Ansys GRANTA MI 2021 R1

GRANTA MI
Configuration Guide

Contents

1 Who should read this document?

2 Certificate setup for GRANTA MI applications

2.1 About the certificates 6
2.2 Install the certificates and copy the certificate thumbprints 7
2.3 Configure MI:Server to use the certificates 8
2.4 Configure GRANTA MI applications to use the client SSL certificate 9
2.5 Verifying the certificate setup 9

3 User Manager authentication configuration

3.1 GRANTA MI system security options 11
3.2 Prerequisites and requirements for User Manager 12
3.3 Enabling User Manager authentication 13
3.4 Opening User Manager 13
3.5 Adding system users 13
3.6 SSL/HTTPS configuration for User Manager 14
3.7 Kerberos SSP configuration 16
3.8 Application configuration settings—Modules.config 17
3.9 Additional configuration for User Manager Authentication 19
3.10 Restoring the default User Manager Admin account 22

4 Custom authentication for GRANTA MI

4.1 Custom authentication for MI:Server 23
4.2 Custom authentication for MI:Viewer 24
4.3 Custom authentication for MI:Remote Import 24

5 Search and indexing configuration

5.1 Enabling Search Suggestions in MI:Viewer 26
5.2 Setting up search synonyms 26
5.3 Controlling which file types are indexed 27
5.4 Setting record and file size limits for indexing 27
5.5 Optimizing index creation performance 28
5.6 Using HTTPS communication for Elasticsearch 29
5.7 Changing the location of the full text index 29
5.8 Changing the port used by Elasticsearch 30
5.9 Using Elasticsearch for GRANTA MI with drive encryption technologies 30

6 Service Layer IIS configuration

6.1 WCF HTTP Activation 31
6.2 Application Initialization 31
6.3 Dynamic content compression 31

1 Who should read this document?

This document describes how to change various GRANTA MI system configuration settings. It is aimed at administrators who may want to modify system configuration settings after initial installation, in particular to enable use of non-Windows authentication. In most cases, a default GRANTA MI installation will work without the need to make any of the configuration changes documented in this guide.

This guide is organized as follows:

- Section 2 — **mandatory** SSL certificate configuration to enable Favorites Lists in One MI/Explore, and also for MI:Viewer Search Suggestions.
- Section 3 — enabling and configuring User Manager, Granta's user management application.
- Section 4 — required configuration to use a custom authenticator/role provider developed using the MI:Server API.
- Section 5 — search and indexing configuration for MI Search Server, the GRANTA MI system search engine based on Elasticsearch.
- Section 6 — IIS default settings for the Granta Service Layer.

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

2 Certificate setup for GRANTA MI applications

IMPORTANT: The certificate configuration for Favorites Lists described below is **mandatory**; without it, users will see multiple config errors when they use the One MI Explore app.

SSL certificates are used to secure communication between the MI:Server application server and some GRANTA MI applications in order to enable specific features:

- *Favorites Lists* in One MI/Explore and MI:Materials Gateway rely on certificates to securely transfer data between MI:Server and the Service Layer. **Configuration of certificates as detailed below is mandatory**; without it, config errors will appear in the Explore app.
- The *Search Suggestions* feature in MI:Viewer relies on certificates to securely transfer data between the MI:Server Search Service and the MI:Viewer application. Certificate setup to support MI:Viewer Search Suggestions is optional; without it, the feature will simply not be available in the application.

2.1 About the certificates

Two SSL certificates are required, one for the MI:Server, and one for the client applications (MI:Viewer, Service Layer). Any type of SSL certificate (e.g. self-signed, CA-signed) can be used.

Note that a PFX copy of the client certificate is required; if you are using generated, self-signed certificates, ensure that you export the client certificate to a PFX file, as you will need to provide this PFX file and the password when you add the client certificate to the Service Layer or MI:Viewer application.

The same client certificate is used for all GRANTA MI applications on the same machine, and so you only need to add the client certificate in one client application–Service Layer or MI:Viewer–you don't need to do it for each application.

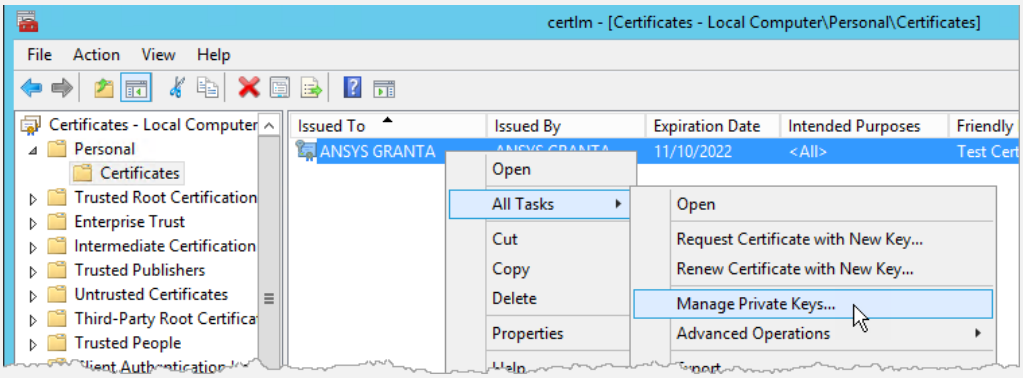
Certificate information is stored in C:\ProgramData\Granta\GRANTA MI\connection.xml as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<ConnectionDetails useWindowsAuthentication="false">
  <Url>localhost</Url>
  <User allowAnonymousAccess="false">
    <Username>{username}</Username>
    <Password>{encryptedpassword}</Password>
    <Domain>{domainname}</Domain>
    <CertificatePath>C:\ProgramData\Granta\GRANTA MI\clientCertificate.pfx</CertificatePath>
    <CertificatePassword>{encryptedpassword}</CertificatePassword>
    <ServerCertificate>{server certificate thumbprint}</ServerCertificate>
    <ClientCertificate>{client certificate thumbprint}</ClientCertificate>
    <SearchServicePort>9400</SearchServicePort>
  </User>
</ConnectionDetails>
```

2.2 Install the certificates and copy the certificate thumbprints

1. On the MI:Server application server, add the server and client certificates to the Local Machine store using MMC (Windows Microsoft Management Console).

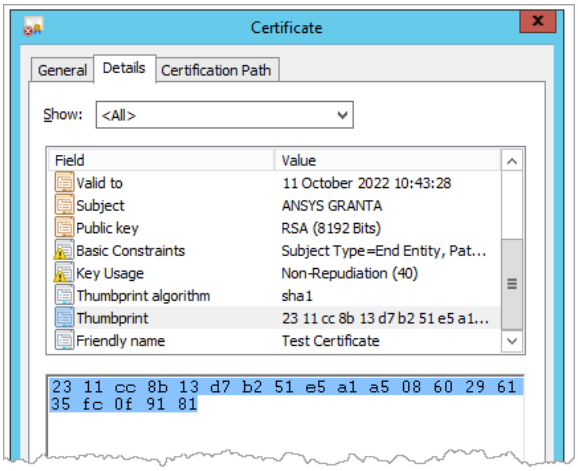
2. **Windows Server 2012 and Windows 10 OS only**: modify the Private Key permissions on the client certificate to grant access to MI:Viewer and Service Layer as follows:
   a. In the Certificate Manager tool, select the client certificate you just added, right-click, and choose **All Tasks > Manage Private Keys**. For example:



   b. Add the IIS app pool users to the allowed *Group or user names*:
      - *IIS AppPool\MIViewer_AppPool* on the machine domain
      - *IIS AppPool\MIServiceLayer_AppPool* on the machine domain

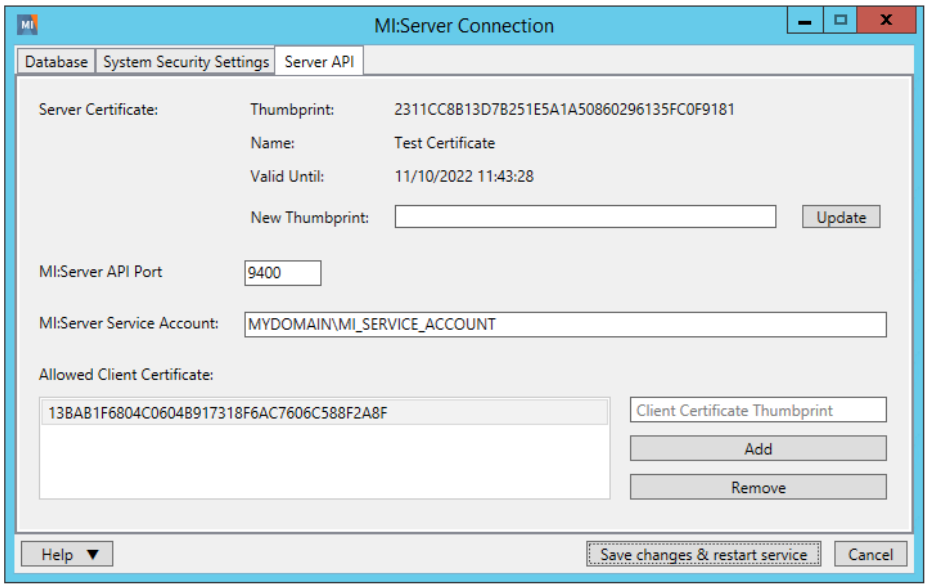
3. If you are using generated, self-signed certificates, export the client certificate to a PFX file, as you will need to provide this PFX file and the password later when you add the client certificate to the Service Layer/MI:Viewer application.

4. For each certificate, copy the thumbprint to a text file as follows:
   a. In the Certificate Manager tool, locate the certificate and open it.
   b. Click on the *Details* tab , highlight the thumbprint value and press CTRL-C to copy the text, then paste the text into a text editor such as Notepad++, removing any spaces between the hexadecimal characters.



2.3 Configure MI:Server to use the certificates

1. On the MI:Server application server, open the MI:Server Connection tool and click the *Server API* tab.
2. Paste the **server** certificate thumbprint into the *New Thumbprint* field and click **Update**.
3. If the MI Service Account is not a member of the Windows Administrators group on the server, enter the account name in the *MI:Server Service Account* field. You don't need to enter anything here if the MI service account has Administrator privileges on the server.
4. Under *Allowed Client Certificate*, paste the thumbprint of the **client** certificate into the field above the *Add* button, then click **Add**.



5. Click **Save changes & restart service**.

The server certificate should now be bound to the port specified in the *MI:Server API Port* field, port 9400 by default. To check, use `netsh http show sslcert` to view the SSL server certificate bindings and the corresponding client certificate policies for the port, for example (The "Certificate Hash" value shown here is the certificate thumbprint):

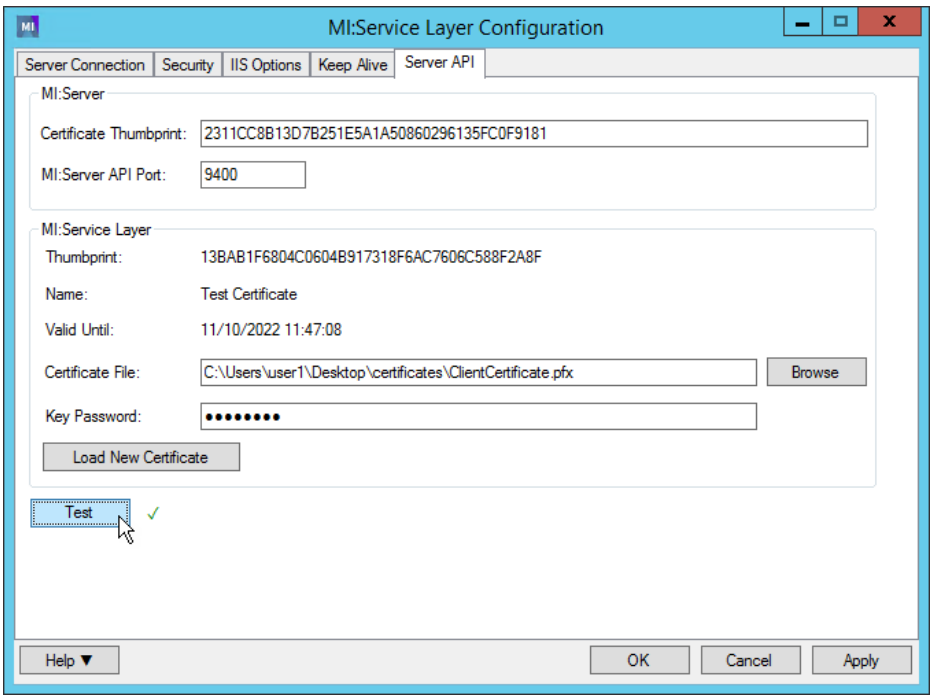
```
netsh http show sslcert ipport=0.0.0.0:9400
```

```
C:\Windows\system32>netsh http show sslcert ipport=0.0.0.0:9400

SSL Certificate bindings:
-------------------------

    IP:port                      : 0.0.0.0:9400
    Certificate Hash             : 2311cc8b13d7b251e5a1a50860296135fc0f9181
    Application ID               : {23cc5191-8325-4a04-a21f-d17108f255d3}
    Certificate Store Name       : (null)
    Verify Client Certificate Revocation : Enabled
    Verify Revocation Using Cached Client Certificate Only : Disabled
    Usage Check                  : Enabled
    Revocation Freshness Time    : 0
    URL Retrieval Timeout        : 0
    Ctl Identifier               : (null)
    Ctl Store Name               : (null)
    DS Mapper Usage              : Disabled
    Negotiate Client Certificate : Enabled


C:\Windows\system32>
```

2.4 Configure GRANTA MI applications to use the client SSL certificate

If the Service Layer and MI:Viewer are both installed on the same application server, you only need to add the client SSL certificate in one of these applications; it doesn't matter which one.

1. On the application server, open the Service Layer Configuration tool or the MI:Viewer Configuration tool and click on the *Server API* tab.
2. In the *MI:Server* section, paste the ***server*** certificate thumbprint into the *Certificate Thumbprint* field and ensure the port number here is the same as specified in the MI:Server Connection tool (9400 by default).
3. Click **Browse** to locate and load the ***client*** certificate PFX file, enter the certificate key password, then click **Load New Certificate**.
4. Click **Test** to check the certificate has been loaded.



2.5 Verifying the certificate setup

Open GRANTA MI Explore from the One MI application or by entering the application URL in a browser:

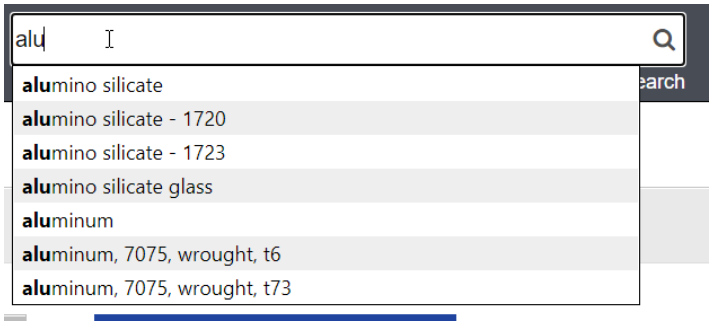
http://<*appservername*>/grantami/#/explore

Check that no 'Encountered error while searching for record lists' errors are displayed.

Open MI:Viewer by entering the application URL in a browser:

http://<*appservername*>/mi

Type a string into the Quick Search box in the application toolbar; you should see a dropdown list of search suggestions, for example:



3 User Manager authentication configuration

GRANTA MI has three different *system security modes* which determine how users are authenticated and authorized. The default mode for GRANTA MI is to use Windows® Active Directory for both user authentication and authorization, but User Manager, Granta's user management application, can be used instead of Windows for user authorization, and it can also be used for user authentication, allowing any assigned administrator to add users to GRANTA MI and move them between groups and roles.

3.1 GRANTA MI system security options

GRANTA MI system security options are set in the MI:Server Connection tool, on the System Security Settings tab. The available options are:

Windows Authentication / Windows authorization (default mode)

- Access to the system and user privileges within GRANTA MI are determined by membership of Windows security groups that are mapped to Granta system roles (Admin, Grant, Power User, Write, or Read).
- Users authenticate to GRANTA MI applications (MI:Viewer, MI:Explore, MI:Toolbox etc.) using their normal Windows Active Directory (AD) credentials.

Windows Authentication / User Manager authorization

- Access to the system and user privileges within GRANTA MI are managed in User Manager, where Granta administrators can add pre-existing Windows users to the GRANTA MI system, and then assign them to different roles.
- Access to resources is determined by a rule engine which works out who can read or change individual resources based on their role.
- Users authenticate to GRANTA MI applications (MI:Viewer, MI:Explore, MI:Toolbox etc.) using their normal Windows Active Directory (AD) credentials.

User Manager authentication / User Manager authorization

- Access to GRANTA MI and user privileges within the system are both managed in User Manager, without any reference to Windows user identities or domains. Granta Administrators can create and delete users in the User Manager tool and add them to/remove them from different roles.
- Access to resources is determined by a rule engine which works out who can read and change individual resources based on their role.
- Users log into GRANTA MI tools and applications using their GRANTA MI (User Manager) username and password.

Custom authentication/authorization

A custom authenticator/role provider developed using the MI:Server API may be used to perform user authentication instead of Windows or User Manager; see Section *4, Custom authentication for GRANTA MI*.

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).

Support for OpenID Connect authentication is a Limited Availability feature in this release. 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.

3.2 Prerequisites and requirements for User Manager

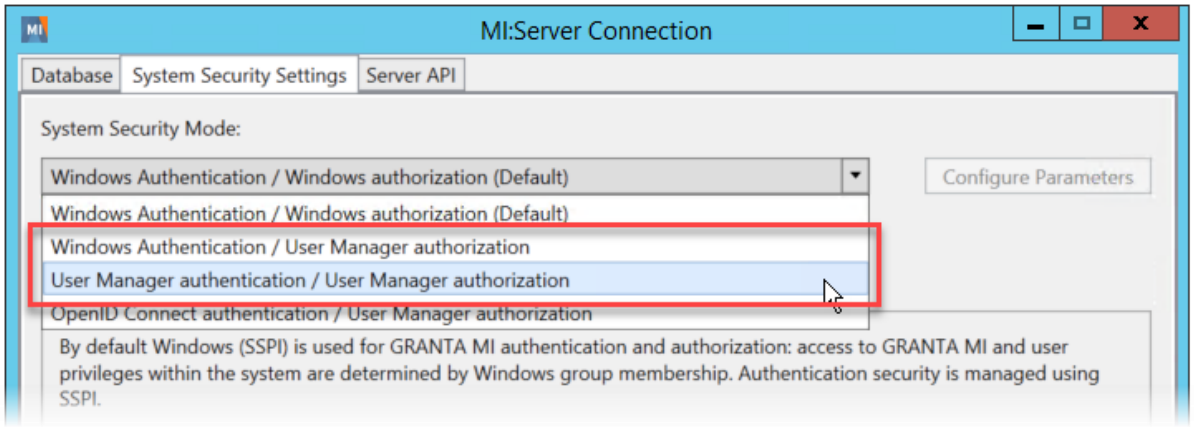
5. If you are running MI:Server under a domain service account (the default configuration) and not a LocalSystem account, you will need to reserve the User Manager URL for non-administrator users and accounts as follows:
   a. Open a Command prompt window using **Run as Administrator**.
   b. Enter this command, with the relevant domain and account name:

```
> netsh http add urlacl url=http://+:9000/ user=DOMAIN\accountname
```

6. If the User Manager application will be running over SSL or HTTPS, some additional configuration is required; see Section *3.6*.
7. If using Windows Authentication, the GRANTA MI service account needs permissions to query the domain. Usually this requirement can be satisfied by the account being a member of the domain or the machine being on the domain (when running as LocalSystem).
8. If using User Manager authentication:
   a. The authentication settings for the MI:Viewer, Service Layer, and Remote Import applications must be configured individually, as described in Section *3.9*.
   b. To ensure that login credentials and password reset notification emails can be delivered to users, the SMTP email settings in MI:Server Manager (Email Notifications>SMTP Settings) **must be configured**. If the email server is not configured, users can be inadvertently locked out of the system if an Administrator performs a password reset (the password will be changed, but the user will not receive an email notification with their new password).
9. The default SSP for User Manager application authentication is NTLM. To use Kerberos instead, see Section *3.7*.

3.3 Enabling User Manager authentication

Open the MI:Server Connection tool and click on the System Security Settings tab to see the options available for User Manager authorization and authentication:



Depending on which User Manager configuration you choose here, some **mandatory** additional setup is necessary:

Windows Authentication / User Manager authorization selected

In User Manager, add the GRANTA MI application connection account (the account used by GRANTA MI applications to connect to the GRANTA MI application server) as an authorized system user; see *Adding system users*.

User Manager authentication / User Manager authorization selected

You will need to modify the default authentication settings for MI:Viewer, the Service Layer, and Remote Import; see *Additional configuration for User Manager Authentication*.

3.4 Opening User Manager

To open the User Manager application, enter the URL in the browser. By default, this is the name of your MI:Server host appended by **:9000**. For example:

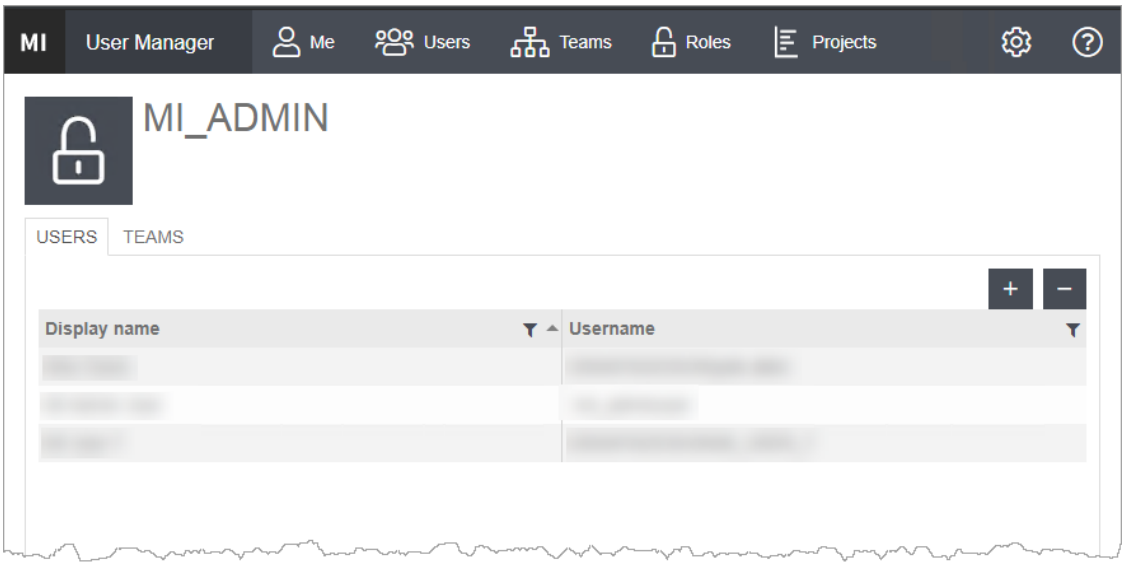
http://*your_mi_server_host*:9000

3.5 Adding system users

After turning on User Manager authorization in MI:Server Manager, you will automatically be added as an Admin user in User Manager. The GRANTA MI application connection account, used by GRANTA MI applications to connect to the GRANTA MI application server, must also be added as an authorized system user. To do this, open User Manager and follow these steps.

1. Add the GRANTA MI connection account as a new system user: click on Users in the toolbar, click the '+' Add button, enter the domain-qualified application connection account name in the Username field, and enter a User Manager display name, for example, Miconnection.

2. Assign this new user to the MI_ADMIN role: click on Roles in the toolbar, double-click MI_ADMIN in the list, click the '+' Add button.

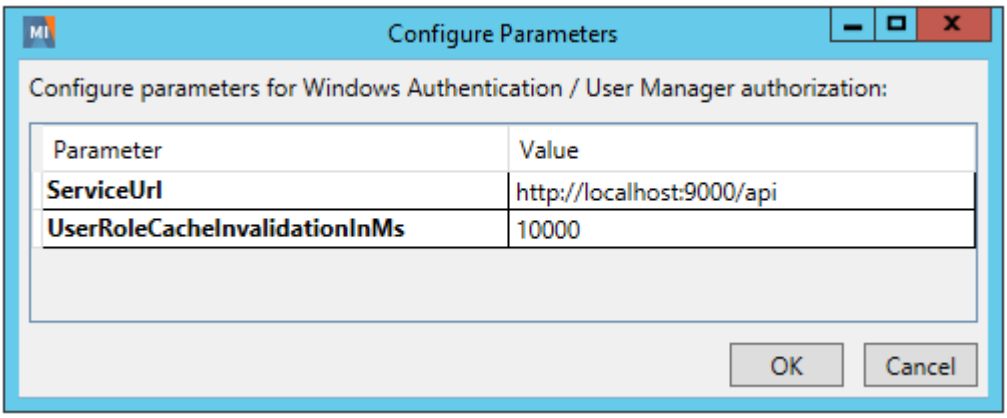


To add more users (for example, via a bulk import), and to assign users to system roles, teams, and projects, see the User Manager help.

3.6 SSL/HTTPS configuration for User Manager

To use User Manager under SSL (https), the following configuration steps are required:

1. On the System Security Settings tab of the Server Connection tool, modify the **ServiceUrl** parameter to include https in the User Manager URL. The address of the server must match the address that the SSL certificate issued to (which is not necessarily the FQDN of the server).



2. Bind the SSL certificate to the port number using netsh as follows:
   a. Open a Command prompt window using **Run as Administrator**.
   b. Enter the following command:

   ```
   netsh http add sslcert ipport=0.0.0.0:9000 certhash=<hash> appid={id}
   ```

   where

   - The **ipport** parameter specifies the port being used by User Manager; by default, this is port 9000.
   - The **certhash** parameter specifies the thumbprint of the SSL certificate (see below for information on how to get the thumbprint in IIS Manager).
   - The **appid** parameter is a GUID that can be used to identify the owning application; it is required for the command, but its value is not used

   Tip: If SSL has been configured for IIS (e.g, for MI:Viewer) then type **netsh http show sslcert** and then just copy and paste the certhash and appid from the posting for the IIS binding.

3. If you are running MI Server under a non-administrator domain service account (the default option for installation), you need to add an HTTPS URL reservation using netsh.

   In a Command prompt window with administrative privileges (**Run as Administrator**), enter this command:

   ```
   netsh http add urlacl url=https://+:9000/ user=DOMAIN\username
   ```

   where *DOMAIN* and *username* are the domain and service account name. Ensure that you specify **https** in the URL here.

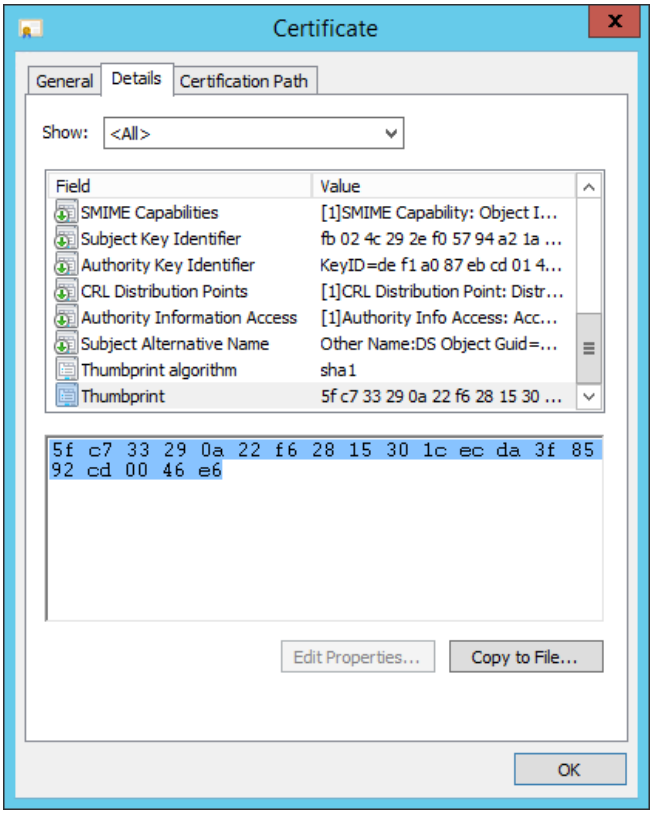
   Note that if this URL reservation fails (for example, because http access has already been set up on this URL), you will need to delete the existing reservation using `netsh http delete urlacl url=http://+:9000/`, and then add the new reservation as shown above.

4. Finally, restart the GRANTA MI service.

Please refer to the documentation for your version of Microsoft Windows for more detailed information on configuring SSL.

To get an SSL certificate's thumbprint

1. Open IIS Manager on your server.
2. Navigate to the 'Default Web Site' node.
3. Right-click and select **Edit Bindings**.
4. Select your https entry in the list of Site Bindings and click **Edit**.
5. Select the correct certificate in the **SSL Certificate** list, click **View**, click on the **Details** tab and scroll down to the Thumbprint
6. Highlight the thumbprint value and press CTRL to copy the text. For example:



7. Copy the thumbprint of the certificate into a text editor, such as Notepad, and remove all spaces between the hexadecimal characters. One way to accomplish this is to use the text editor's find-and-replace feature and replace each space with a null character.

3.7 Kerberos SSP configuration

In Windows environments, the default SSP (security support provider) for the User Manager application is NTLM.

Kerberos can be used in preference to NTLM by setting the authentication mode specified in the application configuration file Modules.config to Negotiate. Negotiate selects Kerberos unless it cannot be used.

> **Note:** Kerberos can only be used for User Manager application authentication if the GRANTA MI service is running as LocalSystem, and not as a named service.

Configuration steps:

1. In a text editor, open Modules.config:

   C:\Program Files\Granta\GRANTA MI\Server\bin\MIModules\Modules.config

2. Set the `UMS.AuthMode` property to `Negotiate`. For example:

```
<add key="UMS.AuthMode" value="Negotiate" encrypted="false" />
```

3. Save the file and then restart the GRANTA MI service.

3.8 Application configuration settings—Modules.config

User Manager application configuration settings are stored in Modules.config file, and include options for specifying:

- The security support provider (SSP) for the User Manager application.
- Use of SSL security; see also Section 3.5
- The port number used by the User Manager application.
- The User Manager application URL used in new account and password reset emails.
- The username and password for the default Admin user, and their Windows username, if using Windows Authentication.
- The password complexity requirements enforced when importing new users into User Manager.
- Use of domain validation when importing Windows users.

The Modules.config configuration file is located in the bin\MIModules subfolder in your MI:Server installation folder. Typically, this will be located here:

C:\Program Files\Granta\GRANTA MI\Server\bin\MIModules\Modules.config

Configuration settings for User Manager are specified using the following format, where <key> and <value> are detailed below.

```
<params>
    <add key="UMS.<key>" value="<value>" />
</params>
```

Note that if you make any changes to these configuration settings, you will need to restart the GRANTA MI service for them to take effect.

Table 1 User Manager Configuration options

Key	Description
UMS.AuthMode	Specifies the SSP for the User Manager application. One of: • **Ntlm** (this is the default mode) • **Negotiate** (use Kerberos in preference to NTLM if possible; otherwise fall back to NTLM). See Section *3.7, Kerberos*. • **Basic** (User Manager as SSP) Example: `<add key="UMS.AuthMode" value="Ntlm" />`
UMS.DefaultStandaloneUser	(User Manager user authentication) Specifies the username of the default Admin user in User Manager. Example: `<add key="UMS.DefaultStandaloneUser " value="miadmin" />`

Key	Description

UMS.DefaultStandalonePassword	(User Manager user authentication) Specifies the password of the default Admin user in User Manager. The password specified during installation is stored in encrypted form, but it is possible to modify/store in in plain text.
	Example (encrypted):
	`<add key="UMS.DefaultStandalonePassword" encrypted="true" value="ASOGNEG23rt203hqwnfakwf///" />`
	Example (unencrypted):
	`<add key="UMS.DefaultStandalonePassword" encrypted="false" value="P455w07d!" />`

UMS.DefaultWindowsUser	(Windows user authentication) Specifies the user (domain\username) who will be the default Admin user in User Manager. Example: `<add key="UMS.DefaultWindowsUser "value="acme\kim.lee" />`
UMS.ExternalURL	(User Manager user authentication) Specifies the URL of User Manager used in new account and password reset emails. Example: `<add key="UMS.ExternalURL" value="http://mi_um/>`
UMS.PasswordRequiredLength UMS.PasswordRequireNonLetterOrDigit UMS.PasswordRequireDigit UMS.PasswordRequireLowercase UMS.PasswordRequireUppercase	(User Manager user authentication) Password complexity requirements used when importing new users into User Manager. The default new password requirements are: • Must include at least 6 characters • Must contain at least 1 of each of the following characters: uppercase alphabetic, lowercase alphabetic, numeric • Must include at least one special character (not alphabetic and not numeric), for example, @, #, $, %, *, +, =. To change these defaults, edit the relevant settings, for example: `<add key="UMS.PasswordRequiredLength" value="8" encrypted="false" /> <add key="UMS.PasswordRequireNonLetterOrDigit" value="false" encrypted="false" /> <add key="UMS.PasswordRequireDigit" value="false" encrypted="false" />`

Key	Description
UMS.SelfHostSSL	Specifies whether to use SSL security for User Manager. Default is *false*. If set to *true*, https must be used to connect to the User Manager website; see Section *3.5*.
UMS.SelfHostPort	Specifies the port to host User Manager (default is port 9000). Example: `<add key="UMS.SelfHostPort" value="9000" />`
UMS.ValidateDomainMembership	(Windows user authentication) Enables/disables domain validation when adding/importing Windows users to the system. By default, domain membership validation is performed when adding Windows users. To allow users who are not in a domain to be added, set this configuration option to "False", for example: `<add key="UMS.ValidateDomainMembership" value="false" />`

3.9 Additional configuration for User Manager Authentication

To use User Manager instead of Windows for user authentication (that is, the **User Manager authentication / User Manager authorization** System Security Mode option in the MI:Server Connection tool), some additional configuration is needed to modify the default user authentication settings in the Service Layer, and in the MI:Viewer and Remote Import web applications. No additional configuration is required for MI:Explore.

3.9.1 Service Layer configuration for User Manager authentication

1. Open the MI:Service Layer Configuration tool.
2. On the **Options** menu, click **Authentication Settings** and then:
   a. Select **User Manager Authenticator** from the list of authenticators.
   b. Under Parameters, select the **ServiceUrl** parameter and click **Edit**, then enter your User Manager URL with **/api** appended to it; for example: **http://localhost:9000/api**
   c. Click **OK** to save the changes and return to the main page.
3. Click **Configure Connection** and then enter the credentials of the account that will be used to connect the Service Layer to MI:Server. This must be an account with an Admin role in User Manager. Leave the **Domain** field empty.
4. Click the dialog [X] **Close** button and confirm you want to save these changes.
5. In IIS Manager, ensure that the Authentication settings for the Service Layer are set as follows:
   - Anonymous Authentication **Enabled**
   - ASP.NET Impersonation **Disabled**
   - Basic Authentication **Disabled**

- Forms Authentication **Disabled**
- Windows Authentication **Disabled**

3.9.2 MI:Viewer configuration for User Manager Authentication

1. Open the MI:Viewer Configuration tool.
2. On the Options menu, click **Authentication Settings** and then:
   a. Select **UserManagerAuthenticator** from the list of authenticators.
   b. Under Parameters, select the **ServiceUrl** parameter and click **Edit**, then enter your User Manager URL with **/api** appended to it; for example: http://localhost:9000/api
   c. Click **OK** to save the changes and return to the main page.
3. Click **Configure Connection** and then enter the credentials for the account that will be used to connect MI:Viewer to MI:Server. This must be a user who has an Admin role in User Manager. Leave the Domain field empty.
4. Click the dialog [X] **Close** button and confirm you want to save these changes.

   The MI:Viewer application web.config file, typically located in C:\inetpub\wwwroot\mi\web.config, will be updated with the relevant membership and role provider configuration settings.
5. In IIS Manager, ensure that the Authentication settings for MI:Viewer are set as follows:
   - Anonymous Authentication **Enabled**
   - ASP.NET Impersonation **Disabled**
   - Basic Authentication **Disabled**
   - Forms Authentication **Enabled**
   - Windows Authentication **Disabled**

3.9.3 Remote Import configuration for User Manager authentication

To configure Remote Import for User Manager authentication, you will need to modify some configuration files, and also make a change to the IIS Authentication settings for the Remote Import web application in IIS Manager, as described, step-by-step, below.

1. Open the Services Microsoft Management Console (MMC) snap-in and stop the **GRANTA MI Remote Import** service.
2. In IIS Manager, ensure that the Authentication settings for the Remote Import web application are set as follows:
   - Anonymous Authentication **Enabled**
   - ASP.NET Impersonation **Enabled**
   - Basic Authentication **Disabled**
   - Forms Authentication **Enabled**
   - Windows Authentication **Disabled**
3. Edit the Remote Import web application configuration file Web.config file (typically located in C:\inetpub\wwwroot\remoteimport) and make the following changes:
   a. In the `<system.web>` element, add `<roleManager>` and `<membership>` elements as shown, inserting your User Manager URL where **indicated**. (Note that the authenticator

name as specified in the default provider and service name attributes, `"User Manager Authenticator"`, must include spaces as shown.)

```
<system.web>
...
  <roleManager enabled="true" defaultProvider="User Manager Authenticator">
    <providers>
      <clear />
      <add ServiceUrl="YourUserManagerURL/api" name="User Manager Authenticator"
         type="Granta.UserManagerAuthenticator.UserManagerRoleProvider,
         Granta.UserManagerAuthenticator" />
    </providers>
  </roleManager>

  <membership defaultProvider="User Manager Authenticator">
    <providers>
      <clear />
      <add ServiceUrl="YourUserManagerURL/api" name="User Manager Authenticator"
        type="Granta.UserManagerAuthenticator.UserManagerMembershipProvider,
        Granta.UserManagerAuthenticator"/>
    </providers>
  </membership>
...
</system.web>
```

b. Save the changes to Web.config and close the file.

4. Edit the Remote Import service config file RemoteImportService.exe.config (in C:\Program Files\Granta\RemoteImportServer) and make the following change:

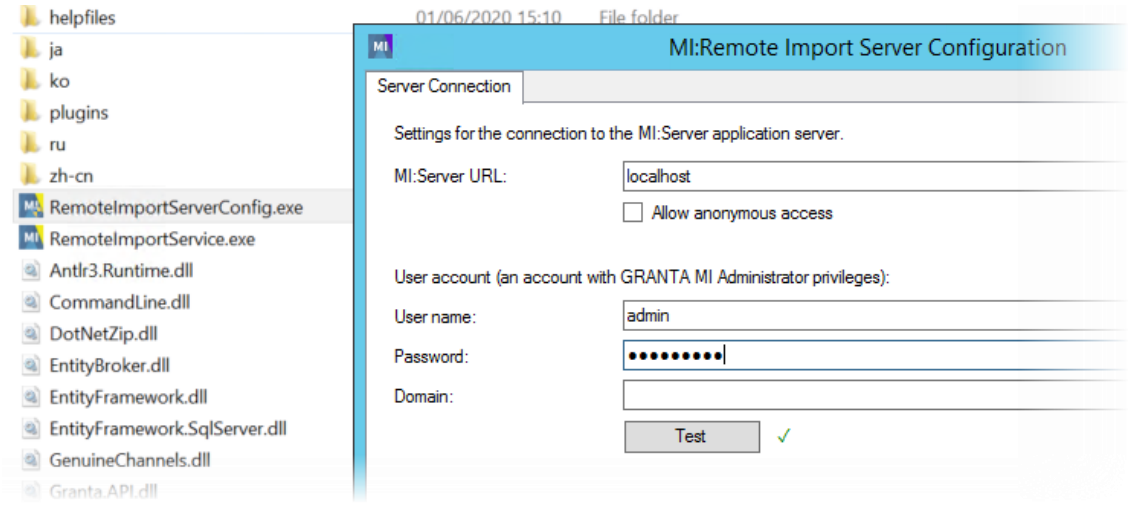
   a. Under `<appSettings>`, locate the `authenticationType` key and change its value to **Custom**. For example:

```
<appSettings>
    <add key="portNumber" value="8780"/>
    <add key="rootDir" value="C:\RemoteImport\" />
    <add key="jobExpiresAfterDays" value="30" />
    <add key="pluginsDir" value="plugins" />
    <add key="authenticationType" value="Custom" />
</appSettings>
```

   b. Save this change and close the file.

5. Specify the User Manager account that will be used by the Remote Import server to connect to the MI:Server using the MI:Remote Import Server Configuration tool located in the

RemoteImportServer folder. If setting up User Manager for the first time, enter the default administrator credentials: username = **admin** and password = **P455w07d!**, for example:



Once User Manager is up and running, you change this to any user with Admin privileges in User Manager.

6. In the Services Microsoft Management Console (MMC) snap-in, restart the **GRANTA MI Remote Import** service.

3.10 Restoring the default User Manager Admin account

If you get into a situation where there are no Admin users in User Manager (for example, the last Admin user has been inadvertently deleted), the default User Manager administrator account (username = **admin** and password = **P455w07d!**) can be recreated by simply restarting the GRANTA MI service, allowing you to get back into the system with Administrator access again.

4 Custom authentication for GRANTA MI

Custom authenticators and role providers developed using the MI:Server API may be used to perform user authentication instead of Windows or User Manager, for example, where authorization data already exists in a database for a company or Web site. Custom authentication can be configured in *Mixed Mode* or *Custom* mode:

- **Mixed Mode**: using Windows authentication with a custom role provider
- **Custom Mode**: using a custom authenticator and a custom role provider

We recommend that you contact Granta Support (support@grantadesign.com) for advice before attempting to implement custom authentication.

4.1 Custom authentication for MI:Server

To configure MI:Server to use a custom authenticator or role provider:

1. Copy the DLLs for the custom authenticator/role provider into the MI:Server bin folder.
2. Open the MI:Server Connection tool and click on the System Security Settings tab.
3. Select your custom authenticator from the System Security Mode dropdown list. All authenticator and role provider DLLs found in the bin folder will be listed; if you can't see the authenticator, close the MI:Server Connection tool and restart the GRANTA MI service.
4. Click **Configure Parameters** and set any required parameter values.
5. Click **OK**, then click **Save changes & restart service**.

After the service restart, MI:Server will use the specified authenticator to handle all client requests.

Security configuration settings for custom authentication are stored in the `<Security>` element in the MIServer.exe.config configuration file, located in the MI:Server installation folder:

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

The relevant security properties in this file are:

Property	Description
`authentication`	The authentication mode: **Mixed** or **Custom**
`authenticator`	The custom authenticator to use
`mixedModeRoleProvider`	The role provider to use for Mixed Mode authentication, specified in the format: `mixedModeRoleProvider="FullyQualifiedTypeName, AssemblyName"`
`encryptParameters`	Store parameter values in encrypted format (**True**/**False**)

For example, the configuration settings for mixed mode custom authentication would look like this:

```
<Security authentication="Mixed"
mixedModeRoleProvider="AcmeCo.Auth.MyMixedModeRoleProvider, AcmeCo.Auth"/>
```

4.2 Custom authentication for MI:Viewer

A custom authenticator can be used to authenticate users connecting to MI:Viewer, with users logging in to MI:Viewer using a web form. This is a completely separate procedure to logging in to the server. Whenever the user makes a request through Viewer, their credentials are passed to the server along with the request, so that the server can determine which actions they can perform.

To use a custom authenticator with MI:Viewer, place the custom authenticator DLL files into the bin folder of the MI:Viewer application folder, typically C:\inetpub\wwwroot\mi\bin, and then use the MI:Viewer Configuration tool to select the authentication method as described in Section *3.9.2, MI:Viewer configuration for User Manager Authentication*.

Membership and role provider configuration settings for MI:Viewer are stored in the application web.config file, typically located here:

C:\inetpub\wwwroot\mi\web.config

4.3 Custom authentication for MI:Remote Import

To configure Remote Import for a custom authenticator developed using the MI:Server API, you will need to edit these 2 configuration 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\RemoteImportServer\RemoteImportService.exe.config

Change the Membership and Role Provider information in Web.config

1. In a text editor, open the file C:\inetpub\wwwroot\remoteimport\Web.config
2. Add your custom authenticator as the provider in both the <roleManager> and <membership> elements, for example:

```
<roleManager defaultProvider="MyAuthenticator">
  <providers>
    <clear />
  <add TextFilePath="\App_Data\config\users.txt" name="MyAuthenticator"
type="MyCompany.MyAuthenticator.MyAuthenticatorRoleProvider" />
  </providers>
</roleManager>

<membership defaultProvider="MyAuthenticator">
  <providers>
    <clear />
  <add TextFilePath="\App_Data\config\users.txt" name="MyAuthenticator"
type="MyCompany.MyAuthenticator.MyAuthenticatorMembershipProvider" />
  </providers>
</membership>
```

Change the authentication type in RemoteImportService.exe.config

1. In a text editor, open the Remote Import Service configuration file C:\Program Files\Granta\RemoteImportServer\RemoteImportService.exe.config
2. Locate the authenticationType key under <appSettings> and change its value to Custom; for example:

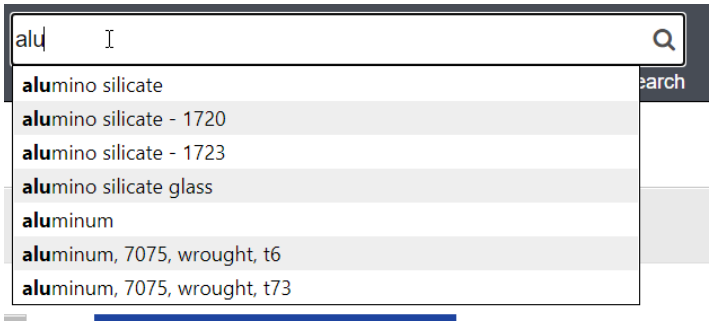
```
    <appSettings>
        <add key="portNumber" value="8780"/>
        <add key="rootDir" value="C:\RemoteImport\" />
        <add key="jobExpiresAfterDays" value="30" />
        <add key="pluginsDir" value="plugins" />
        <add key="authenticationType" value="Custom" />
    </appSettings>
```

5 Search and indexing configuration

Search capability in GRANTA MI is provided by Elasticsearch. Embedded data stored in File Attributes are *indexed*—stored and made searchable—when a database is loaded into GRANTA MI and when that data is modified. You can configure a number of different GRANTA MI search settings.

5.1 Enabling Search Suggestions in MI:Viewer

Elasticsearch supports *Search Suggestions* (autocomplete) functionality in MI:Viewer, where users see suggestions while they type, for example:



This functionality relies on SSL certificates to securely transfer data between the MI:Server Search Service and the MI:Viewer application. When users type search queries, the Search Service checks the MI:Viewer client certificate to verify its identity before serving any search suggestions.

To enable the Search Suggestions feature in MI:Viewer, you need to set up certificates, one for the MI:Server application and one for the MI:Viewer client application. See Section 2. Certificate setup for GRANTA MI applications, for details.

On Windows Server 2012 OS only

On Windows Server 2012 R2 only, if search suggestions are not available after carrying out the certificate configuration, check that the additional configuration detailed in Step 2 on page 7 has been carried out on the machine running MI:Viewer.

5.2 Setting up 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, to allow for variations in British English/American English.

For example, where **mold** and **mould** are defined as synonyms:

- a search for **mold** returns records containing **mold** or **mould**
- a search for **mould** returns records containing **mold** or **mould**

Stemming applies on top of synonyms, and so a search for **mould** also returns records containing **moldable** or **molding**

Search synonyms are defined in the SearchSynonyms.txt file and apply to all your Granta databases. SearchSynonyms.txt is located in the MI:Server application config folder, for example:

C:\Program Files\Granta\GRANTA MI\Server\config\SearchSynonyms.txt

You specify search synonyms as a list of comma-separated keywords or phrases, for example:

```
aluminum,aluminium
carburetor,carburettor,carburator
PBT,Polybutylene Terephthalate
```

Synonyms should consist of alphanumeric characters only; any non-alphanumeric characters (e.g. period, ampersand, parenthesis) will be treated as spaces.

After making changes to SearchSynonyms.txt, you will need to reload each database in MI:Server Manager to force the database search index to be rebuilt.

5.3 Controlling which file types are indexed

By default, Elasticsearch will attempt to index all common document types stored as embedded media in GRANTA MI. You can prevent Elasticsearch from indexing documents with specific file name extensions by setting the following attribute on the `<Search>` element in the MI:Server application configuration file, MIServer.exe.config:

fileTypesToExcludeFromIndexing

Specify the file name extensions as a space-separated list, including the period.

For example:

```
<Search
    fileTypesToExcludeFromIndexing=".test, .old"
    textIndexLocation="http://localhost:9200/"
    ...
```

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.

5.4 Setting record and file size limits for indexing

By default, Elasticsearch will attempt to index all records up to 150MB in size, and embedded media documents up to 100MB. Any records or documents larger than this will not be indexed. If required, you can adjust these limits by setting the following attributes on the `<Search>` element in the MI:Server application configuration file, MIServer.exe.config:

indexingMaxRecordSizeBytes

Records that are larger than this will not be indexed. The value must be specified in Bytes; the default limit is 150MB (150000000 Bytes).

indexingMaxFileSize

Embedded media documents larger than this will not be indexed, but all other text in the record **will** be indexed. The value must be specified in Bytes; the default limit is 100MB (100000000 Bytes).

For example:

```
<Search
    indexingMaxRecordSizeBytes="110000000"
    indexingMaxFileSizeBytes="90000000"
    textIndexLocation="http://localhost:9200/"
    ...
```

Note that these configuration limits are set to ensure Elasticsearch does not run out of memory when indexing; if you increase them, and Elasticsearch runs out of memory, indexing will fail.

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.

5.5 Optimizing index creation performance

Databases are loaded/reloaded into GRANTA MI automatically, and the search indexes rebuilt if necessary, whenever the GRANTA MI service is started or restarted. Loading or reloading databases manually in MI:Server Manager also causes the search indexes to be rebuilt.

To optimize loading of multiple databases, GRANTA MI will load up to 3 databases concurrently, and these will be indexed concurrently. If building/rebuilding multiple search indexes at the same time causes performance issues on your search server, you can modify the `ConcurrentDatabaseLoadThreshold` app setting in MIServer.exe.config to reduce the number of databases that are loaded concurrently, and consequently reduce the number of search indexes that are built concurrently.

```
<appSettings>
...
<add key="ConcurrentDatabaseLoadThreshold" value="3"/>
...
```

Note that setting this to just 1 should make the search server more stable, but will mean database loading takes longer.

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.

5.6 Using HTTPS communication for Elasticsearch

To enable encryption of communications in Elasticsearch for GRANTA MI, you need to perform the following steps:

1. Generate a certificate authority (CA) and a named X.509 certificate.
2. Update elasticsearch.yml to point at the certificate. For example:

```
xpack.security.enabled: true
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.keystore.path:
C:\ProgramData\Elastic\Elasticsearch\config\certs\localhost.p12
xpack.security.transport.ssl.truststore.path:
C:\ProgramData\Elastic\Elasticsearch\config\certs\localhost.p12
xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.keystore.path:
C:\ProgramData\Elastic\Elasticsearch\config\certs\localhost.p12
xpack.security.http.ssl.truststore.path:
C:\ProgramData\Elastic\Elasticsearch\config\certs\localhost.p12
```

3. Restart the Elasticsearch for GRANTA MI service.
4. Add the CA generated in Step 1 to your trusted CAs (through Microsoft Management Console).
5. Edit MIServer.exe.config to replace “http” with “https” in the `textIndexLocation` attribute of the `Search` element. For example:

```
<Search textIndexLocation="https://localhost:9200/"
    ...
```

5.7 Changing the location of the full text index

The location of the full text index data written by Elasticsearch for GRANTA MI is specified during installation. The default location is on the GRANTA MI application server here:

$PROGRAMDATA\Granta\GRANTA MI\Elasticsearch\data

To use a different location, edit the `path.data` setting in the elasticsearch.yml configuration file:

```
---------------------------------- Paths ----------------------------------
#
Path to directory where to store the data (separate multiple locations by comma):
#
path.data: $ {PROGRAMDATA}\Granta\GRANTA MI\Elasticsearch\data
```

The elasticsearch.yml configuration file is located in the GRANTA MI Program data folder as follows:

$PROGRAMDATA\Granta\GRANTA MI\Elasticsearch\config

5.8 Changing the port used by Elasticsearch

By default, port 9200 is used for the Elasticsearch service. To change this, you will need to modify the Elasticsearch and MI:Server application configuration files as follows:

1. Open the elasticsearch.yml configuration file located in the GRANTA MI Program data folder ($PROGRAMDATA\Granta\GRANTA MI\Elasticsearch\config).
2. Find the `http.port` setting.
3. Uncomment the line and specify the port you want to use instead. For example:

```
# ---------------------------- Network -----------------------------
#
# Set a custom port for HTTP:
#
http.port: 9800
```

4. Save your changes to elasticsearch.yml.
5. Open the MIServer.exe.config file, located in the MI:Server application *bin* folder (C:\Program Files\Granta\GRANTA MI\Server\bin).
6. Find the `Search` element and replace the port number specified in the `textIndexLocation` attribute with the new one. For example:

```
<Search textIndexLocation="https://localhost:9800/"
    ...
```

7. Save the file, and then restart the *Elasticsearch for GRANTA MI* and *GRANTA MI* services.

5.9 Using Elasticsearch for GRANTA MI with drive encryption technologies

Hard drive encryption is a basic security measure in many enterprises, and Elasticsearch for GRANTA MI can be used with disk encryption technologies such as Microsoft BitLocker. To enable BitLocker, refer to Microsoft's instructions, for example:

- https://support.microsoft.com/en-us/help/4028713/windows-10-turn-on-device-encryption
- https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-how-to-deploy-on-windows-server

6 Service Layer IIS configuration

The Service Layer provides an interface between MI:Server and end-user applications including MI:Viewer, MI:Materials Gateway, One MI, MI:BoM Analyzer, One MI, supporting programmatic access to materials data stored in GRANTA MI.

The following IIS configuration options are set automatically when the Service Layer is installed.

6.1 WCF HTTP Activation

The MI Service Layer requires the 'WCF HTTP Activation' feature to be installed/enabled in IIS.

You can check that WCF HTTP Activation is enabled in IIS using the Windows Server Manager tool.

The non-HTTP Activation features of IIS are enabled in addition to the HTTP Activation features, making it easier to enable Net.TCP communication with the Service Layer.

6.2 Application Initialization

To improve the responsiveness of the Service Layer, especially for first requests, the Keep Alive feature is enabled by default. This feature depends on IIS Application Initialization:

- In IIS 7.5, Application Initialization is available as a separately-installable Microsoft module.
- In IIS 8.0, Application Initialization is built-in, but the feature still needs to be installed; this is done automatically during Service Layer installation.

The GRANTA MI Installation Manager will enable IIS Application Initialization, if it is available, before running the MI:Viewer or Service Layer installers, and the Service Layer installer will automatically enable Keep Alive. Keep Alive can also be enabled and disabled from the MI:Service Layer Configuration tool.

For older versions of IIS, Application Initialization is not supported, and so if you are using an older version, the **Keep Alive** option in the MI:Service Layer Configuration tool will be unavailable (greyed out).

6.3 Dynamic content compression

When hosted in IIS, the Service Layer can benefit from IIS dynamic content compression of its responses. This reduces the network traffic, at the expense of a moderate increase in CPU usage.

'Dynamic content compression' is an optional module of IIS that will be automatically installed as part of the Service Layer installation, if it is not already present on the IIS server, and dynamic content compression will be enabled on the Default Web Site. To turn on dynamic content compression manually, use IIS Manager as described here (external link):

- Enable HTTP Compression of Dynamic Content (IIS 7)