Installation and Configuration Guide

E-resept Forskrivningsmodul

Thula – Nordic Source Solutions

Date | 08/04/2013

Software version | 50
Document version | 2.2
Document status | Approved

Author | Thula
Contributor(s) | [Contributor(s)]

Distribution | Customer

File name | E-resept FM - Installation and Configuration Guide.docx

© 2013 thula®

The document is only intended for Thula personnel and customers
Style and contents are confidential

Table of Contents

1 Document control ... 3
1.1 Revision tracking ... 3
1.2 Document source, storage and distribution ... 3
1.3 Revision history ... 3
1.4 Related documents ... 4
1.5 Reader comments ... 4
1.6 Glossary ... 4
2 Introduction ... 5
3 Prerequisites ... 5
3.1 Hardware and software requirements ... 5
3.2 Database ... 5
3.2.1 ... 5
3.2.2 Creating a SQL Server authentication SQL Server login ... 6
3.3 Certificates ... 6
3.3.1 Installing the local organizational certificate ... 7
3.3.2 Installing the RF organizational certificate ... 8
3.3.3 Installing smart card certificates ... 8
3.4 Messaging folders ... 8
4 Installation and Configuration ... 9
4.1 Installing FM for the first time ... 9
4.1.1 Server installation ... 9
4.1.2 Client installation ... 11
4.1.3 Configuring the application server ... 13
4.1.4 Configuration using the administration client ... 17
4.2 Advanced configuration ... 18
4.2.1 Registry settings ... 18
4.2.2 User management web service ... 19
4.2.3 SmartCard drivers ... 20
4.2.4 Manually starting and stopping the application server ... 20
4.2.5 Installing multiple instances of the server on the same machine ... 21
4.2.6 Using multiple application servers for failover and load balancing ... 23
4.3 Installing e-resept FM on a computer with previous version ... 25
4.4 Monitoring of the FM server ... 25
4.4.1 WMI objects ... 25
4.4.2 FM Performance counters ... 26
4.4.3 WCF performance counters ... 27

1 Document control

This section describes how to version, file, distribute and improve this document.

1.1 Revision tracking

This document is subject to revision control so that after each formal change a new version shall be created with a new data and revision number. At any given time the revision with the highest version number is considered the official and valid version of this document.

1.2 Document source, storage and distribution

The source of this document is maintained by Thula. It is stored in the Thula document repository in the following folder:

- E-resept \ System Documentation \ Paper Based

This document shall be distributed in PDF format only.

1.3 Revision history

Date	Version	Author/Approved by	Description
			Release 2.8.0
2012-11-06	2.2	Elisa C Stead	Updating screenshots with Thula logo, review FMM's changes, minor language modifications.
2012-11-06	2.1	Fernando Meira	Added final steps of the FM client installation, using the shortcut.
			Release 2.7.0
2012-09-12	2.0	Magnús Kristjánson	Reformatted using new Thula template.
			Release 2.6.0
2012-05-23	1.5	Viðar Júlíusson	Updating information on UserManagement web service
2012-05-22	1.4	Atli Sturluson	Added documentation on performance counters and WMI.
			Release 2.4.0
2012-05-22	1.3a	Elisa C Stead	Logo update, formatting, style. No content changes.
2012-05-18	1.3	Ægir Örn Leifsson	Added information about installations running multiple application servers on a single database.
			Release 2.3.80
2012-03-08	1.2e	Atli Sturluson	Added information on how to install multiple instances of the server on the same machine.
2012-03-08	1.2d	Viðar Júlíusson	Added information on UserManagement web service
2012-03-03	1.2c	Elisa C Stead	Updated screenshots, logo, and company name. Some style changes & reference updates.
			Release 2.3.70
2012-02-02	1.2b	Fernando Meira	Updated section about the installation of certificates and step 3 of the installation wizard.
2012-02-01	1.2a	Atli Sturluson	Added section about messaging folders

			Release 2.3.40
2011-11-02	1.1a	Ægir Örn Leifsson	Added information about software version on the front page. This document version relates to version 2.3.40 of the FM.
2011-10-31	1.0	Bjarni Ívarsson	Added prerequisite section covering hardware and software requirements + database configuration + certificate installation
2011-10-28	1.0g	Gísli Harðarson	Updated screen shots of setup procedure and Configuration Wizard
2011-09-30	1.0f	Gísli Harðarson	Updated information about Configuration Wizard
2011-09-19	1.0e	Gísli Harðarson	Added information about Configuration Wizard
2011-09-14	1.0d	Magnús Kristjánsson	Created based on existing installation memo

1.4 Related documents

The following background documents are relevant to this guide:

Document	Description
E-resept FM – EPJ API and Technical Specification	EPJ API and technical specification for the Prescription Module.

- Related document 1

1.5 Reader comments

If you have any comments on the contents of this document please send those by e-mail to egir.leifsson@thula.is. If a review result in changes, all user of this document should be notified.

1.6 Glossary

Abbreviation	Explanation or web reference
Forskrivningsmodul	Prescription module. The software being described in this document.
FM	Forskrivningsmodul.
EPJ	Electronic patient journal. A computerized patient record/journal system that communicates with the FM through the FM EPJ API and import/export of patient data (described in user help included with the Administration portion of the FM
API	An application programming interface (API) is an interface implemented by a software program that enables it to interact with other software. See http://en.wikipedia.org/wiki/API.
RF	Reseptformidleren. Reseptformidleren er et sentralt elektronisk helseregister/database som de aller fleste meldinger i e-resept går gjennom. Her oppbevares den elektroniske resepten og her slettes den, 4 uker etter at den er blitt ugyldig, det vil si ferdig ekspedert eller utløpt på dato.

2 Introduction

This administrator guide describes how to install, update and configure the e-resept Prescription Module (FM) using the installers and configuration wizard.

This guide also explains how to import patients and prescriptions into a freshly created FM.

3 Prerequisites

3.1 Hardware and software requirements

The technical requirements are described in a separate document: ***E-resept FM – EPJ API and Technical Specification***. It is important that the requirements listed in that document are followed to the letter.

Before installing the FM these steps should be carried out:

1. Install all mandatory and optional updates in Windows Update (may need to be done several times, since some updates don't become available until others have been installed).

2. If the .NET Framework v4 is not installed, it should be installed from here: http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=17718

3.2 Database

The FM uses a Microsoft SQL Server database to store all data. A free version of SQL Server 2008R2 Express is available from here (this link is also provided in the configuration wizard):

http://www.microsoft.com/download/en/details.aspx?id=23650

The FM application server requires a user account on the database server that has the following server roles:

- ***dbcreator***
- ***public***
- ***sysadmin***

The FM application server can use either Windows authentication or SQL Server authentication to authenticate to the database. If you choose to use Windows authentication, it is important to note that the FM application server will be running under the Network Service user account and will need to have access to the database as that account.

It is possible to change the user account that the service runs under (in the Services management tool in Windows), but that is not recommended since that setting will be reset when the FM application server is upgraded.

3.2.1

The following steps should be followed in order to create a login in SQL Server using Windows authentication. This authentication model is recommended if the SQL Server and FM application server are running on the same machine, or if ***Active Directory*** is being used (in which case the application server will use the credentials of the computer account when accessing network resources). Note that these steps are for SQL Server 2008R2 Express and may differ slightly for other versions of SQL Server:

1. Startup ***Microsoft SQL Server Management Studio*** (included in the SQL Server 2008R2 Express version linked to in section **Error! Reference source not found.**, and also available as a separate download from Microsoft).)
2. Select ***File -> Connect Object Explorer…*** from the menu.
3. Type in the server name (e.g. localhost\sqlexpress) and press the ***Connect*** button.
4. Open the ***Security -> Logins*** node in the ***Object Explorer*** tree.
5. Right click the ***Logins*** node and select ***New Login…*** from the popup menu.
6. Press the ***Search…*** button on the top-right of the ***Login-New*** dialog.
7. Type in ***Network Service*** into the search field and press the ***Check Names*** button. If the Network Service is not found, make sure that "From this location:" is set to the local computer, not the active directory.
8. Press the ***OK*** button.
9. Select the ***Server Roles*** page, and check the ***dbcreator***, ***public*** and ***sysadmin*** server roles.
10. Press the ***OK*** button.

3.2.2 Creating a SQL Server authentication SQL Server login

The following steps should be followed in order to create a login in SQL Server using SQL Server authentication. This authentication mode is recommended if the SQL Server and FM application server are running on different machines and if Active Directory is not being used. Note that these steps are for SQL Server 2008R2 Express and may differ slightly for other version of SQL Server.

1. Startup ***Microsoft SQL Server Management Studio***.
2. Select ***File -> Connect Object Explorer…*** from the menu.
3. Type in the server name (e.g. localhost\sqlexpress) and press the ***Connect*** button.
4. Open the ***Security -> Logins*** node in the ***Object Explorer*** tree.
5. Right click the ***Logins*** node and select ***New Login…*** from the popup menu.
6. Select the ***SQL Server authentication*** radio button.
7. Type in the desired ***login name*** (e.g. eReseptFM) and ***password***.
8. Uncheck the ***Enforce password expiration*** and ***User must change password at next login*** check boxes.
9. Select the ***Server Roles*** page, and check the ***dbcreator***, ***public*** and ***sysadmin*** server roles.
10. Press the ***OK*** button.

3.3 Certificates

The FM uses 4 different kinds of certificates, these are:

1. The local organizational certificate (including a private key).
2. The RF organizational certificate.

3. Smart card certificates.

4. The CA Certificates used to validate the authenticity of the certificates described above.

Note that the first two (as well as any CA certificates) ***MUST*** be installed in the ***Local machine*** certificate store in order for the FM application server to be able to use them. The FM application server runs under the ***Network Service*** user account, and needs to be able to access the certificates from that account. The first two certificates can be installed by the FM application – in the Administration client. The second certificate can also be installed during the first application setup, using the Installation Wizard. Nevertheless, the following instructions present an alternative to install and setup the required certificates.

3.3.1 Installing the local organizational certificate

The steps below should be followed in order to install the local organizational certificate (usually provided as a .p12 file), and granting read access to the private key to the FM application server. Note that these steps are for Windows 2008R2 and may differ slightly for other versions of Windows:

1. Startup ***mmc.exe*** (Microsoft Management Console).

2. Select ***File -> Add/Remove Snap-in*** from the menu.

3. Select ***Certificates*** in the list, and press the ***Add*** button.

4. Select ***Computer Account***, and press the ***Next*** button.

5. Select ***Local Computer***, and press the ***Finish*** button.

6. Close the ***Add or Remove Snap-ins*** window by pressing the ***OK*** button.

7. Open the ***Certificates (Local Computer) -> Personal -> Certificates*** node in the tree.

8. Right click on the ***Certificates*** node and select ***All tasks -> Import*** from the popup menu.

9. In the ***Certificates Import Wizard***, press the ***Next*** button.

10. Browse to the file containing the certificate, and press the ***Next*** button.

11. Type in the password for the private key, and press the ***Next*** button.

12. Select the ***Personal*** store as the location for the certificate and press the ***Next*** button.

13. Press the ***Finish*** button, the certificate should now be in the ***Personal*** store under ***Local computer.***

14. Move any CA certificate imported along with the local organizational certificate from the ***Personal*** certificate store to the ***Trusted Root Certificate Authorities*** store using drag and drop.

15. Right click the imported organizational certificate, and select ***All tasks -> Manage Private Keys…*** from the popup menu.

16. In the ***Permissions*** dialog, click the ***Add…*** button.

17. In the ***Select Users*** dialog type in “network service” into the search field, and press the ***Check Names*** button, followed by the ***OK*** button.

18. Make sure that the “Network Service” account has read access to the private key (should be the default).

19. Close the ***Permissions*** dialog by pressing the ***OK*** button.

3.3.2 Installing the RF organizational certificate

The following steps should be followed in order to install the RF organizational certificate (required for any communication with the RF):

1. Startup ***mmc.exe*** (Microsoft Management Console).

2. Select ***File -> Add/Remove Snap-in*** from the menu.

3. Select ***Certificates*** in the list, and press the ***Add*** button.

4. Select ***Computer Account***, and press the ***Next*** button.

5. Select ***Local Computer***, and press the ***Finish*** button.

6. Close the ***Add or Remove Snap-ins*** window by pressing the ***OK*** button.

7. Open the ***Certificates (Local Computer) -> Personal -> Certificates*** node in the tree.

8. Right click on the ***Certificates*** node and select ***All tasks -> Import*** from the popup menu.

9. In the ***Certificates Import Wizard***, press the ***Next*** button.

10. Browse to the file containing the certificate, and press the ***Next*** button.

11. Press the ***Finish*** button, the certificate should now be in the ***Personal*** store under ***Local computer.***

12. Move any CA certificate imported along with the local organizational certificate from the ***Personal*** certificate store to the ***Trusted Root Certificate Authorities*** store using drag and drop.

3.3.3 Installing smart card certificates

The FM uses a driver from BuyPass (BuyPass Access Enterprise, not provided as a part of FM) which needs to be installed in order for smart card access to work. The installation of that driver is not detailed in this document; please refer to instructions provided by BuyPass.

3.4 Messaging folders

The PM application server uses two folders for dropping and picking up messages that are sent to external systems. These folders must exist so that the application server starts and works properly. As a default, these folders are:

- **For incoming messages**: “..\fm_inbox”, i.e. this is relative to the folder where the server application is installed. E.g. if it is installed in the folder “d:\prog\legedata\fmmodul\eresept forskrivningsmodul”, then the folder “d:\prog\legedata\fmmodul\fm_inbox” will be used.

- **For outgoing messages**: “..\..\outbox”, so this would translate to “d:\prog\legedata\outbox”.

The server will try to create these folders during the installation process, but the user running the server (default is Network Service) will usually not have the privileges needed to create folders, so this will fail and a warning message is displayed. To resolve this, the user must open Windows Explorer

and manually create these two folders and give the user running the service full permissions to read and write to them.

4 Installation and Configuration

Each release of FM contains two installer packages, one for the application server and one for the client. The application server installer contains the application server executable as well as a configuration wizard that is used to configure the system for the first time.

The client installer contains the FM client, as well as an administrator client. It is recommended to run both installers on the machine that will host the application server.

4.1 Installing FM for the first time

4.1.1 Server installation

1. In the Installers folder, under Application Server, click on ***setup.exe*** to install the application server. A window opens:

2. Press the ***Next*** button. In this window you can select the folder where the FM server will be installed:

3. Press the ***Next*** button. In this window you confirm the installation and are ready to install the FM server:

4. Pressing the ***Next*** button will start the install process:

5. When the installation is complete, this window displays. Press the ***Close*** button to complete the server installation:

Now a shortcut has been created on the Desktop to start the configuration tool for the server (see chapter 4.1.3 for configuring the server). This shortcut can also be found on the start menu in folder ***eResept Forskrivningsmodul***.

4.1.2 Client installation

1. To install the e-resept Prescription Module client, click on the ***setup.exe*** file in the Installers\Client folder. A window opens:

2. Press the ***Next*** button. In this window, the installation location can be selected:

3. Press the ***Next*** button. In this window you confirm the installation and are ready to install the FM client:

4. Pressing the ***Next*** button will start the install process:

5. When the installation is complete, this window displays. Press the ***Close*** button to close the wizard.

To complete the client installation, execute the shortcut located in "C:\Program Files\eResept Forskrivningsmodul\ FM Klient Installasjon", or “C:\Program Files (x86)\eResept Forskrivningsmodul\ FM Klient Installasjon” in 64-bit systems. It needs to be run with Administrator privilege.

6. This window confirms that the installation was successful. Press the ***Ok*** button to close the window. Now the eResept FM client is ready to be used.

A shortcut has also been created on the start menu in folder ***eResept Forskrivningsmodul*** to run the Administration client. However, that cannot be run until the application server has been configured.

4.1.3 Configuring the application server

1. Clicking on the desktop icon created in the after successful installation of the server opens a tool for setting up the system for the first time. Running it requires administrative privileges since it manipulates system settings. Use this application to set up and configure a new database, connect to that database and create an admin user that can log into the Admin Client.

Since the installed application server does not start automatically after install (it does after a restart) there is a button to start it. Alternatively the service can be started using the built in ***Services*** management tool in Windows.

When the wizard detects that the application server has started, information about that is shown and the Next button becomes enabled.

2. In the second step you must make sure that Microsoft Sql Server is installed or available, or download and install Sql Server Express from the link provided by download button. If the database server has been installed and the plan is to connect using Windows Authorization then make sure that the Network Service user has been given privileges to the database server, and then press the confirm button. That makes it possible to go to the next step in the installation wizard.

3. When configuring the connection to the database server the user can choose to use Windows authentication, Sql Server authentication or configure the connection manually (not recommended). The user must enter the name of database server or the name of the server and the name of the Sql Server instance if the database server was installed as a named instance as in the screen shot below. Note that Sql Server Express is by default installed as named instance with the name ***sqlexpress***. If the user chooses Sql Server authentication then user name and password for the Sql Server must also be entered. Before being able to go to the next step, the connection must be verified. If the application server cannot connect to the database server using the information provided, then an error message is shown.

If the verification is successful, information about the server will be displayed and the „next“ button will be enabled. Changing any parameter of the connection information requires the user to re-validate the connection.

4. If the user has chosen a new (or previously created but empty) database, the next step is to import the database schema for the FM. Pressing the install button creates the database. This step is skipped if the connection string provided in the previous step points to an existing e-resept database.

   When the “Install RF certificate” option is selected, the default RF certificate is installed (when pressing the button to create the database) and set as the certificate to be used for communications with the RF. This can certificate can also be installed/altered at a later stage using the Admin client.

The next step is to create a user in the e-resept database. This user must be assigned username and password. A BuyPass smart card can be associated with the user by inserting a smart card in an attached card reader and providing the correct PIN code. The created user

can then be used to access the Admin client using username and password or by signing in using only the smart card. It is required that the application server has access to the installed BuyPass certificates. Use Microsoft Mangement Console with the Certificates snap-in to view and alter permissions to certificates. See section 3.3 for details.

5. After successful installation of a new database, the system must be configured using the Administration client. If the FM client has also been installed on the computer, the button to run the Administration client will be enabled.

4.1.4 Configuration using the administration client

The final step to set up the application server is to run the administration client, either directly from the configuration wizard, or from your computer's start menu. Note that to do this the FM client must be

installed. See details on the Administration client features in the provided help file. It can be accessed by pressing F1 while running the Administration client.

4.2 Advanced configuration

The configuration in this chapter is intended to be done by a system administrator, since it requires knowledge of the database, and administrator privileges on all computers being configured.

4.2.1 Registry settings

The following settings must be present in the registry and configured according to the location of the e-resept database and application server.

4.2.1.1 Client settings

For the client to find the application server, a string value must be added to the registry, either in HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE, as shown below.

HKEY_CURRENT_USER:

Operating system	HKEY_CURRENT_USER Key value and name
32 bit OS	[HKEY_CURRENT_USER\SOFTWARE\Theriak\eResept Forskrivningsmodul\Client] "ServerAddressAndPort"="*name_of_computer_running_application_server*:8903"
64 bit OS	[HKEY_CURRENT_USER\SOFTWARE\Wow6432Node\Theriak\eResept Forskrivningsmodul\Client] "ServerAddressAndPort"=" *name_of_computer_running_application_server*:8903"

HKEY_LOCAL_MACHINE:

Operating system	Key value and name
32 bit OS	[HKEY_LOCAL_MACHINE\SOFTWARE\Theriak\eResept Forskrivningsmodul\Client] "ServerAddressAndPort"="*name_of_computer_running_application_server*:8903"
64 bit OS	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Theriak\eResept Forskrivningsmodul\Client] "ServerAddressAndPort"=" *name_of_computer_running_application_server*:8903"

This configuration is typically done in HKEY_LOCAL_MACHINE since then a single registry value is sufficient for all users of the same computer. The possibility to configure the server address in HKEY_CURRENT_USER is primarily aimed at hosted environments where different users of the same computer need to connect to separate application servers.

When the FM client reads the server address from the registry, it starts by looking in HKEY_CURRENT_USER and if nothing is found there, reads the address from HKEY_LOCAL_MACHINE.

Also see section 4.2.6.2 for more detailed information about how the client obtains a server address.

4.2.1.2 Application server settings

The connection string used by the application server to connect to the database is stored in the following registry values and must be configured correctly for the server to operate. If the configuration wizard was run then these settings have already been created and configured.

Operating system	Key value and name
32 bit OS	[HKEY_LOCAL_MACHINE\SOFTWARE\Theriak\eResept Forskrivningsmodul\Server] "DatabaseConnectionString"="*enter_your_database_connection_string_here*"
64 bit OS	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Theriak\eResept Forskrivningsmodul\Server] "DatabaseConnectionString"="*enter_your_database_connection_string_here*"

4.2.2 User management web service

The web service exposes a single endpoint for external clients to connect. The web service conforms to WS-I Basic Profile 1.1.

The user management web service is turned off by default. The switch to turn it on/off is in the advanced view in the system configuration window. By default the configuration is set to run the web service on http://localhost:8000/UserManagement. The default port number is 8000 but that can be configured in the advanced view. By default the service is configured for none secure communication (HTTP transport protocol). Note that the service url is fixed on localhost and “/UserManagement”. Only the port and the transport protocol (http/https) can be configured. If the service is running as the user “Network Service” then the user might need to reserve the namespace. See http://msdn.microsoft.com/en-us/library/ms733768.aspx on how to configure it.

4.2.2.1 Secure Mode

To run the web service in a secure mode (HTTP transport protocol), the port must be configured to use a SSL certificate. That is required so that the web service knows what certificate to use to crypt the communication. The configuration for that must be done manually on the server that has the service installed. Once the web server has been configured to run in secure mode the service will be available only on https://localhost:port/UserManagement where port is the port number configured. In secure mode the WSDL definition is not available.

4.2.2.1.1 Configuring SSL Certificate on Windows Server 2003 or Windows XP

In Windows Server 2003 or Windows XP, use the HttpCfg.exe tool in "set" mode on the Secure Sockets Layer (SSL) store to bind the certificate to a port number. The tool uses the thumbprint to identify the certificate, as shown in the following example.

```
httpcfg set ssl -i 0.0.0.0:8012 -h 0000000000003ed9cd0c315bbb6dc1c08da5e6
```

- The **-i** switch has the syntax of *IP*:*port* and instructs the tool to set the certificate to port 8012 of the computer. Optionally, the four zeroes that precede the number can also be replaced by the actual IP address of the computer.
- The **-h** switch specifies the thumbprint of the certificate.

For more information see http://msdn.microsoft.com/en-us/library/ms733791.aspx

4.2.2.1.2 Configuring SSL Certificate on Windows Vista or Windows Server 2008

Use the Netsh.exe tool, as shown in the following example.

```
netsh http add sslcert ipport=0.0.0.0:8000 certhash=0000000000003ed9cd0c315bbb6dc1c08da5e6
appid={00112233-4455-6677-8899-AABBCCDDEEFF}
```

- The **certhash** parameter specifies the thumbprint of the certificate.

- The **ipport** parameter specifies the IP address and port, and functions just like the **-i** switch of the Httpcfg.exe tool described.

- The **appid** parameter is a GUID that can be used to identify the owning application.

For more information see http://msdn.microsoft.com/en-us/library/ms733791.aspx

4.2.2.2 Metadata Exchange (WSDL)

If the service is configured to run in a none secure mode then it will automatically expose it's WSDL via the url http://localhost:port/UserManagement/mex where the port is the number configured. It is therefore highly recommended not to use none secure mode except when testing or developing a client against the web service.

4.2.3 SmartCard drivers

For an e-resept installation that is communicating externally, the BuyPass SmartCard drivers must be installed in order for the SmartCards to work. Additionally, the BuyPass certificates must be imported into the trusted root certificate store for the local computer. See section 3.3 for details.

4.2.4 Manually starting and stopping the application server

1. If needed, the application server can be stopped and started from the computer's task manager by right-clicking on the computer toolbar. Select the **Services** tab, and find the entry called **eResept Forskrivningsmodul Server**: If the configuration wizard was run then the service should already be running.

2. Right-click on the server, and select **Start Service.** When the status changes from Stopped to Running, the server is ready to use:

4.2.5 Installing multiple instances of the server on the same machine

Note: This section describes advanced usage of the e-resept Prescription Module and should only be done by computer support personnel who are familiar with Windows services and the Windows Registry.

The server program can be configured to run multiple instances of the Windows Service, where each instance uses a different database. This can be useful in a hosted or terminal service environment where multiple organisations are sharing the same physical server machine.

This configuration is not supported by the server setup program, so this needs to be done manually by installing the Windows Service(s) and adding the necessary Windows Registry settings. This section describes the procedure for this installation.

This discussion assumes that the server program has already been installed as described section 4.1.1. Then there should already be one instance of the service running, with the name “eResept Forskrivningsmodul Server”. This instance does not need to be removed.

Install service instance

To install additional instances of the eResept Forskrivningsmodule service, we first need to add the required service instances(s). This is done using the InstallUtil command line utility that is part of the .Net Framework. Open a command line window (must be run as an administrator) and enter the following commands (you may need to alter the directory names, depending on where the server was installed and which version of the .Net framework is installed):

- `cd “C:\Program Files (x86)\eResept Forskrivningsmodul Server”`
- `C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil /servicename="eResept Instance1" "eResept Forskrivningsmodul Server.exe"`

This will install a new Windows Service called “eResept Instance1”. If the servicename parameter is not specified, it defaults to “eResept Forskrivningsmodul Server”. Each instance must have a unique servicename. Do not start the new service instance until it has been configured as described below.

To remove a service instance, use the /u parameter of InstallUtil:

- `C:\Windows\Microsoft.NET\Framework64\v4.0.30319\InstallUtil /u /servicename="eResept Instance1" "eResept Forskrivningsmodul Server.exe"`

Creating a new database

A new database must be created for each instance of the service. *Different server instances cannot share the same database*. Installing a second copy of the database is not directly supported by the Configuration utility described in section 4.1.3. There is however a workaround for this:

- Stop the default server instance “eResept Forkrivningsmodul Server” if it is running.
- Run the Regedit program and find the server configuration registry key as described in section 4.2.1.2. Rename the “Server” key to e.g. “ServerXX”. This will trick the server and the Configuration utility to see this as a new installation and create a new database.
- Start the default server instance
- Run the Configuration utility as described in section 4.1.3 to create a new database.
- In the Regedit program there should now be a new “Server” key with a “DatabaseConnectionString” value that references the newly created database. Rename this “Server” key to match the “servicename” InstallUtil parameter described above.
- Rename the “ServerXX” registry key back to “Server”
- Restart the default service instance. It will now be using the original configuration.

Configuring a service instance

Any additional instance of the server uses a registry key same “level” as the “Server” key. This key must have the same name as the servicename parameter above. So, for the example service created above and when running on 32 bit Windows is using the registry key

HKEY_LOCAL_MACHINE\Software\Theriak\eResept Forskrivningsmodul\eResept Instance1

This key has the same purpose as the "Server" registry key for the default instance, so under each key there should be the "DatabaseConnectionString" string value that is set to refer to the database that the instance should use.

You also need to add another string value, "ApiServicePort" which is the port number that is used for communication between the client(s) and this server instance. This needs to be a unique number for each instance. If missing, the default is 8903 (the default service instance uses this default value, so this number is already taken if that instance is used).

The following images show an example where two additional instances have been installed and configured:

Configuring client connection

The e-resept clients that should connect to an extra instance of the server need to be configured by manually changing the port number to use. See section 4.2.1.1 for where the client registry key is located. The “ServerAddressAndPort” value needs to be changed so the port number matches the port number that is defined for the server instance.

4.2.6 Using multiple application servers for failover and load balancing

If multiple application servers are configured to connect to the same database, the application servers will automatically synchronize and cooperate. A single application server will become “master” and the rest will become “slaves”. Both master and slave servers are capable of servicing the FM client and both run the user management web service (if enabled). Only the master server runs services required by the configuration wizard, scheduled tasks (such as the periodic FEST update) and asynchronous communication (i.e. only the master will process incoming messages).

4.2.6.1 Application server configuration

Each application server can be configured to run as either master or slave. This configuration is done in the Windows registry as documented below:

Operating system	Key value and name
32 bit OS	[HKEY_LOCAL_MACHINE\SOFTWARE\Theriak\eResept Forskrivningsmodul\Server]

	"Role"="*Master*" or "Role"="*Slave*"
64 bit OS	[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Theriak\eResept Forskrivningsmodul\Server] "Role"="*Master*" or "Role"="*Slave*"

If an application server is neither configured to run as master nor slave, it will first attempt to run as the master when started. If a master is already running, the application server will fall back to running as a slave.

4.2.6.1.1 Certificates

Certificates used for communication with external parties and CA certificates need to be installed on each application server computer. It is not sufficient to install certificates on the master server.

4.2.6.2 Client configuration

No special configuration is needed for clients running against multiple application servers. A server address can be configured as described in section 4.2.1.1. On every call, the application server will include a list of all application servers currently running against the same database in the response headers. This list is used by the client to build a list of running application servers and the client will proceed to round-robin between all running application servers.

When the client receives a list of running application servers (whitelist), it stores that list in the system registry in the following location:

Operating system	Key value and name
32 bit OS	[HKEY_CURRENT_USER \SOFTWARE\Theriak\eResept Forskrivningsmodul\Client] "ServerWhiteList"
64 bit OS	[HKEY_ CURRENT_USER \SOFTWARE\Wow6432Node\Theriak\eResept Forskrivningsmodul\ Client] " ServerWhiteList "

When the client is started, it starts by reading the application server address as described in section 4.2.1.1 and from the whitelist if available. The combined list is used as the initial whitelist when the client starts communicating with application servers. This means that if a client is to be configured to run against a new installation (e.g. when switching between production and test environments), the whitelist (and blacklist, see the following section) needs to be deleted from the registry and the ServerAddressAndPort value edited in the appropriate location as described in section 4.2.1.1.

Note that the ServerAddressAndPort value can include multiple addresses, separated by a semicolon ";".

4.2.6.2.1 Server list maintenance

As described above, the client will automatically discover all application servers running on the database being used. The client round-robins between those application servers, providing a simple form of load balancing. If an application server stops responding, the client removes the server from the whitelist and places it in a blacklist. Servers in the blacklist are not used by the client unless no server from the whitelist responds to requests, in which case the client proceeds to retry servers from the blacklist.

Servers from the blacklist normally re-enter the whitelist when they are reported as running to the client, by other application servers.

4.3 Installing e-resept FM on a computer with previous version

When installing a new version on a computer with a previous version of the Prescription Module, it is recommended to first uninstall the version already on the computer.

1. Open the computer's Control Panel, and select Programs and Features. A list of all programs installed opens. Locate the two eResept items in the list:

2. For each entry, right click and select Uninstall:

3. When the uninstall is complete for both eResept Forskrivningsmodul Server and eResept Forskrivningsmodul, the install can be completed as described here in sections 4.1.1 and 4.1.2.

4.4 Monitoring of the FM server

The FM server exposes two types of information to enable monitoring of the status of the server. Status information is exposed as Windows Performance Counters and as WMI instrumentation objects.

4.4.1 WMI objects

The FM Server publishes WMI (Windows Management Instrumentation) instrumentation objects for the application server, all running services and scheduled tasks. Three different WMI object types are available:

- **ServiceInfo** - holds information about running services.
- **ScheduleInfo** - holds information about all schedules.
- **ApplicationServerInfo** - holds information about the FM application server.

The WMI objects are published in the **\root\Thula\FM** namespace. The tables below list the information that each WMI object contains.

	ServiceInfo
Name	Name of the service.
State	The state of the service. Available states: Stopped, Initializing, Started, Error and “Unknown State”.
ErrorMessage	Latest error message.
PreviousErrorMessage	Error message that came before the "ErrorMessage"

	ScheduleInfo
Name	Name of the schedule.
State	The state of the service. Available states: Idle, Running, Error and unknown.
LastRun	Time when the scheduler was last run.
ErrorMessage	Latest error message.
PreviousErrorMessage	Error message that came before the "ErrorMessage"

	ApplicationServerInfo
Name	Currently always shows "Application server".
State	The state of the server. Available states: Stopped, Initializing, Started, Error, “Unknown State”.
Role	Time when the scheduler was last run.
ErrorMessage	Latest error message.
PreviousErrorMessage	Error message that came before the "ErrorMessage"
HasBeenConfigured	Indicates if the server has been configured, i.e. if the connection string value from the Windows Registry is valid and the database has been initialized.
DatabaseConnectionString	The database connection string defined in the Windows Registry (see section 4.2.1.2)
ServiceName	Usually shows “eResept Forskrivningsmodul Server”. When running multiple instances of the FM server on the same computer, this shows the service name as described in section 4.2.5.
ClientApiUrl	Shows the address of the client API, e.g. “net.tcp://localhost:8903”

4.4.2 FM Performance counters

Windows Performance Counters are named counters that can be read by the Performance monitor built into Windows and by system monitoring software.

The FM Server provides performance counters that show the number of messages for each communicating party and each message state. These performance counters are in the counter group "eResept Prescription Module". The following communication parties are shown:

Address Register	Messages sent to the Address Register.
FEST	FEST update messages.
Reseptformidleren	Messages sent to the RF

Sent async	Messages sent asynchronously (through folder-dropping)
Received async	Messages received asynchronously (through folder-dropping)

Messages for each communication party are grouped by the current state of the message as shown in the table below. The name of each performance counter is a combination of the communication party name and the state in the table below, e.g. the counter "Address Register Successful" shows number of Address Register messages that have been sent and replied successfully.

Name	Description
... Duplicate	Number of duplicate messages received since the service was started, i.e. messages that have already been received and processed successfully but are then received again. This only applies to the “Received async” communication party.
... Pending	Number of messages that are pending to be processed. A message should only be in this state for a very short time. If messages pile up in this state, it is an indication of very high load on the server, or a failure in processing messages.
... Sent	Number of messages that have been sent but have not received a reply (AppRec). This only applies to the “Sent async” communication party.
... Successful	Number of messages that have been processed successfully since the service started.
... Failed	Number of messages that have failed to process since the service was started.
... Nacked	Number of NACK messages (negative AppRec) received since the service was started.

4.4.3 WCF performance counters

The Windows Communication Foundation provides a host of performance counters for hosted services, individual service operations and for service endpoints. The most relevant counters for the FM server are in the performance counter group "ServiceModelService 4.0.0.0". These show the communication between the FM server and the clients. A separate instance of this counter is available for every service exposed by the FM server.

Name	Description	Comment
Calls	The number of calls to a service.	This value should steadily rise. Note that if this value stops rising unexpectedly (i.e. not following the set trend), that might indicate a connection problem.
Calls Per Second	The number of calls to this service per second.	Monitor this value to detect trends and fluctuations in the messaging load. Note that if this begins to drop unexpectedly (i.e. not following the set trend), that might indicate a connection problem.
Calls Duration	The average duration of calls to a service.	This value can fluctuate with the overall load on the solution and the load composition. If the calls duration starts to drift above the set trend, this may indicate extreme load or other performance problems.
Calls Failed	The number of calls with unhandled exceptions in a service.	
Calls Failed Per Second	The number of calls with unhandled exceptions in this service per second.	This counter should typically have a value of zero or close to zero.
Calls Faulted	The number of calls to this service that returned faults.	

Calls Faulted Per Second	The number of calls to this service that returned faults per second.	This counter should typically have a value of zero or close to zero.
Calls Outstanding	The number of calls to this service that are in progress.	This value can fluctuate with the overall load on the solution and the load composition. If the calls outstanding start to drift above the set trend, this may indicate extreme load or other performance problems.