GRANTA MI™ version 11

GRANTA MI
Configuration Guide

GRANTA
MATERIAL INTELLIGENCE

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

www.grantadesign.com

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

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

Document version: MI11/01
Published: December 2017

Contents

1 Who should read this document?

This document describes how to change various GRANTA MI system configuration settings. It is aimed at administrators who are responsible for configuring and maintaining GRANTA MI.

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 —Changing the ports used by the Remote Import application
- Section 3—Configuring GRANTA MI applications for User Manager authentication
- Section 4—Configuration for use of a custom authenticator with MI:Server
- Section 5—Recommended IIS settings for the Granta Service Layer

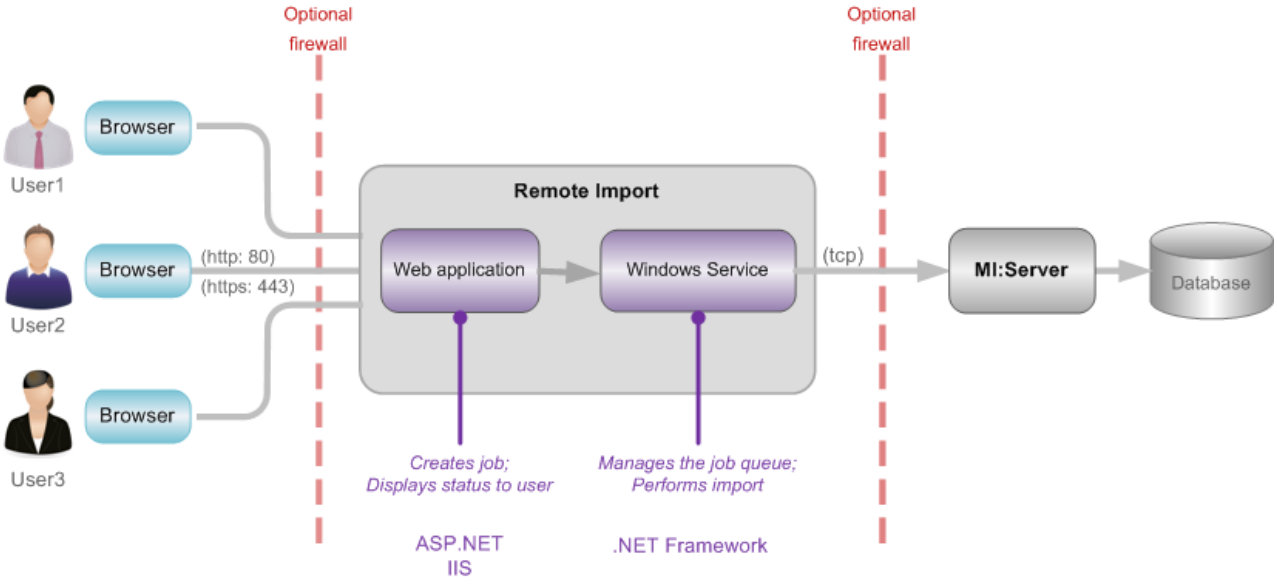
We welcome your feedback on Granta help and documentation; please email your comments to: mailto:docs@grantadesign.com

2 Remote Import application configuration

The Remote Import application provides a simple web browser interface through which any authorized user can upload data stored in Excel or text files using importer 'templates' set up by the GRANTA MI database administrator.

Remote Import consists of two components, both of which must be installed on the same server:

- The **Web Application** submits jobs to the Service and displays the status of jobs to the users.
- The **Windows Service** manages the queue of jobs and submits the data to MI:Server.



Remote Import is included in the GRANTA MI installation package and is installed using the Installation Manager, as described in the *GRANTA MI Installation Guide*.

In the following configurations, the Application Name of the Web Application has been set to the default of 'remoteimport' (set on the **IIS Configuration** page of the Remote Import Setup wizard).

2.1 Ports used by Remote Import

There are two ports used by Remote Import, which are set during product installation:

- The default port used to connect Remote Import to MI:Server is port 8738.
- The default port used to connect the Remote Import Service with the Remote Import web application is port 8780. If you need to change this port number, you will need to make the change in two separate configuration files.

Edit the Remote Import application file

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

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

Edit the Remote Import service configuration file

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

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

2.2 Configuration for custom authentication

To configure the Remote Import web application for custom authentication, you will need to modify two separate configuration files.

Edit the application configuration file 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>
```

Edit the service configuration file RemoteImportService.exe.config

1. In a text editor, open the 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>
```

3 User Manager configuration

User Manager, Granta's user management application, may be used for user authorization and/or authentication in GRANTA MI.

3.1 GRANTA MI System Security Modes

The default mode for GRANTA MI is Windows Authentication / Windows authorization. You can switch to a different mode and use User Manager for authorization and/or authentication in the MI:Server Connection Tool (**Options > System Security Settings**).

Windows Authentication / Windows authorization

By default, GRANTA MI is configured to use Windows® Active Directory for both user authentication and authorization.

Windows Authentication / User Manager authorization

In this mode, users authenticate to GRANTA MI tools (MI:Viewer, MI:Toolbox etc.) using their normal Windows Active Directory (AD) credentials, while their user privileges within GRANTA MI are managed through User Manager.

Granta administrators can add pre-existing Windows users to the GRANTA MI system in User Manager, and assign them to different roles.

User Manager Authentication / User Manager authorization

Access to GRANTA MI and user privileges within GRANTA MI 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 granted to groups of users via a *rule engine* which specifies who can read, write, and change resources. Users log into GRANTA MI tools and applications using their GRANTA MI usernames and passwords.

3.2 Prerequisites and requirements

- For Windows user authentication (with either Windows authorization or User Manager authorization), 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 local system).
- If you are running the GRANTA MI service using a domain Service Account and not the LocalSystem account, you will need to use the **netsh** command to reserve the User Manager URL for non-administrator users and accounts (`add urlacl` to port 9000). For example:

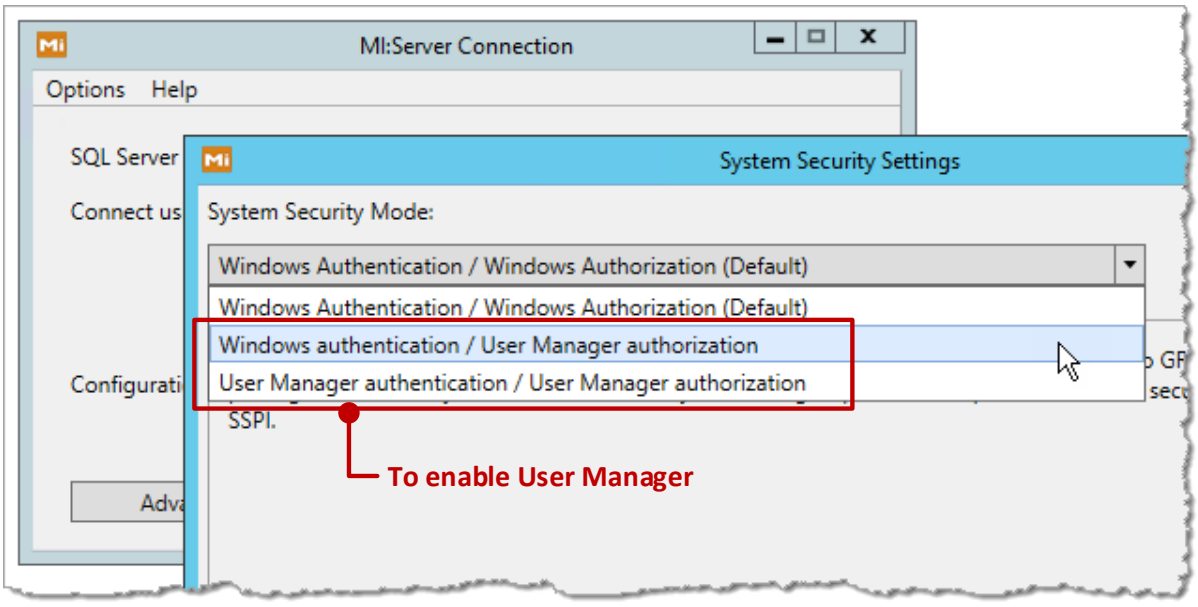
```
netsh http add urlacl url=http://+:9000/ user=ACMECORP\mi_service_user
```

- If User Manager will be used for user authentication:
  a. The authentication settings for the MI:Viewer, MI Service Layer, and Remote Import applications must be configured individually, as described in Section *3.5*.
  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 inadvertantly locked out of the system if an Administrator performs a password reset (the password will be changed, but the user will not be receive an email notification with their new password).
- If the User Manager application will be running over SSL or HTTPS, some additional configuration is required; see Section *3.6*.

3.3 Enabling User Manager

The System Security Mode for GRANTA MI is specified in the MI:Server Connection Tool.

The default mode is Windows Authentication / Windows authorization. To enable use of User Manager, you need to select the required option in the System Security Settings dialog (**Options > System Security Settings**):



Note: If User Manager will be used instead of Windows to authentication GRANTA MI users (i.e. **User Manager authentication / User Manager authorization** mode), additional configuration is needed to modify the default authentication settings in MI:Viewer, the Service Layer, and Remote Import; see Section *3.5*. (This additional configuration is not necessary if Windows authentication is used.)

3.4 Opening the User Manager application

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://my_mi_server_host:9000

3.5 Additional configuration for User Manager Authentication

If **User Manager authentication / User Manager authorization** is selected as the System Security Mode, some additional configuration is needed to modify the default user authentication settings in MI:Viewer, the Service Layer, and Remote Import.

(Note that this additional configuration is not required if **Windows Authentication / User Manager authorization** mode is selected as the System Security Mode.)

3.5.1 MI:Viewer configuration for User Manager Authentication

To configure the M:Viewer application for User Manager authentication:

1. Open the MI:Viewer Configuration tool.
2. To select the User Manager authenticator:
   a. On the **Options** menu, click **Authentication Settings**.
   b. Select **UserManagerAuthenticator** from the list of authenticators.
   c. 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
   d. 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.

In IIS Manager, ensure that the Authentication settings for MI:Viewer are set as follows:

Enabled:	Anonymous Authentication, Forms Authentication
Disabled:	ASP.NET Impersonation, Basic Authentication, Windows Authentication

3.5.2 Service Layer configuration for User Manager authentication

To configure the Service Layer for User Manager authentication:

1. Open the MI:Service Layer Configuration tool.
2. Select the User Manager authenticator:
   a. On the **Options** menu, click **Authentication Settings**.
   b. Select **User Manager Authenticator** from the list of authenticators.
   c. 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**
   d. Click **OK** to save the changes and return to the main page.

3. Click **Configure Connection** and then and then enter the credentials for 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.

In IIS Manager, ensure that the Authentication settings for the Service Layer are set as follows:

Enabled:	Anonymous Authentication
Disabled:	ASP.NET Impersonation, Basic Authentication, Forms Authentication, Windows Authentication

3.5.3 MI:Remote Import configuration for User Manager authentication

To configure the Remote Import web application for User Manager authentication, you will need to modify a number of XML configuration files, and also make a change to the IIS Authentication settings for the MI: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 Design - Remote Import** service.
2. Edit the Remote Import 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. In the `<authentication>` element, set the mode to `Forms` and add the authentication `loginURL` attribute as shown:

```
<authentication mode="Forms" >
```

```
   <forms loginUrl="~/LogOn/Main" defaultUrl="~"
name=".GrantaRemoteImportFormsAuth"/>
</authentication>
```

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

3. Edit the Remote Import server config file RemoteImportService.exe.config (typically located 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.

4. Edit the MI:Server connection details specified in the GRANTA MI connection.xml configuration file (typically located in C:\ProgramData\Granta\GRANTA MI\connection.xml) to make the following changes:

   a. Edit `<Username>` and `<Password>` to specify the credentials for a User Manager Admin account. If setting up User Manager for the first time, enter the default administrator credentials: username = **admin** and password = **P455w07d!** Once User Manager is up and running, you can edit this file again to change this to any user with Admin privileges in User Manager.

```
 <ConnectionDetails useWindowsAuthentication="false">
     <Url>your_mi_hostname</Url>
     <User allowAnonymousAccess="false">
         <Username>your_admin_name</Username>
         <Password>your_admin_password</Password>
         <Domain></Domain>
     </User>
```

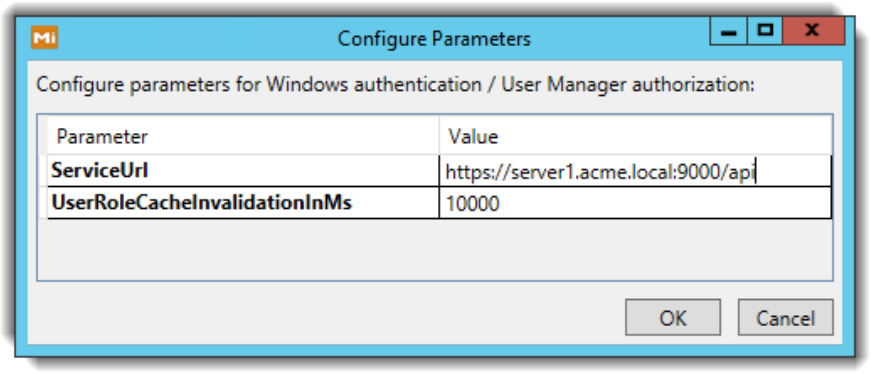
5. In IIS Manager, ensure that the Authentication settings for the MI:Remote Import web application are set as follows:
   - Anonymous Authentication **Enabled**
   - ASP.NET Impersonation **Enabled**
   - Basic Authentication **Disabled**
   - Forms Authentication **Enabled**
   - Windows Authentication **Enabled**

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

3.6 SSL (https) configuration for User Manager

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

1. In the Server Connection tool, specify the address at which User Manager can be found:



   The scheme must be modified to have **https**, and 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. Modify the User Manager Modules.config file to set the configuration key `UMS.SelfHostSSL` to 'True'. (See Section 3.8 to see where you can find this file.)

3. Bind the SSL certificate to the port number using the netsh.exe tool, as shown in the following example:

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

   - 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 *3.6.1* 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 (for example, for MI:Viewer) then you can run **net http show sslcert** and then just copy and paste the certhash and appid from the posting for the IIS binding.

   If you are running MI Server under a domain service account (the default option for installation) then you need to do the following additional steps:

4. From an Administrator command prompt, give permission to the service account to access port 9000:

```
> netsh https add urlacl=https://+:9000 user=<domain service account>
```

   Ensure that you specify **https** here.

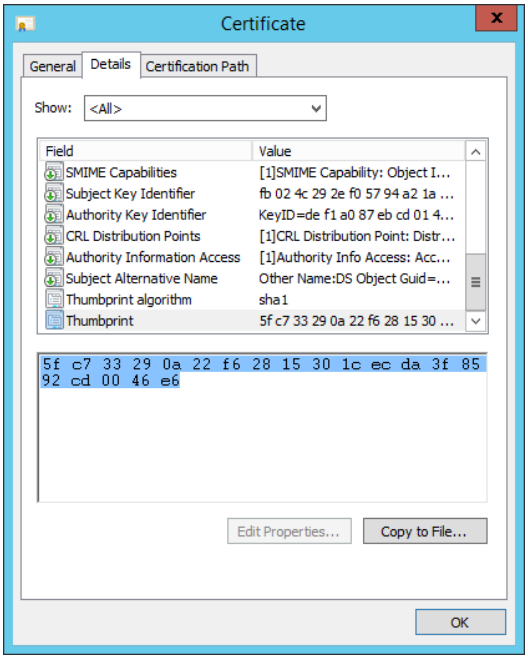
5. Edit the Modules.config file again to ensure `UMS.AuthMode` is explicitly set to *Ntlm* rather than the default of *Negotiate*.

6. Finally, restart the GRANTA MI service.

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

3.6.1 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+C to copy the text.



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 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.

3.8 User Manager application configuration file

The GRANTA MI Modules.config file includes several User Manager application configuration settings which can be modified, if required, including:

- The authentication mode for the User Manager application, one of: **Basic** (User Manager authentication), **Ntlm** (Windows authentication), or **Negotiate** (Kerberos authentication).
- The User Manager application URL used in new account and password reset emails.
- Use of SSL security; see also Section *3.6*
- 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 port number used by the User Manager application.

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 MI:Server for them to take effect.

Table 1 User Manager Configuration options

Key	Description
UMS.AuthMode	Specifies whether to use the User Manager's own authentication or to use Windows authentication. Possible values are **Basic** (User Manager; the default), **Ntlm** (for Windows Authentication) **Negotiate** (use Kerberos authentication in preference to Ntlm if that mode of authentication is available in the Windows domain). Example: `<add key="UMS.AuthMode" value="Basic" />`
UMS.DefaultStandaloneUser	When using User Manager for both authentication and authorization, this specifies the username of the default Admin user in User Manager. Example: `<add key="UMS.DefaultStandaloneUser " value="miadmin" />`

Key	Description

UMS.DefaultStandalonePassword	When using User Manager for both authentication and authorization, this 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	When using Windows authentication with User Manager authorization, this specifies the Windows username of the user who will be the default Admin user in User Manager. Example: `<add key="UMS.DefaultWindowsUser "value="mycorp\alex.jones" />`
UMS.ExternalURL	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
	These settings allow you to configure 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="4" encrypted="false" />`
	`<add key="UMS.PasswordRequireNonLetterOrDigit" value="false" encrypted="false" />`
	`<add key="UMS.PasswordRequireDigit" value="false" encrypted="false" />`

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 *3.6*.
UMS.SelfHostPort	Specifies the port to host User Manager (default is port 9000). Example: `<add key="UMS.SelfHostPort" value="9001" />`

Key	Description
UMS.ValidateDomainMembership	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 Windows users who are not in a domain to be added, set this configuration option to "False", for example: `<add key="UMS.ValidateDomainMembership" value="false" />`

4 Custom authentication for MI:Server

GRANTA MI can be configured to use custom (3rd party) authentication and/or custom authorization. These options are not offered in the Installation Manager but can be configured manually after initial software installation. Supported configuration options include:

- Windows authentication and custom authorization (sometimes referred to as "Mixed mode").
- Custom authentication and custom authorization. You should contact GRANTA Support (support@grantadesign.com) for advice on how to configure this.

4.1 Mixed Mode authentication

To configure mixed mode authentication with a custom authenticator, you need to edit the MI:Server configuration file *MIServer.exe.config* file located in the *bin* folder in the MI:Server installation folder to change the authentication mode to `Mixed` and to specify the role provider (authentication provider). For example:

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

4.2 Security Support Provider (SSP)

The default SSP for MI:Server and User Manager is Negotiate. SSP Negotiate will normally choose Kerberos, but will fall back to using NTLM if that is not possible.

5 Recommended IIS settings for the Service Layer

The Service Layer provides extra reporting capabilities for GRANTA MI, and supports programmatic access to materials data, for example, from MI:Viewer, MI:Materials Gateway, MI:Explore, MI:BoM Analyzer, and custom tools.

The Service Layer can be installed and uninstalled from the GRANTA MI Installation Manager; see the *GRANTA MI Installation Guide* for details. It can also be installed via an MSI installer.

When the Service Layer is installed using the GRANTA MI Installation Manager, the IIS configuration options described below are automatically set correctly; when installing via the MSI installer, you should use IIS Manager to check that these settings are configured correctly after completing the installation.

5.1 Application Pool 'Load User Profile' option

When using the Service Layer on a non-server operating system such as Windows 7, use IIS Manager to ensure that the **Load User Profile** option in the Advanced Settings of the Application Pool is set to False. This will help to prevent 503 (service unavailable) browser errors when using MI:Viewer or MI Service Layer.

(On Windows Server 2008 machines, Load User Profile is set to False by default, but on Windows 7 machines it may be set to *True* by default: in this case, you will need to change the setting to *False* using IIS Manager.)

5.2 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.

5.3 WCF Non-HTTP Activation

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.

5.4 Application Initialization

To improve the responsiveness of MI Service Layer, especially for first requests, the Keep Alive feature should be enabled for the Service Layer. The Keep Alive 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 when the Service Layer is installed via GRANTA MI Installation Manager.

  You should refer to your IIS Manager documentation for information on manually installing Application Initialization in IIS.

The GRANTA MI Installation Manager will enable IIS Application Initialization on Windows Server 2012 or later, before running the MI:Viewer or Service Layer installers. It does not do this on earlier versions of Windows, so you still have to install the IIS extension yourself on Windows Server 2008R2 or Windows 7.

The Service Layer installer will automatically enable keep alive if IIS Application Initialization is available. Keep Alive can also be enabled and disabled from the MI:Service Layer Configuration tool (**Options > Keep Alive**); see the Help for the MI:Service Layer Configuration tool for more information.

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

5.5 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. Although it typically will be installed, it is possible that it may not be installed on all systems, and we recommend that you should install it.

Once installed, dynamic content compression will typically be enabled on the Default Web Site. It should be turned on for both the Service Layer and MI:Viewer.

To turn on dynamic content compression, use IIS Manager as described here (external link):

- Enable HTTP Compression of Dynamic Content (IIS 7)

When installing the Service Layer via the Installation Manager, the IIS Dynamic Content Compression Windows Feature is automatically installed on machines where it is not already installed.