

*GRANTA MI™ version 11*

# **GRANTA MI**

# **Administrator's Guide**

GRANTA MI™ is the leading system for materials information management in engineering organizations. It enables you to control, analyze, and securely share critical corporate data on materials and processes, managing the materials information lifecycle.

[www.grantadesign.com](http://www.grantadesign.com)

© Granta Design 2018 All rights reserved

CES Selector and GRANTA MI are trademarks of Granta Design Ltd. For other Granta product trademarks, see [www.grantadesign.com/smallprint.htm](http://www.grantadesign.com/smallprint.htm)

Adobe®, Adobe® PDF, and Acrobat® are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Microsoft®, Excel®, PowerPoint®, Internet Explorer®, SQL Server®, Windows®, and Windows Server® are registered trademarks of Microsoft Corporation or its subsidiaries in the United States or other countries.

Granta Design Ltd. makes reasonable efforts to explicitly acknowledge all trademarks cited in our literature or on our website. If you would like us to add or alter an acknowledgement, please [contact us](#).

Release notes, documentation, and Knowledge Articles for the current and all previous GRANTA MI releases are all available on the Granta Support website. Go to [www.grantadesign.com](http://www.grantadesign.com) and click SIGN IN to log into your My Granta page, then click on **Documentation**.

We welcome your feedback on this document. Please let us know if anything is unclear, if you spot an error, or have an idea for new content, by emailing [docs@grantadesign.com](mailto:docs@grantadesign.com)

Document version: MI11/03  
Published: April 2018

## Table of Contents

<b>1</b>	<b><i>Introduction.....</i></b>	<b>5</b>
1.1	IT Systems/Network Administrator .....	5
1.2	SQL Server Administrator .....	5
1.3	GRANTA MI application administrator .....	5
1.4	Granta database administrator .....	5
1.5	User assistance for GRANTA MI .....	6
1.6	Your feedback.....	6
<b>2</b>	<b><i>GRANTA MI system overview.....</i></b>	<b>7</b>
2.1	MI:Server .....	7
2.2	Database server .....	8
2.3	MI:Viewer .....	9
2.4	MI:Admin and MI:Toolbox .....	10
2.5	Ports used by GRANTA MI software .....	11
<b>3</b>	<b><i>MI:Server application administration .....</i></b>	<b>12</b>
3.1	Configuring the MI:Server-SQL Server connection .....	13
3.2	System security settings .....	14
3.3	Indexing software (iFilters).....	16
3.4	Configuring Notifications.....	16
3.5	MI:Server Cache Files .....	20
3.6	Max-min cache update delay .....	20
3.7	Restarting the GRANTA MI service .....	21
3.8	MI:Server log files.....	21
<b>4</b>	<b><i>MI:Viewer application administration .....</i></b>	<b>23</b>
4.1	Configuring the MI:Viewer-MI:Server connection .....	23
4.2	Configuring custom authentication settings .....	23
4.3	Enabling access to analysis reports in MI:Viewer .....	24
4.4	Setting the MI:Viewer home page .....	24
4.5	Enabling access to large, externally-stored files .....	25
4.6	Changing display settings in datasheets.....	28
4.7	Changing the default unit systems .....	29
4.8	Modifying default search mask behavior .....	29
4.9	Managing search stop words .....	30
4.10	Embedded media support.....	30

---

4.11	Increasing the maximum report size .....	32
4.12	MI:Viewer log files.....	33
4.13	MI:Viewer configuration files .....	34
<b>5</b>	<b><i>MI:Toolbox application administration .....</i></b>	<b><i>35</i></b>
5.1	MI:Toolbox configuration files .....	35
5.2	Configuring plug-in shadowing.....	36
<b>6</b>	<b><i>Granta database administration .....</i></b>	<b><i>37</i></b>
6.1	Logging in to MI:Admin .....	37
6.2	Locking the database while making changes .....	38
6.3	Defining and modifying the database schema .....	38
6.4	Managing profiles.....	39
6.5	Access control for database items .....	40
6.6	Record version control .....	40
6.7	Managing templates stored in the database .....	41
6.8	Managing database home pages.....	41
6.9	Managing attribute and parameter help pages .....	42
6.10	Managing FEA exporters .....	43
6.11	Managing configuration files.....	44
6.12	Importing templates for MI:Optimize .....	45
6.13	Applying Product Risk data updates.....	45
<b>7</b>	<b><i>Application Activity reporting .....</i></b>	<b><i>46</i></b>
	<b><i>Appendix A. MI:Server Audit Logging.....</i></b>	<b><i>47</i></b>
	<b><i>Appendix B. Troubleshooting .....</i></b>	<b><i>50</i></b>

# 1 Introduction

This document gives an overview of the different GRANTA MI administration tasks, and the various tools provided to carry them out.

Administration of the GRANTA MI system may be distributed between a number of different people in your organization. You will require at least one user with privileges to administer the GRANTA MI system configuration. You may also have additional users with privileges to administer the GRANTA MI databases. The same person may carry out both of these roles, but it is not required. Neither of these roles require Windows or SQL Server administration privileges, but the GRANTA MI system administrator will require co-operation from the IT systems/network administrator and the SQL Server administrator for initial installation and system setup.

## 1.1 IT Systems/Network Administrator

An IT systems/network administrator will need to:

- Provision the GRANTA MI host server(s)
- Ensure MI Administrators are able to access the application server where GRANTA MI applications are installed.

## 1.2 SQL Server Administrator

A SQL Server Administrator will need to:

- Restore GRANTA MI databases to SQL Server, and back them up
- Set up the appropriate user logins to allow access MI databases from GRANTA MI

## 1.3 GRANTA MI application administrator

The application administrator is typically responsible for updating, security, and troubleshooting of GRANTA MI applications:

- Ensuring that the databases hosted on SQL Server can be accessed from GRANTA MI applications
- Upgrading MI databases when required
- Managing GRANTA MI system and database security groups
- Setting the access control mode for GRANTA MI
- Configuring system-wide features such as automated email notifications.

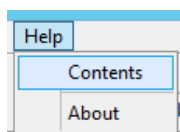
## 1.4 Granta database administrator

A GRANTA MI database administrator is a data specialist who may typically be responsible for:

- Modifying the structure and properties of GRANTA MI databases
- Implementing permission-based access control and version control in MI databases
- Managing the templates used for searching, reporting, and exporting data from MI databases
- Defining custom profiles, used to group data into meaningful collections for particular groups of MI:Viewer users
- Loading and managing profile and database home pages.

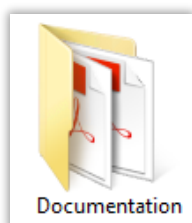
## 1.5 User assistance for GRANTA MI

User assistance for GRANTA MI is delivered in a number of different ways:



### Help for application users

Help for all GRANTA MI applications and tools, providing procedural information on how to use the features within the application, is installed along with the software and can be accessed from the Help menu.



### Reference documentation on the MI:Server or MI:Toolbox host

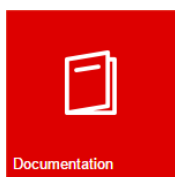
GRANTA MI reference documentation aimed at IT Administrators, Granta System Admins and Data Administrators, and people importing/exporting data, is installed on the MI:Server and MI:Toolbox host servers during product installation.

- For MI:Server, typically, this will be in  
C:\Program Files\Granta\GRANTA MI\Server\Documentation
- For MI:Toolbox, PDF documentation is installed in a Documentation subfolder within each plugin



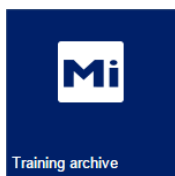
### Reference documentation in MI:Viewer

The GRANTA MI reference documentation is copied to the MI:Viewer host server during product installation, and can then be accessed by all users from the MI:Viewer **Help** menu.



### Documentation on the Granta Support website

Release notes, documentation, and Knowledge Articles for the current and all previous GRANTA MI releases are all available on the Granta Support website. Go to [www.grantadesign.com](http://www.grantadesign.com) and click **SIGN IN** to log into your My Granta page, then click on **Documentation**.



### GRANTA MI training videos on the Granta Support website

Short videos aimed at experienced users and Granta administrators are available on the Support website, exploring a range of topics including tabular data, embedded equations and logic, and best practices for importing and exporting data. Go to [www.grantadesign.com](http://www.grantadesign.com) and click **SIGN IN** to log into your My Granta page, then click on **MI Training archive**.

## 1.6 Your feedback

We welcome your feedback on Granta help and documentation; please email your comments to: <mailto:docs@grantadesign.com>

For product-related questions, please contact [Granta Technical Support](#).

## 2 GRANTA MI system overview

GRANTA MI is a materials database system consisting of a core module – MI:Server – and a range of platform, add-on, and data modules. The following sections introduce the core GRANTA MI software components – MI:Server, MI:Viewer, MI:Admin and MI:Toolbox.

### 2.1 MI:Server

The GRANTA MI application server, MI:Server, is the hub of the GRANTA MI software deployment. It is hosted as a Windows service. Two Windows applications are provided for MI:Server configuration and management:

- **MI:Server Manager** – for configuring MI:Server settings, including database settings, security groups, notifications and licensing details.
- **MI:Server Connection tool** – for configuring the connection between the MI:Server application server and the database server where the MI:Server configuration database is stored.

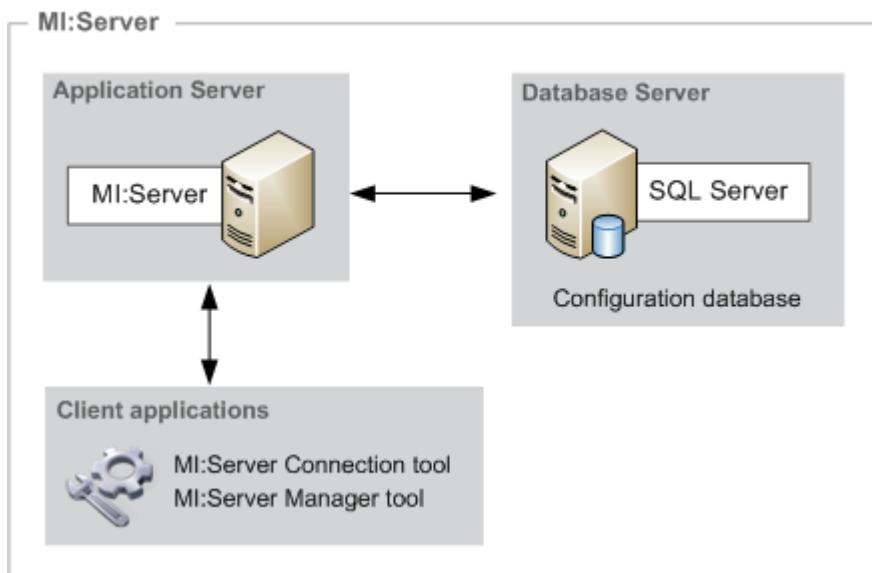


Figure 1. Components of MI:Server

The **configuration database** for MI:Server is hosted in SQL Server. It stores

- Which databases are loaded in GRANTA MI, and their connection details
- Currency conversions
- Notification information
- Some authorization information.

The MI:Server Manager tool can be used to modify many of the settings stored in the configuration database.

## 2.2 Database server

GRANTA MI runs on Microsoft SQL Server. The database server hosts:

- The configuration database for MI:Server, storing GRANTA MI server-wide configuration settings.
- GRANTA MI databases storing the materials information for end users, for example, Granta materials reference data modules, data from in-house testing and design and other proprietary sources, and trusted references.

Database utilities such as back-up are not part of GRANTA MI functionality. Regular back-ups and other management tasks should be carried out by SQL Server Management Studio or a third party management tool.

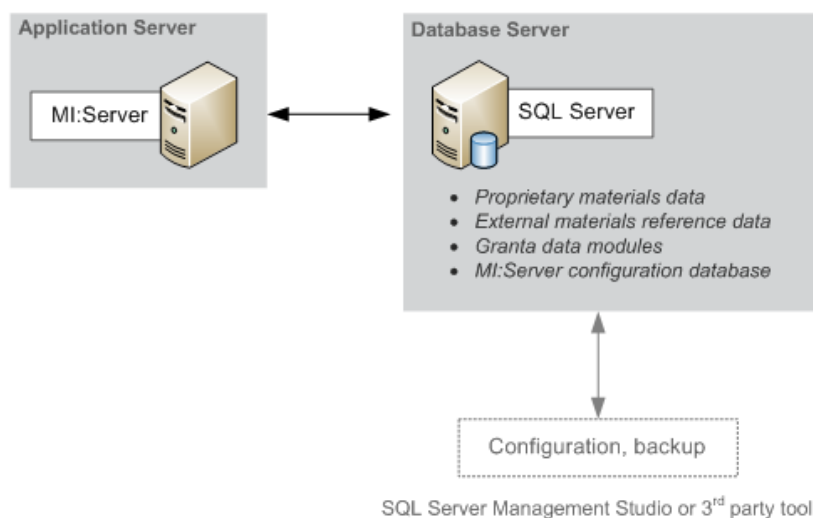


Figure 2. MI:Server and the SQL Database Server

A SQL Server account with administrative privileges (dbcreator) is required to create the GRANTA MI configuration database during MI:Server installation.

Once installed, MI:Server communicates with SQL Server using the login specified during installation, which must be an account with a db\_owner database-level role for all Granta databases, including the configuration database. Typically, when using SQL Server Authentication, this account is named *MIUser*, and when using Windows Authentication, this is the account under which the MI:Server service runs (for example, *MIServiceAccount*).

SQL Server authentication options for GRANTA MI are covered in detail in the *GRANTA MI Installation Guide*.

The settings that define how MI:Server connects with SQL Server, including the authentication mode and user credentials, are initially set during MI:Server installation, and can subsequently be modified using the MI:Server Connection tool; see Section 3.1.



## 2.3 MI:Viewer

The GRANTA MI web server, MI:Viewer connects to the MI:Server application server and provides tools to browse, query, report on, edit, import, and export data. It is hosted in Microsoft Internet Information Services (IIS), and is a stateless presentation layer relying on MI:Server for all business logic and transactions with the database layer.

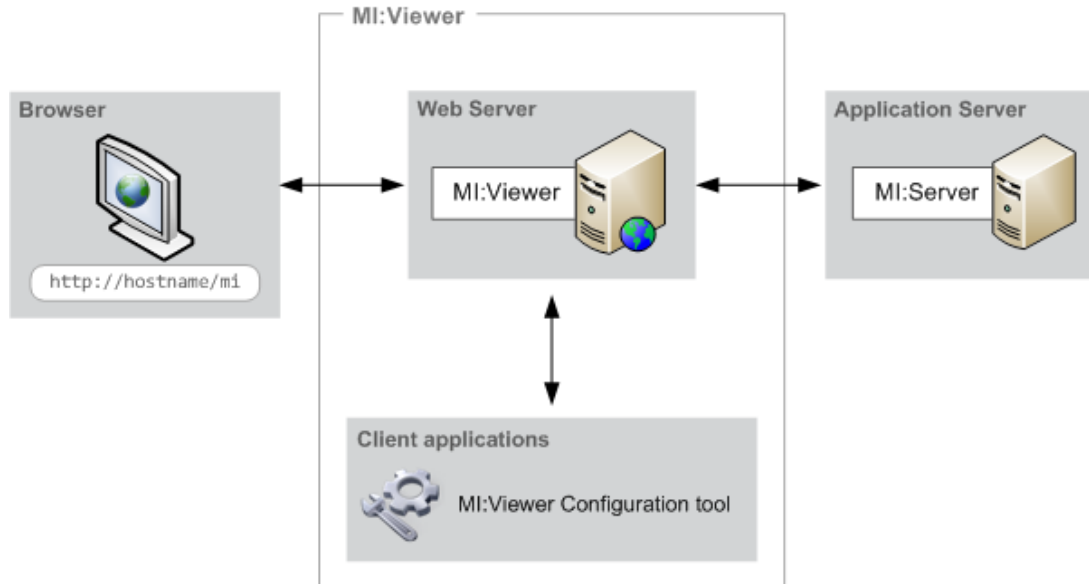


Figure 3. MI:Viewer implementation

The MI:Viewer Configuration tool is used to set the connection between MI:Viewer and MI:Server. The connection between MI:Viewer and MI:Server is persistent, but, if broken, is renewed upon the next connection request.

See Section 4, [MI:Viewer application](#).

## 2.4 MI:Admin and MI:Toolbox

MI:Admin is the Windows client application used for database administration.

MI:Toolbox is a Windows client application for importing, processing, and manipulating large quantities of materials data. It is a framework to host a suite of plug-ins, with data manipulation functionality provided by the plug-ins.

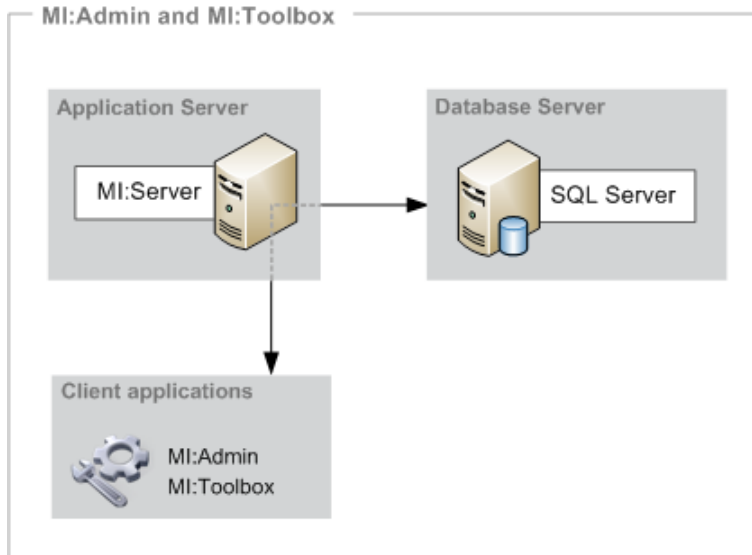
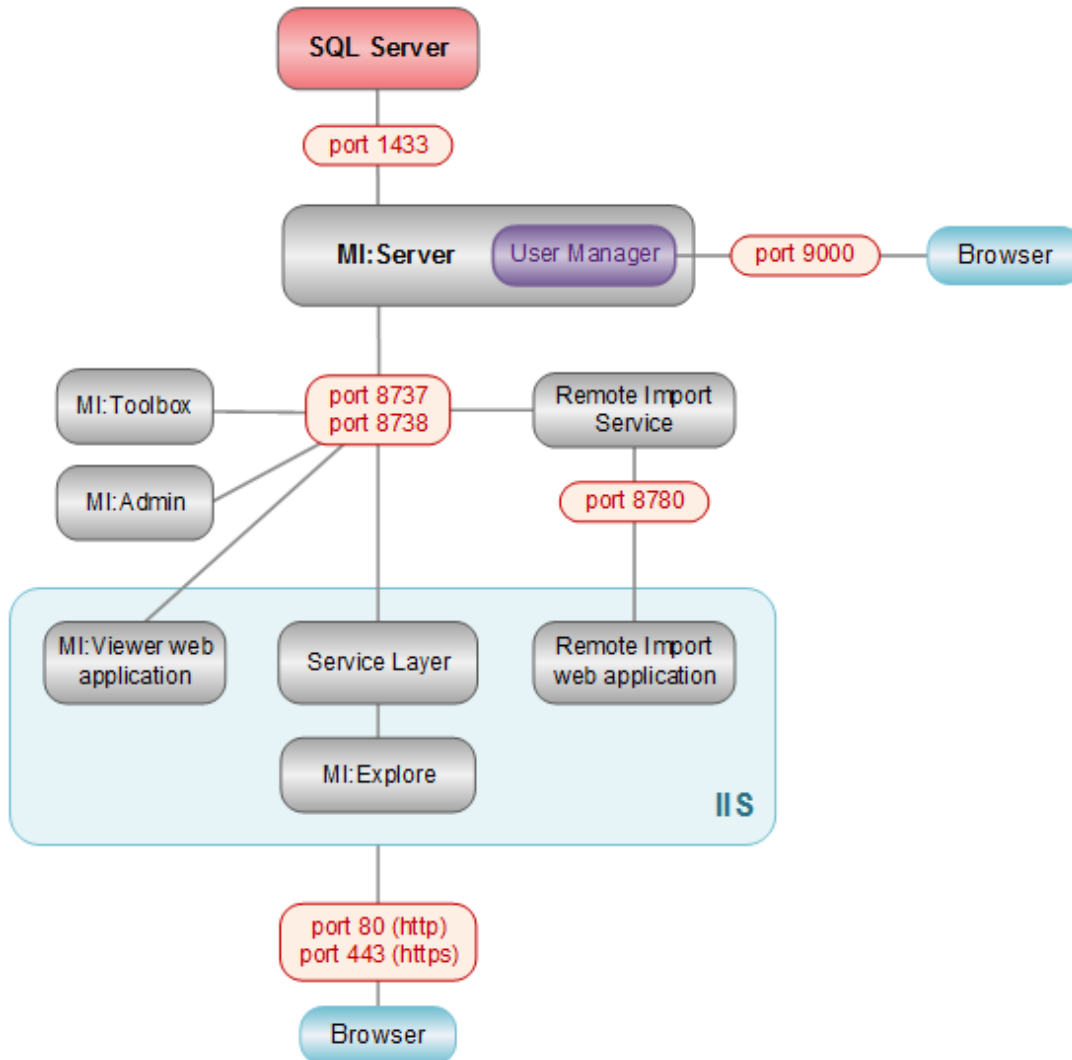


Figure 4. Windows client applications MI:Admin and MI:Toolbox

## 2.5 Ports used by GRANTA MI software

GRANTA MI Windows clients connect to MI:Server on ports 8737/8738 using the TCP protocol "gtcp". The ports are opened on the server on which MI:Server is installed, not the client machine.

The GRANTA MI system requires the following ports to be opened through the firewall of the computer on which MI:Server is installed, when it is deployed across a network.



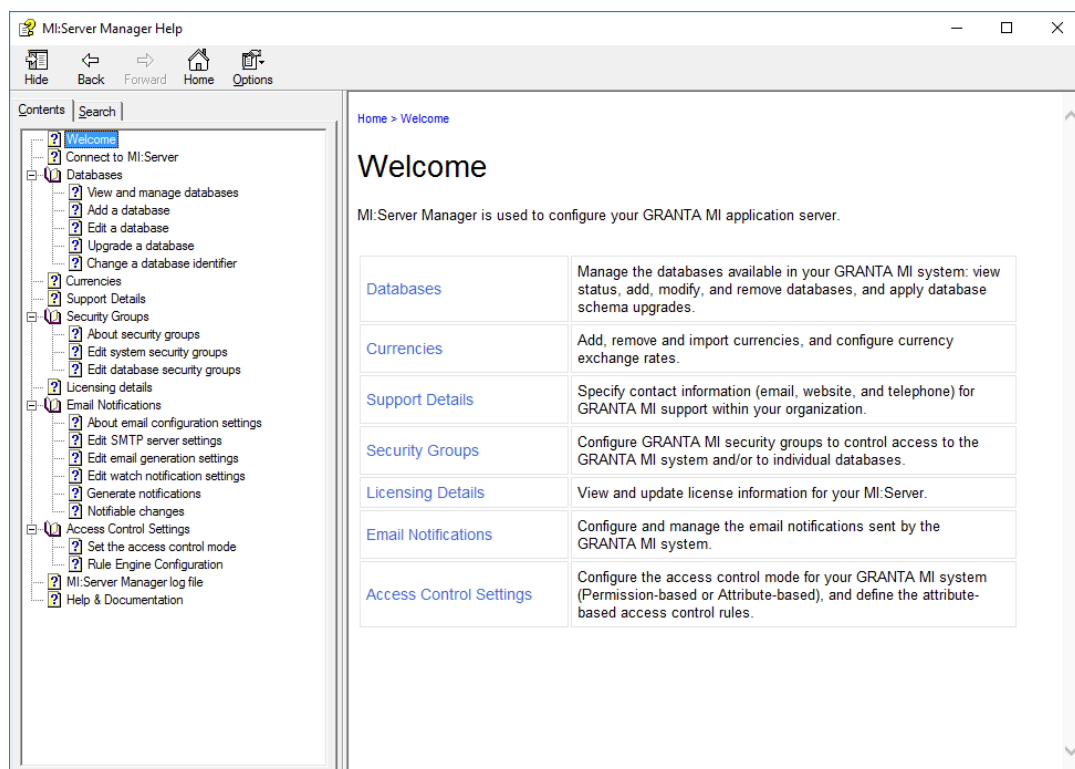
For details of configuration options for User Manager, including how to specify a different port, see the *GRANTA MI Configuration Guide*.

### 3 MI:Server application administration

Two tools are provided for configuration and management of the GRANTA MI application server:

- **MI:Server Connection** – use this tool for
  - Changing the credentials used for the connection between MI:Server and the SQL Server instance where the GRANTA MI configuration database is installed; see [3.1](#).
  - Changing GRANTA MI system security (user authentication/authorization) settings; see [3.2](#).
- **MI:Server Manager** – use this tool to carry out a number of administration tasks on the application server, including:
  - Adding and removing databases, monitoring database status and availability, changing database authentication credentials, and making databases read-only.
  - Defining system and database security groups.
  - Viewing and modifying GRANTA MI license information.
  - Configuring email notification settings; see also Section [3.3](#).
  - Generating watch notifications.
  - Selecting the GRANTA MI Access Control mode (permission-based or attribute-based).
  - Viewing and modifying the currencies and exchange rates used in GRANTA MI.
  - Identifying a support contact in your organization for GRANTA MI queries.

See the Help for the MI:Server Manager application for detailed information on all the above tasks.



### 3.1 Configuring the MI:Server-SQL Server connection

The connection between MI:Server and the SQL Server instance where the GRANTA MI configuration database is installed is initially set up during product installation, and can subsequently be configured using the MI:Server Connection tool. This is a Windows client tool that is installed on the same machine as on the MI:Server, and requires Administrator privileges on the server.

Changes made within the MI:Server Connection tool will require an MI:Server restart. This will cause all GRANTA MI client applications to lose their connection to MI:Server for a short period. All the memory-based caches for the databases in the list will be reloaded. If the databases are large, this may take some time. Disk-based (full text search) caches are not affected.

#### 3.1.1 About the GRANTA MI configuration database

The GRANTA MI configuration database, hosted on Microsoft SQL Server, stores GRANTA MI server-wide configuration settings, including:

- Which GRANTA MI databases are available to GRANTA MI users, and their connection details
- Currency conversions
- Notification information
- Some authorization information.

The configuration database may be hosted in the same SQL Server as the materials databases, or it may be in a separate SQL Server.

To establish a connection between the MI:Server application and the configuration database, the following information is required:

1. The name of the SQL Server hosting the database.
2. The authentication information required to connect to the SQL Server: 'Windows Authentication' is the default option.
3. The name of the MI configuration database on the selected SQL Server (usually *MIConfig*).

This connection is initially set up during MI:Server installation, and can subsequently be modified using the MI:Server Connection tool.

#### 3.1.2 To set or change the configuration database connection settings

Open the MI:Server Connection tool, **Start > Programs > GRANTA MI > MI Server Connection**, and then modify the configuration settings:

Option	Description
SQL Server	This is the name of the server where the SQL Server database that GRANTA MI will use is installed, and the name of the SQL Server instance where GRANTA MI databases are installed. For example: <i>mydbserver\SQL2012</i>
Connect using	This specifies how MI:Server will authenticate to the selected SQL Server instance. <ul style="list-style-type: none"> <li>• <b>Windows Authentication</b> (default) – MI:Server authenticates using the Windows account under which the GRANTA MI service is currently running, for example, <i>MIServiceAccount</i>.</li> <li>• <b>SQL Server Authentication</b>: enter credentials for an existing login on the SQL Server instance, with db_owner database-level role for the GRANTA MI</li> </ul>

Option	Description
	configuration database. To use this option, the SQL Server must have Mixed Mode authentication enabled. (Note that, by default, SQL Server 2012 enables only Windows Authentication.)
Configuration database	All GRANTA MI configuration databases found on the specified SQL Server instance are listed here. If you can't see the database you need here, check your SQL Server authentication settings.
Advanced...	<ul style="list-style-type: none"> <li data-bbox="486 472 1385 600"> <b>Additional Connection parameters:</b> enter any additional connection string parameters here, delimited by a semicolon. For example, to increase the connection timeout to 120 seconds, and to specify a machine to use as a failover partner server where database mirroring is enabled:           <div data-bbox="582 611 1217 795" style="border: 1px solid #ccc; padding: 5px; margin: 10px 0;"> <p data-bbox="614 629 906 651">Additional Connection parameters</p> <p data-bbox="630 669 1150 719">You can specify additional SQL Server connection parameters, for example, to change the connection timeout.</p> <p data-bbox="630 734 1031 761">Failover Partner=RAVEN;Connect Timeout=120</p> </div> </li> <li data-bbox="486 819 1385 1043"> <b>Connection Delay:</b> Normally, MI:Server will reconnect to the SQL Server instance immediately after a restart. Where SQL Server is installed on the same machine as MI:Server, it may be useful to set a delay to ensure that SQL Server is ready for the connection, for example, after a machine reboot. The maximum value allowed is 900 seconds (15 minutes). The delay time will depend on your particular configuration of hardware and software. A typical value might be 30–180 seconds.           </li> </ul>

MI:Server will be automatically restarted after making any configuration changes in the MI:Server Connection tool. This will cause all GRANTA MI client applications to lose their connection to MI:Server for a short period. All the memory-based caches for the databases in the list will be reloaded. If the databases are large, this may take some time. Disk-based (full text search) caches are not affected.

### 3.2 System security settings

By default, GRANTA MI uses Windows Active Directory for both authentication and authorization. However, other configuration options are available:

- User Manager, the Granta user management web application, can be used instead of Windows for user authentication and/or authorization.
- A custom authenticator, developed using the GRANTA MI Software Development Kit (SDK) can be used to authenticate GRANTA MI users.

You can select different combinations of authentication and authorization provider in the MI:Server Connection tool, which provides the following system security mode options:

- **Windows Authentication / Windows Authorization** —Users log in to the system using their Windows credentials, and their Windows group membership determines what they can do and the resources they can access within GRANTA MI. This is the default configuration.

- **Windows Authentication / User Manager authorization** — Users log in to the system using their Windows credentials, and their membership of User Manager groups determines what resources they see and what they can do in GRANTA MI.
- **User Manager authentication / User Manager authorization** — Users log in to GRANTA MI with their User Manager credentials, and their User Manager group membership determines what they can see and do within the system.
- A custom authenticator for user authentication can also be selected; see 3.2.2.

### 3.2.1 Changing the MI:Server system security mode

1. Open the MI:Server Connection tool: **Start > Programs > GRANTA MI > MI Server Connection**
2. On the **Options** menu, click **System Security Settings**.
3. Select one of the options on the list of system security modes.

If you select the **User Manager authentication / User Manager authorization** option, you need to enter the username and password for an Administrator account in User Manager. The account will be created, if it does not already exist. The password must be a minimum of 6 characters, and must include at least one uppercase character (A-Z), lowercase character (a-z), digit (0-9), and non-alphanumeric character (not a letter or a digit).

Note also that if you select this option, you will also need to configure the User Manager authentication for use with the MI:Viewer, MI Service Layer, and MI:Remote Import software components; see the *GRANTA MI Configuration Guide*.

4. Click **OK** and then click **Save changes & restart service**.

MI:Server will automatically be restarted. This will cause all GRANTA MI client applications to lose their connection to MI:Server for a short period. All the memory-based caches for the databases in the list will be reloaded. If the databases are large, this may take some time. Disk-based (full text search) caches are not affected.

### 3.2.2 Selecting a custom authenticator

To use a custom authenticator developed using the GRANTA MI Software Development Kit (SDK) for user authentication in GRANTA MI:

1. Close the MI:Server Connection tool, if it is open.
2. Copy the custom authenticator dll into the bin folder within the MI:Server installation folder, typically C:\Program Files\Granta\GRANTA MI\Server\bin.
3. Open the MI:Server Connection tool: **Start > Programs > GRANTA MI > MI Server Connection**
4. On the **Options** menu, click **System Security Settings**.
5. Click **Advanced**.
6. Select the custom authenticator from the list and click **Configure Parameters** to specify any parameter settings. These will depend on the authenticator.
7. Back in the MI:Server Connection main window, click **Save changes & restart service**.

The GRANTA MI service will automatically restart; when it comes back, it will be using the new authenticator.

### 3.3 Indexing software (iFilters)

iFilters (“indexing filters”) allow the text content of different files types imported into a GRANTA MI database to be indexed, enabling those files to be searched in GRANTA MI. Storage and display of files does not require an iFilter, only searching.

GRANTA MI does not include any indexing software. To ensure that text within Microsoft Office and Adobe® PDF files stored in GRANTA MI is searchable, iFilters must be installed on the GRANTA MI application server.

- **Office iFilters.** If Microsoft© Office is not installed on your GRANTA MI server, then Office iFilters will need to be installed to allow any *.docx*, *.pptx*, or *.xlsx* files in the GRANTA MI database to be searched. Office iFilters are included in Microsoft Office Filter Packs, which can be downloaded from the Microsoft Download Center [here](#).
- **PDF iFilters.** Use of the Adobe PDF iFilter is not supported with GRANTA MI. The GRANTA MI Version 11 download package includes a compatible third-party PDF iFilter which has been evaluated against GRANTA MI Version 11, and which is licensed for use with GRANTA MI. See the README in the download package for information about installing this.

Note that Granta cannot guarantee the working of any third party iFilter.

### 3.4 Configuring Notifications

The Notifications feature in MI:Viewer allows users to monitor changes to records, folders, and data of interest. Users can “watch” specific records, folders, and data, and view notifications about any changes made to items on their “watch list”. Users may be able to check their notifications in MI:Viewer (**Settings > Notifications**), and/or receive auto-generated email notifications about changed items. Notifications shown to users will only include information that they have permission to see.

To configure Notifications, you need to carry out the following steps:

1. In MI:Viewer, enable the Notifications feature, and specify who will be able to see the Notifications tab in MI:Viewer and request notification updates. See [3.4.1](#).
2. In MI:Server Manager, configure the notification email settings. See [3.4.2](#).
3. Optionally, set up a notifications scheduled task. See [3.4.4](#).

#### 3.4.1 Enabling/disabling Notifications

GRANTA MI administrators can control the availability of Notifications functionality in MI:Viewer via two options under the *Notifications options* heading on the **Admin** page, **General** tab.

**Notifications options**

These options control the availability of the Notifications features within MI:Viewer.

Enable Notifications - all users can add items to their watch list and receive email notifications of changes.

Show the Notifications tab only to Admin users – only MI Administrators can see the Notifications tab, and interactively view/load notifications for watched items.



Option	Description
<b>Enable Notifications</b>	<p>Enables and disables the Notifications feature in MI:Viewer. When enabled (check box is selected), users will be able to add items to their watch list, receive email notifications (if this is configured) and may also be able to check their notifications on the <b>Notifications</b> tab, depending on the 2nd option setting, described below.</p> <p>When disabled (check box is not selected), this feature will be turned off for all users. No users will see the <b>Notifications</b> tab or be able to add items to watch lists, and no email notifications will be auto-generated.</p>
<b>Show the Notifications tab only to Admin users</b>	<p>This option allows you to prevent non-Admin users from checking for notification information about their watched items.</p> <p>When this check box is selected, only Admin users will see the <b>Notifications</b> tab. Users who are not administrators will not see the <b>Notifications</b> tab, but will still be able to add items to watch lists and receive automatically-generated notification emails (if configured).</p> <p>When this check box is not selected, all users will see the <b>Notifications</b> tab.</p>

### 3.4.2 Configuring email settings for Notifications

Configuration for email notifications about watched items is done in MI:Server Manager, on the Email Notifications pages. This includes:

- SMTP server settings for notification emails.
- General email settings (message content, email frequency and queuing options, trusted domains) for watch notification emails. The emails are sent by GRANTA MI as MIME format, with both an and a plain text part. It is the email client of the receiving user which determines what is displayed. Times in emails are in UTC.
- Per-user watch notification settings (whether or not a user receives watch notifications, which items they receive notifications for, and their email details).

See the Help for MI:Server Manager for detailed information about these settings.

### 3.4.3 Generating notifications from a command prompt

Notifications are generated by running miserver.exe with the **notifications** argument, either in a command window or as a scheduled task. In a default installation, the executable is located in:

```
C:\Program Files\Granta\GRANTA MI\Server\bin
```

You can also generate notification emails by running a batch file from the command prompt.

In all cases, information on the notification email generation process is written to the MI:Server notifications log file, see [3.4.5](#).

To generate notification emails from a command window:

1. Open a command window, and go to the *bin* folder of the MI:Server installation folder.
2. Enter the command **miserver.exe notifications**, plus any required command-line options. For example:



```

C:\Program Files\Granta\GRANTA MI\Server\bin>miserver.exe notifications
Executing notifications <Processes notifications>:
Notifications processed successfully
C:\Program Files\Granta\GRANTA MI\Server\bin>_

```

With no command-line arguments specified, notification information is generated from watched items in all databases in your GRANTA MI system. To include only notifications from specific databases, use one of the following command-line options:

#### **-i:dbkey**

Include notifications for the specified database only; For multiple databases, repeat the **-i** option for each database:

```
miserver.exe notifications -i:MI_MandP_5.31.2m
```

```
miserver.exe notifications -i:metals_db -i:composites_db
```

#### **-x:dbkey**

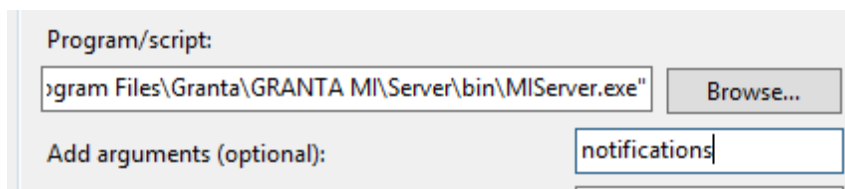
Include notifications for all databases except the specified database. To exclude additional databases, repeat the **-x** option for each one. For example

```
miserver.exe notifications -x:test_db -x:alloys_temp
```

You can use either one of these two command line options, but not both; that is, you can specify the databases for which you want to notifications, or the databases for which you do not want notifications. If you don't specify any notifications options, notification emails will include notifications from all databases in the system.

### 3.4.4 Setting up a notifications scheduled task

Using the Windows Task Scheduler, you can set up a scheduled task to run the `miserver.exe` program with the notifications argument, for example:



The **notifications** argument is case sensitive; use the **-i** or **-x** command-line arguments described in the previous section, if required, to include or exclude specific databases.

When setting the user to **Run as**, specify the same account used to run the MI Service, for example, *MIServiceAccount*.

Note that, for notifications to run successfully:

- This account must be able to query your user management system for the email addresses;
  - If managing MI users using Active Directory, the specified account needs to be a domain account
  - If managing MI users with User Manager, the account should have MI administrator privilege.
- This account should be given "Log on as a batch job" user rights on the server (by default, only the LocalSystem account has the privilege to be logged on as a batch job).
- Do **not** select the **Do not store password** option; if the password is not stored, the task will only have access to local resources and, most importantly, will not be able to access SQL Server:

Security options

When running the task, use the following user account:

TECHCOMMS-TEST\MiServiceAccount Change User or Group...

Run only when user is logged on

Run whether user is logged on or not

Do not store password. The task will only have access to local computer resources.

Run with highest privileges

### 3.4.5 Notifications logging

The notification email generation process writes its own log file, MIServer.Notifications\_{date}.log, separate to the main MI:Server log. Times in the log file are in UTC.

The default location of this log file is in a Logs folder in %PROGRAMDATA%. In a default installation, this will be:

```
C:\ProgramData\Granta\GRANTA MI\Server\Logs
```

The name and location of the notifications log file is set in the configuration file log4net.notifications.config, located in the config folder in the MI:Server installation folder. To change the default notifications log file name or location, you need to edit log4net.notifications.config and edit the following element to specify an alternative location/filename:

```
<file value="..\Logs\MIServer.Notifications_%date{yyyy-MM-dd_HH-mm-ss}.log"...
```

### 3.4.6 Notifications information in the Application Activity Summary

Notification emails are logged in the GRANTA MI Application Activity Summary.

### 3.5 MI:Server Cache Files

MI:Server generates a cache of data for each database for full text searching. Synchronous caching is enabled as the default, so only one database caches at a time. The default location of these files is in a subfolder in the MI:Server installation folder, typically:

```
C:\Program Files\Granta\GRANTA MI\Server\Caches
```

To manually refresh the cache for a database, you must remove the database from the configuration and add it again. For large databases, it may take some time before the database is available to the GRANTA MI system again.

The location of the MI:Server Caches folder is specified in the configuration file `MIServer.exe.config`, located in the `bin` folder in the MI:Server installation folder. To change the default location for cache files, you need to edit `MIServer.exe.config` and modify the `<Search>` element to specify a suitable folder. It is important that the folder you set is accessible for reading and writing by the SYSTEM user on the local machine.

The GRANTA MI service must be restarted after any changes to `MIServer.exe.config`; see Section 3.7.

### 3.6 Max-min cache update delay

For performance optimization reasons, changes to maximum and minimum values of numeric (integer, range, point and date) attributes are not written to the database immediately, but after a short (1 minute) delay.

This means that max and min values shown on the MI:Viewer Search page may be out-of-date for a short (<2 minutes) period after any changes, until the cache is updated.

If this is unacceptable, the update delay can be reduced or removed altogether, at the cost of slower writes to the database, via a change to the MI:Server config file `MIServer.exe.config`, located in the MI:Server `bin` folder.

1. Edit `MIServer.exe.config` and locate the line under `<configSections>` where `Search` properties are defined. For example:

```
<Search cachepath="..\Caches" cacheUpdater="Synchronous"
optimiseTime="23:30:00" stopWords="www; http" maxFieldLength="20000" />
```

2. Add a new `minMaxCacheUpdateDelay` attribute to this line to specify the required delay; zero means keep the min-max cache up-to-date on every commit.

For example:

```
<Search minMaxCacheUpdateDelay="00:00:00" cachepath="..\Caches"
cacheUpdater="Synchronous" optimiseTime="23:30:00" stopWords="www; http"
maxFieldLength="20000" />
```

The GRANTA MI service must be restarted after any changes to `MIServer.exe.config`; see Section 3.7.

## 3.7 Restarting the GRANTA MI service

Restarting the GRANTA MI service will cause all GRANTA MI client applications to lose their connection to MI:Server for a short period. All the memory-based caches for the databases in the list will be reloaded. If the databases are large, this may take some time. Disk-based (full text search) caches are not affected.

### 3.7.1 To restart the service from Windows Services:

1. Open the Services Microsoft Management Console (MMC) snap-in.
2. Locate the **GRANTA MI Service** and restart it.

### 3.7.2 To restart the service from the command line:

The GRANTA MI service can also be restarted from the command line. You must stop it and then start it again using two separate commands.

1. Open a command prompt on the server on which MI:Server is installed.
2. Type: **net stop GRANTAMIService**  
You will be notified that the service is stopping.
3. Type: **net start GRANTAMIService**  
You will be notified that the service is starting.

## 3.8 MI:Server log files

You can download MI:Server log files from the **Download MI:Server logs** panel on the MI:Viewer **Admin>Logging** tab. Downloaded files are saved in a zip file that includes:

- Daily MI:Server application logs that include startup and shutdown information, errors, warning messages, and additional information.
- Notifications logs, containing information on MI:Server notifications service events.
- Data Updater logs.

### MI:Server.log

By default, the MI:Server log file, MI:Server.log is located in the %PROGRAMDATA% folder here:

```
C:\ProgramData\Granta\GRANTA MI\Server\Log\
```

The name and location of the MI:Server log file is specified in the configuration file log4net.config, located in the config folder in the MI:Server installation folder.

### Logs for client applications

Logs for the various GRANTA MI installers, and for the MI administration/configuration applications including MI:Admin, MI:Server Manager, MI:Server Connection, MI:Toolbox are stored in the local

part of your user profile, the precise location is dependent on your operating system. Typical locations are:

%USERPROFILE%\AppData\Local\Granta Design\MI\logs

%USERPROFILE%\Local Settings\Application Data\Granta Design\MI\logs

The default log file names and locations are specified in the application configuration files located in the config folder in the MI:Server installation folder. To change default log file name or location for an application, you need to edit the appropriate configuration file.

## 4 MI:Viewer application administration

### 4.1 Configuring the MI:Viewer-MI:Server connection

MI:Viewer requires a connection to MI:Server. This connection is set up when MI:Viewer is installed and can be edited subsequently using the MI:Viewer Configuration tool.

#### To change the connections details between MI:Viewer and MI:Server:

1. Open the MI:Viewer Configuration tool:  
**Start > All Programs > GRANTA MI > MI Viewer Configuration**
2. Click **Configure Connection**.
3. Enter the hostname of the computer on which MI:Server is installed. When MI:Server and MI:Viewer are on the same computer, this will be localhost.
4. Enter the credentials of the account that will be used by MI:Viewer to connect to MI:Server:
  - If using Windows authentication to MI:Server, you should enter the user name, password, and domain of a Windows account: this account must be a member of the MI\_ADMIN group. We recommend that you specify an account that has a password that does not expire.
  - If using User Manager authentication to MI:Server, enter the username and password of a User Manager Administrator account here (typically, the account specified when MI:Server was installed). Leave the Domain field empty.
5. Click **OK**, then, on the **File** menu, click **Save** to save the connection details.

### 4.2 Configuring custom authentication settings

The MI:Viewer web application uses IIS for authentication by default. Upon installation of MI:Viewer, 'Windows Authentication' and 'Basic Authentication' are both enabled. IIS authentication settings are edited using Microsoft Internet Information Services (IIS) Manager.

Custom (third-party) authenticators can also be developed for MI:Viewer using the GRANTA MI Software Development Kit (SDK). Settings for custom authenticators can be modified in the MI:Viewer Configuration tool.

#### To change custom authentication settings:

1. Open the MI:Viewer Configuration tool.
2. On the **Options** menu, click **Authentication Settings**.
3. Select the custom authenticator for the list of available authenticators, and set any required parameters. The available parameters will depend on the custom authenticator implemented.
4. Click **OK**, then close the tool and click **Yes** to save the changes.

### 4.3 Enabling access to analysis reports in MI:Viewer

Analysis reports can be used in MI:Viewer and MI:Explore to analyze lists of materials or substances in a GRANTA MI database. This may include Granta reference data modules and/or your company's own in-house data.

Analysis reports are provided by MI:Reports, an optional software component that enables analysis of different aspects of product design and risk.

To run an analysis report, users submit the report to a report job queue. Processing of the reports in the queue is handled by the Granta Service Layer, which runs each report in sequence, one at a time ('asynchronously'). Users can view their submitted reports on the queue, and download reports that have completed, in the Report Monitor, which is accessed via a link on the Report page in MI:Viewer.

#### To enable access to analysis reports and to the Report Monitor:

1. Open the MI:Viewer Configuration tool.
2. On the Options menu, click **Custom Reports**.
3. Select **Enable Custom Reports in MI:Viewer** and then enter the URL for the Service Layer. If https is being used, the URL should reflect this.

Example: `http://hostname.acme.local/mi_servicelayer`

Note that this must be an absolute URL; relative URLs (e.g. including "localhost" or the 127.0.0.1 loopback) are not permitted here.

4. Click **OK**, then close the tool and click **Yes** to save your changes.

The URL specified here is used for both of the following:

- To identify the location of the Service Layer FormatReports service, which is used to queue reports submitted from MI:Viewer.
- To specify the URL for the Report Monitor, the tool where MI:Viewer users can view/download the reports they have submitted.

This URL is stored in the MI:Viewer configuration file `appSettings.config`, typically located here:

```
C:\inetpub\wwwroot\mi\App_Data\config\WebConfigFragments\appSettings.config
```

### 4.4 Setting the MI:Viewer home page

The application home page defines the first page displayed to MI:Viewer users after they have logged in. It typically fills the whole browser window, and may include text, images, and scripts, as well as links to GRANTA MI profiles, databases, and searches of interest. When an application home page is not present, MI:Viewer opens displaying the home page of the current profile for the user.

An application home page is defined as an HTML or ASPX file, and must be located in the MI:Viewer installation folder. For example:

```
C:\inetpub\wwwroot\mi\homepage.aspx
```

For more information about creating home pages for MI:Viewer, refer to the *GRANTA MI:Viewer Home Page Author Guide*; see Section 1.5.



## To add an application home page to MI:Viewer

The application home page and any related files must be copied into the correct location within the MI:Viewer installation folder as follows:

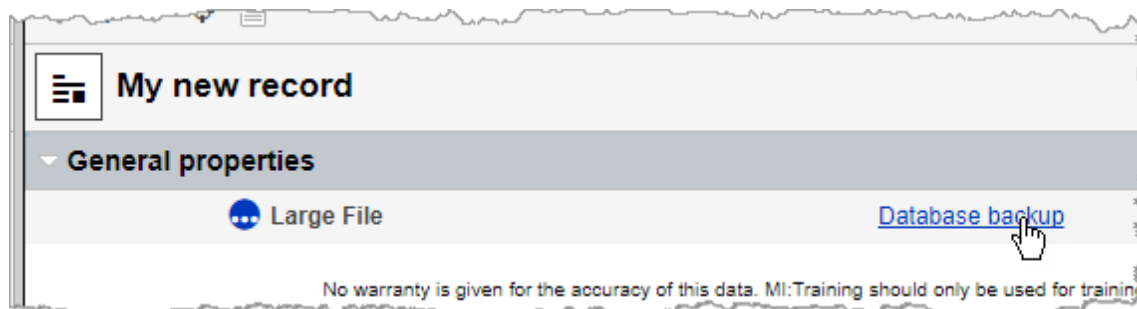
1. Create an HTML or ASPX file and save it as `homepage.aspx` or `homepage.htm`.
2. Copy the home page file into the MI:Viewer installation folder. For example:  
`\inetpub\wwwroot\mi\homepage.aspx`
3. Copy any additional resources used in the home page, such as images, CSS, or scripts, into a subfolder named `systemhomepage` under the MI:Viewer installation folder. For example:  
`\inetpub\wwwroot\mi\systemhomepage`

No further steps are required: in a default installation, GRANTA MI will automatically detect the presence of the application home page named `homepage.aspx` located in the folder specified above.

## 4.5 Enabling access to large, externally-stored files

Files of up to 500 MB in size may be stored as File attributes in GRANTA MI. Files that are larger than this (up to a maximum size of 2 GB) can be stored on disk outside the MI database and accessed via specially-configured hyperlink attributes.

Clicking on the hyperlink will cause the file to be downloaded to the user's machine. The download can be interrupted, and does not block accessing MI:Viewer or any other browser operation.



Note that files larger than 2 GB are not supported.

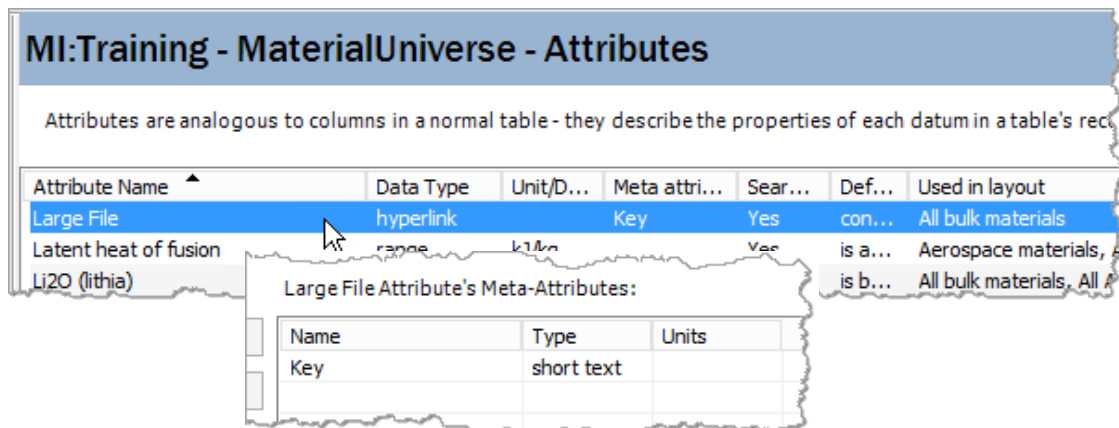
To use this feature, it is necessary to carry out the following configuration steps:

- In MI:Admin, define a hyperlink attribute with a short text meta-attribute that will be used to specify the location of linked files.
- Add a new `<RemoteFiles>` element to the MI:Viewer configuration file `ViewerSettings.config` that identifies (a) the root folder of the target file(s), and (b) the meta-attribute used to store the relative path to files within this root folder.
- In MI:Viewer, for records that will include links to external files, edit the hyperlink attribute to specify the target filename and to add a specially-formatted address string.

## Configuration procedure

1. In MI:Admin, create a hyperlink attribute with a short text meta-attribute that will be used to specify the relative location of the target file.

For example, here we have defined a hyperlink attribute called *Large File* with a short text meta-attribute called *Key*:



2. Add the new attribute to all appropriate MI:Viewer layouts.
3. Edit the ViewerSettings.config file located in the web application installation folder; typically: C:\inetpub\wwwroot\mi\App\_Data\config and insert a new element in the <MIWeb> section, as follows:

```
<RemoteFiles rootPath="pathname" attributeName="meta_attribute_name" />
```

where *pathname* is the folder where the files are located, and *meta\_attribute\_name* is the name of the meta-attribute defined above in Step 1 (*Key* in this example).

For example:

```
<MIConfig>
  <MIWeb readOnly="false" forceHTTPS="false" quickSearch="true">
    <RemoteFiles rootPath="D:\Data\Backups" attributeName="Key" />
  </MIWeb>
  <Graphs width="540" height="360" printableWidth="1050" printable>
```

Note:

- Make sure that the folder specified by `rootPath` exists (D:\Data\Backups in this case)
  - Ensure that the IIS Application Pool used by MI:Viewer has read and write access to the root folder; in a default installation, this is a local account known as **IIS AppPool\MIViewer\_AppPool** on the server where Viewer is installed. Use the Security tab in the Windows Properties dialog for the folder (D:\Data\Backups in this example) to grant Modify rights to the Application Pool account. Note if you are using a non-default account for the Application Pool, you will need to change the permissions for that account.
4. Move the files to be referenced into the folder specified in `rootPath`. You can use sub-folders to organize files if required.

5. For each file you wish to make available, create a new record, specifying the hyperlink attribute as follows:

- a. **Description:** enter the text you wish to see displayed as the hyperlink text, in our example, this is "Database backup".
- b. **Address:** enter the following string exactly as shown:

```
/mi/RemoteFile/Get?attributeId={attributeId}&recordId={recordId}&databaseKey={databaseKey}
```

The GRANTA MI application name in IIS is named 'mi' by default; if you have changed this default, then use the appropriate name in place of **mi** at the start of the address.

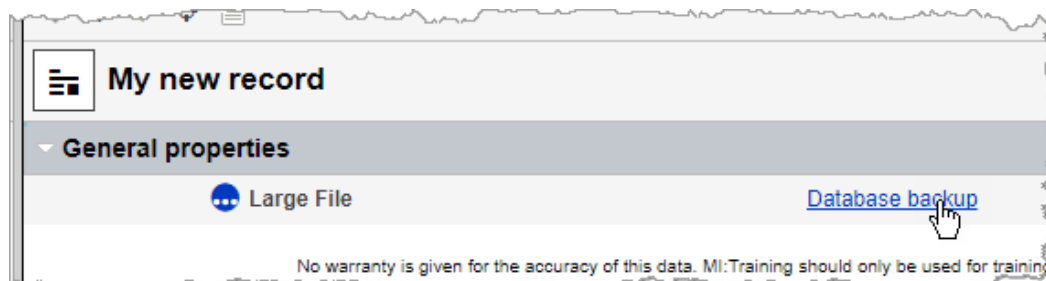
- c. **Target:** the value of this field is not used, since the file will be downloaded.
- d. **Key:** enter the relative path to the file from the root folder. For example:

The screenshot shows a web form titled "My new record : Large File". It has four tabs: "Data", "Quality Rating", "Access Control", and "Notes". The "Data" tab is selected and expanded, showing the following fields:

- Description:** Database backup
- Address:** /mi/RemoteFile/Get?attributeId={attributeId}&recordId={n}
- Target:** Current pane (dropdown menu)
- Key:** MI\_29012018183241.bak

At the bottom of the form, there is a disclaimer: "No warranty is given for the accuracy of this data. MI:Training should only be used for training purposes. Any other use is not supported by Granta."

When everything is correctly configured, the attribute will then be displayed on the record datasheet in MI:Viewer as follows:



Clicking on the hyperlink will cause the file to be downloaded to the user's machine.

## 4.6 Changing display settings in datasheets

A number of settings relating to the display of functional graphs, XY charts and links in MI:Viewer can be configured by editing the relevant configuration files located in the MI:Viewer App\_Data folder, typically:

```
C:\inetpub\wwwroot\mi\App_Data\config\ViewerSettings.config
C:\inetpub\wwwroot\mi\App_Data\config\WebConfigFragments\appSettings.config
```

### 4.6.1 Functional graph settings

Functional graphs settings are defined in the `<Graphs>` element in ViewerSettings.config. You can modify:

- The width (in pixels) of functional graphs.
- The height (in pixels) of functional graphs.
- The maximum number of points the graph can have and still be displayed in the datasheet: if the graph includes more points than this, it will not be displayed in the datasheet, but can still be viewed by clicking on the graph link. Enter a negative number here to indicate that there is no limit, that is, the graph will always be displayed in the datasheet.

### 4.6.2 XY chart settings

Settings for XY charts in a report are defined in the `<XYCharts>` element in ViewerSettings.config.

- Whether or not to XY charts are available in reports.
- Whether or not to allow XY charts can include data from different tables (ignored if XY charts are not allowed.)
- The maximum number of bubbles that will be displayed on XY charts. (Gathering data for XY charts is a memory intensive task, and this setting exists to limit load on the server.)

### 4.6.3 Max number of links shown on a datasheet

The maximum number of linked records to list on a datasheet is defined in the `<Links>` element in ViewerSettings.config. Above this limit, the records are listed in the Related Records pane.

### 4.6.4 Showing min/max values for range attributes

By default, both the minimum and maximum range values for closed range attributes will be displayed on datasheets, where they are present. This can be altered to show only the maximum value when the minimum is zero.

This is defined in the appSettings.config file located in the webConfigFragments subfolder, typically:

```
C:\inetpub\wwwroot\mi\App_Data\config\webConfigFragments
```

To show only the maximum value when the minimum is zero, add the following line to the file:

```
<add key="DisplayZeroBoundedRangesAsUnbounded" value="true" />
```

Note: although an attribute with a zero minimum will be displayed in the same way as one with no minimum set, the search behavior for each will be unchanged.

## 4.7 Changing the default unit systems

To change the default unit systems for different locales, edit ViewerSettings.config, located in the MI:Viewer App\_Data folder:

C:\Inetpub\wwwroot\mi\App\_Data\config\ViewerSettings.config

For example:

```
<DefaultUnitSystems default="Metric">
  <Item key="en-US" value="US Customary" />
  <Item key="en-US" value="US Imperial" />
</DefaultUnitSystems>
```

## 4.8 Modifying default search mask behavior

In MI:Viewer, record names are excluded from searches performed using search masks by default. It is possible to change this behavior, so that record names are included in searches run using a Search Mask.

To do this, you need to edit the MI:Viewer configuration file appSettings.config, located in the App\_Data\config\ webConfigFragments subfolder in the MI:Viewer installation folder. For example, in a typical installation, this would be:

C:\Inetpub\wwwroot\mi\App\_Data\config\webConfigFragments\appSettings.config

**To modify the default search mask behavior:**

1. In a suitable editor, open the configuration file appSettings.config.
2. Locate the attribute `Search.IncludeRecordNamesWhenUsingSearchMask` within the `appSettings` element, and change its value.
3. To include record names:

```
<add key="Search.IncludeRecordNamesWhenUsingSearchMask" value="true"/>
```

4. To exclude record names:

```
<add key="Search.IncludeRecordNamesWhenUsingSearchMask" value="false"/>
```

5. Save and close the appSettings.config file.

## 4.9 Managing search stop words

Certain words can be defined as stop words, that is, words that will not be included in text searches carried out in MI:Viewer. By default, the following words are included in the GRANTA MI search stop list:

a	be	into	on	then	was
an	but	is	or	there	will
and	by	it	such	these	with
are	for	no	that	they	
as	if	not	the	this	
at	in	of	their	to	

The Granta MI Administrator can add words to the search stop list and remove words from it by editing the MIServer.exe.config configuration file. Only edit this file if you are confident with editing XML syntax.

MIServer.exe.config is located in the bin subfolder in your MI:Server installation folder. For example, in a typical installation, this will be:

```
C:\Program Files\Granta\GRANTA MI\Server\bin\MIServer.exe.config
```

### To edit the list of stop words:

1. Open MIServer.exe.config in a text editor.
2. In the <Search> element, locate the stopWords attribute. For example:
 

```
<Search cachepath="..\Caches" enableFunctionalDataCache="false"
cacheUpdater="Synchronous" optimiseTime="23:30:00"
stopWords="www; http" />
```
3. Type the words you want to add to the search stop list, separated by commas, semi-colons or spaces. For example:
 

```
stopWords="because; doesn't; very"
```
4. To remove a word from the default stop list, precede it with a minus (-). For example:
 

```
stopWords="-the; -into"
```

## 4.10 Embedded media support

GRANTA MI can store a range of different file types, for example, image files, Microsoft Office documents, and PDF files. This functionality is known as GRANTA MI's 'Embedded Media' capability, with embedded media items stored as **File** or **Picture** data types.

- Files can be uploaded in MI:Viewer, or through the MI:Toolbox Text Importer or Excel Importer plug-ins.
- The text content of embedded files, for example, PDFs or Office documents, can be searched in MI:Viewer so long as the relevant indexing software is installed – see Section 3.3.
- The contents of embedded media files cannot be edited in GRANTA MI.

### 4.10.1 File size limitations

Table 1 Maximum recommended file size for embedded media items

Data type	Max. size	Notes
Picture	10 MB	
File	500 MB	For files larger than 500 MB, we recommend storing the file outside of the GRANTA MI database and linking to it using a hyperlink attribute; see Section 4.5.  Files larger than 2 GB are not supported.

#### Embedded media items in tabular data

While the above recommendations hold for tabular data, users need to be aware that adding lots of files in tabular data can quickly make the datasheet impractical to load and/or edit. Editing tabular data requires fetching all the rows (and their media data) from the database and saving back again.

### 4.10.2 Display of embedded media files

MI:Viewer can display files with the following file extensions. A file can be stored even if it cannot be displayed. The user will be offered the option of downloading the file locally instead, if permitted by the web browser security settings. The list of files that can be displayed is stored in the configuration database, and listed below. Storing and searching does not require an entry, only display. If you wish to display a content type/file extension that is not in the list, please contact [Granta Support](#).

Table 4-2. Files that can be displayed in MI:Viewer

File Extension	Content Type
txt	text/plain, Plain Text
htm, html	text/html, HTML
css	text/css, Cascading Style Sheet
xsl, xml	text/xml, XML
bmp	image/bmp, Bitmap Image
gif	image/gif, GIF Image
ico	image/icon, Icon Image
jfif	image/jpeg, JPEG File Interchange Format Image
jpe, jpeg, jpg	image/jpeg, JPEG Image
png	image/png, PNG Image
pdf	application/pdf, Adobe Acrobat Document
config	application/xml
xsd	application/xml
doc, docm, docx, dot, dotx, dotm	application/msword, Microsoft Word
rtf	application/msword, Microsoft Word
csv	application/vnd.ms-excel, Microsoft Excel

File Extension	Content Type
xls, xlt, xla, xlsx, xltx, xlsx, xlsm, xltm, xlam, xlsb	application/vnd.ms-excel, Microsoft Excel
mdb	application/msaccess, Microsoft Access
pot, pps, ppa, pptx, potx, ppsx, ppam, pptm, potm, ppsm	application/vnd.ms-powerpoint, Microsoft Powerpoint
Eps, ps	application/postscript, Postscript
fdf	application/vnd.fdf, Adobe Acrobat Forms Document
tar	application/x-tar, Winzip File
tgz	application/x-compressed, Winzip File
xdp	application/vnd.adobe.xdp+xml, Adobe Acrobat XML Data Package File
xfdf	application/vnd.adobe.xfdf, Adobe Acrobat Forms Document
z	application/x-compress, Winzip File
zip	application/x-zip-compressed, Winzip File
eml	message/rfc822, Internet Email Message
wav	audio/wav, Wave Sound
wma	audio/x-ms-wma, Windows Media Audio File
mp3	audio/mpeg, MP3 Audio File
mpeg, mpg	video/mpeg, MPEG Video File
mov	video/quicktime, QuickTime Movie File

#### 4.11 Increasing the maximum report size

The Service Layer can sometimes generate large reports that exceed the configured maximum for MI:Viewer. To increase the configured size, you need to edit a setting in the web service configuration file `bindings.config`, typically located here:

```
C:\inetpub\wwwroot\mi\App_Data\config\webConfigFragments\serviceModel
```

You should only edit this file if you are familiar with XML syntax.

1. In a text editor, open the `bindings.config` file.
2. Locate the `maxReceivedMessageSize` attribute within the `ReportFormatter` `<basicHttpBinding>` element as shown below, and increase the size (specified in BYTES).

```
<binding name="ReportFormatter" closeTimeout="00:01:00"
  openTimeout="00:01:00" receiveTimeout="00:10:00" sendTimeout="00:05:00"
  allowCookies="false" bypassProxyOnLocal="false"
  hostNameComparisonMode="StrongWildcard" maxBufferSize="524288"
  maxReceivedMessageSize="104857600"
  messageEncoding="Text" textEncoding="utf-8" transferMode="Buffered"
  useDefaultWebProxy="true">
```

3. Save and close the `bindings.config` file.



## 4.12 MI:Viewer log files

MI:Viewer writes log files of its activities to App\_Data\logs in the MI:Viewer installation folder, typically: C:\inetpub\wwwroot\mi\App\_Data\logs

A number of different log files may be generated:

- MIViewer.log – application error, warning, information, and debug messages.
- Sessions.log – user session information, showing who has logged into MI:Viewer.
- RoundTripInfo.log – round-trip information.

The logs are set to roll over on a daily basis. The log files from the previous day have their date appended, for example, MIViewer.2018-01-30.log.

The names and locations of the MI:Viewer log files are set in the configuration file log4net.config, located in the App\_Data\config folder in the MI:Viewer installation folder. To change the default log file names or locations, you need to edit log4net.config to specify alternative folder and/or filenames. The specified folder can be anywhere you choose, but a folder on the same drive as the MI:Server installation folder is recommended. A full or relative path may be used. The folder must be accessible for reading and writing by the MI:Viewer worker process on the local machine.

Users with administrator privileges for the GRANTA MI system can view and change MI:Viewer logging options: in the MI:Viewer toolbar, click on **Admin** and then click the **Logging** tab.

### 4.12.1 Changing the logging level

The logging level determines the amount of information that is logged in the MI:Viewer.log file. The higher the logging level, the more information is written to the log file.

The levels are named after the severity of events they are used to track, and go from logging only the highest severity events (level= ERROR) to logging all events (level = DEBUG):

- ERROR – Log only runtime errors or unexpected conditions, where software has not been able to perform some function.
- WARN – In addition to errors, also log information about less serious problems that did not result in an unrecoverable error.
- INFO – In addition to errors and warnings, also log information relevant to the general running and management of your system, where things are working as expected. This is the default logging level for MI:Viewer.
- DEBUG – This is the most verbose logging level, including detailed information about all event types that may diagnostically helpful to developers, IT, and system administrators.

By default, any changes to the logging level made on the **Logging** tab will remain in effect until the MI:Viewer application restarts. To save the selected level as the new MI:Viewer application default, select **Persist this change to the config file**.

The default logging level is specified in the MI:Viewer configuration file log4net.config, typically located here: C:\inetpub\wwwroot\mi\App\_Data\log4net.config

### 4.12.2 Additional logging options

- **Round-trip logging.** When enabled, round-trip information (URL, user, and time taken) for requests is written to RoundTripInfo.log. This allows you to monitor the availability and performance of MI:Viewer processes. Round-trip logging is disabled by default as it degrades application performance and can result in very large log files. For that reason, we recommend enabling round-trip logging only if instructed to do so by Granta Support.
- **Show page load statistics.** When enabled, you can view data on page load and round trip times in MI:Viewer:
  - Data for the tree view are shown in a Debug tab on the left of the application window
  - Data for the page shown in the main pane are shown at the bottom of the page.

### 4.12.3 Downloading MI:Viewer event log files

You can download MI:Viewer application log files containing application error, warning, information, and debug messages, from the **Download log files** panel on the **Admin>Logging** tab in MI:Viewer.

Log files are downloaded in a zip file.

- To download a single log file, select it from the list under **Single Log File** and click **Download Log File**. By default, all log files from the last 7 days are listed here. To see more or fewer log files in the list, enter the number of days in the **Time span** box and click **Apply filter**.
- To download all log files from a specified time period, choose the start and end dates and then click **Download All Log Files**. The files will be downloaded as a single zip file.

## 4.13 MI:Viewer configuration files

File	Stores
web.config	ASP.NET application configuration settings. Location: C:\inetpub\wwwroot\mi\web.config
connection.xml	Connection credentials used to connect to MI:Server (see 4.1) Location: %PROGRAMDATA%\Granta\GRANTA MI\connection.xml
ViewerSettings.config	Settings relating to the display of functional graphs, X-Y charts and links (see 4.4); settings to enable access to large, externally-stored files from MI:Viewer (see 4.5). Location: C:\inetpub\wwwroot\mi\AppData\config\ViewerSettings.config
appSettings.config	Display settings for closed range attributes; default search mask behavior. Location: C:\inetpub\wwwroot\mi\AppData\config\webConfigFragments\appSettings.config
log4net.config	Application logging settings, including the default application log file name and location. Location: C:\inetpub\wwwroot\mi\AppData\config\log4net.config

## 5 MI:Toolbox application administration

The MI:Toolbox client application is used for bulk data processing and data analysis via a suite of plug-ins. MI:Toolbox may be installed on the same host as MI:Server, but is more usually installed on remote hosts.

All the GRANTA MI Windows clients connect to MI:Server on ports 8737/8738 using the TCP protocol "gtcp". The ports are opened on the server on which MI:Server is installed, and not the client machine.

### 5.1 MI:Toolbox configuration files

The plug-ins available to an installation of MI:Toolbox are set by two configuration files.

- PlugInConfigLocations.config, which specifies where MI:Toolbox will look for its plug-in information.
- PlugIns.xml, which contains the details of a collection of plug-ins.

#### 5.1.1 PlugInConfigLocations.config

PlugInConfigLocations.config is an XML configuration file that contains a list of one or more <PlugInConfig> elements, which typically look like this:

```
<PlugInConfig config="..\plugins\PlugIns.xml" />
```

Each <PlugInConfig> element points to a PlugIns.xml file containing the details of a collection of plug-ins.

In a default installation, PlugInConfigLocations.config is located in the config folder of the MI:Toolbox installation folder, typically:

```
C:\Program Files\Granta\GRANTA MI\Toolbox\config\PlugInConfigLocations.config
```

#### 5.1.2 PlugIns.xml

This XML configuration file specifies:

- the name of the buttons in the MI:Toolbox toolbar – PlugInButton
- the name of the pages in the *Select a Plug-in Module* dialog – PlugInTab
- the location of each plug-in, relative to the 'plugins' directory – PlugInDirectory

For example, the elements for the Import plug-ins are:

```
<PlugInButton id="importButton" image="Images\import.ico"
localisationCategory="Buttons" localisationKey="Import"/>
<PlugInTab id="importTab" localisationCategory="Tabs" localisationKey="Import"/>
<PlugInDirectory path="Importers\Excel" button="importButton" tab="importTab"/>
<PlugInDirectory path="Importers\Bulk" button="importButton" tab="importTab"/>
<PlugInDirectory path="Importers\Text" button="importButton" tab="importTab"/>
```

In a default installation, the Toolbox plugins folder is:

```
C:\Program Files\Granta\GRANTA MI\Toolbox\plugins
```

## 5.2 Configuring plug-in shadowing

In some installations, it is useful for some or all of the plug-ins used by a client installation of MI:Toolbox to reside on a network location. This may be the case when a set of custom plug-ins has to be maintained.

When plug-in shadowing is set up, a server-hosted collection of plug-ins is copied to the client's machine. These files are automatically updated when the files on the server change. This applies to the plug-in and all associated files, for example, templates.

### Step 1: Configuring the Network Folder

To host a collection of plug-ins on a server:

1. Create a network-accessible folder.
2. Put a PlugIns.xml file in the folder, along with the plug-in folders to be hosted.  
The layout of the folder and the PlugIns.xml file should be of the same form as the plug-ins folder in a standard installation of MI:Toolbox (appropriate names may be chosen for the plug-in folders, as long as the PlugIns.xml file matches).
3. Ensure permissions are set correctly for clients to read the folder (you may wish to not allow write permissions). However, none of the plug-in files themselves should be set to 'Read-only'.

### Step 2: Configuring MI:Toolbox

To configure MI:Toolbox plugins on the client machine:

1. Locate the config folder Program Files\Granta\GRANTA MI\Toolbox\config
2. Open the configuration file PlugInConfigLocations.config in a text or XML editor.
3. Create an entry pointing to the PlugIns.xml file in the network folder, and add an attribute `shadow`, which indicates that the file specified is not local and thus needs to be shadowed.

The `shadow` attribute's value indicates the folder (without trailing '\') where it should store the shadow for that location. For example:

```
<PlugInConfig config="\\bob\Downloads\PlugIns\PlugIns.xml"
shadow="..\..\shadow" />
```

– would add the plug-ins specified in bob's shared PlugIns.xml, by maintaining a copy in "`..\..\shadow`".

4. Ensure permissions are set correctly for users to read and write to the local shadow folder.  
When MI:Toolbox is started, the plug-ins are automatically checked and are copied to the client machine when the files on the network have a later date than the files on the client. The shadowed plug-ins are accessible as usual through the toolbar.

---

**Note:** If the plug-in on the client machine has a later date than the file on the network, then it will not be overwritten by the network version.

---

## 6 Granta database administration

A range of different administration tasks can be performed for GRANTA MI databases using the MI:Admin tool. You do not need to have administrative privileges in the GRANTA MI system or on the SQL Server where the database is installed to use MI:Admin. However, if database security has been implemented on any of the managed databases, then you will need adequate administration privileges for them in order to make any modifications.

MI:Admin can be used to:

- Define and modify your database schema (6.3)
- Define and manage profiles, used to group databases and tables into meaningful collections for particular audiences (6.4)
- Configure permission-based access control for a database (6.5)
- Turn on record version control for a database (6.6)
- Manage the templates used for searching and reporting on data in GRANTA MI (6.7)
- Manage various types of files stored in a database: home page files (6.8), attribute help page files (6.9), FEA exporters (6.10), and MI:Explore application configuration files (6.11)
- Apply Product Risk data updates (6.13)

For detailed information on how to carry out these tasks in MI:Admin, see the Help in the MI:Admin application (**Help > Contents**).

**Note that MI:Admin does not provide any database backup capability.** Backups of GRANTA MI databases need to be done on your database server using SQL Server Management Studio, by a user with sysadmin privileges on the SQL Server instance.

### 6.1 Logging in to MI:Admin

1. Start the MI:Admin application:  
**Start > All Programs > GRANTA MI > MI Admin**
2. Edit the URL for MI:Server if necessary. If MI:Admin is on the same computer as MI:Server, the URL can be set to localhost.
3. To log into GRANTA MI with your current Windows login account, check the **'Use System Authentication'** box.
4. To log in using a different account, clear the **Use System Authentication** box and enter the credentials of a user with administrative privileges for the GRANTA MI system, that is, a user who is a member of the Admin system security group.
  - If using Windows authentication, enter the user name, password, and domain of a Windows account: this account must be a member of the MI\_ADMIN group.
  - If using User Manager authentication to MI:Server, enter the username and password of a User Manager Administrator account here (typically, the account specified when MI:Server was installed). Leave the Domain field empty.
5. Click **OK**. The MI:Admin application will connect to MI:Server.

## 6.2 Locking the database while making changes

It is recommended that only one user at a time edits a database schema. If you are making changes to a database, it is strongly recommended that non-administrator users should not access the database. This precaution is not required if the database schema is only being viewed.

Users with administrative privileges to the GRANTA MI databases will still be able to access a database when it is locked.

### To lock the database:

1. In the MI:Admin application, connect to MI:Server and then click **Schema**.
2. Select the database from the **Current Database** list and click **Lock** in the toolbar.
3. When you have finished editing the database, click **Unlock** in the toolbar.

## 6.3 Defining and modifying the database schema

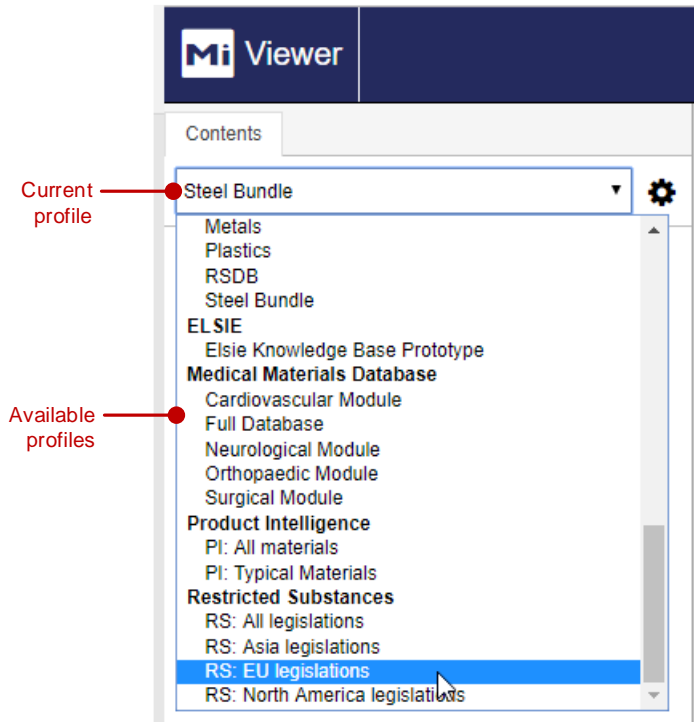
The **Schema** tool in the MI:Admin application is used to define the structure and organization of the database, including:

- what properties are to be stored in the database - the discrete types, parameters, expressions, and constants available;
- the standard names used to uniquely identify physical properties, parameters, and relationships in the database;
- the units and unit systems used in the database;
- the tables in the database, and the attributes associated with them;
- links between tables;
- the subsets and layouts used to present data to MI:Viewer users.
- the access control categories used for attribute-based access control, see Section 6.5;
- the templates available for searching, reporting, and importing data into the database, see Section 6.7;
- the files that contain supporting information for database users, including the database home page (see Section 6.8), help pages for attributes or parameters, and exporter files used to export data in specified formats (see Section 6.9);

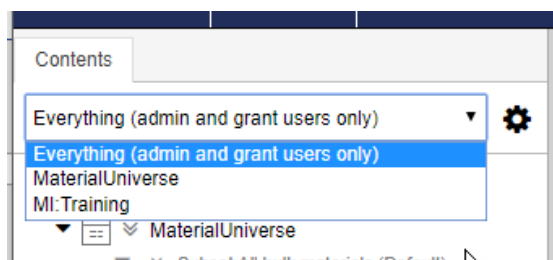
## 6.4 Managing profiles

Profiles are used to group databases and tables into meaningful collections for particular audiences. A profile presents one or more tables, subsets and layouts that may belong to different databases, and may also include a home page.

In MI:Viewer, users can select a profile from the list at the top of the Contents pane; for example:



Users with system security Grant, Power User, or Admin privileges can see an additional 'everything' profile that shows all databases currently loaded in the system:



The home page for a custom profile is displayed in MI:Viewer when the profile is selected from the list in the Contents pane or on clicking **Home** in the MI:Viewer toolbar. For more information about creating home pages for profiles, refer to the PDF document *GRANTA MI:Viewer Home Page Author Guide*; see Section 1.5.

See the Help in MI:Admin for more information: on the **Help** menu, click **Contents**.

### Learn more

- The MI:Admin Help topics under **Profiles tools** cover how profiles can be used in MI:Viewer, and how to manage and edit them in MI:Admin.

## 6.5 Access control for database items

Access control can be used to determine who is allowed to access (view/edit) the tables, records, data, and attributes within a GRANTA MI database. Access control for GRANTA MI is enabled, and the mode selected, on the **Access Control Settings** page in MI:Server Manager.

In a system with permission-based access control, each data item in the database carries its own access control permissions which determine who can read and write that data. Permission-based access control is configured and managed with the MI:Admin **Access Control** tool:

- Permissions are configured and mapped to existing system security roles in an *access control schema*, using the **Access Control Schema Editor**.
- An access control schema is applied to a database in the **Access Control Editor**, where you apply permissions applied to items in the database and set the appropriate read/write access for them.

In a system with attribute-based access control, access to records in the database is granted or denied based on the value of certain security attributes on those records, known as *Access Control Categories*. A 'Rule Engine' determines how the values of these access control categories map to roles within an organization.

- Access Control Categories for a database are defined in the MI:Admin **Schema** tool.
- The Rule engine is selected and configured in MI:Server Manager on the **Rule Engine Configuration** page, under **Access Control Settings**.

### Learn more

- The *GRANTA MI Access Control and Security Guide* provides detailed information about options for access control in GRANTA MI.
- The MI:Admin Help topics under **Access control tools** cover how to use the Access Control Schema Editor and Access Control Editor to configure permission-based access control on a database.

## 6.6 Record version control

Record version control for the tables in a database is turned on in the MI:Admin **Schema** tool. Note that:

- Version control for a table cannot be disabled once it has been enabled.
- Version-controlled tables cannot be deleted.

### Learn more

- The *GRANTA MI Record Version Control* document provides detailed information on implementing version control for tables and records in a GRANTA MI database.
- MI:Admin Help topic **Schema tool>Tables>Enable version control**



## 6.7 Managing templates stored in the database

Templates may be used to provide some useful shortcuts for MI:Viewer users. A number of different types of template may be available in a database:

Template type	Description
Search Masks	Search masks are used to limit the scope of searches performed in MI:Viewer to a specified set of attributes, which can be from different tables. The record name is not searched when a search mask is used. Search masks are defined on the <b>Search Masks</b> page in MI:Admin, and accessed in MI:Viewer on the <b>Search</b> page.
Search Templates	Search templates provide MI:Viewer users with pre-defined searches that include specific attributes and meta-attributes.
Report Templates	Report templates provide MI:Viewer users with a pre-defined set of attributes and meta-attributes used to generate comparison table or X-Y chart report from a database table.

### Learn more

- The MI:Admin Help topics under **Schema tool>Search Masks**, **Schema tool>Search Templates**, and **Schema tool>Report templates** cover how to manage the search masks and templates in a GRANTA MI database.

## 6.8 Managing database home pages

The home page for a database is displayed MI:Viewer when a database is selected in the Contents pane. Typically, it may include an overview of what's in the database, search tools, tutorials, and/or support information. The database home page is visible to all users that have permission to view the database.

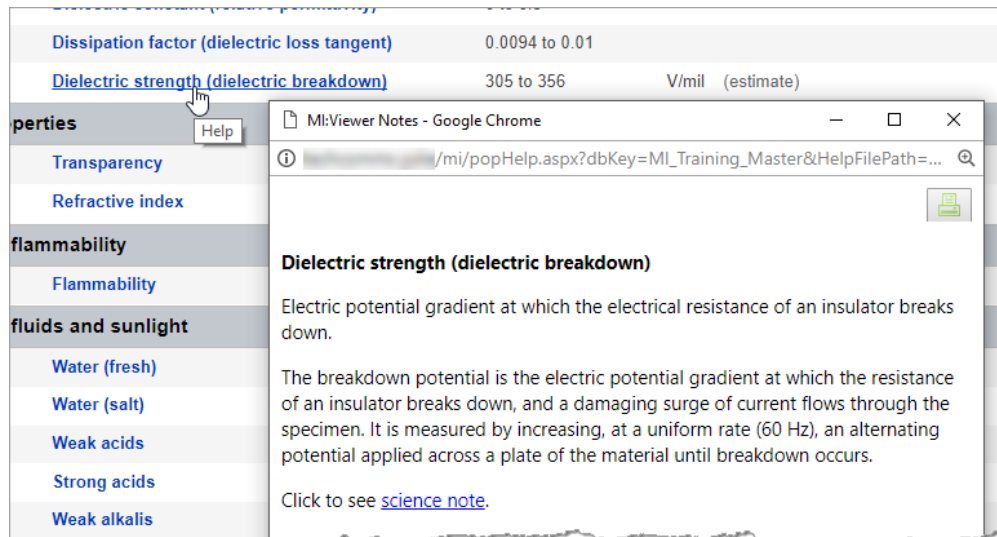
Database home pages are HTML or ASPX files that are created and modified outside of GRANTA MI using a text editor, and then added to the database from the **Files** page in the MI:Admin **Schema** tool.

### Learn more

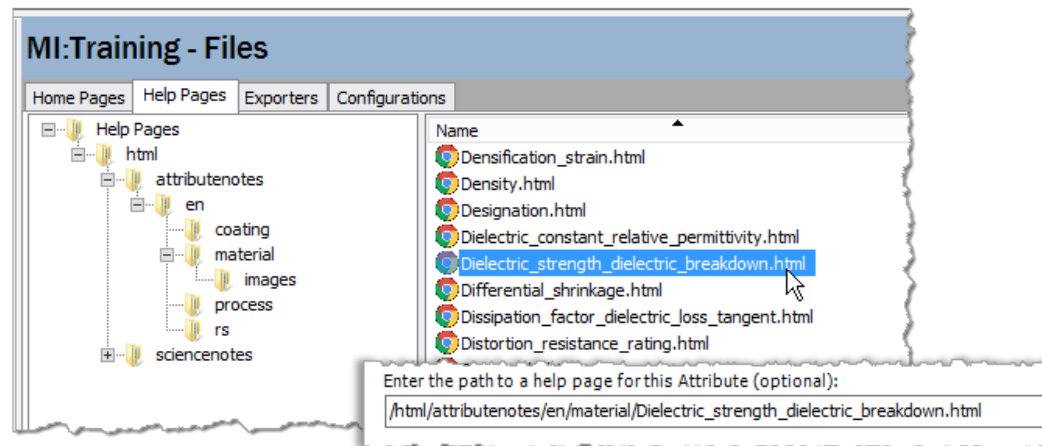
- The *GRANTA MI:Viewer Home Page Author Guide* provides detailed information on how to write application, profile, and database home pages.
- The MI:Admin Help topics under **Schema tool>Files** cover how to manage the database home page files in a GRANTA MI database.

## 6.9 Managing attribute and parameter help pages

Help pages for attributes and parameters in GRANTA MI databases can be used to provide a short definition that is displayed in a pop-up window when the attribute or parameter name is clicked on a datasheet, for example:



Help page files – HTML, image, and CSS files – are defined outside of GRANTA MI and then loaded into the database and associated with specific attributes and parameters in the MI:Admin Schema tool:



### Learn more

- The MI:Admin Help topics under **Schema tool>Files** cover how to manage attribute and parameter help pages in a GRANTA MI database.

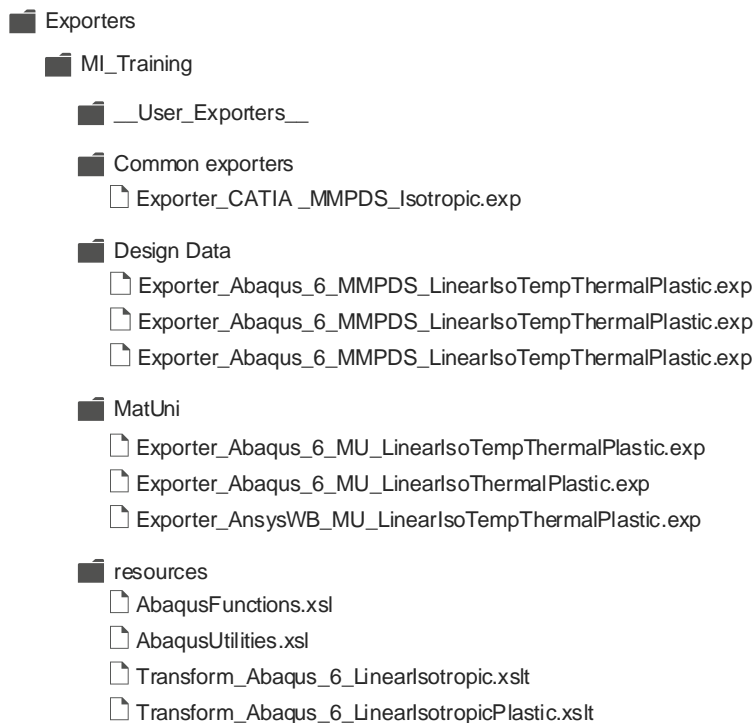
## 6.10 Managing FEA exporters

Exporters for Finite Element Analysis (“FEA exporters”) are used to export materials data in a specific format for use in engineering analysis packages. An exporter for a given FEA package and model is comprised of two (or more) files:

- An exporter configuration file (.exp), an XML file that contains all the information about the exporter, the target FEA package and model, and the attribute data to be exported.
- One or more XSLT files, required to transform the initial XML into the format required by the target FEA package.

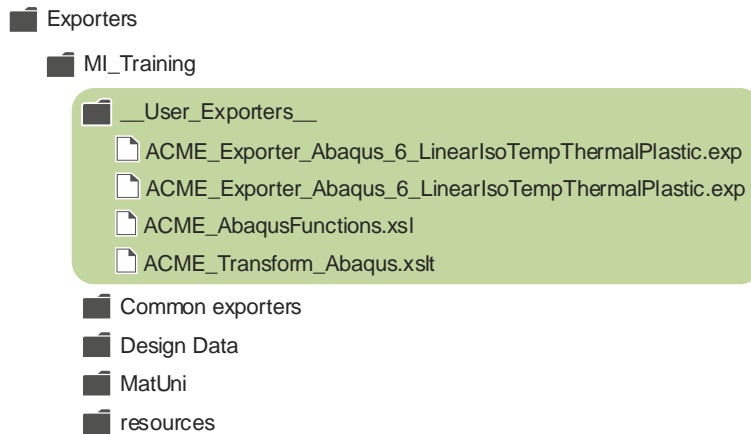
FEA exporter configuration files are stored in the database to which they apply. A range of different exporters are provided with Granta reference databases; when a database is installed, a copy of the configuration files is automatically put in the exporters folder in the MI:Server installation folder, typically: C:\Program Files\Granta\GRANTA MI\Server\exporters

For example:



These exporter files are persistent configuration files; they are not directly accessed or saved by users.

New exporters that you have developed, or Granta exporters that you have modified, should be placed in a \_\_User\_Exporters\_\_ subfolder, and then and then added (“imported”) to the database for which they are written:




---

**Note:** If you modify Granta exporters, it is particularly important that you store the modified files in a `__User_Exporters__` subfolder or they will be overwritten the next time the exporters are updated, and you will lose your changes.

---

To import exporters that you have developed and make them available to MI:Viewer, MI:Explore, or MI:Materials Gateway users, use MI:Admin (**Schema tool > Edit Files > Exporters**). You will require administrative privileges to the database concerned.

- If database security groups have been set for the database, you must be a member of the Admin database security group and a member of one of the system security groups.
- If database security groups have not been set, you must be a member of the Admin system security group.

#### Learn more

- The MI:Admin Help topics under **Schema tool>Files** cover how to manage the FEA exporter files in a GRANTA MI database.

## 6.11 Managing configuration files

Application configuration settings for MI:Explore are specified in JSON format configuration files which are stored in the database. These settings define the “data views” available in MI:Explore, determining:

- The database and table to which the configuration applies.
- The attributes available within the MI:Explore application for searching, filtering, and viewing data.
- Availability of a number of application features such as the thumbnail and scatter plot tabs, data add and edit capabilities, reports, and exporters.
- Application options such as the default unit system, default language, and number formatting settings.

MI:Explore configuration files are created and modified outside of GRANTA MI, and stored in the database to which they apply. A configuration file is provided with each Granta reference database.

The configuration files for a database are managed in MI:Admin (**Schema tool > Edit Files > Configurations**). On the Configurations page, you can organize, export (download), import (upload), and validate configuration files.

#### Learn more

- The *MI:Explore Configuration Guide* provides detailed information on the MI:Explore application configuration settings that may be specified in configuration files.
- The MI:Admin Help topics under **Schema tool>Files** cover how to manage the application configuration files stored in a GRANTA MI database.

## 6.12 Importing templates for MI:Optimize

MI:Optimize is an optional GRANTA MI module that enables MI:Viewer users to optimize material selection by applying 'business rules' - the calculations and preferred material classifications that define an organization's materials selection strategy. These rules, defined in a Microsoft Excel template file, are stored in the database containing the data to which they apply.

MI:Optimize template files are uploaded to the database in MI:Admin.

#### Learn more

- The *GRANTA MI:Optimize Guide* provides detailed information on creating templates for use with MI:Optimize.
- The MI:Admin Help topic **Import an MI:Optimize template** covers how to load templates into a GRANTA MI database.

## 6.13 Applying Product Risk data updates

The **Data Updater** tool in MI:Admin is used to apply data updates to Product Risk or Restricted Substances databases.

See the document *Applying a Product Risk Data Module Update*, included in the update package, for information on planning and carrying out updates using the Data Updater.

## 7 Application Activity reporting

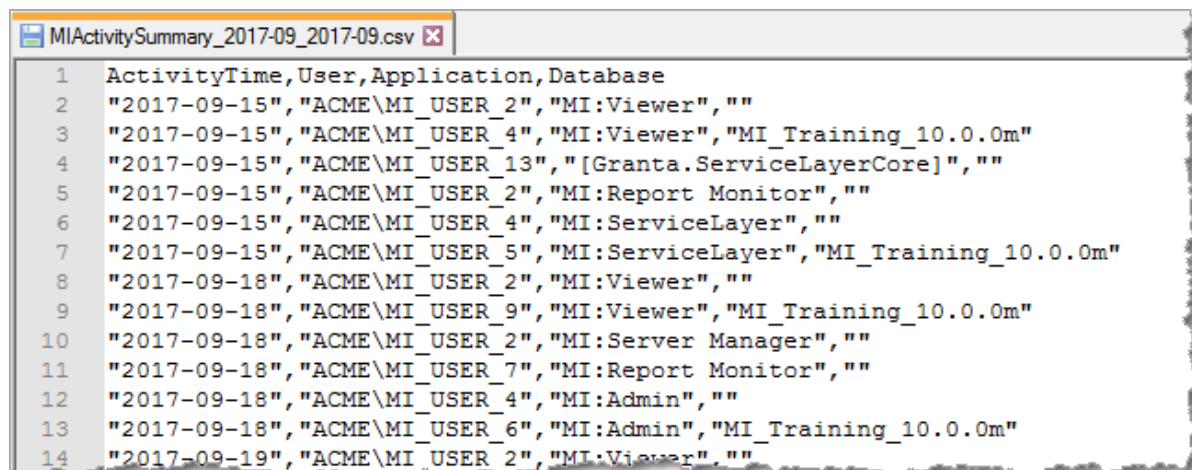
Application Activity reporting information can help you to better understand your system users and their needs.

User activity information for all GRANTA MI applications – which applications and databases were used, by whom, and when – is logged by the MI system. A daily summary of user activity is saved as a CSV format log file that can be downloaded from the Download MI Application Activity Summary panel on the MI:Viewer **Admin>Logging** tab.

- For a file that includes a summary of usage for the current month and the previous two months, select **Last 3 months** then click **Download**.
- For information on usage over specific time period, select the start and end months, then click **Download**.

This report can be used to plot graphs and create tables in Excel to visualize application usage, identify trends, and create key performance indicators for management reports.

Dates in the Application Activity Report are recorded in ISO format, yyyy-MM-dd, for example:



```

MIActivitySummary_2017-09_2017-09.csv
1 ActivityTime,User,Application,Database
2 "2017-09-15","ACME\MI_USER_2","MI:Viewer",""
3 "2017-09-15","ACME\MI_USER_4","MI:Viewer","MI_Training_10.0.0m"
4 "2017-09-15","ACME\MI_USER_13","[Granta.ServiceLayerCore]",""
5 "2017-09-15","ACME\MI_USER_2","MI:Report Monitor",""
6 "2017-09-15","ACME\MI_USER_4","MI:ServiceLayer",""
7 "2017-09-15","ACME\MI_USER_5","MI:ServiceLayer","MI_Training_10.0.0m"
8 "2017-09-18","ACME\MI_USER_2","MI:Viewer",""
9 "2017-09-18","ACME\MI_USER_9","MI:Viewer","MI_Training_10.0.0m"
10 "2017-09-18","ACME\MI_USER_2","MI:Server Manager",""
11 "2017-09-18","ACME\MI_USER_7","MI:Report Monitor",""
12 "2017-09-18","ACME\MI_USER_4","MI:Admin",""
13 "2017-09-18","ACME\MI_USER_6","MI:Admin","MI_Training_10.0.0m"
14 "2017-09-19","ACME\MI_USER_2","MI:Viewer",""

```

This ensures that, when the file is opened in Microsoft Excel, the date field will be interpreted correctly, regardless of your locale, allowing the data to be used in tables and graphs more easily.

Note that Activity Report data generated in older versions of GRANTA MI (before version 10 Update 3) used a date format based on the server's date and time setting.

## Appendix A. MI:Server Audit Logging

MI:Server audit logs allow an auditor to determine what data has been requested by users, when, and what data was delivered to them. In order to achieve this, the following types of information are recorded in the audit log:

- **Security Information:** Who the user is and what role membership they have.
- **Transaction Information:** Which application the request has originated from, and what action they are undertaking to cause data to be accessed. If the application does not supply details of the action, a stack trace will be recorded in a separate log.
- **Permission Information:** The type and ID of all objects in the database that are requested, along with whether the user was denied or permitted access.
- **Location information:** The IP address of the application making the request, and in the case of the IIS hosted applications, the IP address of the user.

The logs will not record any data, only identities of data objects.

As all read and write actions are recorded for all objects for all transactions, the audit logs will be large. It is possible to configure the rollover behavior, which determines how often an audit log is ended and a new one is begun.

In order for MI:Server to generate the audit logs, the feature must be enabled. There are two log files written, the audit log and a stack trace log.

---

**Note:** Turning on audit logging should have no measurable effect on the performance on MI:Viewer for the vast majority of user actions. When the data load is very high (such as for compare reports), performance can be reduced by 5–10%.

---

### A.1 Audit log file format

The Audit log is an ASCII text file. It contains single line entries for the types of information described above. The format is:

```
yyyy-mm-dd hh-mm-ss,sss transaction_id message data
```

The `transaction_id` binds together log entries associated with the same request from the client. The message and data vary depending on the type of entry being written.

The log entry types are:

- SecurityContext: Message="Creating security context for"; Data=UserID & Roles
- Transaction: Message="Transaction created by"; Data=ApplicationName & Action
- dbKey: Message="Current database key"; Data=dbKey
- Permissions: Message="Access permitted/denied for"; Data= ObjectNameEB & ObjectID
- IP\_application: Message="IP Address of application"; Data=IPAddress
- IP\_user: Message="IP Address of user" ; Data=IPAddress
- Transaction\_end="Transaction ended"; Data=

## Notes

- If the application has not supplied an action for the transaction message, then the *Data* will refer the auditor to the stack trace log. The stack trace log shows the stack trace associated with the transaction, cross-referenced by the date, time, and transaction\_id.
- The logs may say *unspecified* for the IP address – this is the client IP address, and not all clients provide their IP address to MI:Server.
- It should not be assumed that a transaction will always be recorded as terminated with an end of transaction statement in the log.
- The text in the stack trace log is provided for information purposes only and should be treated with caution, as this information is provided by the client and as such is subject to manipulation both by the client and by any parties able to intercept communication between the client and server.

## A.2 Enabling audit log file generation

By default audit logging is turned off. To enable audit logging, you need to edit the log4net.config configuration file located in the MI:Server installation folder config subfolder, typically:

```
C:\Program Files\Granta\GRANTA MI\Server\config\log4net.config
```

### Procedure

1. In a text editor, open log4net.config.
2. Locate the following lines near the end of the file:

```
<logger name="Granta.Audit.AuditLog">
  <level value="OFF" />
```

and

```
<logger name="Granta.Audit.AuditStackTrace">
  <level value="OFF" />
```

3. Change the `level` value from "OFF" to "INFO" in both places:

```
<level value="INFO" />
```

4. Save your changes and close the file.

The log files are set to automatically rollover to a new file, and compress the old one, using GZip, at a size limit of 10 MB.

## A.3 Changing the audit log file name/location

By default, MI:Server audit log files are created in the MI:Server Logs folder in %PROGRAMDATA%, typically:

```
C:\ProgramData\Granta\GRANTA MI\Server\Logs
```

The default filename and location of the audit log files is specified in the log4net.config configuration file located in the MI:Server installation folder config subfolder, typically:

```
C:\Program Files\Granta\GRANTA MI\Server\config\log4net.config
```



To change the default filename or location, you need to edit log4net.config and change the following lines:

```
<param name="File" value="..\Logs\MIServer.Audit.log" />  
<param name="File" value="..\Logs\MIServer.AuditStackTraces.log" />
```

A folder on the same drive as the MI:Server installation folder is recommended.

It is important that the folder you have chosen is accessible for reading and writing by the SYSTEM user on the local machine.

## Appendix B. Troubleshooting

Issue	Suggested check or action
Changes to database security settings (e.g. adding users to a database security group) are not immediately applied (Windows authentication only)	Recycle the Viewer application pool to reset the pool users cache. (See Microsoft Support article <a href="#">152526</a> for a workaround.)
Client application cannot contact MI:Server	Check that the necessary port is open through the server firewall. See Section <a href="#">2.5</a>
MI:Server cannot contact database server	Check that the necessary port is open through the server firewall. See Section <a href="#">2.5</a>
User cannot log in to MI:Server	Check that the user is a member of the correct groups, and the groups are set correctly. If a user account has just been added to a Windows group, it may take some time for their permissions to update. If the above is correct, try restarting MI:Server; see Section <a href="#">3.6</a> .
MI:Explore users can't run reports or export data	Popup blocking features on some browsers may prevent some forms in MI:Explore from opening, for example, when trying to run reports or export FE data. If this happens, add the GRANTA MI server URL to the set of sites allowed in the browser's popups security settings.
Website is inaccessible	Check the security permissions on the folders, and for the virtual directory in IIS. Check that the virtual directory has permission to run ASP scripts. Check that the necessary port is open through the server firewall; see Section <a href="#">2.5</a>
Problems with MI:Viewer, but none with the other client applications MI:Admin and MI:Toolbox	Try restarting IIS.
Problems with viewing PDFs in MI:Viewer	Use IIS Manager to check that the HTTP Response Header does not include a 'X-UA-Compatible' setting.

Issue	Suggested check or action
Error in MI:Viewer after generating a large report	Large reports may cause an error in MI:Viewer because the response from the Service Layer exceeds the configured maximum for MI:Viewer. The solution is to increase configured maximum size: see Section 4.11.
Problems with all the client applications: MI:Viewer, MI:Admin, and MI:Toolbox	Try restarting MI:Server; see Section 3.6.
MI:Admin and MI:Viewer fail with a “trust relationship error”	The MI:Server host computer's domain account is no longer trusted by the domain because a database with invalid access control roles has been added. Contact your domain System Administrator.
Problems with an individual database	Try removing the database from the system and then adding it back (in MI:Server Manager) to refresh the caches.