Mobile Inspection Software by Mi-Corporation

Installation Guide

Contents

Introduction
Prerequisites
Operating System
Database Server3
Reporting Server
Mi-Enterprise Apps or Mi-Forms Server3
Installation4
Bundled Prerequisites4
Installation Wizard4
Configuration7
Database Configuration7
Authentication Configuration12
Reporting Configuration13
Background Service Configuration17
Verification
Help & Troubleshooting22
Tutorial Videos22
Help Topics
Further Support24

Introduction

This guide covers the installation and preliminary configuration of the Mobile Inspection Software by Mi-Corporation (MISM). It is designed to provide a walkthrough of the installation process to the point where the system is accessible. Further configuration of specific features will require utilization of help documents provided throughout the installation. If at any point you need further assistance, please contact Mi-Corporation Technical Support at support@micorporation.com

Prerequisites

Operating System

MISM may be installed on the following operating systems:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Virtual machines are supported.

Database Server

MISM requires connection to a SQL Server database server. It is not required that this server resides on the same virtual or physical server as the MISM application software, but a connection between the two must be available.

Supported versions of SQL Server include:

- SQL Server 2008 R2
- SQL Server 2012
- SQL Server 2014

MISM has no specific dependency on SQL Server edition, but your usage of SQL and its performance may dictate specific requirements.

Reporting Server

In order to utilize the reporting capabilities inherent in MISM, an instance of SQL Server Reporting Services must be available. This instance must have access to the SQL Server instance where the MISM database resides.

Mi-Enterprise Apps or Mi-Forms Server

An instance of version 10.0 or later Mi-Enterprise Apps or Mi-Forms Server is required for the purposes of authentication in the MISM server. It is not required that this server resides on the same virtual or physical server as the MISM application software, but a connection between the two must be available.

Installation

MISM is distributed as a single file executable designed to install all components of the system. You should be provided with a file named something like:

Mobile Inspection Software by Mi-Corporation.exe

As an administrator, double click this file on the machine on which you intend to install the MISM application.

Bundled Prerequisites

It is possible that the software will detect missing prerequisite software. If so you will be presented with a screen similar to the one below:



Clicking the "Next" button will advance to the bundled prerequisite installation dialog as shown below:



Allow all of the necessary bundled prerequisites to install to completion.

Installation Wizard

After completing any necessary bundled prerequisite steps, you will be taken to the installation wizard. The first screen of this wizard is shown below:



After clicking "Next", you will be prompted to review the license agreement as shown below:



Once accepting the agreement and clicking "Next", you will be prompted for an installation location for resources related to MISM as shown below:



The default location is as follows:

C:\Program Files (x86)\Mi-Corporation\Mobile Inspection Software\

Note that while some resources will be installed in this location, the MISM server resources will be installed underneath your web root folder in a folder named *MISM*. On typical server installations this means that the full path for the web server resources for MISM will be:

C:\inetpub\wwwroot\mism\

After selecting an installation location, you will be asked to confirm the installation as shown below:

1	Mobile Inspection Software Setup
Ready The S	to Install ietup Wizard is ready to begin the Mobile Inspection Software installation
Click instal	"Install" to begin the installation. If you want to review or change any of your lation settings, click "Back". Click "Cancel" to exit the wizard.
Advanced I	installer < Back Cancel

Click the "Install" button and allow installation to complete. When done you will be shown a dialog indicating that installation was successful:



Click the "Finish" button and the installation wizard will close.

Configuration

After initially installing the MISM software, it is necessary to configure the database that will be used for data storage, the web application, and the reporting server.

Database Configuration

The MISM software requires a SQL Server database for storage of collected inspection data and for visualization and display of that data. This database is not automatically created during the installation of the software. Please follow the steps outlined below to create this database and configure the application.

1) Connect to your database server instance using a tool such as SQL Server Management Studio. Note that this server instance may be hosted on the same machine as the MISM software, but this is not required.



2) Create a database on this instance in line with your data management practices of your organization. The specific name of the database does not matter, but be sure to remember the name so that it can be used for configuration of the MISM software.

8	New Database – 🗖				- 🗆 🗙
Select a page	🔄 Script 💌 🚺	Help			
Options Filegroups	Database name: MISM				
	Owner:		<default></default>		
	Use full-text in	ndexing			
	Logical Name	File Type	Filegoup	Initial Size (MB)	Autogrowth / Maxsize
	MISM	Rows	PRIMARY	4	By 1 MB, Unlimited
	MISM_log	Log	Not Applicable	1	By 10 percent, Unlimited
Connection Server: (local)/sql2012					
Connection: MI-CO\cdpierr					
View connection properties					
Progress					
Ready	٢			Add	> <u>R</u> emove
					OK Cancel

3) When installing the MISM software, a .sql file will be installed that creates the necessary structure of the database. Open this file in the query window editor. If you used default installation settings, the file will be located here:

C:\Program Files (x86)\Mi-Corporation\MISM\Database\MISM Database Schema.sql



4) Insert a line above the initial comment in the query window editor that tells SQL Server Management Studio to use the appropriate database. The specific line is dependent on what

you named the database in step #2. For example if the database was named "MISM", then the line should read: *USE MISM*



5) Click the "Execute" button to run the query. A series of diagnostic lines should be shown in the Messages window.



6) Add an appropriate user to the database such that the web application can access the database, insert data, and run stored procedures. The specifics of this will vary depending on your data security requirements. If you intend to use integrated Windows authentication, be aware that the MISM application will run under the identity of the application pool that is hosting the web app (DefaultAppPool by default). The screenshot below shows granting this permission for such an identity, but the specifics of your setup may require other steps not detailed here.

0	Database User - New	- • ×
Select a page	Script - K Help	
General Owned Schenas		
Membership	User type:	
Securables Extended Projerties	SQL user with login	~
	User game:	
	is apppool\defaultapppool	
	Login name:	
	is apppool/defaultapppool	
	Default gchema:	
Connection		
Server: (ocal)/sgl2012		
Connection: MI-CO\cdipler		
Wew connection properties		
Progress		
C Ready		

	Database User - New		- • ×
Select a page	🖾 Script 👻 🚺 Help		
Owned Schemas Membenhig Membenhig Securable Exervised Properties	Database role genbonkp: For functors d. b. and constraint d. b. platenador d.		
Connection			
Server: (local)'sql2012 Connection: MI-CO'odpierr			
Progress			
C Ready			
		ОК	Carcel

7) On the application server where the MISM software was installed, locate the file named web.config in the web installation folder and open it in a text editor. In typical installations this file will be located at:

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

Web.config - Notepad -		×
Eile Edit Format View Help		
xml version="1.0"?		^
</td <td></td> <td></td>		
For more information on how to configure your ASP.NET application, please visit		
http://go.microsoft.com/fwlink/?LinkId=169433		
>		
<configuration></configuration>		
<configsections></configsections>		
<pre><!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468</pre--></pre>	>	
<pre><section name="entityFramework" nlog"="" type="NLog.Config.ConfigSectionHandler, NLog"></section></pre>		
<sectiongroup name="elmah"></sectiongroup>		
<pre><section name="security" requirepermission="false" type="Elmah.SecuritySectionHandler, Elmah"></section></pre>		
<pre>csection name="errorLog" requirePermission="false" type="Elmah.ErrorLogSectionHandler, Elmah"/></pre>		
<pre><section name="errorMail" requirepermission="false" type="Elmah.ErrorMailSectionHandler, Elmah"></section></pre>		
<pre><section name="errorFilter" requirepermission="false" type="Elmah.ErrorFilterSectionHandler, Elmah"></section></pre>		
<connectionstrings></connectionstrings>		
<pre><!-- Connection String for the Entity Framework to connect to the application database--></pre>		
<pre><add connectionstring="metadata=res://*/MicoModel.csdi/res://*/MicoModel.ssdi/res/MicoModel.ssdi/r</td" name="micontitles"><td>del.</td><td>m:</td></add></pre>	del.	m:
<pre>capbettings></pre>		
<pre><du key="weppages:version" value="5.0.0"></du> </pre>		
<pre>cadu key= weepages.clabuled value= taise // cadu key="begapering of plain" value= taise // </pre>		
<pre>cadu key= freserveLuginori value= true // cadu key= freserveLuginor</pre>		
<pre>cade key= CitentvalladscriptEnabled" value="rule"/\ cade key="CitentvalladscriptEnabled" value="rule"/\ </pre>		
<pre><!-- Flmah configuration settings For more info http://code.google.com/p/elmah/--></pre>		
cald keverelmah.mvc.disableHandler: value="false"/>		
<pre><add key="elmah.myc.disableHandleErrorFilter" value="false"></add></pre>		
<pre><add key="elmah.myc.requiresAuthentication" value="true"></add></pre>		
<pre><add key="elmah.mvc.IgnoreDefaultRoute" value="false"></add></pre>		
<add key="elmah.myc.allowedRoles" value="*"></add>		
<add key="elmah.mvc.allowedUsers" value="Administrator"></add>		
<pre><add key="elmah.mvc.route" value="elmah"></add></pre>		
		× •
		

8) Locate the line that reads:

<add name="micoEntities"

connectionString="metadata=res://*/MiCoModel.csdl\res://*/MiCoModel.ssdl\res://*/MiCoModel.msl;provid er=System.Data.SqlClient;provider connection string="<mark>data source=(local);initial</mark> catalog=mismdb;Integrated Security=SSPI;MultipleActiveResultSets=True;App=EntityFramework"" providerName="System.Data.EntityClient"/>

9) Replace the highlighted section above with a connection string that is suitable for connecting to your database created above.

For instance, if the database server's name is "Server1", the name of the database is "MISM" and you're using integrated security, the line should read as follows:

<add name="micoEntities"

connectionString="metadata=res://*/MiCoModel.csdl\res://*/MiCoModel.ssdl\res://*/MiCoModel.msl;provid er=System.Data.SqlClient;provider connection string="<mark>data source=Server1;initial</mark> catalog=MISM;Integrated Security=SSPI;MultipleActiveResultSets=True;App=EntityFramework"" providerName="System.Data.EntityClient"/>

If instead you are using SQL Server authentication, the connection string may be similar to:

<add name="micoEntities"
connectionString="metadata=res://*/MiCoModel.csdl\res://*/MiCoModel.ssdl\res://*/MiCoModel.msl;provid
er=System.Data.SqlClient;provider connection string="data source=Server1;initial
catalog=MISM;User=user;Password=pass;MultipleActiveResultSets=True;App=EntityFramework""
providerName="System.Data.EntityClient"/>

10) Save the web.config file in your text editor.

Authentication Configuration

The MISM software requires an instance of a Mi-Forms or Mi-Enterprise Apps Server to use for authentication and authorization. This server must be version 10 or later and must be accessible to the MISM server via HTTP(S) protocols. Please follow the steps outlined below to configure the application.

1) On the application server where the MISM software was installed, locate the file named web.config in the web installation folder and open it in a text editor. In typical installations this file will be located at:

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

🔲 Web.config - Notepad 🗕 🗖 🗙
Eile Edik F <u>o</u> rmat <u>V</u> iew <u>H</u> elp
<pre><?xml version="1.0"?> <!-- For more information on how to configure your ASP.NET application, please visit http://go.microsoft.com/fwlink/?LinkId=169433--></pre>
<pre><configuration> <configuration> <configuration> <configsections> <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwlink/?LinkID=237468--> <section name="entityFramework" nolg"="" type="Nlog.Config.ConfigSectionHandler, Nlog"></section> <section name="entity" requirepermission="false" type="Elmah.SecuritySectionHandler, Elmah"></section> <section false"="" name="errorMails requirePermission=" type="Elmah.ErrorMailSectionHandler, Elmah"></section> <section name="errorFilter" requirepermission="false" type="Elmah.ErrorMailSectionHandler, Elmah"></section> <section name="errorFilter" requirepermission="false" type="Elmah.ErrorMailSectionHandler, Elmah"></section> <section name="errorFilter" requirepermission="false" type="Elmah.ErrorFilterSectionHandler, Elmah"></section> <section name="errorFilter" requirepermission="false" type="Elmah.ErrorFilterSectionHandler, Elmah"></section> </configsections></configuration></configuration></configuration></pre>
<pre> <add connectionstring="metadata=res://*/MiCoModel.csdl[res://*/MiCoModel.ssdl[res://*/MiCoModel.mm:
</connectionStrings>
<add key=" name="micoEntities" value="3.0.0.0" webpages:version"=""></add> <add key="webpages:Enabled" value="false"></add> <add key="PreserveLoginUrl" value="true"></add> <add key="ClientValidationEnabled" value="true"></add> <add key="UnobtrusiveJavaScriptEnabled" value="true"></add> <add key="UnobtrusiveJavaScriptEnabled" value="true"></add> <add key="elmah.mvc.disableHandle" value="false"></add> <add key="elmah.mvc.disableHandleErrorFilter" value="false"></add> <add key="elmah.mvc.disableHandleErrorFilter" value="false"></add> <add key="elmah.mvc.disableHandleErrorFilter" value="false"></add> <add key="elmah.mvc.allowedDass" value="false"></add></pre>

2) Locate the lines in this file that read as follows:

<!--the customer name as it will be authenticated by the Authorization Web Service.--> <add key="customername" value="Inspection"/>

 Edit the value highlighted above to indicate the customer name of a customer setup on your Mi-Forms or Mi-Enterprise Apps Server. For example if the name of the customer is "Sierra Creek", edit the lines to read:

<!--the customer name as it will be authenticated by the Authorization Web Service.--> <add key="customername" value="Sierra Creek"/>

4) Locate the lines in this file that read as follows:

<!-- The Authentication Web Service endpoint. It is used by the Membership Provider to authenticate users. --> <endpoint address="http://localhost/mfs/Services/AuthServices.asmx" binding="basicHttpBinding" bindingConfiguration="AuthServicesSoap" contract="AuthServices.AuthServicesSoap" name="AuthServicesSoap"/>

5) If the MISM software and the Mi-Forms or Mi-Enterprise Apps Server are located on the same machine then you do not need to change this line. If, however, the Mi-Forms or Mi-Enterprise Apps Server is located elsewhere, edit the highlighted section to indicate the appropriate connection URL. For instance, if your Mi-Forms or Mi-Enterprise Apps Server is located on a machine named "server2" and requires HTTPS, the lines would be edited as follows:

<!-- The Authentication Web Service endpoint. It is used by the Membership Provider to authenticate users. -->

<endpoint address="<mark>https://server2/mfs</mark>/Services/AuthServices.asmx" binding="basicHttpBinding" bindingConfiguration="AuthServicesSoap" contract="AuthServices.AuthServicesSoap" name="AuthServicesSoap"/>

6) Save the web.config file in your text editor.

Reporting Configuration

The MISM software requires an instance of SQL Server Reporting Services in order to utilize its reporting functionality. Please follow the steps outlined below to configure the application.

 On the application server where the MISM software was installed, locate the file named web.config in the web installation folder and open it in a text editor. In typical installations this file will be located at:

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

	Web.config - Notepad -	□ ×
<u>File Edit Format View H</u> elp		
xml version="1.0"?		^
</td <td></td> <td></td>		
For more information on how to configure you	nr ASP.NET application, please visit	
http://go.microsoft.com/fwlink/?Linkid=16943		
>		
<configsections></configsections>		
Com igsections/	work configuration wight http://go.micnocoft.com/fulink/2LinkTD-227468	
<pre><section name="entityFramework" nlog"="" type="NLog.Config.Con</td><td>figSectionHandler, NLog"></section></pre>		
<sectiongroup name="elmah"></sectiongroup>		
<pre><section name="security" pre="" requirepermissi<=""></section></pre>	on="false" type="Elmah.SecuritySectionHandler, Elmah"/>	
<pre><section name="errorLog" pre="" requirepermissi<=""></section></pre>	.on="false" type="Elmah.ErrorLogSectionHandler, Elmah"/>	
<pre><section name="errorMail" pre="" requirepermiss<=""></section></pre>	ion="false" type="Elmah.ErrorMailSectionHandler, Elmah"/>	
<pre><section <="" name="errorFilter" pre="" requirepermi=""></section></pre>	.ssion="false" type="Elmah.ErrorFilterSectionHandler, Elmah"/>	
ConnectionStrings>	anonk to connect to the emplication detabase .	
<pre>connection String for the Entry Fram codd nome="miceEntities" connectionString</pre>	"motodoto-most //*/MiCoModol codl nost //*/MiCoModol codl nost //*/MiCoMo	dol m
(/connectionStrings)	inecadaca-res.// /hitchodel.csdifres.// /hitchodel.ssdifres.// /hitchod	ue1
(annSettings)		
<pre>cadd kev="webpages:Version" value="3.0.0.0</pre>	3"/>	
<add <="" key="webpages:Enabled" td="" value="false"><td></td><td></td></add>		
<pre><add kev="PreserveLoginUrl" value="true"></add></pre>	· · · · · · · · · · · · · · · · · · ·	
<add key="ClientValidationEnabled" value="</td><td>'true"></add>		
<add key="UnobtrusiveJavaScriptEnabled" td="" va<=""><td>alue="true"/></td><td></td></add>	alue="true"/>	
Elmah configuration settings. For mor</td <td><pre>re info http://code.google.com/p/elmah/></pre></td> <td></td>	<pre>re info http://code.google.com/p/elmah/></pre>	
<pre><add key="elmah.mvc.disableHandler" value="</pre"></add></pre>	"false"/>	
<add key="elmah.mvc.disableHandleErrorFilt</td><td>er" value="false"></add>		
<add key="elmah.mvc.requiresAuthentication</td><td>" value="true"></add>		
<pre><add key="elmah.mvc.IgnoreDefaultRoute" pre="" va<=""></add></pre>	<pre>ilue="false"/></pre>	
<pre><add key="elmah.mvc.allowedRoles" value="*</pre></td><td>·"></add></pre>		
<add key="elmah.mvc.allowedUsers" value="A</td><td>Administrator"></add>		
<add key="elmah.mvc.route" value="elmah"></add>	•	
(>

2) Locate the lines in this file that read as follows:

<!-- the address of the SSRS Reporting Services Web Service API. Usually it is http://myWebServerName/ReportServer. --> <add key="Micoreportserver" value="http://localhost/ReportServer"/>

3) Edit the value highlighted above to indicate the actual URL of the report server as configured in your network. For example if the name of the report server is "Server3" and URL underneath this is "ReportingServer" edit the lines to read:

<!-- the address of the SSRS Reporting Services Web Service API. Usually it is http://myWebServerName/ReportServer. --> <add key="Micoreportserver" value="http://server3/ReportingServer"/>

4) The MISM software will need to access the reporting server with credentials that allow viewing reports. This enables the currently logged in MISM user to view reports without being prompted for a separate set of login credentials that are required by the SSRS server instance. Locate the lines in the file that read as follows:

<!-- the user name of an NT account with permissions to access the Web Services. --> <add key="Micousername" value="username"/> <!-- the password for the NT account. --> <add key="Micopassword" value="password"/> <!-- the domain name for the NT accounts. This can be the machine name if it's a local account. --> <add key="Micodomain" value="domain"/> 5) Edit the highlighted values to reflect the username, password and domain of a valid SSRS user. For instance if the user "bsmith" on the domain "sierracreek" with password "pass" were to be used, the lines would read:

<!-- the user name of an NT account with permissions to access the Web Services. --> <add key="Micousername" value="bsmith"/> <!-- the password for the NT account. --> <add key="Micopassword" value="pass"/> <!-- the domain name for the NT accounts. This can be the machine name if it's a local account. --> <add key="Micodomain" value="screek"/>

- 6) Save the web.config file in your text editor.
- 7) The MISM software comes with a sample report that you may upload to your SSRS server. To do so, first browse to your SSRS instance and login with credentials that will allow publishing a report:



 Click the "Upload File" link and then browse for the report that is bundled with MISM. If you used default installation options, this report will be located at this location: C:\Program Files (x86)\Mi-Corporation\MISM\Reports\Inspections by Inspector.rdl

🕤 😌 🙋 http://localhost:8080/Reports_SQL2012/Pages/Import.aspx?l 🎾 🍷 😋 🛛 🈂 Upload File - Report Manager 🗙		ک ۲0
me	Home My Su	bscriptions Help
SQL Server Reporting Services		
Upload File	Search	Q
	L	
Indext a report (rdl) model (emdl) shared dataset (rsd) report part (rsc) or other resource into Hom		
Jpload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc), or other resource into Hom	e.	
Upload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc), or other resource into Hom File to upload: C:\Program Files (x86)\MI-Corpt Browse	e.	
Upload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc), or other resource into Hom File to upload: C:\Program Files (x86)\Mi-Corp(Browse Name: Inspections by Inspector	e.	
Upload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc), or other resource into Hom File to upload: C:\Program Files (x86)\Mi-Corpo Browse Name: Inspections by Inspector Overwrite item if it exists	e.	
Jpload a report (.rdl), model (smdl), shared dataset (.rsd), report part (.rsc), or other resource into Hom The to upload: C:\Program Files (x86)\Mi-Corp(Browse Name: Inspections by Inspector Overwrite item if it exists	ie.	
Jpload a report (.rdl), model (.smdl), shared dataset (.rsd), report part (.rsc), or other resource into Hom File to upload: C:\Program Files (x86)\Mi-Corp(Browse Name: Inspections by Inspector Overwrite item if it exists OK Cancel	ie.	

9) Create a new data source by clicking the "New Data Source" link and filling the data source with details that will allow it to connect to the database created in the database configuration section above. Note that the specifics of this data source will vary based on your database configuration and access methodologies and the image shown below indicates just one possible setup.

		_ 🗆 🗙
+ 🕞 🧭 http://loc	lhost:8080/Reports_SQL2012/Pages/DataSource.a ♀ マ ♂ 🥔 New Data Source - Report ×	合 ☆ ६
ome		Home My Subscriptions Help
SQL Servei	Reporting Services	
🎽 New Da	ata Source	Search 🔎
Name:	MISM DataSource	
Description:	Data source used to connect to MISM	
	database	
	Hide in tile view	
	Enable this data source	
Data source type:	Microsoft SQL Server	
Connection string:	data source=Server1; initial catalog=MISM	
	~	
Connect using:		
○ Credentials	supplied by the user running the report	
Display th	Following text to prompt user for a user name and password:	
Type or e	Iter a user name and password to access the data source	
Use as	Windows credentials when connecting to the data source	
O Credentials	stored securely in the report server	
User nam	2:	
Password		
Use as	Windows credentials when connecting to the data source	
Use as	Windows credentials when connecting to the data source onate the authenticated user after a connection has been made to the data source	
Use as Impers Windows in	Windows credentials when connecting to the data source onate the authenticated user after a connection has been made to the data source regrated security	
Use as Impers Windows in	Windows credentials when connecting to the data source onate the authenticated user after a connection has been made to the data source legrated security are not required	
Use as Impers Windows in Credentials Test Connection	Windows credentials when connecting to the data source onate the authenticated user after a connection has been made to the data source legrated security are not required	
Use as Impers Windows in Credentials Test Connection	Windows credentials when connecting to the data source onate the authenticated user after a connection has been made to the data source tegrated security are not required	

10) Configure the report to use the data source that was created by hovering over the report, clicking the downward pointing arrow and clicking "Manage" and then navigating to the Data

Sources tab. Check the "A shared data source" radio button and browse for the data source created above.

http://localhost:808	ار المحمد ا
ie	Home My Subscriptions Hel
SQL Server Repor	ting Services
Inspections	s by Inspector Search
Pioperties	Data Sauraa
Parameters	A shared data source
Data Sources	/MISM DataSource Browse
Subscriptions	○ A custom data source
Processing Options	Data source type: Microsoft SQL Server
Cache Refresh Options	Connection string:
Report History	\checkmark
Stapshot Options	Connect using:
Security	Credentials supplied by the user running the report Disclay, the following text to promot user for a user rame and password:
Security	Type or enter a user name and password to access the data source
	Use as Windows credentials when connecting to the data source
	Credentials stored securely in the report server
	User name:
	Password:
	Use as Windows credentials when connecting to the data source
	In personate the authenticated user after a connection has been made to the data source
	Windows integrated security
	Credentials are not required
	Test Connection
	Apply

11) Click "Apply".

Background Service Configuration

While it is possible for administrative users to directly upload exported form data to the MISM system through the web interface, it may instead be useful to configure automatic importing via a Windows service. The MISM software bundles such a service and may be configured as follows:

- Using Windows Explorer, navigate to the Import Service installation folder. If you used default settings during install, this folder will be as follows: C:\Program Files (x86)\Mi-Corporation\MISM\Import Service
- 2) Using a text editor, open the file MiCoWindowsService.exe.config

MiCoWindowsService.exe.config - Notepad	×
<u>F</u> ile <u>E</u> di: F <u>o</u> rmat <u>V</u> iew <u>H</u> elp	
<pre>k?xml version="1.0" encoding="utf-8"?> <configuration> <configsections></configsections></configuration></pre>	
<pre><section name="micoFileProcessorSection" nlog"="" type="NLog.Config.ConfigSectionHandler, NLog"></section> <!-- For more information on Entity Framework configuration, visit http://go.microsoft.com/fwl <section name="entityFramework" type="System.Data.Entity.Internal.ConfigFile.EntityFrameworkSe </configSections--> <micofileprocessorsection></micofileprocessorsection></pre>	sService" /> ink/}LinkID=237468> ction, EntityFramework,
<pre><micofileprocessors> <!-- Example of File Processor configuration. Directory values have to be unique. Files from the directory will be uploaded into the respective connection string databa <!<add directory="c:\temp" connectionString="Server=(local)"/--></micofileprocessors></pre>	se>
<pre> <appsettings> <!--/appSettings--> <!--! configures NLog to write logging data to the console--> <nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd" xmlns:xsi="http://www.w3.org/2001/XML</pre></td><td>Schema-instance"></nlog></appsettings></pre>	
<targets> <!-- NLog uses the concept of target to indicate where log messages are written to.<br-->Targets can be files, the console, databases, SMTP and much more. A full list of target can be viewed in the NLog documentation: http://www.nlog-project.org/targets.html</targets>	s
> NLog can optional format the output using a pattern string, it is also possible to format the output in CSV or XML. The various tokens in this format string are detailed NLog documentation: http://www.nlog-project.org/layoutrenderers.html	in the
> <target eventlog"<br="" filename="logs
<target xsi:type=" layout="\${longdate} \${logger} \${message}" name="file" xsi:type="File">name="eventLog" source="MiCoUploadXMLService"</target>	/\${shortdate}.txt" />
<	>

3) Locate the section of the file that looks like the lines below:

<micofileprocessorsection></micofileprocessorsection>
<micofileprocessors></micofileprocessors>
Example of File Processor configuration. Directory values have to be unique.</td
Files from the directory will be uploaded into the respective connection string database>
<add directory="c:\temp" connectionString="Server=(local)"/
<pre><add connectionstring="Server=(local)" directory="c:\temp"></add>></pre>

4) This service is designed to allow for the specification of multiple MISM instances on a single server. In general, most configurations will only require a single file processor. Using the example SQL Server database configuration above and the expectation that form data files exist in the folder "c:\exports", edit the lines highlighted above as follows:

```
<micoFileProcessorSection>
<micoFileProcessors>
<!-- Example of File Processor configuration. Directory values have to be unique.
Files from the directory will be uploaded into the respective connection string database.-->
<!--<add directory="c:\temp" connectionString="Server=(local)"/>
<add directory="c:\temp" connectionString="data source=Server1;initial
catalog=MISM;Integrated Security=SSPI "/>-->
</micoFileProcessors>
```

```
</micoFileProcessorSection>
```

- 5) Save this file in your text editor.
- 6) Open a command prompt with administrative privileges and navigate to the folder where the service is located.



7) Run the batch file "install.bat". A series of messages indicating success should be displayed.



Verification

After the configuration above, you may wish to verify your setup. To do so, first navigate to the URL where the MISM software is installed.



Login with a set of administrative credentials and you should see a screen similar to the one below. Note that it's normal not to see any charted data after initial installation.

Mobile Inspecton Softwar ×		- 0
→ C Serenity/MISM/Home/Index		☆ 💽 💈
MI-CO Home - Reports Upload data Admin - Help - Aobile Inspection Software by Mi-Corporation		First Last -
Inspection Reports		
Inspections by Inspector	Inspections by Facility	
nspections over tine Today 🔍 Inspector Name ALL 💌	Inspections over the Today V Location Name ALL V Inspector Name ALL V	
Inspections by Inspector =	Inspections by Facility	=
Highcharts.com Inspections by County nspections over the Today V Location County Durham V	Inspections by Type Inspections over time Today Type of Inspection ALL	Highcharts.com
Facility Name Total	Inspections by Type	Ξ

Help & Troubleshooting

The MISM Software includes a number of help and troubleshooting resources.

Tutorial Videos

The MISM software includes a series of helpful tutorial videos. You may access them by clicking on the "Help" menu in the top right of the web application and choosing "Tutorial". This will provide access to a set of videos that describe uploading data, mapping reports, and creating dashboards.



Help Topics

Anywhere you see a "?" in a black circle in the web application indicates that help guidance is available. Click on any one of these for details about how to use a specific feature.

/ 🗋 Mobi	Mobile Inspecton Softwar ×					
$\leftarrow \ \Rightarrow$	C serenity/MISM/Data		☆ 🙋 🗉			
		orts Upload data Admin 👻 Help 👻	First Last -			
Мо	bile Inspectio	XML Upload ×				
	by Mi-Corpor	When selected the uploaded XML file will be used for field mapping only. The data from the file will be onlitted from any reports, charts or widgets.				
	File Upload	Close				
	Please use this form to uploa	ad your MI-Form exported XML files. Data will be immediately reflected in the dashboard(s).				
	Setup XML File: 🗐 🕄	Choose File No file crosen UploadFile				

You may also navigate to the "Help" menu in the top right and then click on "Help Topics" to see a full list of all available help topics.

Mobile Inspecton Softwar ×		- 0 ×
← → C 🗋 serenity/MISM/Help		☆ 🙋 🗏 🗏
MI-CO Home - Reports		First Last -
Mobile Inspection ^{by} Mi-Corporat	Software ion	
Help		
Charts	Please select help topic	
Dashboard		
Filters		
Mapping		
Report		
Report details		
Web.Config Setup		
XML Upload		

Further Support

If you need further support, please visit Mi-Corporation's support website at:

http://support.mi-corporation.com/

Or please email support at:

support@mi-corporation.com