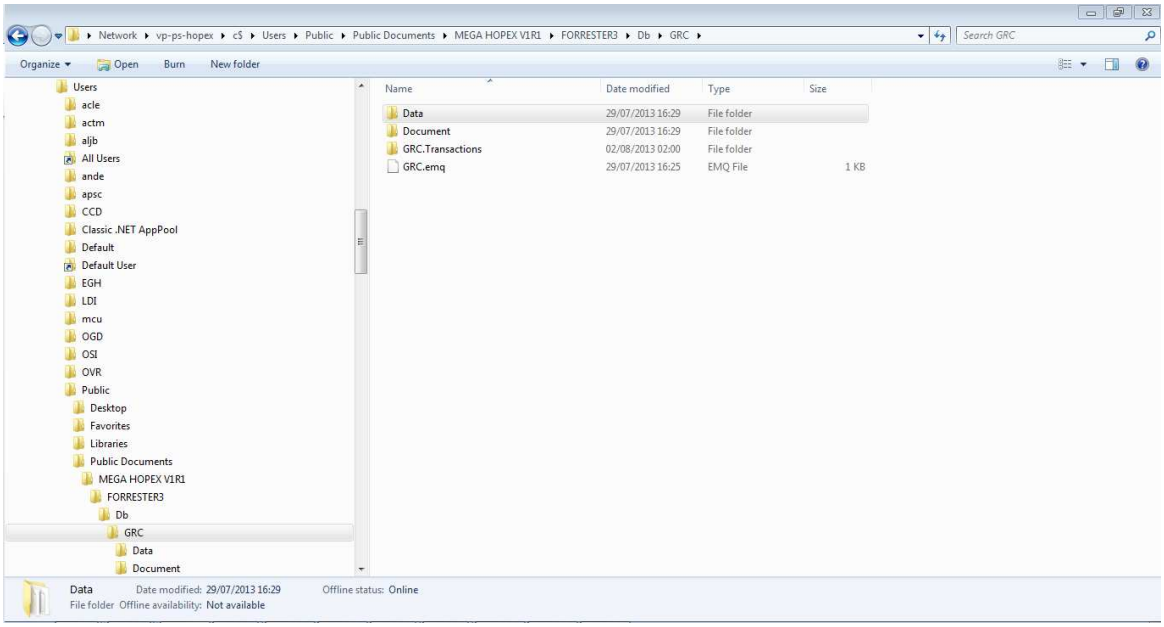
The internal documents (.DAT files)

Some documents can also be stored partially inside the SQL Server/Oracle databases (as references) and partially in .DAT files (generated in the folder of each repository of the migrated environment).

By restoring the SQL Server/Oracle databases, you already retrieved the references. Now you have to copy a folder from source to target.

1. From the source environment, expand the **Db** folder and the sub-folder of the database.

   In this example, on server vp-ps-hopex, we are looking at environment py aRESTER3 from source to target.the migrated environment).ry name, that is because in tX V1R1\FORRESTER3\Db\GRCxa



2. Right-click the **Data** folder and select **Copy**.
3. Paste it at the same level on the target folder.

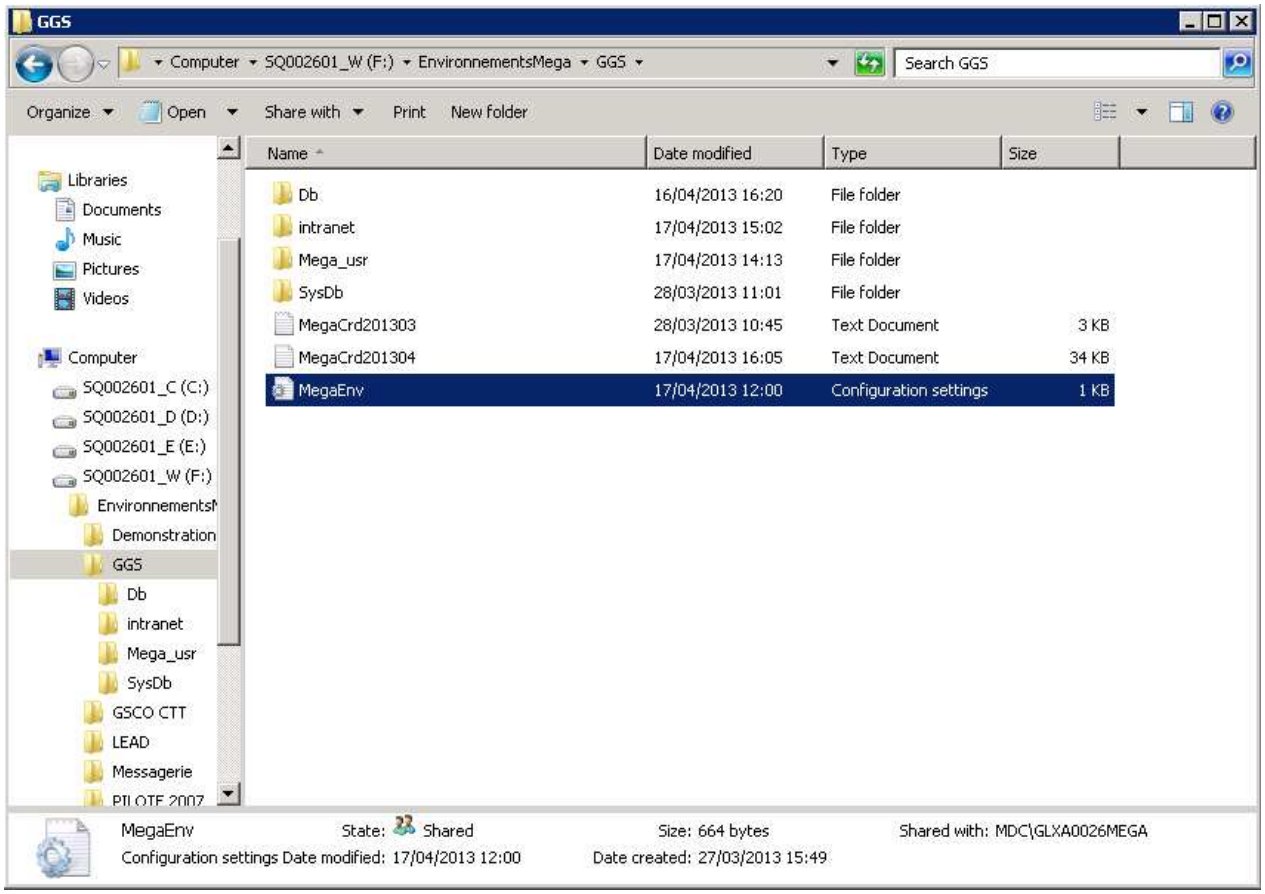
Get the parameters of the environment

For each environment, you need to retrieve certain types of configuration included in:

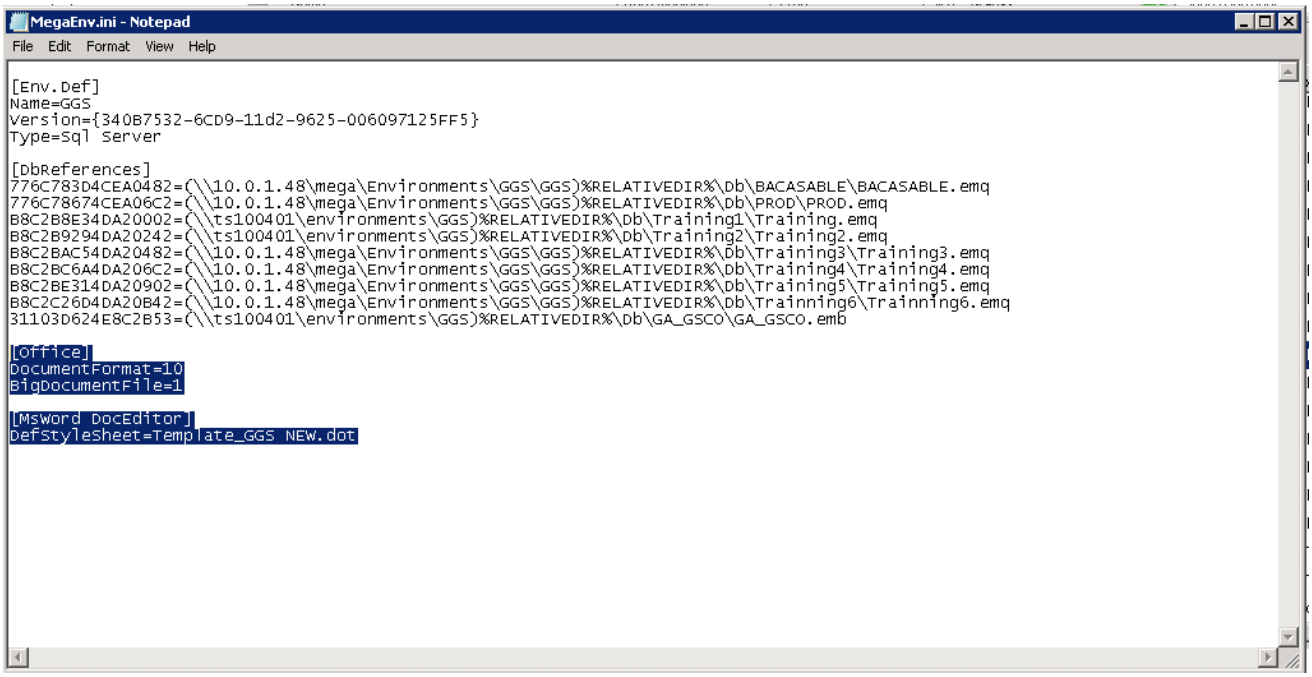
- the **MegaEnv.ini** file
- the **Mega_Usr** folder.

MegaEnv.ini file

The MegaEnv.ini file is located at the root level of each environment (in this example, in the folder tione database. In thga\GGSy afor the GGS environment) on the source server.



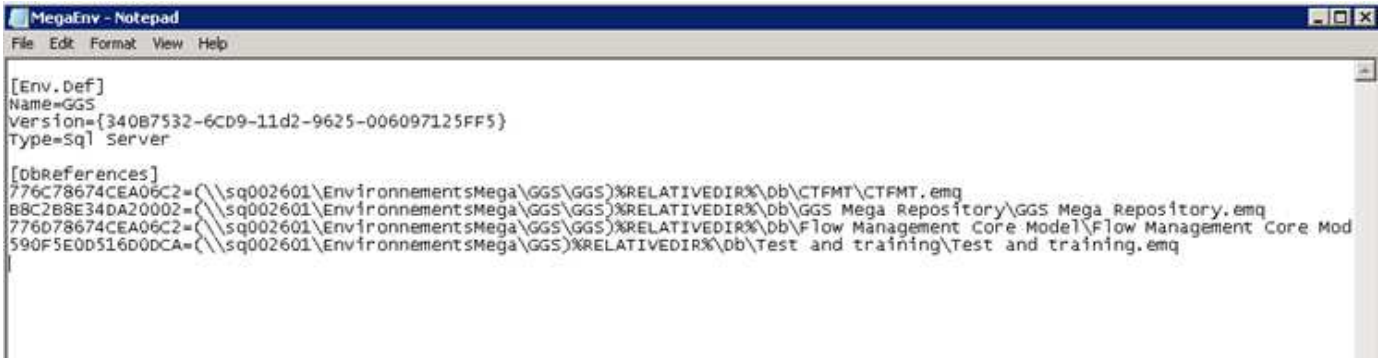
1. Open the **MegaEnv.ini** file on the source server.



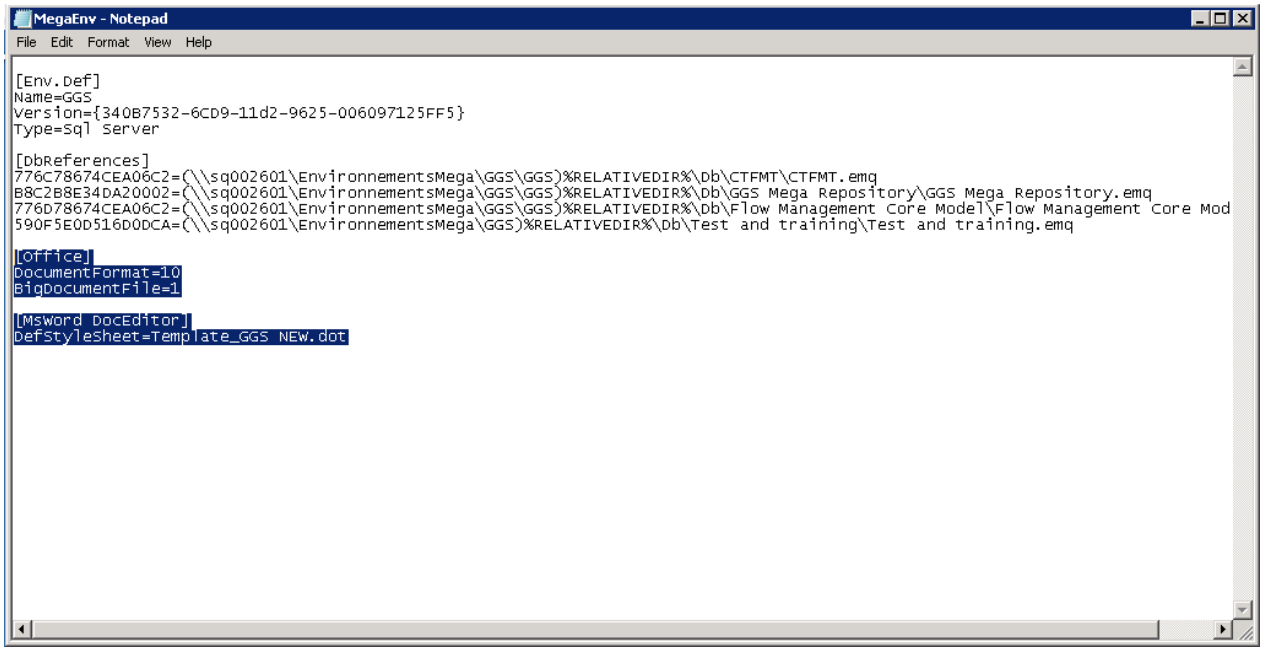
2. Under the [DbReferences] section, you find the environment-specific parameters, like the type of document (DocumentFormat=10 meaning that they were converted from .DOC to .RTF) or the templates used by default.

   Copy this specific section.

3. Open the **MegaEnv.ini** of the target server.



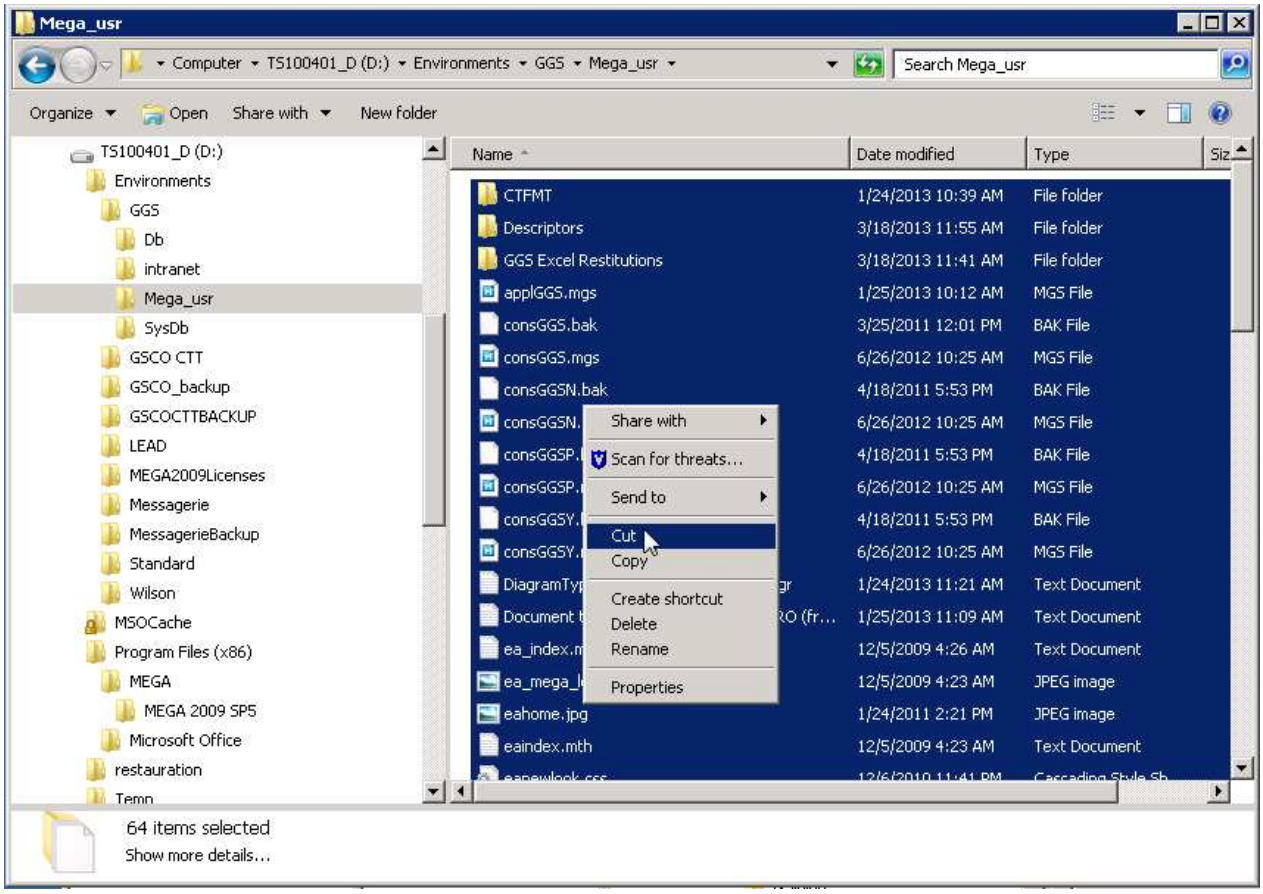
4. Paste this section at the same level in the file and save the document.



Mega_Usr folder

In each environment, there is a **Mega_Usr** ega_Usr, there is a the same level in the file and save tese are environment-specific and correspond to objects in the Mega respositories. It is mandatory to transfer these if you want to keep your customizations.

1. In the source server, go to the root level of your environment.
2. Copy everything included in the **Mega_Usr** folder.



3. Go to the target server in the folder of the duplicated environment.
4. Paste everything in the **Mega_usr** folder.