

Ansys GRANTA MI 2021 R1

GRANTA MI Administrator's Guide

Copyright and Trademark Information

© 2021 ANSYS, Inc. Unauthorized use, distribution or duplication is prohibited.

ANSYS, ANSYS Workbench, AUTODYN, CFX, FLUENT and any and all ANSYS, Inc. brand, product, service and feature names, logos and slogans are registered trademarks or trademarks of ANSYS, Inc. or its subsidiaries located in the United States or other countries. ICEM CFD is a trademark used by ANSYS, Inc. under license. CFX is a trademark of Sony Corporation in Japan. All other brand, product, service and feature names or trademarks are the property of their respective owners. FLEXlm and FLEXnet are trademarks of Flexera Software LLC.

Disclaimer Notice

THIS ANSYS SOFTWARE PRODUCT AND PROGRAM DOCUMENTATION INCLUDE TRADE SECRETS AND ARE CONFIDENTIAL AND PROPRIETARY PRODUCTS OF ANSYS, INC., ITS SUBSIDIARIES, OR LICENSORS.

The software products and documentation are furnished by ANSYS, Inc., its subsidiaries, or affiliates under a software license agreement that contains provisions concerning non-disclosure, copying, length and nature of use, compliance with exporting laws, warranties, disclaimers, limitations of liability, and remedies, and other provisions. The software products and documentation may be used, disclosed, transferred, or copied only in accordance with the terms and conditions of that software license agreement.

ANSYS, Inc. and ANSYS Europe, Ltd. are UL registered ISO 9001: 2015 companies.

U.S. Government Rights

For U.S. Government users, except as specifically granted by the ANSYS, Inc. software license agreement, the use, duplication, or disclosure by the United States Government is subject to restrictions stated in the ANSYS, Inc. software license agreement and FAR 12.212 (for non-DOD licenses).

Third-Party Software

See the legal information in the product help files for the complete Legal Notice for ANSYS proprietary software and third-party software. If you are unable to access the Legal Notice, contact ANSYS, Inc.

Published in the U.S.A.

Table of Contents

| | | |
|----------|--|-----------|
| 1 | Introduction..... | 5 |
| 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 | 6 |
| 1.6 | Your feedback..... | 6 |
| 2 | GRANTA MI system overview..... | 7 |
| 2.1 | MI:Server | 8 |
| 2.2 | One MI | 8 |
| 2.3 | Settings Service | 8 |
| 2.4 | MI:Viewer | 8 |
| 2.5 | Service Layer..... | 8 |
| 2.6 | Remote Import | 8 |
| 2.7 | MI:Admin..... | 9 |
| 2.8 | MI:Toolbox | 9 |
| 2.9 | MI:Workflow, MI:Workflow Designer | 9 |
| 2.10 | Database server | 9 |
| 2.11 | Ports used by GRANTA MI software | 10 |
| 3 | Search in GRANTA MI..... | 12 |
| 3.1 | Supported document types..... | 12 |
| 3.2 | Size limitations..... | 12 |
| 3.3 | How indexing failures are handled | 12 |
| 3.4 | Search synonyms | 13 |
| 3.5 | Search suggestions (autocomplete) | 13 |
| 3.6 | Excluding documents from the index..... | 13 |
| 3.7 | Other search configuration settings..... | 13 |
| 3.8 | AdoptOpenJDK Java Runtime (JRE) | 13 |
| 4 | MI:Server administration | 15 |
| 4.1 | MI:Server admin/config tools..... | 15 |
| 4.2 | System security mode | 15 |
| 4.3 | Configuring Notifications for MI:Viewer users..... | 17 |
| 4.4 | Restarting the GRANTA MI service | 20 |
| 4.5 | MI:Server log files..... | 20 |

| | | |
|----------|--|-----------|
| 5 | <i>MI:Viewer application administration</i> | 22 |
| 5.1 | Configuring the MI:Viewer-MI:Server connection | 22 |
| 5.2 | Enabling access to reporting services..... | 22 |
| 5.3 | Troubleshooting reporting | 23 |
| 5.4 | Providing links to specific records | 23 |
| 5.5 | Setting the MI:Viewer home page | 24 |
| 5.6 | Enabling access to large, externally-stored files | 25 |
| 5.7 | Changing display settings in datasheets..... | 27 |
| 5.8 | Changing the default unit systems | 29 |
| 5.9 | Embedded media support..... | 29 |
| 5.10 | Increasing the maximum report size | 30 |
| 5.11 | MI:Viewer log files..... | 30 |
| 5.12 | Where to find MI:Viewer settings files..... | 32 |
| 6 | <i>MI:Toolbox application administration</i> | 33 |
| 6.1 | MI:Toolbox configuration files | 33 |
| 6.2 | Configuring plug-in shadowing..... | 34 |
| 7 | <i>Remote Import application administration</i> | 35 |
| 7.1 | Configuring the application's connection to MI:Server | 35 |
| 7.2 | Job expiry settings | 35 |
| 7.3 | Application "Home Page" link | 36 |
| 7.4 | Job storage folder location | 37 |
| 7.5 | Upload file size limit | 37 |
| 7.6 | Changing the port number for Remote Import..... | 38 |
| 8 | <i>Granta database administration</i> | 39 |
| 8.1 | Logging in to MI:Admin | 39 |
| 8.2 | Locking the database while making changes | 40 |
| 8.3 | Defining and modifying the database schema | 40 |
| 8.4 | Managing profiles..... | 40 |
| 8.5 | Access control for database items | 40 |
| 8.6 | Creating and applying Data Updates..... | 41 |
| 9 | <i>Application Activity reporting</i> | 42 |
| | <i>Appendix A. MI:Server Audit Logging</i> | 43 |
| | <i>Appendix B. Troubleshooting</i> | 46 |

1 Introduction

This document gives an overview of different GRANTA MI administration activities, 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 SQL logins to allow access to 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:

- Loading the databases hosted on SQL Server into GRANTA MI
- Upgrading MI databases when required
- Managing GRANTA MI system and database security groups
- Setting the access control mode for GRANTA MI (*permission-based* or *attribute-based*)
- Configuring system-wide features such as 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 (*schema*) of GRANTA MI databases
- Implementing permission-based access control and version control in MI databases
- Managing 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

User assistance and training content for GRANTA MI can be accessed in a number of different ways.

Help for application users

Procedural information on how to use the software can be accessed from the Help menu of each application or tool.

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

The complete reference documentation set for GRANTA MI, aimed at IT Administrators, Granta System Admins and Data Administrators, and people importing/exporting data, is installed in a *Documentation* folder on the MI:Server host server during product installation, typically:

C:\Program Files\Granta\GRANTA MI\Server\Documentation

Documentation for MI:Toolbox plug-ins is installed in a *Documentation* subfolder within each plug-in, for example:

C:\Program Files\Granta\GRANTA MI\Toolbox\plugins\Exporters\Excel\Documentation

Reference documentation in MI:Viewer

The complete reference documentation set for GRANTA MI is also copied to a *Documentation* folder in the MI:Viewer web site during product installation, and can then be accessed from the application's Help menu.

GRANTA MI resources on the Granta Support website

Reference documentation, FAQs, training resources, and archive webinar videos for GRANTA MI can all be accessed on the [GRANTA MI Support site](#) (sign-in is required).

GRANTA MI resources on ANSYS Learning Hub

Reference documentation, FAQs, training resources, and archived webinar videos for GRANTA MI can all be accessed on [ANSYS Campus](#) (sign-in is required).

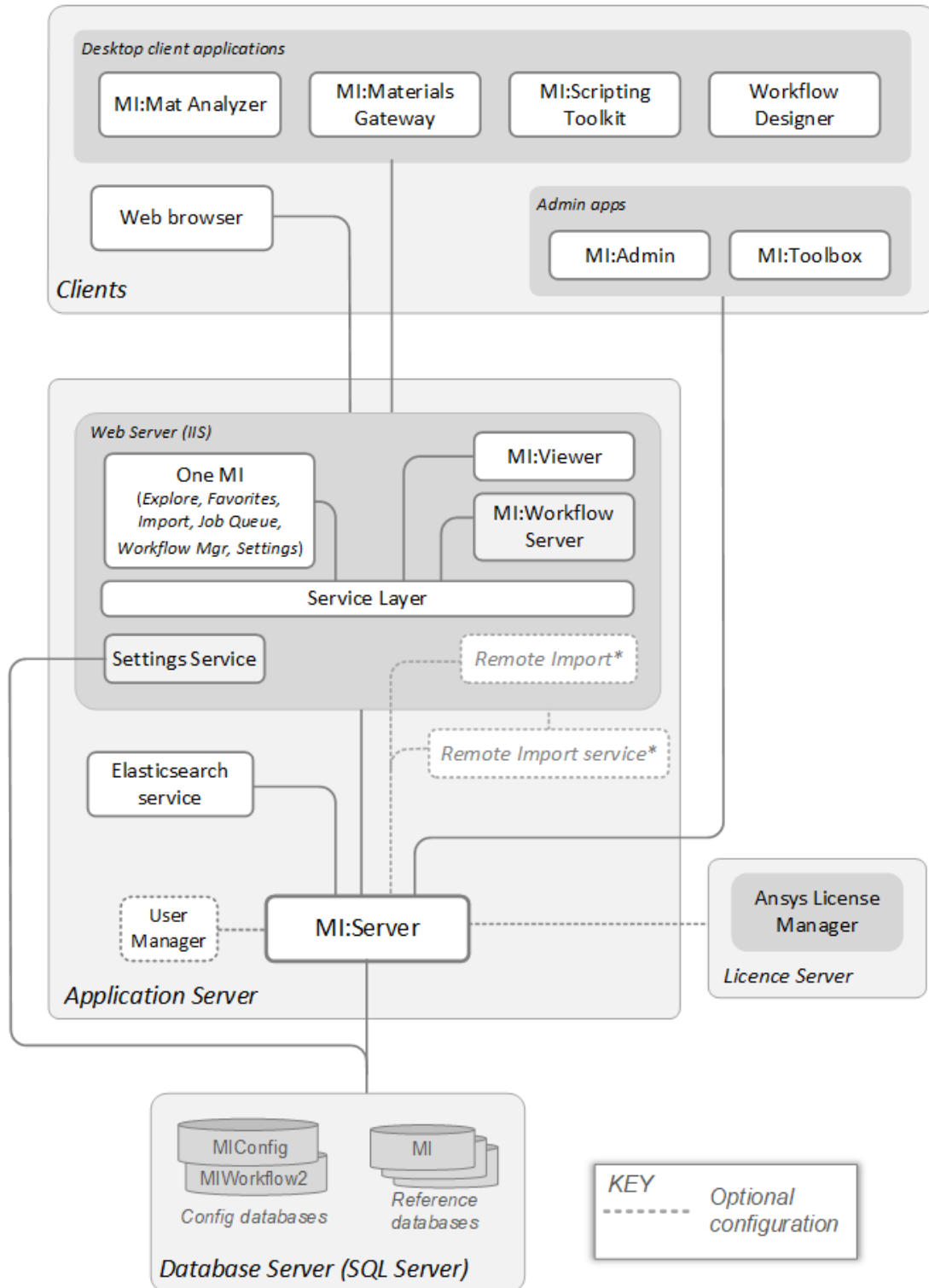
1.6 Your feedback

We welcome your feedback on Granta help and documentation; please email your comments to: granta-docs@ansys.com

For technical or product-related queries, 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 services, web applications, and Windows desktop client applications.



*Support for the standalone Remote Import application will be withdrawn in a future release of GRANTA MI.

2.1 MI:Server

At the heart of the GRANTA MI software deployment is **MI:Server**, the GRANTA MI application server, which is hosted as a Windows service. See Section 4 for information on MI:Server application admin tasks and tools.

2.2 One MI

One MI is a browser-based GRANTA MI application home page that provides a single, streamlined workspace for launching GRANTA MI enterprise applications. The home page can be customized for your organization and your users, with a menu that provides easy access to integrated applications including:

- Explore – finding, visualizing, & applying data
- Favorites – managing lists of favorite materials
- Import – importing data from text and Excel files
- Job Queue – monitoring import and report jobs, and downloading completed reports
- Settings – managing integration settings for MI applications
- Workflow Manager - viewing and progressing active workflows, starting new workflows

2.3 Settings Service

The Settings Service provides a centralized place to store integration settings for interdependent MI applications; settings may be modified using the One MI Settings app.

2.4 MI:Viewer

MI:Viewer is a standalone rich web application that provides tools for browsing, querying, reporting, adding, editing, and exporting data. See Section 5 for details of how to perform these and other MI:Viewer admin tasks.

2.5 Service Layer

The Service Layer is a software component that provides an interface between MI:Server and applications such as One MI, MI:Viewer, and MI:Workflow.

2.6 Remote Import

Remote Import is a standalone web application for uploading data into GRANTA MI.

IMPORTANT While Remote Import is supported in the current release of GRANTA MI, please note that support for it will be withdrawn in a future release. The new, integrated Import app, accessed from the GRANTA MI application home page (One MI), should be

used instead. We encourage customers currently using Remote Import to migrate to the new One MI Import app.

2.7 MI:Admin

MI:Admin is a Windows client application for database administration. It is used to:

- Modify the schema of GRANTA MI databases, for example, adding new tables, attributes
- Configuring permission-based access control for GRANTA MI databases.
- Creating and applying data updates for GRANTA MI databases with the Data Updater.

See Section 8 for more information.

2.8 MI:Toolbox

MI:Toolbox is a Windows client application for bulk data import, processing, and manipulation. It is a framework to host a suite of plug-ins, with data manipulation functionality provided by the plug-ins. See Section 6 for more information.

2.9 MI:Workflow, MI:Workflow Designer

MI:Workflow and MI:Workflow Designer are the server and client applications for defining and managing materials data management workflows. Admin and configuration for MI:Workflow is covered in the *MI:Workflow Configuration Guide*.

2.10 Database server

GRANTA MI databases hosted in Microsoft SQL Server store reference data, data from in-house testing and design and other proprietary sources, and trusted references.

The database server also stores configuration databases for GRANTA MI:

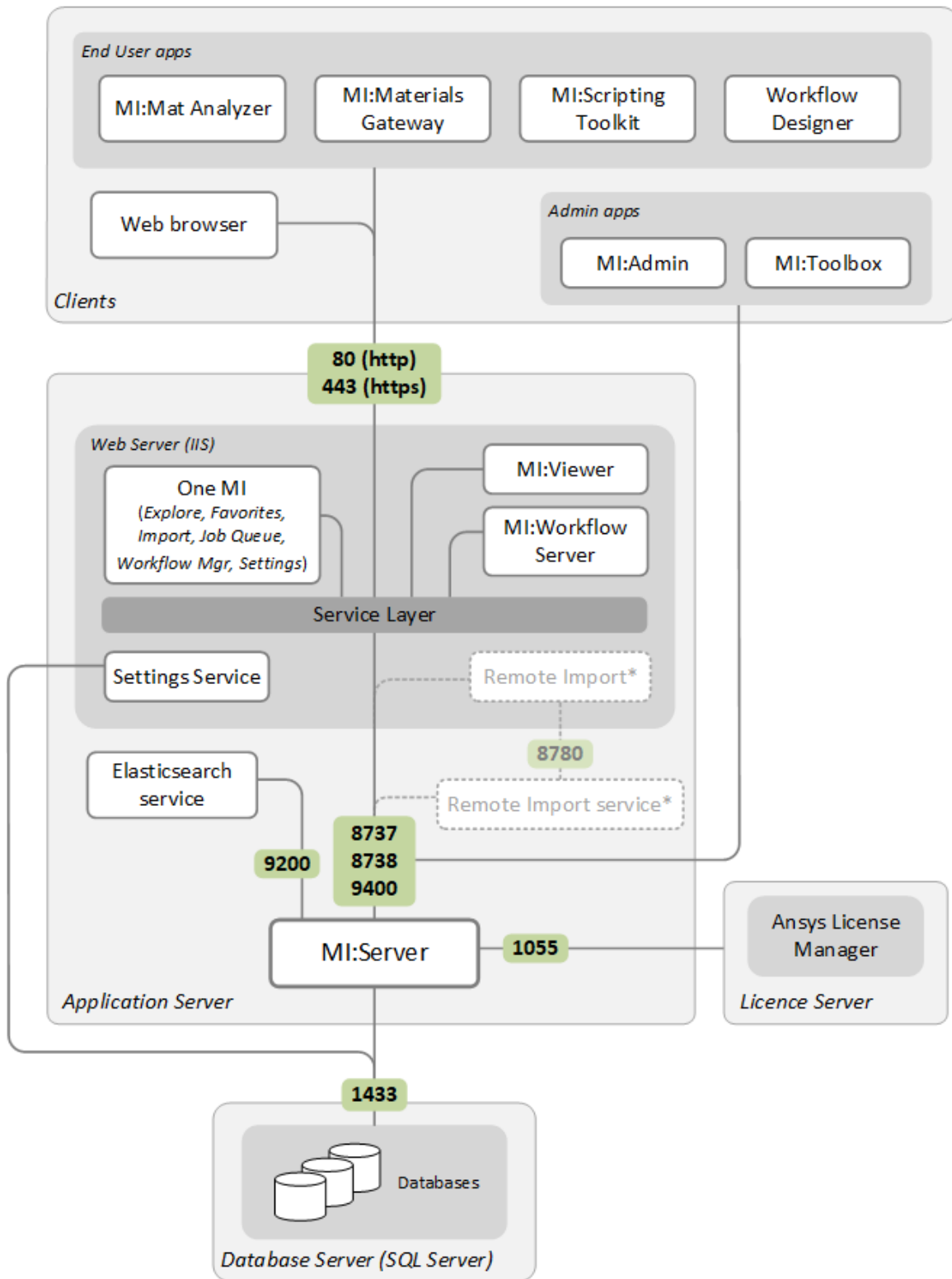
- *MIConfig* – stores settings about the available databases, currency conversion and Notification settings, and data managed by the Settings Service.
- *MIWorkflow2* – stores configuration settings for the MI:Workflow application.

The settings that define how MI:Server connects with SQL Server to access MI databases, 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.

Note that 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.

2.11 Ports used by GRANTA MI software

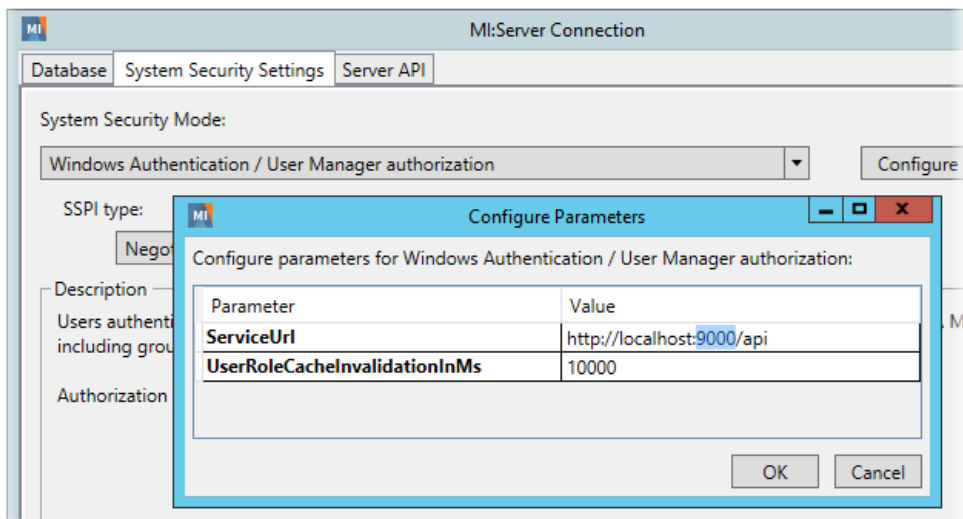
The GRANTA MI system requires the following ports to be opened through the firewall of the computer on which MI:Server is installed, when it is deployed across a network.



The GRANTA MI Windows admin clients (MI:Admin and MI:Toolbox plus MI:Server Manager) connect directly 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.

To change the port used by Remote Import, see Section 7.6 in this document. To change the port used by the Elasticsearch service, see the *GRANTA MI Configuration Guide*.

To change the port used by User Manager, edit the *ServiceUrl* parameter in the System Security Settings page in MI:Server Connection tool and specify the new port number, for example:



3 Search in GRANTA MI

The MI Search Server component provides search capabilities in GRANTA MI. It is built on Elasticsearch, a widely-used, open-source search engine.

The data in database records, including text in embedded documents, is *indexed*—stored and made searchable—by Elasticsearch whenever the database is loaded into GRANTA MI and after any data is modified.

3.1 Supported document types

Elasticsearch will attempt to index all commonly-used document types. Embedded documents that are not a supported file type will not be indexed, and so their contents will not be searchable.

Specific file types can be explicitly excluded from the index via search configuration settings in the MI:Server configuration file MIServer.exe.config; see the *GRANTA MI Configuration Guide* for details.

3.2 Size limitations

By default, records larger than 150 Mbytes will not be indexed, and individual embedded documents larger than 100 Mbytes will not be indexed.

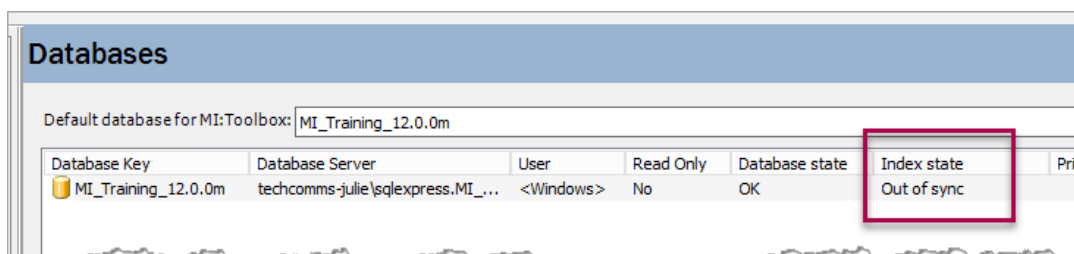
These maximums can be modified via search configuration settings in the MI:Server configuration file MIServer.exe.config; see the *GRANTA MI Configuration Guide* for details.

3.3 How indexing failures are handled

If Elasticsearch has any problem extracting text from an embedded document (for example, if the file is password-protected, or is corrupt in some way), then it will not index that that document, but it will continue indexing the rest of the data on the record.

Even if the contents of an embedded document are not indexed, the file name and file description will still be indexed along with the other data in the record. If the record gets indexed, searches will always return matches in file names and file descriptions.

Where Elasticsearch is unable to index a record, for example because a file is too large, or there is not enough disk space available, or the search service is not running, an 'Out of sync' flag will be shown against the search index for that database in MI:Server Manager and also on the Admin>Databases tab in MI:Viewer:



3.4 Search synonyms

Search synonyms can be used to broaden the scope of searches to include keywords or phrases with the same or similar meaning, or with alternative spellings, for example, allowing for spelling variations. Search synonyms are defined at server-level and applied across all databases and client applications.

See the *GRANTA MI Configuration Guide* for information about defining search synonyms.

3.5 Search suggestions (autocomplete)

Search suggestions (autocomplete), where users see suggestions while they are typing search terms, is a configurable option for MI:Viewer.

See the *GRANTA MI Configuration Guide* for information about configuring search suggestions for MI:Viewer.

3.6 Excluding documents from the index

Individual embedded documents can be excluded from the search index, making the text in them unsearchable, by setting a flag ('Allow file contents to be searched') on the File Attribute datum in MI:Viewer. See the *GRANTA MI Schema Guide* or the MI:Viewer help for more details.

Entire tables can be excluded from the search index, making any data in them unsearchable, via flags set on the table in MI:Admin (*Hide table completely*, *Search table*). See the *GRANTA MI Schema Guide* or the MI:Admin help for more details.

3.7 Other search configuration settings

The *GRANTA MI Configuration Guide* includes detailed information about changing the search and indexing configuration options covered above, and some additional ones including:

- Limiting the number of search indexes that are built concurrently
- HTTPS configuration for Elasticsearch for GRANTA MI
- Changing the default location of the search indices
- Changing the port used by the search service

3.8 AdoptOpenJDK Java Runtime (JRE)

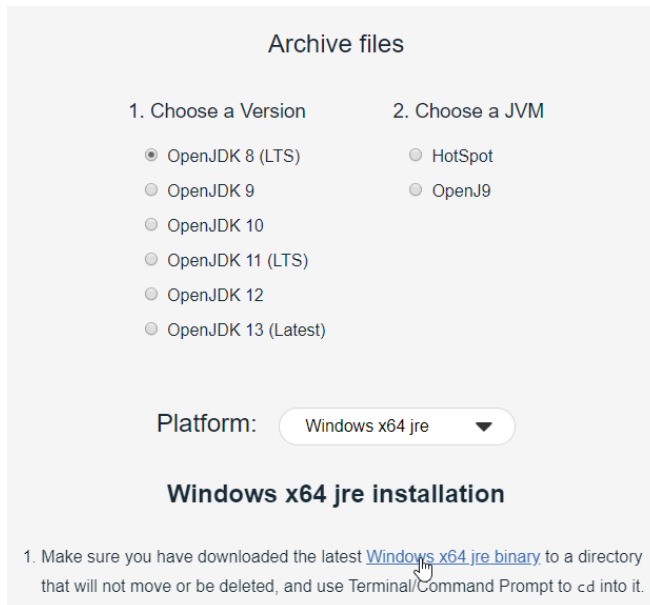
The MI Search Server component includes an OpenJDK Java Runtime Environment (JRE) for internal use by Elasticsearch. This is automatically installed under the installation folder for the Search Server component e.g. C:\Program Files\Granta\GRANTA MI\Elasticsearch\7.3.1\jdk.

Granta and ANSYS will make every effort to release GRANTA MI products with the most current version of AdoptOpenJDK Java Runtime (JRE).

Granta will test the most current commercial ANSYS GRANTA MI release with each subsequent JRE update to confirm compatibility. Customers will be able to install subsequent JRE updates without installing a subsequent GRANTA MI release if, for example, a JRE update contains an important vulnerability fix.

To update the MI Search Server AdoptOpenJDK JRE, follow the steps below. (The Elasticsearch version may be slightly different in your installation.)

1. Go to the AdoptOpenJDK Windows x64 JRE Installation page https://adoptopenjdk.net/installation.html?variant=openjdk8&jvmVariant=hotspot#x64_win-jre and download the archive file onto the GRANTA MI application server via the link in Step 1 on the page. For example:



The screenshot shows the 'Archive files' section of the AdoptOpenJDK website. It is divided into two columns: '1. Choose a Version' and '2. Choose a JVM'. Under '1. Choose a Version', there are radio buttons for OpenJDK 8 (LTS), 9, 10, 11 (LTS), 12, and 13 (Latest). Under '2. Choose a JVM', there are radio buttons for HotSpot and OpenJ9. Below these columns is a 'Platform:' dropdown menu currently set to 'Windows x64 jre'. Underneath the dropdown is the heading 'Windows x64 jre installation' and a numbered instruction: '1. Make sure you have downloaded the latest [Windows x64 jre binary](#) to a directory that will not move or be deleted, and use Terminal/Command Prompt to cd into it.'

2. Stop the *GRANTA MI Service* and the *Elasticsearch 7.3.1 (ElasticsearchServiceForMI)* services.
3. Rename the folder `C:\Program Files\Granta\GRANTA MI\Elasticsearch\7.3.1\jdk` to `jdk_backup`
4. Extract the .zip downloaded in Step 1 above and copy the extracted folder into `C:\Program Files\Granta\GRANTA MI\Elasticsearch\7.3.1`.
5. Rename the new folder to **jdk**.
6. Restart the *ElasticsearchServiceForMI* service and the *GRANTA MI service*.

The `jdk_backup` folder may be deleted once you are happy that everything is working correctly.

4 MI:Server administration

4.1 MI:Server admin/config tools

Two tools are provided with MI:Server for configuration and management of your GRANTA MI application server:

| Tool | Capabilities |
|-----------------------------|---|
| MI:Server Connection | <ul style="list-style-type: none"> Configuring the credentials used by MI:Server to connect to the SQL Server instance where the GRANTA MI configuration database is installed. Changing the GRANTA MI system security mode; see 4.2. Configuring the certificate information required to enable the Search Suggestions feature in MI:Viewer. |
| MI:Server Manager | <ul style="list-style-type: none"> Adding databases to the GRANTA MI system, and removing databases, monitoring database status and availability, configuring database authentication credentials, making databases read-only. Defining system and database security groups. Configuring email notification settings; see also Section 4.3. 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. |

See the Help in each of these tools for detailed information on all the above tasks.

4.2 System security mode

By default, GRANTA MI uses Windows Active Directory for both authentication and authorization. Other configurations are supported:

- User Manager, the Granta user management web application, can be used instead of Windows for user authentication and/or authorization.
- Users can be authenticated against an identity provider system using industry standard OpenID Connect with OAuth 2.0 (OIDC).

Support for OpenID Connect authentication is a Limited Availability feature introduced in GRANTA MI 2020 R2. This means that it is available for customers to use in production, but has limited support and documentation. Only a limited number of identity providers are supported in this release and there are additional configuration requirements to implement OIDC authentication as a Single Sign-On solution for GRANTA MI. Contact Ansys Granta Technical Support for information on supported OIDC identity providers, and for configuration and setup documentation.

4.2.1 Setting system security options

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.

You will 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 you will also need to configure the User Manager authentication for use with the MI:Viewer, Service Layer, and Remote Import software components; see the *GRANTA MI Configuration Guide* for details.

OpenID Connect authentication / User Manager authorization

GRANTA MI users authentication against an identity provider system using industry standard OpenID Connect with OAuth 2.0 (OIDC). This is a Limited Availability feature introduced in GRANTA MI 2020 R2; see note at the bottom of page 15.

Custom authenticator

Where this has been configured, a custom authenticator can also be selected here; see [4.2.2](#).

4.2.2 Configuration for a custom authenticator

To use a custom authenticator:

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 System Security Settings tab, click **Advanced** and select the custom authenticator from the list. Click **Configure Parameters** to specify any parameter settings; these will depend on the authenticator.
5. Click **Save changes & restart service**. The GRANTA MI service will automatically restart; when it comes back, it will be using the new authenticator.

4.3 Configuring Notifications for MI:Viewer users

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 [4.3.1](#).
2. In MI:Server Manager, configure the notification email settings. See [4.3.2](#).
3. Optionally, set up a notifications scheduled task. See [4.3.4](#).

4.3.1 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 |
|--|---|
| Enable Notifications | <p>Enables/disables the Notifications feature in MI:Viewer.</p> <p>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 Notifications 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 Notifications tab or be able to add items to watch lists, and no email notifications will be auto-generated.</p> |
| Show the Notifications tab only to Admin users | <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 Notifications tab. Users who are not administrators will not see the Notifications 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 Notifications tab.</p> |

4.3.2 Configuring email settings for Notifications

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

- SMTP server settings for notification emails for MI:Viewer users.
- 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.

4.3.3 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:

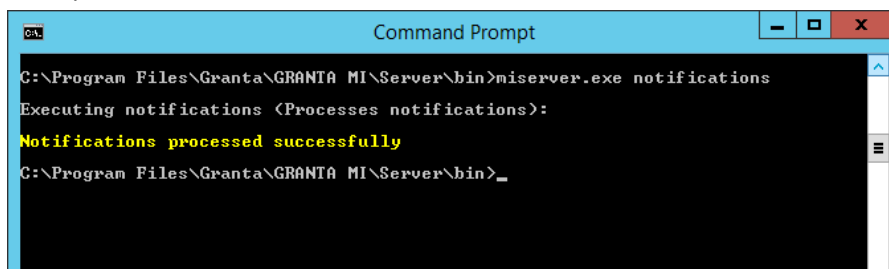
```
C:\Program Files\Granta\GRANTA MI\Server\bin
```

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 [4.3.5](#).

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:



```

Command Prompt
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

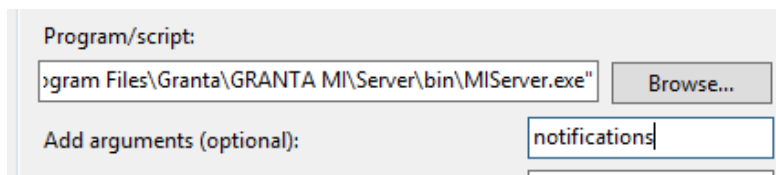
Include notifications for all databases except the specified database. To exclude additional databases, repeat the **-x** option for each one. For example

```
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.

4.3.4 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:

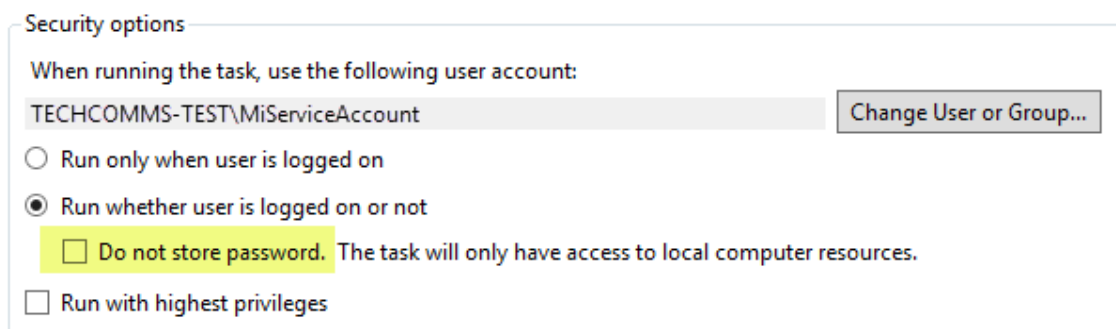


The **notifications** argument is case sensitive; use the **-i** or **-x** command-line arguments described in the previous section, if required, to include or exclude specific databases.

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:



4.3.5 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%`, typically:

```
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"...
```

4.3.6 Notifications information in the Application Activity Summary

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

4.4 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.

4.4.1 To restart the service from Windows Services:

In the Services Microsoft Management Console (MMC) snap-in, locate the **GRANTA MI Service** and restart it.

4.4.2 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.

4.5 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.

MIServer.log

By default, the MI:Server log file, MIServer.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.

5 MI:Viewer application administration

5.1 Configuring the MI:Viewer-MI:Server connection

To allow MI:Viewer to connect to MI:Server, account credentials must be specified in the MI:Viewer Configuration tool: **Start > All Programs > GRANTA MI > MI Viewer Configuration**

5.2 Enabling access to reporting services

The Service Layer provides services that enable reports summarizing or analyzing data to be created as background jobs by MI:Viewer users. Reports submitted from MI:Viewer are placed on a job queue, which may contain different types of job (report jobs, import jobs), submitted by multiple users. Jobs are run one at a time ('asynchronously') on the queue, and scheduling and management of jobs is handled by the GRANTA MI Async Job Service.

Users can view their own jobs on the queue and download their completed reports in the GRANTA MI Job Queue application, which can be opened directly from links on the Reports page in MI:Viewer:

The screenshot illustrates the workflow for running reports in MI:Viewer. It shows three main components:

- Select Report Content Dialog:** A dialog box with a green notification bar that says "Your report has been submitted. Click here to view/download reports." A red arrow points from this notification to the "Run Reports" dialog.
- Run Reports Dialog:** A dialog box titled "Run Reports View / Download Reports..." showing a list of reports that can be run on the records currently in the Record List. The reports listed are "Substances To Materials" (with an XL icon) and "Substances To Specifications" (with an SX icon). A red arrow points from this dialog to the "Job Queue" table.
- Job Queue Table:** A table with columns: Completion d..., Duration, Job Name, Description, Job Pro..., Type, and Scheduled start. The table contains several rows of job data, including "Substances To Products", "Comparison Table", "Lowalloysteel,AISI4130,airmelted,", and "Substances To Specifications".

5.3 Troubleshooting reporting

If you experience issues with asynchronous reports, for example, when MI:Viewer is configured to use anonymous access, you can force MI:Viewer to run reports synchronously by adding the following setting in the MI:Viewer appSettings.config file:

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

This file is typically located here:

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

5.4 Providing links to specific records

MI:Viewer datasheet and index URLs can identify a record by its Record History ID, Record GUID (RGUID) or Record History GUID (RHGUID):

| Record identifier | URL parameter |
|------------------------------|-------------------|
| Record History ID | history |
| Record history GUID (RHGUID) | recordHistoryGuid |
| Record GUID (RGUID) | recordGuid |

In a version-controlled record, the Record History GUID will return the latest version of the record, while the Record GUID can be used to return a specific record version.

5.4.1 Index URL examples

Include the MI:Viewer index (index.aspx) and a record identifier in the URL for a link that opens the MI:Viewer web application home page and loads the record datasheet. For example:

```
http://acmeserver/mi/index.aspx?history=11331
http://acmeserver/mi/index.aspx?recordHistoryGuid=d0237d48-ddd2-4916-b24c-86ba51f25b52
http://acmeserver/mi/index.aspx?recordGuid=0000098c-000e-4fff-8fff-dd92ffff0000
```

5.4.2 Datasheet URL examples

For a link that opens just the datasheet in the browser (no application toolbar, Browse tree, or search tools), include datasheet.aspx in the URL instead of index.aspx; in addition to the record identifier, you must also specify the database key where the record is located. For example:

```
http://acmeserver/mi/datasheet.aspx?history=11331&dbkey=MI_Training
http://acmeserver/mi/datasheet.aspx?dbkey=MI_Training&recordHistoryGuid=d0237d48-ddd2-4916-b24c-86ba51f25b52
http://acmeserver/mi/datasheet.aspx?recordGuid=0000098c-000e-4fff-8fff-dd92ffff0000&dbkey=MI_Training
```

Note that, on following a datasheet URL, the user will be immediately redirected to the equivalent URL with the record history id (if recordHistoryGuid is used) or the record id (if recordGuid is used). For example, this URL with a Record History GUID:

```
http://acmeserver/mi/datasheet.aspx?dbkey=MI_Training&recordHistoryGuid=d0237d48-
ddd2-4916-b24c-86ba51f25b52
```

resolves as

```
http://acmeserver/mi/datasheet.aspx?dbkey=MI_Training&history=11331
```

This URL with a Record GUID:

```
http://acmeserver/mi/datasheet.aspx?dbkey=MI_Training&recordGuid=0000098c-000e-
4fff-8fff-dd92ffff0000
```

resolves as

```
http://acmeserver/ mi/datasheet.aspx?dbkey=MI_Training&record=131862
```

5.5 Setting the MI:Viewer home page

The application home page (also referred to as the *system* 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*.

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:

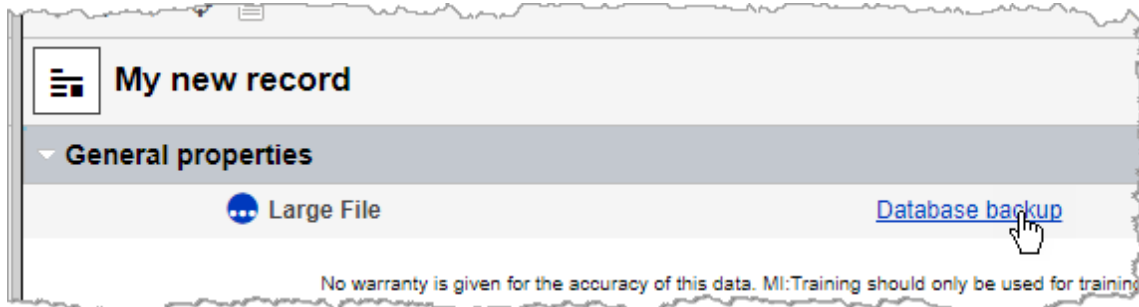
```
\inetpub\wwwroot\mi\systemhomepage
```

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.

5.6 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.

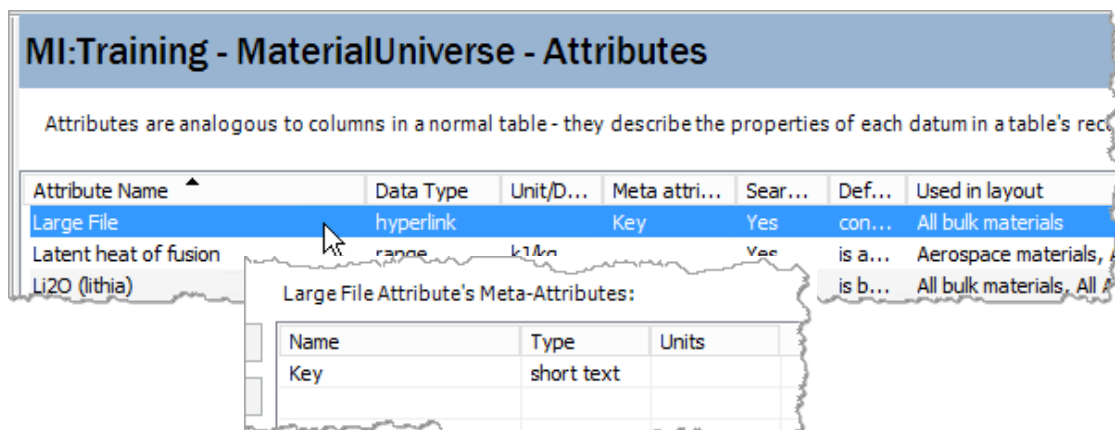
To use this feature, it is necessary to carry out the following configuration steps:

- 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="true" />
</MIConfig>
```

Note:

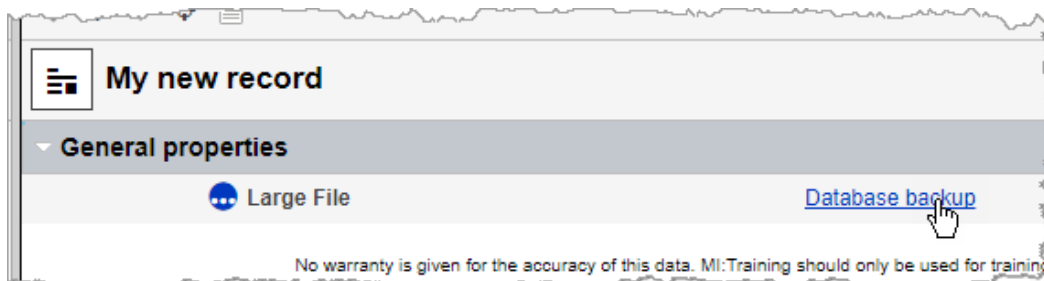
- Make sure that the folder specified by `rootPath` exists (D:\Data\Backups in this case)
 - Ensure that the IIS Application Pool used by MI:Viewer has read and write access to the root folder; in a default installation, this is a local account known as **IIS AppPool\MIViewer_AppPool** on the server 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:

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.

5.7 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
```

5.7.1 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.

5.7.2 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.)

5.7.3 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.

5.7.4 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.

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 Advanced 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, by changing the `minMaxCacheUpdateDelay` value in the `<Search>` section of the MI:Server configuration file `MIServer.exe.config`. The delay is specified in HH:MM:SS format; setting this to 00:00:00 will keep the min-max cache up-to-date on every commit. For example:

```
<Search textIndexLocation="http://localhost:9200/"
minMaxCacheUpdateDelay="00:00:00" indexingQueryBatchSize="5000"
IncludeRecordNamesWhenUsingSearchMask="false" cachepath="..\Caches"
cacheUpdater="Synchronous" />
```

The `MIServer.exe.config` configuration file is located in the MI:Server `bin` folder, for example:

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

Note that the GRANTA MI service must be restarted after any changes to `MIServer.exe.config`.

5.8 Changing the default unit systems

To specify the default unit system 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>
```

5.9 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.
- The contents of embedded media files cannot be edited.
- Many common file types can be viewed within MI:Viewer; files that cannot be displayed can be downloaded and viewed locally with the appropriate, where this is permitted by the web browser security settings.

5.9.1 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 5.6. 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.

5.10 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 can 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.

5.11 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.

5.11.1 Changing the logging level

The logging level determines the amount of information that is logged in the MIViewer.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`

5.11.2 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.

5.11.3 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.

5.12 Where to find MI:Viewer settings files

| File | Location and contents |
|-----------------------|---|
| web.config | C:\Inetpub\wwwroot\mi\web.config ASP.NET application configuration settings |
| connection.xml | %PROGRAMDATA%\Granta\GRANTA MI\connection.xml MI:Server connection information; see 5.1. |
| ViewerSettings.config | C:\Inetpub\wwwroot\mi\AppData\config\ViewerSettings.config Settings relating to the display of functional graphs, X-Y charts and links; see 5.4). Settings to enable access to large, externally-stored files from MI:Viewer; see 5.6. |
| appSettings.config | C:\Inetpub\wwwroot\mi\AppData\config\webConfigFragments\appSettings.config Display settings for closed range attributes; see 5.7.4. |
| log4net.config | C:\Inetpub\wwwroot\mi\AppData\config\log4net.config Application logging settings, including the default application log file name and location. |

6 MI:Toolbox application administration

The MI:Toolbox client application is used for bulk data processing and data analysis via a suite of plug-ins.

6.1 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.

6.1.1 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
```

6.1.2 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
```

6.2 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.

7 Remote Import application administration

IMPORTANT While Remote Import is supported in the current release of GRANTA MI, please note that support for it will be withdrawn in a future release. The new, integrated Import app, accessed from the GRANTA MI application home page (One MI), should be used instead. We encourage customers currently using Remote Import to migrate to the new One MI Import app.

Users with administrative privileges for GRANTA MI can edit some settings for the standalone Remote Import application by clicking **Settings** in the Remote Import application toolbar, or and/or by editing the relevant configuration files directly.

7.1 Configuring the application's connection to MI:Server

The information used to connect the Remote Server application with MI:Server is initially set during installation and can be modified on the Settings page in the Remote Import application. Required details are:

- The hostname of the computer where MI:Server is installed. This can be set to *localhost* if MI:Server and Remote Import are installed on the same server.
- The username, password, and Windows domain (for systems with Windows Authentication) of the account that will be used by Remote Import to authenticate to MI:Server. This account must be a member of the GRANTA MI system security Admin (MI_ADMIN) role.

7.2 Job expiry settings

Import jobs that have completed successfully may be saved for a period of time, during which they remain on the Job List and users can view the job log; data files associated with the job are also stored in the Job storage folder.

At the end of the specified job expiry period (set to 1 month by default), the job and all associated data files are automatically deleted. Job log files are not deleted when the job is deleted. Failed jobs will not be deleted.

You can change the amount of time before completed jobs are automatically deleted under **Configure job expiry settings** on the Settings page.

Configure job expiry settings

Completed jobs will be deleted after the following amount of time:

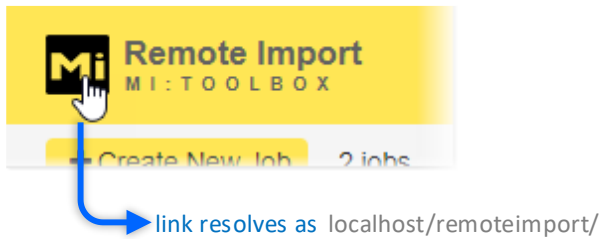
1 day 1 week **1 month** 3 months 1 year never

Save [Clear all completed jobs](#)

Completed jobs can be cleared at any time by clicking **Clear all completed jobs**.

7.3 Application "Home Page" link

The "MI" logo at the top of the Remote Import page provides "Home" button functionality, allowing users to quickly return to the Remote Import home page from any other page within the application:



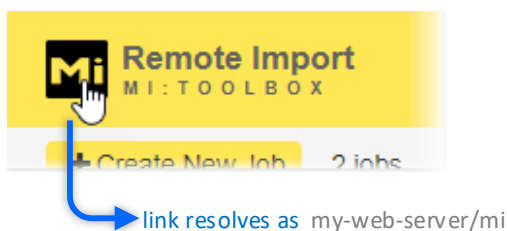
The URL used for this link is specified with the `HomepageUrl` setting in the Remote Import configuration file `Web.config`, typically located in `C:\inetpub\wwwroot\remoteimport`.

By default, this Home Page URL is set to the Remote Import application home page as follows:

```
<appSettings>
  <add key="webpages:Version" value="2.0.0.0" />
  <add key="PreserveLoginUrl" value="true" />
  <add key="ClientValidationEnabled" value="true" />
  <add key="UnobtrusiveJavaScriptEnabled" value="true" />
  <add key="InfiniteScrollEnabled" value="true" />
  <add key="ToolboxWebService:ConnectionPort" value="8780" />
  <add key="ToolboxWebService:ConnectionUseSSL" value="false" />
  <add key="rootDir" value="C:\RemoteImport\" />
  <add key="TlsSecurityProtocolType" value="Tls12, Tls11, Tls, Ssl3" />
  <add key="HomepageUrl" value="~/\" />
</appSettings>
```

To change the target URL for the Remote Import 'Home' button, for example, to open the MI:Viewer application instead, edit `Web.config` and specify the MI:Viewer application URL as the `HomepageUrl`, for example:

```
<add key="rootDir" value="C:\RemoteImport\" />
<add key="TlsSecurityProtocolType" value="Tls12, Tls11, Tls, Ssl3" />
<add key="HomepageUrl" value="http://my-web-server/mi" />
</appSettings>
<log4net>
```



If MI:Viewer and Remote Import are installed on the same server, you can use `localhost` in the URL, for example: `<add key="HomepageUrl" value="http://localhost/mi" />`

7.4 Job storage folder location

By default, completed Remote Import jobs are saved in C:\RemotImport\jobs until they expire. To change this default location, you need to edit two separate configuration files, as described below.

- The folder you specify must be on the same server as Remote Import.
- If the folder does not exist, Remote Import will create it.
- You should ensure that there is a reasonable amount of free disk space for the folder.
- You should ensure that both the Remote Import Service and Web Application have permissions to write to the folder.

Procedure:

1. Edit the Remote Import Service configuration file:
 - a. Locate the folder C:\Program Files\Granta\GRANTA MI\RemotImportServer
 - b. Open the *RemotImportService.exe.config* file in a text editor.
 - c. Locate the `<appSettings>` element and change the value of the `rootDir` key.
 For example: `<add key="rootDir" value="C:\MyDataImport" />`
 The new `rootDir` value here must be the same as `rootdir` in the Remote Import web application (Step 2c below).
 - d. Save the *RemotImportService.exe.config* file.
2. Edit the Remote Import Web Application configuration file:
 - a. Locate the folder C:\inetpub\wwwroot\remoteimport
 - b. Open the file *Web.config* in a text editor.
 - c. Locate the `<appSettings>` element and change the value of the `rootDir` key.
 For example: `<add key="rootDir" value="C:\MyDataImport" />`
 The new `rootdir` value must be the same as that set for `rootdir` in the Remote Import service (Step 1c above).
 - d. Save the *Web.config* file.

7.5 Upload file size limit

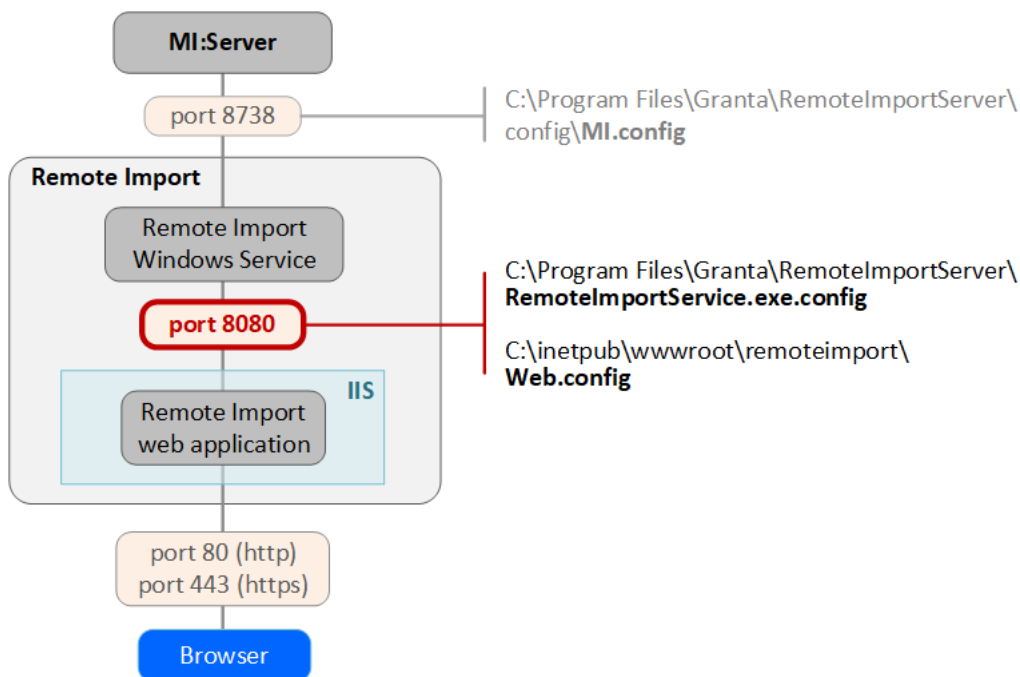
The maximum size of a file for upload in Remote Import is slightly less than 1 GB. You can change this maximum by making the following edits to the Remote Import web application configuration file *Web.config*, located in the Remote Import application installation folder, typically:

C:\inetpub\wwwroot\remoteimport

1. Open the *Web.config* file in a text editor.
2. Locate the `<httpRuntime>` element and change the value of the `maxRequestLength` attribute to the new value in KB. The default value is "1048576".
3. Locate the `<requestLimits>` element and change the value of the `maxAllowedContentLength` attribute to the new value in bytes. The default value is "1073741824".
4. Save the file. The new value is used immediately.

7.6 Changing the port number for Remote Import

The default port used to connect the Remote Import Service with the Remote Import web application is port 8780:



If you need to use a port other than port 8780 for the connection between the Windows service and the web application, you will need to make the changes to these 2 files:

- the Remote Import web application configuration file `Web.config`, typically located here: `C:\inetpub\wwwroot\remoteimport\Web.config`
- the Remote Import service configuration file `C:\Program Files\Granta\RemotelImportServer\RemotelImportService.exe.config`

Change the port number in `Web.config`

1. In a text editor, open the file `C:\inetpub\wwwroot\remoteimport\Web.config`
1. Locate the following line and change this value to the new port number:

```
<add key="ToolboxWebService:ConnectionPort" value="8780" />
```

Change the port number in `RemotelImportService.exe.config`

1. In a text editor, open the file `C:\Program Files\Granta\RemotelImportServer\RemotelImportService.exe.config`
2. Locate the port number key under `<appSettings>` and change its value to the same port number as specified in `Web.config`. For example:

```
<appSettings>
  <add key="portNumber" value="8780"/>
  ...
```

8 Granta database administration

A range of different administration tasks can be performed for GRANTA MI databases using the MI:Admin tool. For full information about using MI:Admin, see the MI:Admin Help system. Detailed reference information on the GRANTA MI database schema, including advice on schema design best practice, is provided in the *GRANTA MI Schema Guide*.

You do not need 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:

- Modify the schema of GRANTA MI databases.
- Define and manage Profiles.
- Configure permission-based access control for GRANTA MI databases.
- Create and apply updates that can be used to modify the content of GRANTA MI databases (data and/or schema), for example to keep different databases in sync.

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.

8.1 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 (MI_ADMIN) system security group.
 - If using Windows authentication, enter the username, password, and domain of a Windows account.
 - If using User Manager authentication, 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. To authenticate against an OIDC identity provider, where this is configured, click the **OIDC** button. Support for OpenID Connect authentication is a Limited Availability feature introduced in GRANTA MI 2020 R2. This means that it is available for customers to use in production, but has limited support and documentation. Only a limited number of identity providers are supported in this release, and there are additional configuration requirements to implement OIDC authentication as a Single Sign-On solution for GRANTA MI. Contact Ansys Granta Technical Support for information on supported OIDC identity providers, and for configuration and setup documentation.
6. Click **OK**. The MI:Admin application will connect to MI:Server.

8.2 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.

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.

8.3 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.

For full information about using MI:Admin to edit your database schema, the MI:Admin Help system. See also the *GRANTA MI Schema Guide* for detailed reference information on the GRANTA MI schema, including advice on schema design best practice.

8.4 Managing profiles

The **Profiles** tool in the MI:Admin application is used to define Profiles 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.

See the *GRANTA MI Schema Guide* for more on how Profiles are used in GRANTA MI, and refer to the help for MI:Admin for detailed information about how to define and modify Profiles.

8.5 Access control for database items

The access control mode (Permission-based or Attribute-based) is set 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.

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.

8.6 *Creating and applying Data Updates*

The **Data Updater** tool in MI:Admin can be used to copy or clone GRANTA MI data, schemas, and/or databases. With the Data Updater, you can create Updates that may be used to:

- create a copy of an entire database, for example, to create a non-production version for development, testing, or diagnostics;
- add, modify, or delete some of the data and/or schema items in a database, for example, to maintain data consistency between two or more copies of the same database;
- create an exact copy of a database schema, without any data at all, for example, for testing or troubleshooting without any sensitive data.

Updates saved as XML files can be shared with other users in your organization, who can them upload, verify, and apply them to a target database using the Data Updater.

Note that only full MI System Administrators can use Data Updater; use by local Database Administrators is not supported.

See the Data Updater help topics in the MI:Admin help for detailed information about creating and applying data updates.

The Data Updater tool can also be used to update GRANTA MI reference databases such as Restricted Substances; this is covered in the *Applying a Product Risk Data Module Update* document included in the Restricted Substances update package.

9 Application Activity reporting

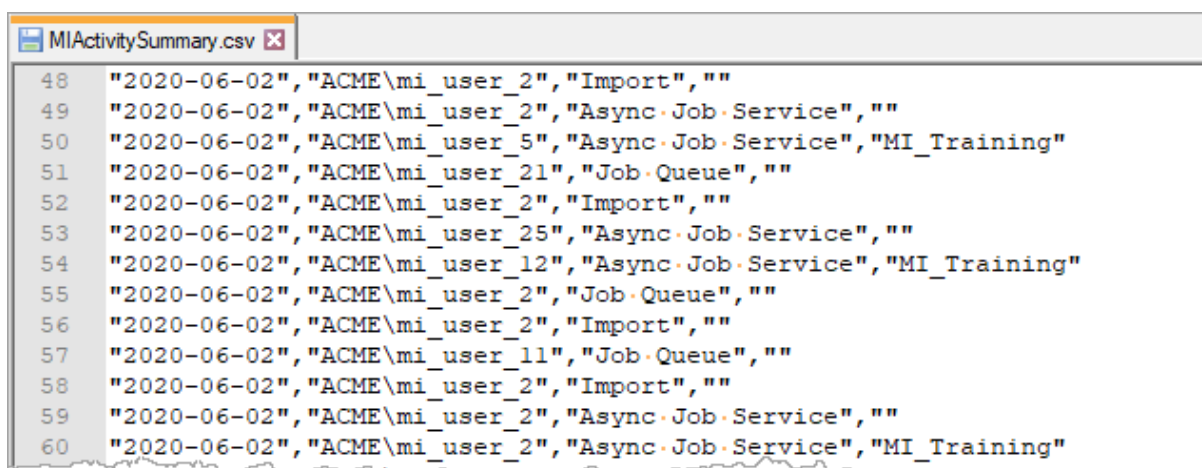
Application Activity reporting information can help you to better understand your system users and their needs.

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.csv
48 "2020-06-02","ACME\mi_user_2","Import",""
49 "2020-06-02","ACME\mi_user_2","Async.Job.Service",""
50 "2020-06-02","ACME\mi_user_5","Async.Job.Service","MI_Training"
51 "2020-06-02","ACME\mi_user_21","Job.Queue",""
52 "2020-06-02","ACME\mi_user_2","Import",""
53 "2020-06-02","ACME\mi_user_25","Async.Job.Service",""
54 "2020-06-02","ACME\mi_user_12","Async.Job.Service","MI_Training"
55 "2020-06-02","ACME\mi_user_2","Job.Queue",""
56 "2020-06-02","ACME\mi_user_2","Import",""
57 "2020-06-02","ACME\mi_user_11","Job.Queue",""
58 "2020-06-02","ACME\mi_user_2","Import",""
59 "2020-06-02","ACME\mi_user_2","Async.Job.Service",""
60 "2020-06-02","ACME\mi_user_2","Async.Job.Service","MI_Training"

```

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 152526 for a workaround.) |
| Client application cannot contact MI:Server | Check that the necessary port is open through the server firewall. See Section 2.11 |
| MI:Server cannot contact database server | Check that the necessary port is open through the server firewall. See Section 2.11 |
| User cannot log in to MI:Server | Check that the user is a member of the correct roles/groups, and the role/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 4.4. |
| 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 2.11 |
| Problems with MI:Viewer, but none with the other client applications MI:Admin and MI:Toolbox | Try restarting IIS. |

| Issue | Suggested check or action |
|--|--|
| 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. |
| 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 5.10. |
| Problems with all the client applications: MI:Viewer, MI:Admin, and MI:Toolbox | Try restarting MI:Server; see Section 4.4. |
| 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. |
