Installation Guide Process Platform 6.0

Sub title: Installation Guide for System Architects
Owner: Resultmaker Research & Development
Version: 6.0.1
Revision: 2013-02-24

Anders Nielsen, Lars Pedersen, Carsten Just von Thun

Contents

1 About this document

This document describes how to install a Resultmaker Process Platform™ on a single server but with various options on a multi-server setup. This document will not cover the complete process for installation on multiple servers.

The reader should have some technical background e.g. operations personnel. No programming experience is required to complete the installation.

Since the Resultmaker Process Platform™ requires Microsoft Windows and SQL Server the reader should either have the knowledge to install these or the basis software should be installed by qualified personnel.

If the document is followed from start to end you should end up with a fully operational one-server setup of Resultmaker Process Platform™ fully equipped with sample content[1] and ready for additional content development.

We will conclude the document with a *Where do I go now* chapter explaining the next steps after installation.

2 Requirements overview for Resultmaker Process Platform™

2.1 Resultmaker Process Platform™ version and 6.0

Minimum requirements for hardware and for Microsoft software

- Xeon 3 GHz, 4-8GB ram or equivalent and minimum 50GB hard disk space + Space for Data
- Microsoft Windows Server 2008 R2 64 bit Service Pack 2, web edition or better
- Microsoft SQL Server 2008 64 bit Service Pack 1, standard edition
- .NET 2.0, .NET 3.0, .NET 3.5 and .NET4.0
- Internet Information Server

Software installation requirements for Process Platform™

- A default installation of Windows Server 2008 with IIS and all updates applied
- Http Redirect and IIS 6 Compatibility must be installed
- .NET 2.0, 3.0, 3.5 and 4.0 must be installed and configured correctly (set to Danish culture)
- Install SQL Server 2008 (with Reporting Services) in Mixed Mode
- At least Service Pack 1 must be applied to SQL Server 2008
- A backup job for the user databases and the transaction log. The transaction log should be truncated to save disk space
- Optional installation of a SMTP service

The following is needed for external access

- Optionally but recommended, a domain name and an external IP for the server
- http (TCP port 80) access to the server for browsing and content development
- Optionally https (TCP port 443) to the server for browsing the server securely
- Access from the server to certificate revocation site at crl.certifikat.dk on port 80 (resolves to 62.243.75.213)
- Access from the server to SMTP server on TCP port 25
- RDP (TCP port 3389) access to the server for remote maintenance
- Windows File and Printer Sharing (TCP ports 139 and 445) for accessing the server file system

Information the Installation specialist needs

- SQL Data location, e.g. C:\SQLData
- SQL Log location, e.g. C:\SQLLogs
- SQL Backup location, e.g. C:\SQLBackup
- SQL Instance information, Default or named instance
- SMTP address (only none authenticated relay is supported)
- What websites are used (Id, Name, Location, Host name)

3 Prerequisites for hardware and software

3.1 Resultmaker Process Platform™ version 6

Minimum requirements for hardware and for Microsoft software

- Xeon 3 GHz, 4-8GB ram or equivalent and minimum 500GB hard disk space
- Microsoft Windows Server 2008 64 bit Service Pack 2, standard edition
- Microsoft SQL Server 2008 64 bit Service Pack 1, standard edition
- .NET 2.0, .NET 3.0 and .NET 3.5
- Internet Information Server

The latest generation of the Process Platform™ runs on Microsoft Windows Server 2008 64 bit and Microsoft SQL Server 2008 SP1 as well as R2 versions. Itanium processors are not supported at this time. Both the SQL Server and the OS should be in standard editions or better. We recommend that the operative system is fully updated before installing the database.

Resultmaker applications will run on any hardware supported by Microsoft Windows Server 2008 and the Microsoft SQL Server 2008 64 bit. The higher load on the server expected the better hardware should be installed.

3.1.1 Application server

The application server is both the frontend and the backend server. A fair starting point for the application server is a single core Xeon 3 GHz, 3-4 GB ram and around 50GB hard disk space. It is advised to setup the hard disk in a raid. The raid should be any raid that secures the data, e.g. raid 1 or 5. Setting up the hard drives in a RAID setup is an optional procedure, not described in this document.

3.1.2 Database server

Most of the components in the Resultmaker Process Platform™ use a database. The most intense work in the system will also happen on the database server. This is why the hardware recommendations are higher. We recommend using a dual core Xeon 3 GHz with 6GB ram and 500 GB hard disk space. As for the application server it is recommended that the hard disk is in a raid setup. The actual space needed depends a lot on load and scaling.

4 External access

The following is needed for external access

- Optionally but recommended, a domain name and an external IP for the server
- http (TCP port 80) access to the server for browsing and content development
- Optionally https (TCP port 443) to the server for browsing the server securely
- Access from the server to certificate revocation site at crl.certifikat.dk on port 80 (resolves to 62.243.75.213)
- Access from the server to SMTP server on TCP port 25
- RDP (TCP port 3389) access to the server for remote maintenance
- Windows File and Printer Sharing (TCP ports 139 and 445) for accessing the server file system.

In order for users and process consultants to access the server to full extend the standard installation may not be sufficient.

There are basically two approaches: One way is to access the server by the server name (or internal IP), and another way is to assign a domain name and an external IP address to the server.

The first approach is commonly used in smaller networks for internal demonstration purposes. The second approach is commonly used when external customers need access or in case that the company is separated in more than one internal network. In both cases configuration modifications are needed post install. Please refer to the section called *Post installation configuration* for more information.

The firewall openings for both approaches are *http (port 80)* and optionally *https (port 443)*. The https protocol is not required and will require a server certificate installed. The installation is explained in the section *Installation of Resultmaker applications*.

If the server certificate is installed or if client certificates are used, access from the server to revocation servers is needed. For Danish certificates this server is *crl.certifikat.dk* (resolves to 62.243.75.213) which is accessed on port 80. This can be verified directly in the certificates and might change.

Resultmaker applications and the customer solutions developed on the server will most likely need to send emails. This can either be error mails or in the customer solutions *invitation* mails. In both cases a *SMTP server* is needed. The SMTP server must be setup to accept relay from the installed server. The regular SMTP port is used which is port 25. Please also note that authentication is not supported and restricted access e.g. by IP to the SMTP is recommended. Alternatively a SMTP service can be installed easily on the server itself. This is not recommended since mail send from the server have a higher chance be caught in SPAM filters.

The process consultant or server maintenance personnel will most likely need Remote Desktop and Windows File and Printer Sharing access to the server. Remote Desktop is needed because the server will probably be installed this way. Windows File and Printer Sharing access may be needed to update files on the server. These files can be images or other content or in relations to server maintenance.

For these reasons it is advised that the firewall is opened so Remote Desktop and Windows File and Printer Sharing access is allowed. The default port for the Remote Desktop Protocol (RDP) is TCP 3389. The main ports for Windows File and Printer Sharing are TCP 139 and TCP 445. *Since this is considered a dangerous protocol from a security point of view it is advised to allow it with caution.*

5 Architectural server setup

This section will go over an architectural server setup, which can be used as inspiration for building a multi-server setup. The section is an addition to the documents premise of a single server setup. If you are setting up a single server, some elements of this section may not apply to you. We work with three different types of servers, Frontend, Backend and Database.

5.1 Frontend

The frontend holds the .NET web application which the end user sees. It communicates with the Backend server through http (TCP port 80) and with the Database server through SQL (TCP port 1433). The Frontend might also have several custom integrations to external systems. This is usually through secured web services. The end user connects to the Frontend through either http or https in cases where an SSL server certificate has been setup. SSL is recommended to ensure a secure communication between the Frontend and the end user. The Frontend server should be placed in a DMZ and should not be exposed to any other communication other than http or https. The end user might log in with a certificate but this does not require https.

5.2 Backend

This server is the core of the Resultmaker Process Platform™ and should be deployed in a secure environment with very strict access. All communication within the backend server is per default not encrypted and neither is the communication with the Database server (TCP port 1433).

If it is preferred that the internal communication is encrypted this can be setup. As on the Frontend server, custom integrations to external systems can be setup and they may communicate encrypted and through https.

5.3 Database

The Database server does not hold any Resultmaker Process Platform™ specific software. Instead it holds databases used by Frontend and Backend servers. The database never initiates connections and should not be allowed to either.

5.4 Architectural drawing

Below is an example of how a three server setup can be. In this setup we see external systems as being remote services. These systems could instead be located either directly on the servers or within the same company network. In this case https might not be required. In other cases where external suppliers are used the choice of http or https might be fixed. This goes for standard integrations to the Danish CPR and CVR. In these cases the suppliers have defined what security scheme should be used, which at the moment is proprietary security schemes with use of username and password for CPR and certificate based WS-Security for CVR.

The setup presented below does not illustrate load balancing even though The Process Platform™ can out of the box be load balanced on the frontend server and the database server. The database server can implicitly be load balanced through a cluster. The backend server consists of several web services which each can be divided out on separate servers.

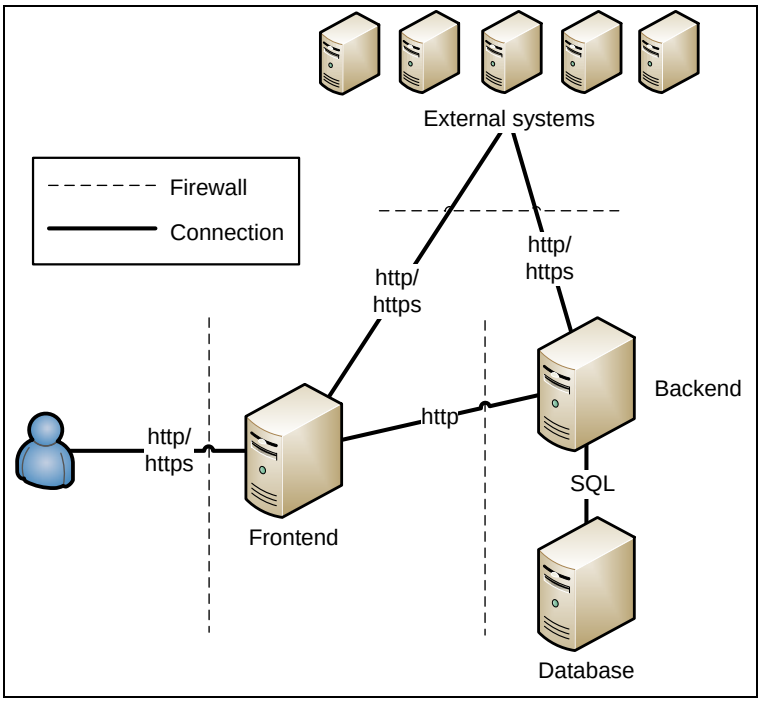


Figure 1: Basic three server setup with external integrations 6.0

7 Microsoft software installation – Process Platform™ v6.0

The basis of Resultmaker applications is Microsoft Windows Server 2008 R2, Internet Information Server, .NET and SQL Server 2008. The Resultmaker applications have been tested and verified with a default installation of the Microsoft components and special setups may or may not interfere.

Software installation requirements for Process Platform™ version 6

- A default installation of Windows Server 2008 with IIS and all updates applied
- HttpRedirect and IIS 6 Compatibility must be installed
- .NET 2.0, 3.0, 3.5, 4.0 must be installed and configured correctly (set to Danish culture)
- Install SQL Server 2008 (with Reporting Services) in Mixed Mode
- At least Service Pack 1 must be applied to SQL Server 2008
- A backup job for the user databases and the transaction log. The transaction log should be truncated to save disk space
- Optional installation of a SMTP service

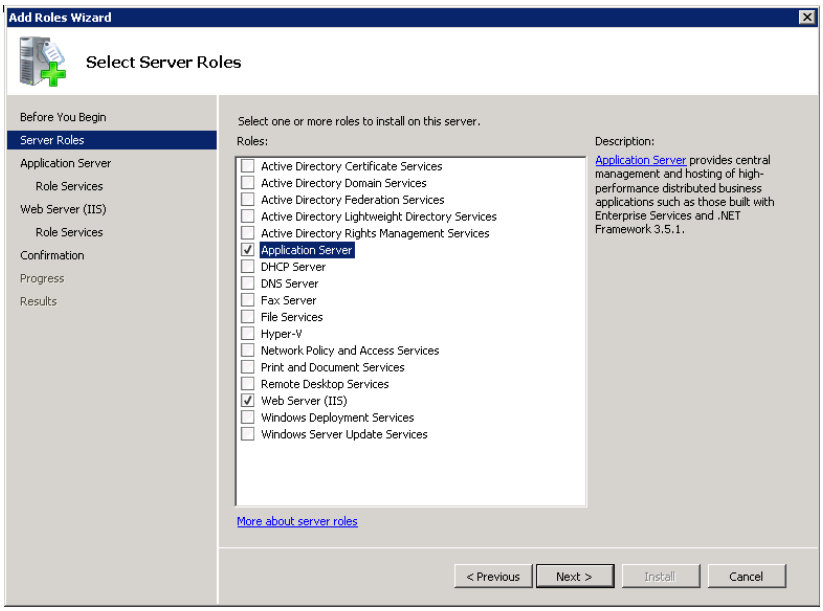
Information the Installation specialist needs

- SQL Data location, e.g. C:\SQLData
- SQL Log location, e.g. C:\SQLLogs
- SQL Backup location, e.g. C:\SQLBackup
- SQL Instance information, Default or named instance
- SMTP address (only none authenticated relay is supported)
- What websites are used (Id, Name, Location, Host name)

7.1 Step 1: Microsoft Server 2008 and IIS

Microsoft Windows Server 2008 should be installed in the English edition. All current updates and Service Packs should be applied and the Internet Information Server (IIS) should be installed. It is expected that the Program Files folder resides in ***C:\Program Files*** and the IIS wwwroot resides in ***C:\Inetpub\wwwroot***. If this is not correct Resultmaker applications installation will not complete.

Add roles and features to the server as shown by the following screenshots:



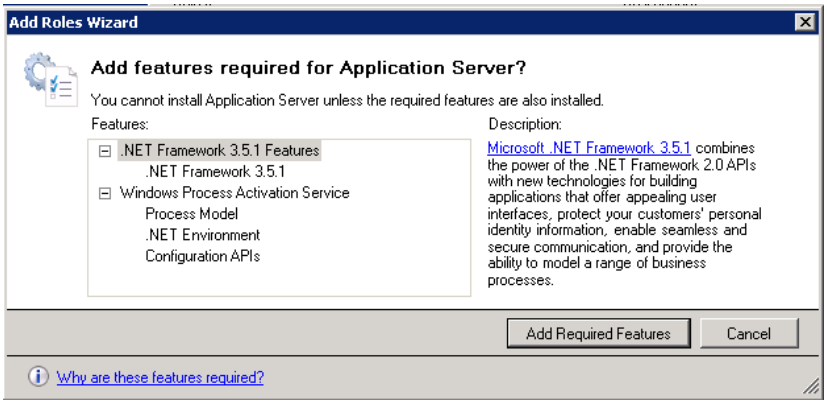


Figure 2 - When selecting "Application Server" this window appears

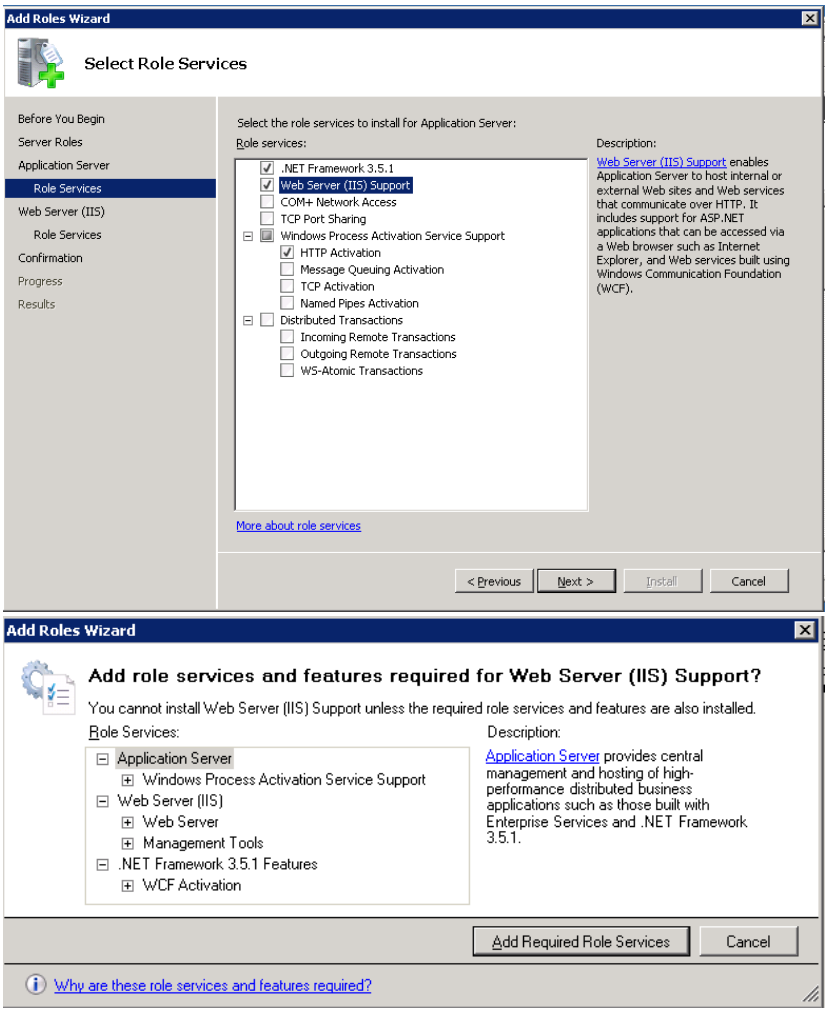


Figure 3 - When selecting "Web Server (IIS) Support" this windows appears

Please make sure that **Web Server (IIS) - Role services** is setup accordingly to the table below. Notice that all marked with ***Install*** are required while blank cells are optional.

WEBSERVER		
	Common HTTP Features	
		Static Content	Install

		Default Document	Install
		Directory Browsing	Install
		HTTP Errors	Install
		HTTP Redirection	Install
		WebDAV Publishin	
	Application Development		
		ASP.NET	Install
		.NET Extensibility	Install
		ASP	Install
		CGI	Install
		ISAPI Extensions	Install
		ISAPI Filters	Install
		Server Side Includes	Install
	Health and Diagnostics		
		HTTP Logging	Install
		Logging Tools	Install
		Request Monitor	Install
		Tracing	Install
		Custom Logging	
		ODBC Logging	
	Security		
		Basic Authentication	Install
		Windows Authentication	Install
		Digest Authentication	Install
		Client Certificate Mapping Authentication	Install
		IIS Client Certificate Mapping Authentification	Install
		URL Authorization	Install
		Request Filtering	Install
		IP and Domain Restrictions	Install
	Performance		
		Static Content Compression	Install
		Dynamic Content Compression	Install
	Management Tools		
		IIS Management Console	Install
		IIS Management Scripts and Tools	Install
		Management Service	Install
		IIS 6 Management Compatibility	Install
		IIS 6 Metabase Compatibility	Install
		IIS 6 WMI Compatibility	Install
		IIS 6 Scripting Tools	Install
		IIS 6 Management Console	Install
	FTP Server		
		FTP Service	
		FTP Extensibility	
	IIS Hostable Web Core		

7.2 Step 2: Installation of Microsoft .NET framework (3.5.1 and 4.0)

7.2.1 .Net Framework 3.5.1 installation

Microsoft .Net Framework 3.5.1 is installed during the IIS installation. (see above).

To install .NET 3.5.1 enter the ***Server Manager > Features > Add Feature Wizard*** and check the ***.NET Framework 3.5.1 Features***. This will give you a dialog as shown on the below image.

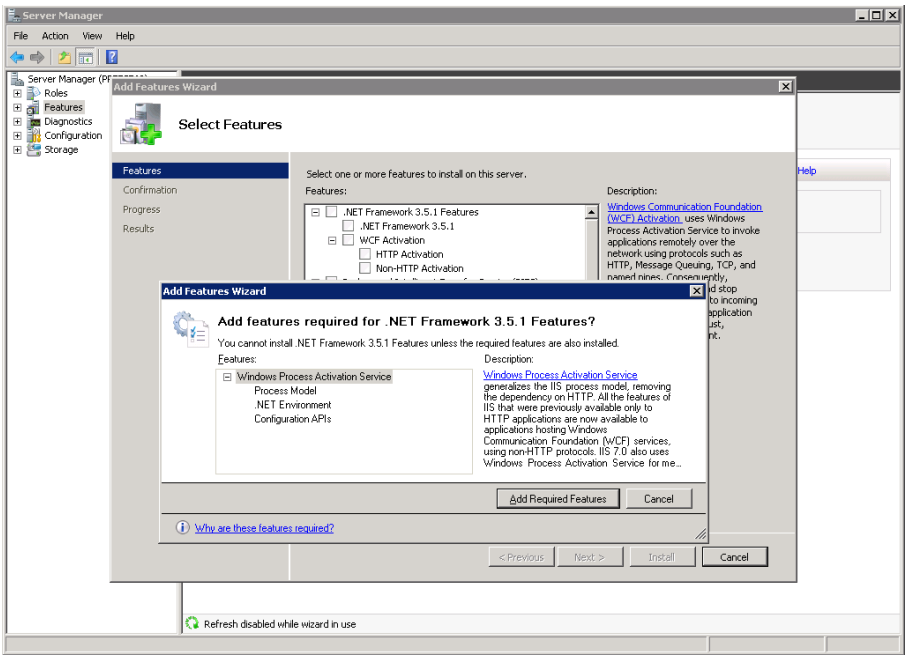


Figure 1: Adding .NET 3.5 Feature

This will result in all .NET Framework 3.5.1 Features will be enabled

Figure 2: .NET 3.5 enabled

To make sure that date and time formats are handled correctly in the system configuration to the ASP.NET is required. The Culture settings must be set to ***da-DK*** and UI culture to ***da***. This is done from the IIS management console by selecting the ***Default Web Site*** and double clicking the ***.NET Globalization*** icon. The settings should be setup as below picture.

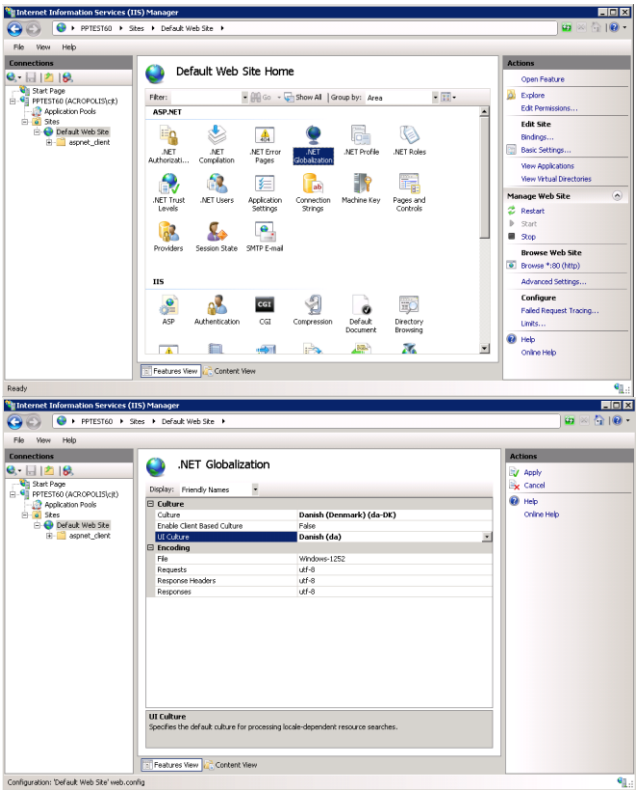


Figure 3: Setting Culture settings in .NET in Windows Server 2008

7.2.2 .Net Framework 4.0 Installation

.NET 4.0 also needs to be installed. After download from the Microsoft website (search for **dotnetfx40_full_x86_x64.exe**) and installation you must go to the IIS Manager and activate .NET 4.0 as described below.

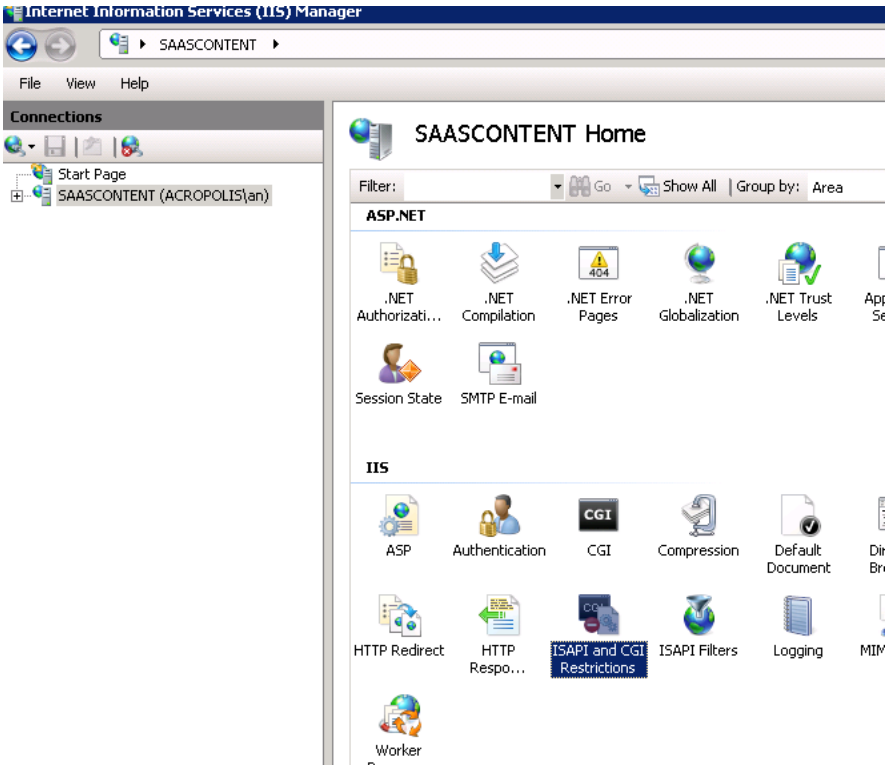


Figure 4: How to find the ISAPI and CGI Restrictions

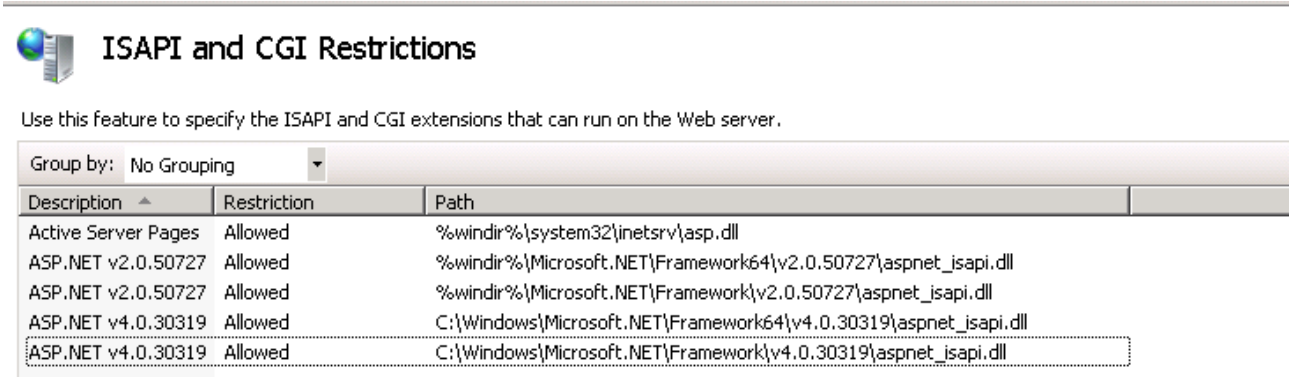


Figure 5: It's the two Restrictions in the bottom that needs to be Allowed

7.3 Step 3: Website preparation

Depending on the Architectural server setup that is decided it might be needed to prepare the Application server(s) for installation.

7.3.1 Split frontend and backend server setup

In a split frontend and backend server setup the frontend is on one server and the backend is on another. It does not matter if the SQL server is on a separate server or not.

The split setup works out of the box and the default setup for the Installation specialist does not needs to be changed.

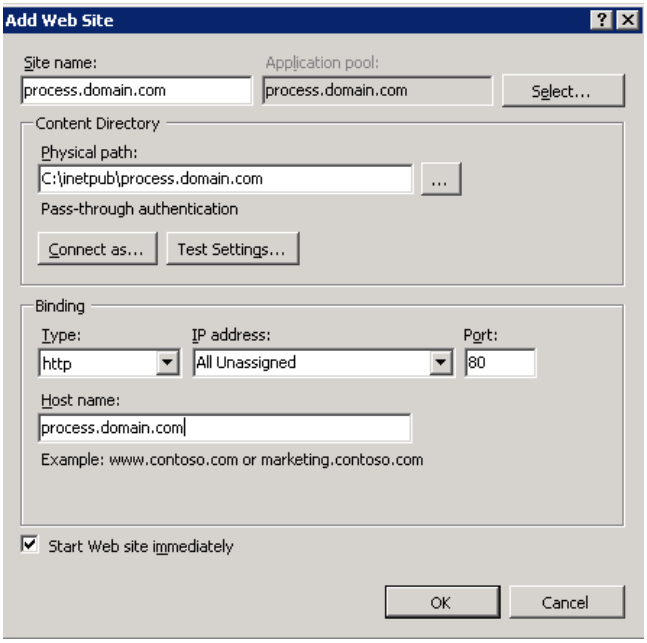
7.3.2 Combined frontend and backend server setup

When the frontend and backend server is on the same server the web application needs to be separated for security purposes. It should never be allowed for the end user to have access to the backend applications.

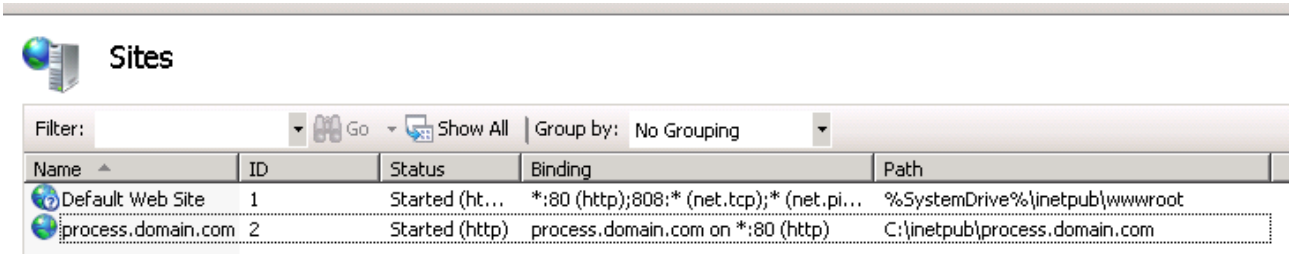
7.3.3 Creating a new web site

Please use the following procedure when creating a new web site.

Go to IIS > Sites > Add Web Site… > Fill out the dialog



Please note that the best practice is to use the same folder name as the web site name. Host name binding is optional and depends on setup. How to bind web site to host names is not covered by this manual. After clicking OK, the following information will be shown.



Please note that **only** port 80 is supported for backend applications and both port 80 and 443 (https) for frontend applications.

7.3.4 What the Installation specialist needs to know

The Installation specialist needs to have full information about all the web sites in the installation

- Web site Id
- Web site Name
- Web site default folder
- Host name used to access the site

7.3.5 Adding security

If the backend and frontend is on the same server IP security should be added so only the server itself can access the backend applications.

This is done at [Web site name] > IP Address and Domain Restrictions

This is explained in more details at **Installation of Resultmaker applications and databases > Step 4: Optional: Setting up web site security**

7.4 Step 4: Microsoft SQL Server 2008

Resultmaker Process Platform supports both the Standard and the Enterprise editions. The SQL Server 2008 must be installed in Mixed Mode and there is no requirement for what the *sa* password is. There are also no requirements for what user the SQL Server runs under. It is recommended to run it under Local System for easy installation. Reporting services must also be installed and the default names for web folders and database names should be used. The collation must be set to ***Danish_Norwegian*** to make sure that the system and user databases are in sync.

The following features must be enabled during the installation

- Database Engine Service
- Reporting Services
- Client Tools Connectivity
- Client Tools Backwards Compatibility
- SQL Server Books Online
- Management Tools – Basic
- Management Tools – Complete

The Process Platform™ supports any file setup for databases and they can be at any drive. For installation purposes the installation specialist needs full information about the location of the databases.

- Data location, e.g. C:\SQLData
- Log location, e.g. C:\SQLLogs
- Backup location, e.g. C:\SQLBackup

With this information he can prepare automated scripts that will install the databases in correct locations. SQL instances is also supported, and information about this should also be given before installation

If the SQL Server 2008 installation does not include Service Pack 1 you must apply the Service Pack 1 manually at this point.

To make sure that the SQL Server runs a smoothly as possible it is advised to setup backup maintenance jobs. These should backup the user databases and logs. Afterwards the transaction log should be truncated. Failing to do this may have the server run out of hard disk space too fast.

7.5 Step 5: Optional: Installation of SMTP Service

Resultmaker applications will need a SMTP Server to work properly. The mail sending is used for invitation mails and other system mails. This step is optional because it is not required that the SMTP service is installed on the server itself. Another way of handling mail sending is by using a company mail server. If using a company SMTP server make sure that it do not require authentication, that it allows mail relaying and that there are no firewall blocking the traffic to the SMTP server from the server holding the Resultmaker applications.

If you instead choose to install SMTP service on the same server you should follow this procedure. To install smtp service go to ***Server Manager > Add Features > SMTP server***.

When this is completed you will have a working SMTP Service with default settings. Please be aware that some recipient mail servers do not allow this simplified way of installing a SMTP server which may lead to blocking of mails. If this procedure does not work it is advised to use a company SMTP server instead.

7.6 Step 6: Handling Windows Updates

Default installations of the operative system will have Windows Updates to automatically download and install updates. This will also result in an automatic restart of the system which might come at an inconvenient time of the day and week. It is considered best practice on a production environment to have a fixed service window for installing the update and for restarting the server thus disabling automatic installation and restart. It is not recommended to just disable restart and continuing updating since this might clutter the server in the long run.

In most cases the server will be part of a domain which probably will control the updates. It is the policy for the server these setting must be changed. For servers outside domains changes to registry might be needed. How to setup domain policy or server registry is not covered by this document.

8 Installation of Resultmaker applications and databases

The installation process is divided in steps and it is important that the steps are followed one by one and that a step is not skipped. Failing to execute the installation in the defined steps may lead to an unsuccessful installation. If you are planning to clone the server post installation you should read the next section “Using virtualization and server cloning” which explains that method of server installation. For a first time installation or no cloning you should proceed ahead in this section.

8.1 Step 1: Resultmaker databases

First step is to install the Resultmaker databases which all come in a single SQL script. This script will create a series of databases and assign a user to them. All the access rights from the applications to databases are handled in the script.

The SQL Server gives several options for what recovery mode the databases should run under. We recommend using the *Full recovery mode* as this will give the best data security.

8.2 Step 2: Resultmaker applications

The next step after a successful installation of databases is to install all the Resultmaker applications. To aid you with this the Resultmaker applications is prepared with a proprietary tool which generates deployments packages. A package is a folder containing a series of scripts in a hierarchy of folders. A package for an environment thus will consist of a folder containing subfolders. The following procedure must be followed when installing a package.

1) First copy the folder to the server. It may be a good idea to also copy the folder to other storage facilities for record keeping purposes.
2) Run the file ***_setup.cmd*** by ***right clicking*** it and selecting “Run as administrator” or running it from the command prompt, which must also be “Run as administrator”.
    a. This *must* be done from the server itself. You cannot run the script from a share due to security settings in windows. Also make sure that you have full administrative rights to install on the server.
    b. The file must be run in its own file context. This means that you cannot copy the path to the file and run it from “Run” in the start menu, or in a command prompt (without being in the folder where the file is). The reason for this is that the _setup.cmd file contains relative references which might not work.
    c. A command prompt will show and the script will start executing. Most of the time you will see something happening from installers running in passive mode (without user interaction) but you might also experience no response from script at all. In these situations just wait, or see step 4 for a way to determine if the script is still running.
    d. The script is designed not to require user interactions but there are two exceptions.
        i. When applications are being uninstalled the script may be set to prompt the user. This will require an OK from the Okay/Cancel box. In these situations you must be suspicious of three things. Are there multiple applications in the dialog? Are one or more of the applications to be uninstalled not a Resultmaker product? Does the uninstall action seem unintended?
        ii. External applications may not support passive installations which may require user interactions.
3) During the execution of the script a log file will be generated. If in doubt if the script is running the log file size can be monitored, if it increases the script is running for sure. If it’s not increasing at all for a longer period of time (10 minutes) the script could be failing and Resultmaker should be consulted. Otherwise you can uninstall all applications and start over again.

4) When the script is done the installation log will be presented to you. The log is raw and unformatted in regard to error handling. Searching for the word ***fail*** gives a good impression whether the script ran successfully, but the word fail can appear in the log without the script having failed. If there is reason to believe that the script has failed, the log can be sent to Resultmaker for analysis.

When all scripts are completed on all servers, the base installation is complete.

8.3 Step 3: Optional: Setting up security for Helper Services and Audit Trail System

Resultmaker Process Platform™ comes with two helper solutions to aid system administrators and platform support personnel. They are called *Helper Services* and *Audit Trail System*. Explaining how to use these two applications goes beyond the scope of this document but is explained in supplementary operations documentation.

To setup security first create a local windows user. The username and password will be needed each time a user tries to use the Helper Services or Audit Trail System. Optionally the user can have the password set to "***never expires***" and "***unable to change password***". After the user has been created anonymous access must be disabled and integrated security must be enabled for each of the two web sites. The users must also have permission to the web sites which is done by ***right-clicking*** the web site ***(ATS/HelperService)*** in the ***IIS*** and choose ***permissions***. From here the above user should be added with ***read*** access (default access when adding the user). The access should be tested externally to confirm that it is correct.

8.4 Step 4: Optional: Setting up web site security

If you are installing the Process Platform backend applications on the same server as the frontend application you potentially have a security issue. Even though it is best practice to install on multiple servers with high quality firewall as security it is not required. In many setups it is decided to use a ***single-server-setup***. In this kind of setup it is highly recommended to implement a security scheme which shields the backend applications from the end user. The simple way to do this is to setup an extra web site so you would have the ***Default Web Site*** and a custom web site holding the frontend applications.

8.4.1 Requirements

- The deploy tool scripts must be setup to use multiple web sites
- A dedicated hostname for the frontend site

Deploy tool scripts

Before installation of the Process Platform applications, make sure that you have is correct and multiple web site supported scripts. If not the frontend might redirect to a false URL when called.

Dedicated hostname

You will need a dedicated hostname for the frontend site in order to implement this security scheme. This is needed for the IIS to route the traffic to the correct web site. The Process Platform will try to call the backend applications on http://127.0.0.1/ meaning that the Default Web Site must have a blank header section meaning no required hostname filter. The dedicated hostname, which could be looking like this "process.mydomain.com", is applied in the deploy tool scripts by Resultmaker or the associated partner.

8.4.2 Setting up the Frontend site (IIS 7.x – Windows Server 2008)

First you must create a new web site. This is done from the IIS management console. You will be able to specify the host header for the site which must be the same as the name described above. The usual name for the web site is the same name as the hostname. Set the web site to use .NET 2.0 runtime (classic pipeline mode) when defining the Application pool.

You will now have two web sites where the frontend web site is empty and needs to be filled up.

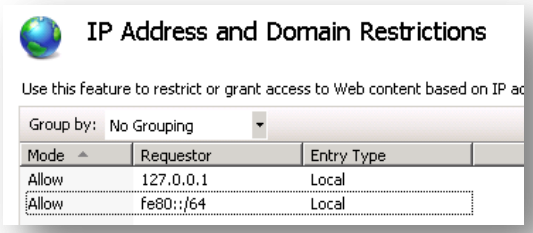
Right click the web site and add new virtual directories / applications with below settings.

Alias	Path	Type
RMFrontend	[DefaultWebSiteRootFolder]\RMFrontend	Application
static	C:\FileRepository\public\static	Virtual Directory
public	C:\FileRepository\public	Virtual Directory

Setting up IP security

Go to the Default Web Site, double click IP Address and Domain Name Restrictions.

- Right click, select **Edit Feature Settings…** and set the value for **Access for unspecified clients** to **Deny**.
- Right click, select **Add Allow Entry…**, set **Specific IP address** to **127.0.0.1**, click **OK**
- Right click, select **Add Allow Entry…**, set **IP address range** to **fe80::** and **Mask or Prefix** to **64**, click **OK** *(this is a IPv6 address with a mask). The latter is found by doing a IPConfig from a command prompt.*



Figur 6 - End result

8.5 Step 6: Optional: Changing the timeout settings

In the Frontend it is normal behavior to be warned about an upcoming session timeout. This looks similar to the dialog box in Figure 7.

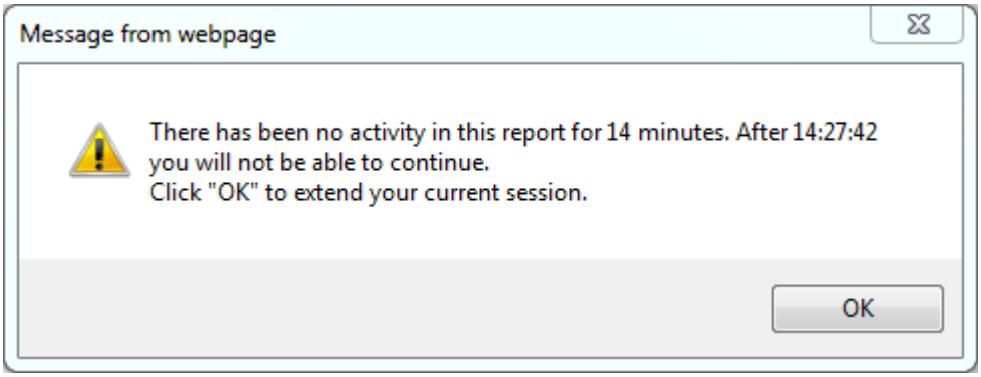


Figure 7 Session timeout warning after 14 minutes idle time (roughly 75% of 20 minutes)

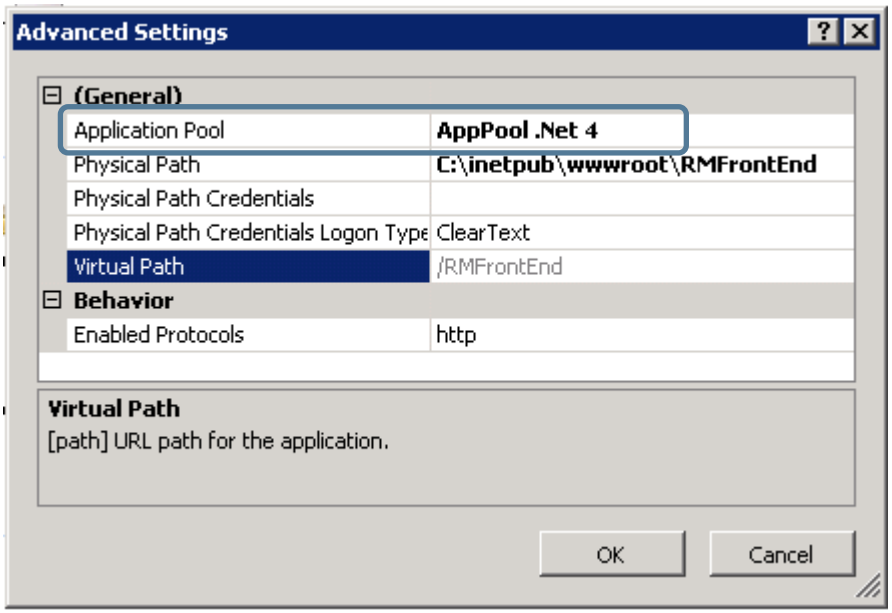
The warning appears when 75% of the timeout period has elapsed and there has been no activity on the page. In the example the timeout is 20 minutes, which is the default installation setup. By clicking OK in the dialog box, the timeout period is renewed.

The settings that need to be controlled in order to prolong or shorten the timeout settings are the App Pool Idle Time-out and the ASP.NET Session Timeout.

Session timeout specifies the number of minutes a session can be idle before it is abandoned. The timeout attribute cannot be set to a value that is greater than 525,600 minutes (1 year) for the in-process and state-server modes.

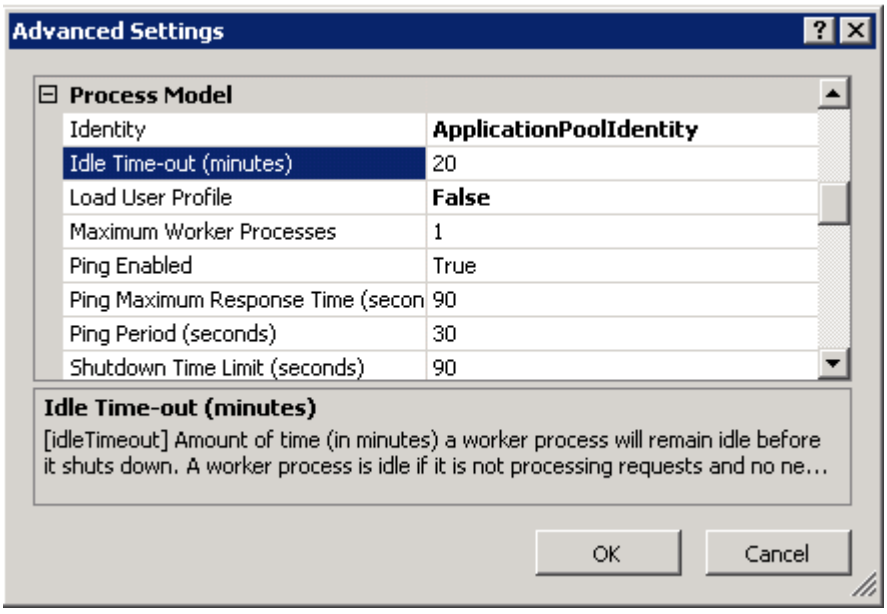
Application Pool – Idle time-out is the amount of time in minutes a worker process will remain idle before it shuts down. A worker process is idle if it is not processing requests and no new requests are received.

The App Pool Idle Time-out can be seen and changed in the Advanced Settings of the application pool running the Frontend web application. Find the application pool running the Frontend in the IIS RMFrontend applications Advanced Settings.



Figur 8 Advanced IIS Settings for RMFrontend web application

Once the name of the application pool is identified, open the Advanced Settings for that application pool.



Figur 9 Advanced IIS settings for an application pool

Here the Idle Time-out can be modified.

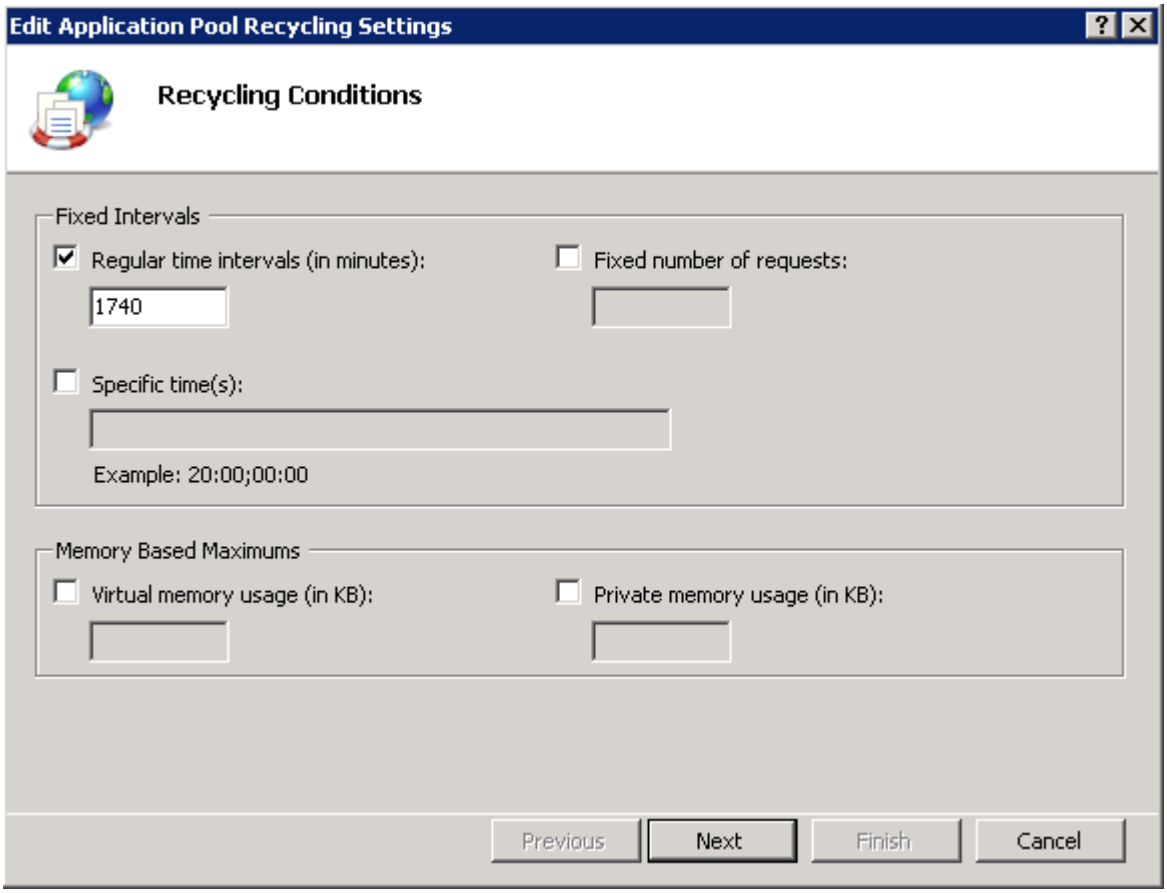
The session timeout can be seen and modified in the web.config in the sessionState node.

```
<system.web>
   <sessionState timeout="20" />
<system.web>
```

It is possible to see the current time-out settings on the SelfCheck page:

http://[PPServer]/RMFrontEnd/SelfCheck.aspx

Apart from that the App Pool is recycled by the IIS on a regular basis, which is normally once every day. This means that the session can be torn down and the user can experience a sudden loss of session. In order to mitigate such problems in production use, it is possible to set the Recycle conditions, so that the recycling occurs at night or another more convenient time. This is done in the application pools Recycling Settings.



Figur 10 Application Pool Recycling Setttings

8.6 Step 7: Optional: A SSL certificate can be installed

When the first two steps have been completed the platform has been installed but you may want to enhance the user experience by installation a SSL Certificate as well. This part is optional but will make sure that the use of the platform is secure to the end user.

In this document we will describe two ways on how to request and install a SSL certificate. When obtaining a new certificate a request file must be generated from the server. First go into the ***Internet Information Server Management Console*** and locate the ***Default Web Site***. ***Right click*** and choose ***properties*** and select the ***Directory Security*** tab.

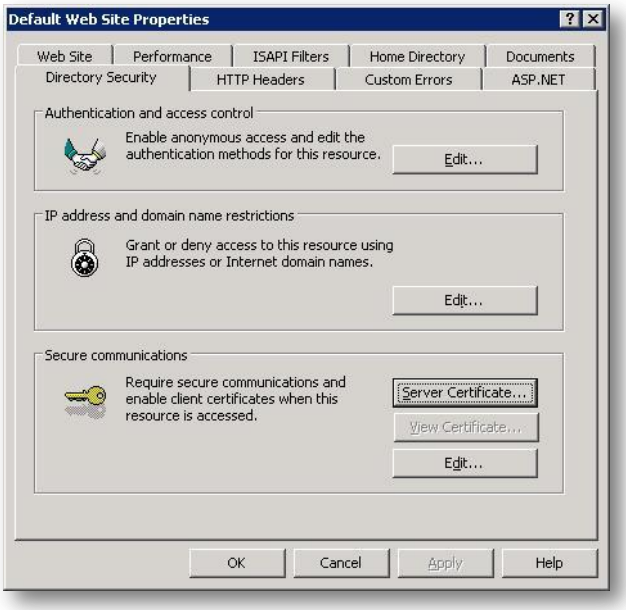


Figure 11: Directory Security in IIS. Click Server Certificate to start the installation process

After clicking the button as displayed above go through the guide as displayed in these two images.

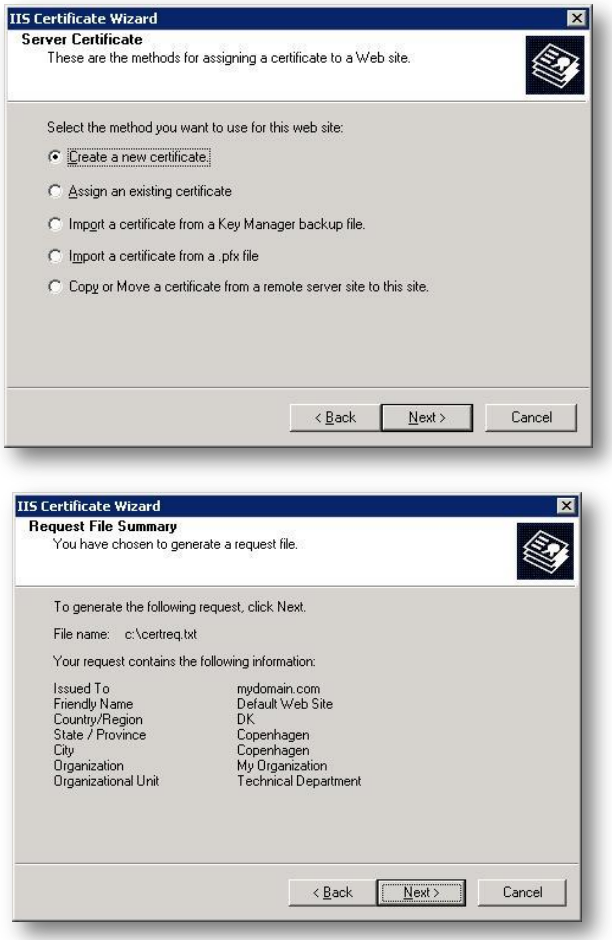


Figure 12: Displayed two of the dialogs in the Request a new SSL certificate process

As you can see we have put in dummy info in this request. You should be aware that the *Issued To* (called common name in the process) is a very important field. This field denotes what domain the server should hold. Failing to do this correctly may lead to false certificate that will display an error for the end user.

When the request has been completed and the SSL certificate of choice have received the request, they will generate a certificate response. This is processed through the same interface as where you requested the certificate, but now the options will look like the below image.

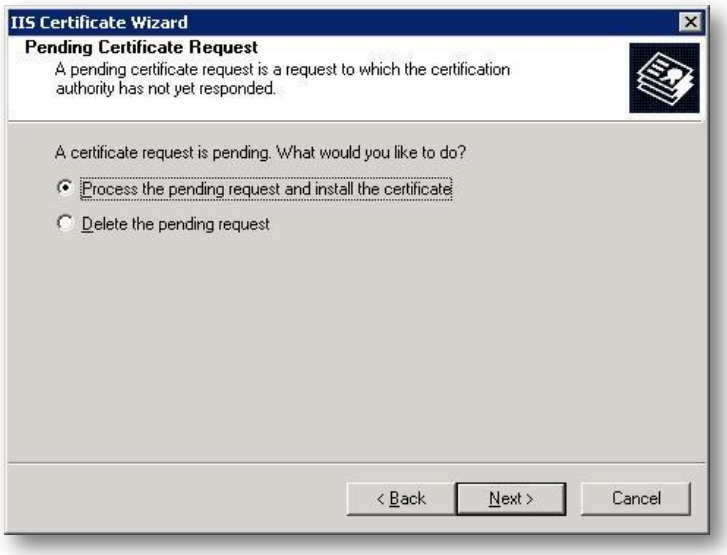


Figure 13: Shows the Pending Certificate Request dialog

The process is straight forward now and you should use the default port for SSL. When the process has been completed the SSL certificate is ready to use by typing ***https://servername*** in the browser.

8.7 Step 8: Optional: Client tools can be installed

The main installation does not include client tools (Resultmaker Process Designer?) and they must be installed separately if needed. It is possible to install the client tools directly on the server. This can be beneficial in situations where the server is used for demonstration and network connections can be an issue. The common way to use the system is by installing client tools on client machines though. How to install these tools are described in supplementary documentation which also covers basic usage of the client tools.

To sum up the following needs to be done

- Deploy Resultmaker databases
- Use the installation script to install all the Resultmaker applications
- Change the settings for the Event Log
- Optionally set security for Helper Servicers and ATS
- Optionally install a SSL Server Certificate to facilitate secure browsing (https)
- Optionally install client tools directly to server for easy testing and demonstration purposes

8.8 Step 9: Optional: Installation of Process Platform™ Front End in SharePoint

This section covers the steps needed to enable the Process Platform™ Frontend in Microsoft SharePoint 2007. Before starting this enabling you must have a fully installed Microsoft SharePoint 2007 on application server used as frontend server. The Process Platform™ Frontend runs in a Web Part in the SharePoint site collection.

8.8.1 Installation

First step is to install the SharePoint site collection application in the default SharePoint installation. This will be used as a base for the Frontend installation. In most situations this is enough to prepare the installation of the Process Platform™ Frontend. If you are using Resultmaker Deploytool to setup your environment SharePoint Frontend application should piggy back a SharePoint Stub in Resultmaker Deploytool. The SharePoint stub in the Deployment Tool has a path, which should point to the installation location of the SharePoint site collection on the server. The SharePoint Front End, uses this path and installs itself inside the same site collection. It then merges some configuration settings into the web.config file of the site collection.

8.8.2 SharePoint configuration

After the installation SharePoint needs to be configured. To be able to run the SharePoint Front End as a Web Part in the SharePoint site collection, it is required to give all the Front End assemblies *"Full Trust"*. If you install the SharePoint Frontend on a fresh install of Microsoft SharePoint, you do not need to do anything before running the Deployment Tool install script. The install script will edit all the settings for the Web Part to run, and it will copy a new Code Access Security policy file onto the server, which has all the Front End assemblies specified with Full Trust.

If you install the SharePoint Front End on a site collection, where you or someone else already installed other 3rd party Web Parts or applications, they might have changed the security settings and policy file as well. If this is the case, then you cannot just run the Deployment Tool install script, because it will use a new security policy file, which does not contain the security settings of the already installed Web Parts and applications. Instead you must merge the included security settings for the Frontend into the policy file already in place – or the other way around.

In the *web.config* file there is a *securityPolicy* section, where the policy files are referenced. The path to the securityPolicy element is: ***configuration/system.web/securityPolicy***. Here the Deployment Tool script will create a new trustLevel element, which points to the new policy file.

To find out which policy is used by the site collection, find the *trust* node, which is also inside the system.web section of the web.config file. Here you define which level to use and you can refer to the trustLevels defined in the securityPolicy node.

When the Deployment Tool script is run, a trustLevel called *WSS_Minimal_Resultmaker* is created, and it is also set as the current trust level. As the name of the trust level implies, the policy file is based on the WSS_Minimal policy file, which is the default trust level used for a new SharePoint installation.

8.8.3 Inserting OCFrontEnd-hosting Web Part into the Web Part Gallery

1. Open the default SharePoint web page in the browser (typically ***http://[COMPUTERNAME]***).
2. Open ***Site Actions / Site Settings***
3. Find ***Galleries*** column and click ***Web Parts*** to display Web Part Gallery. If the "Web Parts" is missing in the Galleries part, select the ***Go to top level site settings*** in the ***Site Collection Administration*** section.
4. Click ***New*** on the Web Part Gallery list.
5. Find ***Resultmaker.OC.FrontEnd.WebParts.ResultmakerOCFrontEnd*** entry on the list of available Web Parts (typically the last entry on the list) and ***mark*** its checkbox. Optionally, its default name ***ResultmakerOCFrontEnd*** preceding the ***.webpart*** extension may be changed to any other name. This name will be used later to reference this Web Part.
6. Click ***Populate Gallery*** button at the top of the list. The newly added Web Part should now be visible in Web Part Gallery.

8.8.4 Adding OCFrontEnd-hosting Web Part to the web page

1. Go to the web page where the OCFrontEnd has to be displayed (if the page doesn't exist yet, first create a new one as "***Web Part Page***"; this is beyond the scope of this document to describe how to do it).
2. Click "***Add a Web Part***" on the page area where OCFrontEnd Web Part is to be added.
3. Find ***OCFrontEnd Web Part*** by its name in the pop-up list (typically in ***All Web Parts / Miscellaneous*** section). ***Mark*** its checkbox and click ***Add*** button. The newly added Web Part should now display its name on the page that it has been added to.
4. Click ***edit*** on the right of the added Web Part to edit its properties if needed (beyond the scope of this document).
5. Click ***Exit Edit Mode*** in the upper-right corner of the page.
6. The OCFrontEnd Web Part should now display its content. If it does not, remove ***?PageView=Shared*** from the address bar and press ***Enter*** to open the modified address.

9 Installing and maintaining certificates

This section describes what actions need to be taken when installing and maintaining certificates on a Resultmaker Process Platform™. The reader should have basic system administrator knowledge on Microsoft Windows Server 2003 and especially how to use the Management Console (MMC). He should also be familiar with X.509 certificates. All screenshots have been created in Microsoft Windows Server 2003.

9.1 Certificate basics

An X.509 certificate is used for two main purposes, to sign and to encrypt data. This is done by the usage of the private-public key pair contained in the certificate. Either one of the two keys in the key pair can encrypt data so that only the other key in the key pair can decrypt the data.

The private key is only known and held by the certificate owner while the public key is known to *everyone*. Everyone is this context means people that the certificate owner communicates with. Both the private key and the public key are *globally* unique.

The procedure for sending signed and encrypted data to a recipient where both the sender and recipient have a certificate is as follows.

First let us go over the signing part. The sender uses his private key to sign the data. Then he sends the data to the recipient who is able to verify the signing of the data using the sender's public key.

Since the sender is the only one who has that private-public key pair the recipient is able to verify the signing.

Second part is the encryption data. The sender this time takes the recipient's public key and encrypts the data. He then sends the data to the recipient who can decrypt the data using the recipient's private key.

Since he is the only who has that he is the only one who can decrypt the data.

These two actions are then combined into the following steps. Sign with sender private key, encrypt with recipient public key, sending the data, decrypt with recipient private key, and then verify sign with sender public key.

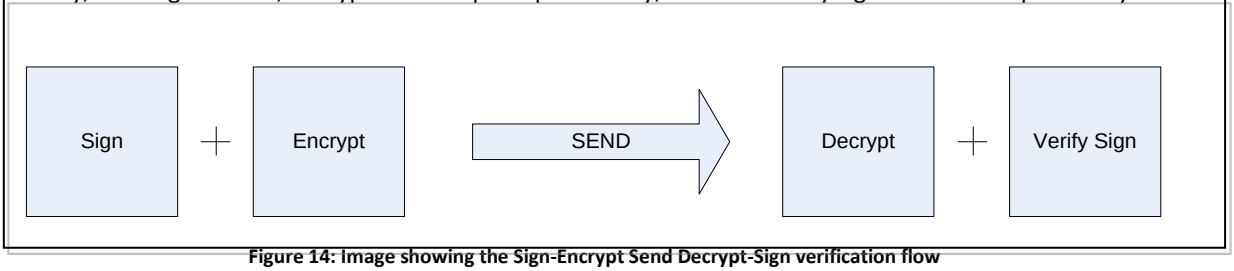


Figure 14: Image showing the Sign-Encrypt Send Decrypt-Sign verification flow

9.1.1 Contents of a certificate

The certificate contains several information fields. Some which is useful in this context.

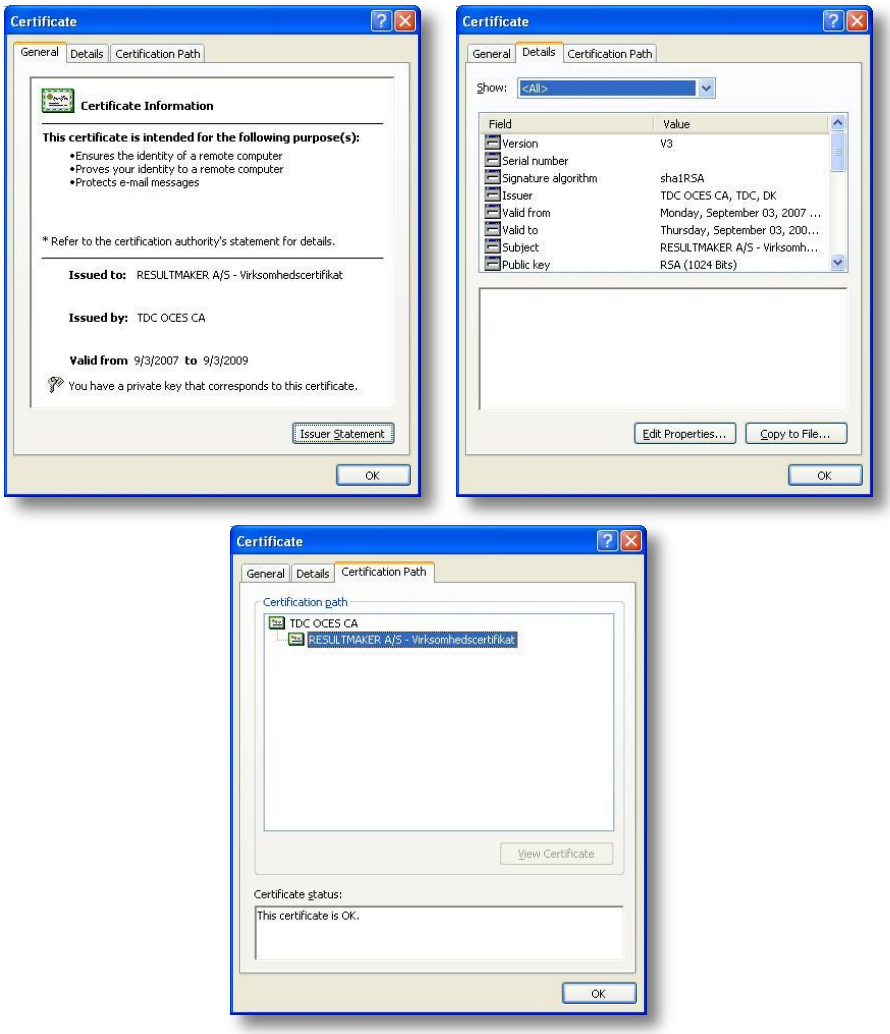


Figure 15: Displays the three tabs a certificate

The above images show a *Certificate* where the private key is available for the current user. This can be verified by text *"You have a private key that corresponds to this certificate"* on the image to the left.

Just above that text there is three fields, *Issued to*, *Issued by* and *Valid from/to*. The *Issued to field* shows who or what the certificate is issued to. If the certificate is an SSL server certificate this field will display the domain name. Failing to run the environment under the same name will generate a warning in the end users browser. *Issued by* is the CA (Certificate Authority) who issued the certificate in the first place. This CA is vouching for the authenticity of the certificate. So basically if you do not trust the CA you shouldn't trust the certificate.

Valid from/to field is important since when the date passes the valid to date the certificate will no longer be valid and this will again show a warning in the end users browser. Please note that the certificate still work past the valid to date and it's only the client who decides if it's still okay to trust the certificate. Expired certificates are one of the most common problems of running an environment. It's often not decided who's responsible for updating the certificates.

In the *details tab* you will find a field called *thumbprint*. This holds a unique hash value of the certificate. Resultmaker uses this to identify the certificate uniquely. In the details tab you will also find *CRL Distribution Points*. In this field information about the Certificate Revocation List is stored. You will usually find a URL for the

CRL, which will be used when verifying the certificate. This is why one of the firewall requirements is to let traffic through to this URL.

9.1.2 Certificate types

All certificates consist of a private key and a public key pair as explained above - but sometimes you only have the public key of a certificate. The common way to understand it is that if you have a private key for a certificate you also own that certificate and if you do not have the private key the certificate is owned by someone else.

We work with four + one kinds of certificates; *SSL, Employee, Personal and Company*. The extra certificate type is Company certificates where only the public key is present. In common speak these are referred to as *Public Keys*.

The SSL certificates are used for frontend servers and enable the https communication between the server and the end user. For a SSL certificate to work the private key must be present on the server.

Employee, Personal and Company certificate are what is called client certificates. The Employee certificate holds a CVR number while the Personal certificate holds a PID number. The PID number can be exchanged to a CPR number using a web service. Neither of these certificates is used within the environment but only when logging into the frontend. The Company certificate on the other hand is used within the environment. The main purposes are to authenticate towards external systems and for mail signing.

The *Public key* only Company certificates are used for sending encrypted data to external parties.

9.1.3 Certificate stores

There are several types of stores for certificates. When maintaining a Resultmaker Process Platform™ only the personal store on the Local Computer is used. A common mistake is to install certificates under the current user instead of the Local Computer. Since the default setting of the Resultmaker applications requires certificates to be stored in the personal store of the Local Computer, placing them elsewhere will not work unless configuration is updated. This information is not covered by this document but Resultmaker can be consulted regarding it.

To enter the certificates view the following procedure can be followed. From a command prompt or from the run menu type MMC. This will give you the following dialog.

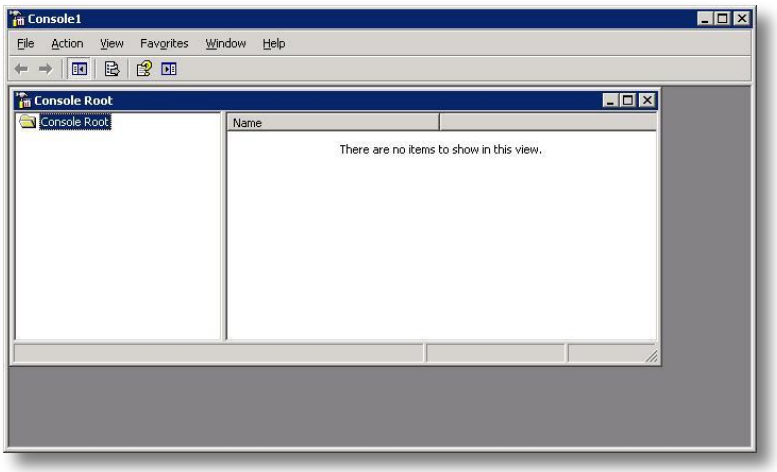


Figure 16: MMC startup dialog

Then click ***File > Add/Remove Snap-in*** and the click ***Add***. That will give you the following dialog.

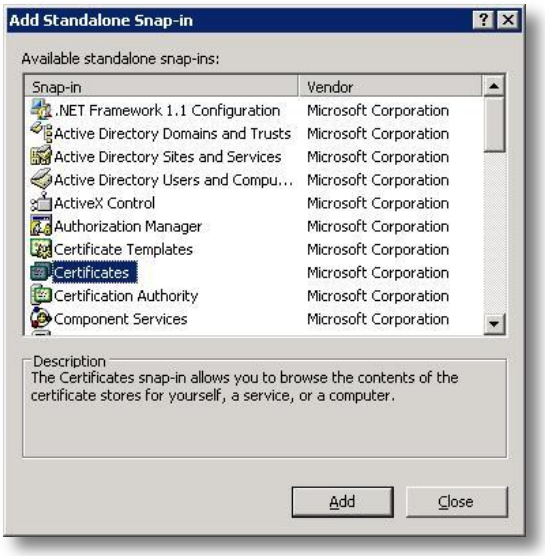


Figure 17: MMC Snap-in dialog

From this dialog click ***Certificates*** and then ***Add***. The following dialog will be shown.

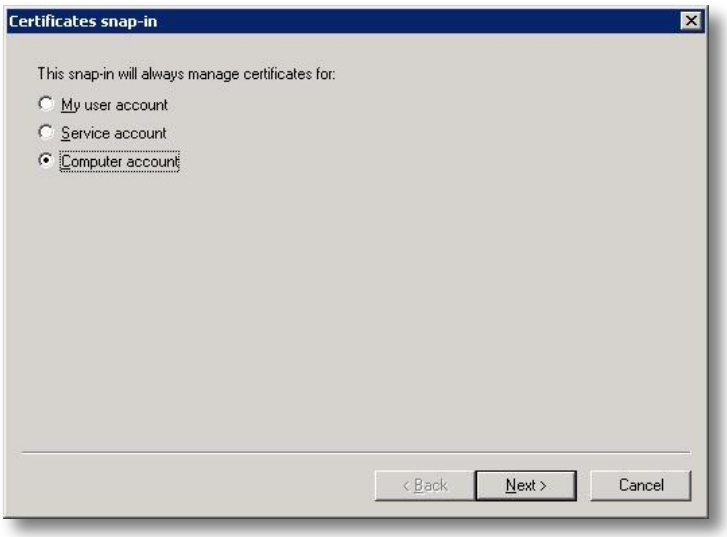


Figure 18: Certificates Snap-in dialog

Make sure you choose the ***Computer account*** and the click ***Next*** and then ***Finish***. That will give you the following dialog.

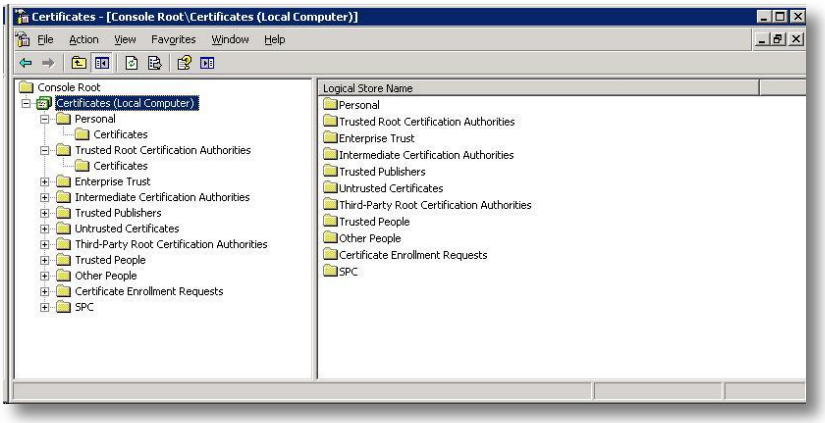


Figure 19: Shows certificates of the Local Computer

9.2 Installing the certificate the first time (through TDC)

When installing the certificate the first time you will probably have an email from TDC with a link. This link will start a guide on the TDC web site. As a result of this guide you have two things on your computer: A certificate - most likely installed in the personal store under the user which clicked on the link - and secondly some TDC certificate software called "*TDC Digital Signatur CSP*" as seen under Add/Remove programs.

If you try to export the certificate you will be prompted with a TDC password box and you will end up with a certificate (a pfx file) with strong protection where there the possibility to export is removed. To avoid this first remove the TDC Digital Signatur CSP software and then follow the rest of this document.

9.3 Installing the certificate with DanID

During 2009 Danish certificates is no longer hosted with TDC but instead with DanID. This has some changes in the way you handle the certificate.

It has actually become a bit easier now since all you have to do is first create a safety copy of the certificate which results in an html file. Then you need to right click the html file and choose Firefox to open it. Note that you need at least Firefox 3.5 to do this. You will be shown an error saying that Firefox is not supported and a button making you able to download the certificate as pcks12 file. You can now install this certificate. *Make sure that you make the certificate exportable when installing.*

9.4 Removing the certificate strong protection

Removing the password from a certificate can be tricky since it's not possible directly to see if password is required or not when certificate is used.
In the following it is assumed that the certificate is installed in any store with or without password but with the private key and with a possibility to export the private key. If this is not the case you cannot remove the password from the certificate.
The reason the password needs to be removed is because having a password on the certificate will result in a password dialog popping up whenever a private key is requested by an application, which the application cannot handle. Furthermore the application would also need to know the password of the certificate.

9.4.1 Step 1: Finding the certificate

First open the Management Console (MMC) and go to the Certificates Store as described in the previous section *Certificate Stores*. Make sure to open the correct location, either Local User or Local Computer.
If the certificate is installed under a different user than the one you are logged into the server as then you must login as that user instead. In the personal store you will most likely find the certificate. Verify it's the correct certificate by double clicking it. Also make sure that the private key is present as explained in the section *Contents of a certificate*.

9.4.2 Step 2: Exporting the certificate

After finding the certificate the next step is to export it. This is done by ***right clicking*** the ***certificate*** and choosing ***All Tasks > Export***. This action will produce the following dialog.

Figure 20: First image of Certificate Export

If the "*Yes, export the private key*" is not visible, it means that when this certificate was imported it was marked as none exportable. Without this enabled you cannot proceed. You must find where the certificate was installed in the first place and export it from that location.

The next dialog will have the "*Enable strong protection*" checkbox enabled by default. This must be *disabled* as in the screenshot below.

Figure 21: Second image of Certificate Export

The third dialog will prompt you for a password. Putting in a password here will make sure that others can't install the certificate without the password. Even though these two fields must be left blank so the password can be removed.

Figure 22: Third image of Certificate Export

Finally you must specify a location for the certificate (the .pfx file).

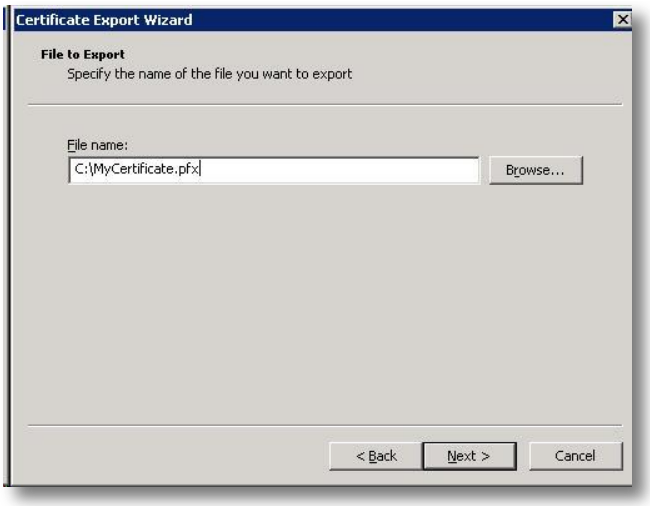


Figure 23: Fourth image of Certificate Export

The final dialog is a confirmation dialog. After this you will have a certificate with no password protection. For security reasons this file should never be distributed.

9.4.3 Step 3: Importing the certificate

The importing step is fairly easy. Simple just ***open the MMC*** again and import the certificate in the ***Local Computer > Personal Store***. If the certificate already exists remove it first and then import.

If the certificate is used on several machines the .pfx file can be used over and over again.

9.5 Read access to the private key

By default, only local administrators have access to private keys installed in the local machine "*personal*" store. In some cases Resultmaker applications require that private key access be given to other users. The following procedure must then be carried out.

1. ***Unzip*** the file ***FindCert.zip*** to a folder on the server

2. Find the thumbprint of the certificate used for these applications. This certificate will be a customer specific certificate and will be described in customer specific documentation
3. Open the file FindCert.bat in notepad and edit the thumbprint hash value to the value of the certificate you want to find
4. Save the FindCert.bat and double click it.
5. The output will display a filename which is located in the folder
   C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys
6. Locate the file through the *Explorer* and right click it and choose the *security* tab
7. Click ***add…***, choose ***Locations*** and select the ***local computer***. It is very important that you do not search in the domain for the user to be added
8. Add the desired user (usually ***Network Service***) and grant it the default ***read*** rights

Carefully distinguish between domain and local users. The domain version of the Network Service is not the same as the local version which is the default identity for .net application pools.

Selecting the domain version when the local one is required will be wrong and the application will not work.

There is no directly way to verify if it's the domain user or the local machine user of the Network Service you have added after you are done. If in any doubt at all remove the user and do the steps over again.

You need to do this procedure again if you renew the certificate or if you just reinstall it.

9.6 Finding the private key identifier

When private key identifier is needed in a configuration file the Certificate Tool which comes with the Webservice Enhancements 3.0 installer is needed. The tool is found at Start > Programs > Microsoft WSE 3.0 > Certificate Tool and will show the below dialog.

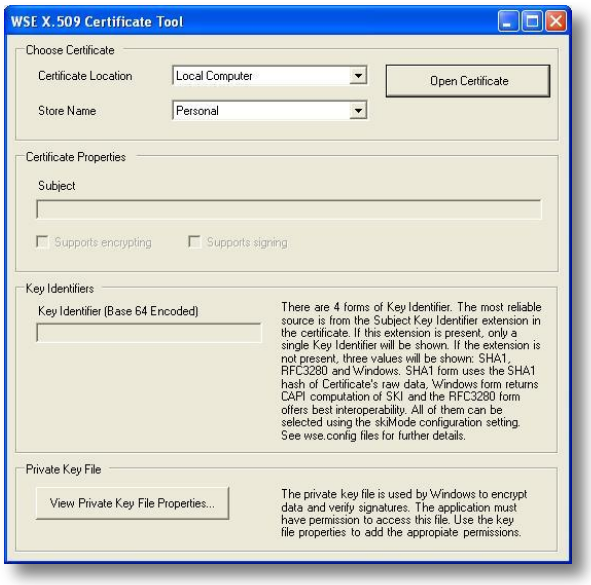


Figure 24: The Webservice Enhancement 3.0 Certificate Tool

Make sure that you choose the Local Computer and Personal Store. Then click Open Certificate and choose the certificate you need the private key identifier. The information will be displayed in the field Key Identifier (Base 64 Encoded).

9.7 Renewal of a certificate

Before a certificate expires it is strongly recommend renewing it. Depending on whom the certificate authority is this can be done in different ways. This document will therefore not go over any renewal procedures. When a renewed certificate is received most the above steps can be repeated and the certificate should be handled as a "*new*" certificate.

9.7.1 Certificates in Resultmaker applications

After a certificate has been updated there might be updates to Resultmaker configuration files. This depends on what certificate it is and what it is used for.

SSL certificates

The SSL Certificate of an environment can upgraded without changing any Resultmaker application configuration files. Failing to upgrade the SSL Certificate successfully might bring the environment down since the frontend is setup to redirect https if a user enters with http. Resultmaker should be contacted if this default behavior should be changed.

Company certificates

The platform might not have any company certificates installed at all but they are required in three cases. Please note that all changes to Resultmaker applications configurations should be done only after consulting Resultmaker. The reason is that we keep a copy of the configuration files and changing it locally only will lead to that the Resultmaker copy and the local copy will become out of sync.

First there is the SAML frontend version. This frontend will require having a company certificate with a private key installed. Changing this certificate will require an update of the frontend configuration and that the step *Read access to the private key* is carried out again.

Secondly the CVR Online 3.0 implementation requires a company certificate with a private key. When upgrading this certificate, the CVR application configuration needs updated with the new certificate thumbprint and with the key identifier obtained in the step *Finding the private key identifier*. Finally the step *Read access to the private key* must also be carried out again.

9.8 Installation of SSL Server Certificates (DanID)

This section describes how to install and assign SSL Certificates purchased from DanID. The basics will be the same for most vendors though.

9.8.1 The Request

First a Certificate Request must be made. This is done from web server. Full explanation is provided on DanID's website. The Request will produce what we call a *Certificate Request*, a base64 encoded file which will show as a public key if renamed to .cer. The request is send to the certificate vendor.

9.8.2 The Response

DanID will reply with a *Certificate Response*, which is used on the exactly same server as where the request was made. Again full explanation is found on the DanID website. Completing this procedure will result in a SSL certificate installed on the server and can be found by accessing the web site where it was created.

9.8.3 Intermediate Certification Authorities

In order for the DanID SSL Certificates to be valid for the end user the root certificates chain must be installed in *Intermediate Certification Authorities* in *Local Computer* from the MMC. The full chain can be found on the DanID website and in the time of writing the file is called *tdc-sslchain-20091026.p7b*. For other SSL vendors this chain will

most likely not be valid or may not even be required. Note that a full reboot of the server might be required for the change to be applied fully.

9.8.4 Exporting the SSL Certificate to a PFX file

After completed installation a PFX file can be made for safe storage of the certificate or for use on multiple servers. Limitations for usage might apply and should be verified with the SSL vendor.

The actual export is done from the IIS management console. No further guide is included in this document.

9.8.5 Installing SSL Certificates from a PFX file

Installation of a SSL Certificate is done through the IIS management console in Windows Server 2003 and through the MMC in Windows Server 2008. The MMC can be used in the Windows Server 2003 as well. In both cases the certificate must be assigned to the correct web site after the installation.

The Intermediate Certification Authorities must also be installed in other for the certificate to be valid.

9.8.6 Verifying a SSL certificate

To make sure that a SSL certificate is correctly installed external access to the server must be tested. It is important that the URL starts with "*https*".

Figure 25: Shows how IE displays a secure connection

In the above picture you can notice the *Lock* which indicates that this connection is secure and therefore that the SSL certificate is correctly installed.

10 Deploying content

After the above installation is complete the server needs some content in order to work. Instead of deploying content the client tools can be used directly to develop content. The latter is not recommended though.

10.1 Process Platform 6.0 content deployment

10.1.1 Step 1: Deploying content

The content deployment on Process Platform 6.0 happens with the Content Deployment Tools, which consist of the Export Tool and the Content Import Service.

The Export Tool is used on the Test/development server to extract Process Platform content and save this in a zip file.

The Content Import Service is a windows service, that is installed as part of the Process Platform installation. It monitors the folder – usually “C:\Importfolder\” for new zip files containing content, which is then pushed into the Process Platform.

See Figure 4 that show the Content deployment architecture.

Process Platform Content can be of the following content types.

- Workflows (Processes)
- Forms (Questionnaires)
- PDF templates
- Word templates
- Script files
- Data Export Definition files
- Xslt files
- Images

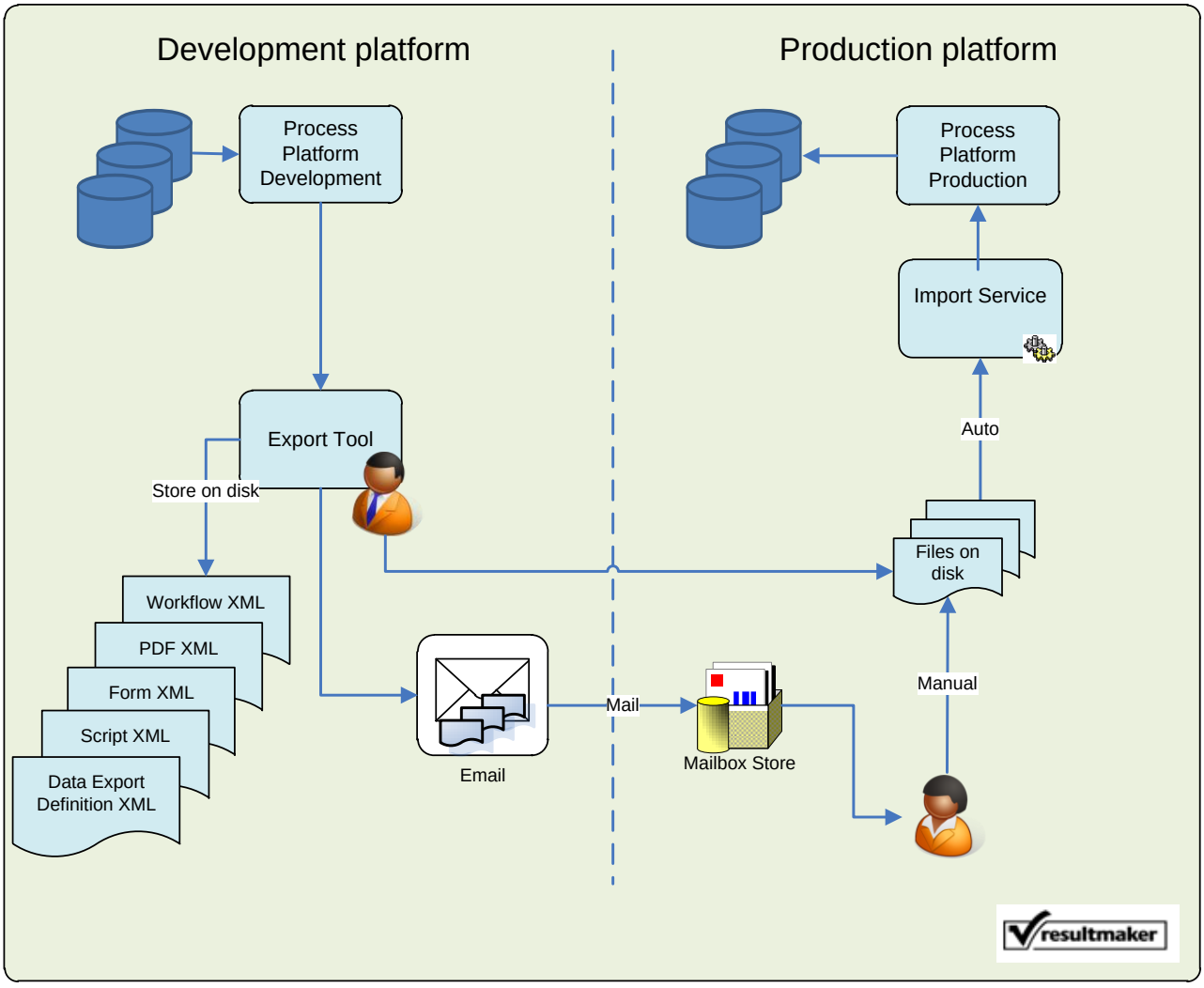


Figure 4 Content deployment architecture

For each folder put in c:\importfolder the import service will create at least two subfolders, a backup and a done folder. The backup folder contains backups of the content already on the server (if any) when the new content is deployed. In this way it is possible to make a *rollback* of the deployed content. The done folder contains all the content that has been deployed correctly into the database.

If a third folder is created called *Failed*, it means that some of the content import failed and the *import.log* must be checked. This log will display the problems which occurred during the import. The full understanding of the error messages is beyond of this document, and if help is needed Resultmaker can be consulted.

11 Testing the installation

After the installation has been completed it is recommended that the environment is tested. This is done by going through each of the sample projects. By directing your browser to the frontend of the server you will see a number of sample projects. Each sample project displays some functionality of Resultmaker Process Platform™. Each test case is not described here, but the procedure is straight forward. Start each project and try it out to the end. After you have gone through all sample projects you have tested the primary functionality.

12 Using virtualization and server cloning

This section covers the procedure on server cloning in a virtual environment. This section should be read as is and gives no warranties for installing Resultmaker applications in a virtual setup. In a medium or high performance setup Resultmaker does not recommend using virtualization. Working with virtualization can be a major advantage for fast deployment of new servers though. Since no warranties are giving by Resultmaker in this regard a cloning of a server might not have the expected results.

First step is to setup up a server following the above standard installation procedure. This includes deploying sample content, configuration and testing as well. Second step is to take a *snap shot* of the server. A snap shot is a common way to say “copy the server”. Make sure that the two servers do not run on the same network at the same time until at least one is given a new name. After the server has its name change the final step is to run the configuration procedure again as described above. You should test the server again to make sure it’s working as intended.

Virtualization can also be used in another scenario. If you create a presentation environment and set it up perfectly as you need it for a presentation and the take a snap shot you will always have a perfect image for future presentations. This can save huge amounts of time. Take snap shots at the correct time can be tricky but the only downside is that they take up lots of space.

13 Upgrading an existing server

If you are in a situation where the server you are installing already contains a Resultmaker Process Platform™ you can choose to try upgrading the server instead. If you do not want to save any data it is advised that you reinstall the operating system and start from the beginning of this document. If you instead would like to save your existing data proceed reading the section for a procedure. You should know that upgrading a server where it is required to keep data is not always successful since both custom actions could have been made since last reinstall and that the structure of the data you backup may not match the structure of what the new software expect. Furthermore the procedure will not handle all data in all databases. This is done to make the procedure simpler. In special cases this procedure cannot be used.

13.1 Content files

The folder *C:\FileRepository* contains most of the content files in the system. The folder needs to be backed up to ensure rollback procedure.

13.2 Registry

The registry key *HKEY_LOCAL_MACHINE\SOFTWARE\Resultmaker* should be backed up and the deleted.

13.3 Remove applications

Before removing applications you should backup the two folders *C:\inetpub\wwwroot and c:\program files\Resultmaker*.
In add/remove programs, uninstall the following programs:

All versions

- Every program starting with **Resultmaker** (ie Resultmaker BlueBox)
- ABCpdf .Net
- Microsoft Web Service Enhancements
- PdfServer2

Then all Resultmaker web applications should be deleted from *IIS Manager*. The content of *c:\inetpub\wwwroot* and *c:\program files\Resultmaker* should be almost empty. The remaining items should be deleted manually.

13.4 Databases

There are several databases in Resultmaker Process Platform™, which all needs to be backed up first. This is to ensure a rollback procedure in case any problems should occur during the upgrade.

Post the install, database versions must be checked. If the installation files did not upgrade the databases, they need to be upgraded manually. The required database version depends on the installed software version. Current database that needs to be checked are the following.

Version 6.0

- [Prefix]_ProcessEngine (version 6030)
- [Prefix]_Ats30 (version 3110)
- [Prefix]_FileStore (version 3020)
- [Prefix]_TokenServiceData (version 2022)
- [Prefix]_TransactionData (version 2311)

Make sure the databases are also verified that they have data in them. Missing data could mean that the upgrade was not successful and Resultmaker should be consulted.

13.5 The installation

If the above steps did not go wrong you are now ready for installing the upgraded software. This is done in the same way as when installing from scratch.

14 Monitoring Process Platform™

This section describes in general terms how to monitor a Resultmaker Process Platform™ in relations to operations. Firstly we describe how to monitor the basics and after how to monitor the Resultmaker applications. To use these guidelines in operation an external tool should be used. There are no recommendations to what tools can be used at this point.

14.1 Platform and environment structure

We define that a *Platform* consists of *Environments* and that an environment consists of servers. The environments are typical named production, staging/qa, test and development. Each of these environments consist of the server types PPFE, INTEGRATION, PPBE and one or more database servers. As this document is a generic document no actual server names are mentioned. Instead we work with generic logical names. These are PPFE, INTEGRATION and PPBE. Please refer to customer specific platform documentation for a mapping between these names and the actual server names.

To simplify the monitoring process only the server types are used here. The mapping between server types and server names should be used when implementing monitoring. Furthermore the below descriptions only covers a single environment but can be used on every environment that the platform consists of.

14.1.1 Load balancing

Load balanced servers should be handled separately. It is not best practice to monitor a frontend server externally through a load balancer unless you can be absolutely sure that you know what frontend server you reach. Failing to do this may lead to only monitoring one of several servers. Instead best practice is to monitor the individual servers directly.

14.1.2 Multiple network adapters

Many servers today come with more than one network adaptor. Depending on how the server is setup monitoring through the incorrect network adaptor may lead to false results. Consider this if the server has a main network adaptor and a service adaptor. Monitoring through the service adaptor may not reveal problems with the main adaptor. Best practice is to monitor through the same adaptor as the end user uses.

14.2 Monitoring of hardware and basic operative system applications

This section describes general approach on how to monitor the system hardware and system applications. It should be taken as recommendations since an operation department might have completely other ways to monitor a system. This section also uses the terms *Warning Flag* and *Consult Resultmaker.* These might be handled completely different from customer to customer. The warning flag is a way to say that something is not critical or fatal for the Resultmaker applications. Several warning flags should result in a Consult Resultmaker event. The Consult Resultmaker is used when it is not expected that operation personnel can handle the errors by themselves. When operation personnel get more familiar with the Resultmaker applications they might be able to solve more and more issues without needing external help. Also depending on the support agreement with the Resultmaker or other partners *Consult Resultmaker* might mean that a partner should be consulted instead of Resultmaker directly.

14.2.1 System and Application memory

Process Platform™ version 6 runs on Windows Server 2008 64 bit thus removing the discussing of the 2GB memory limit. This doesn't remove the possibility of out of memory exceptions since the system can be installed with little memory still.
It is advisable to both monitor the IIS worker process and the system memory usage. On high load setups the process may run out of memory and an IISRESET is required to fix the problem. To counter this issue the Process

Engine has a scheduled IIS worker process recycle each day at 4am. Tweaking the system should be not being done without consulting Resultmaker.

The Resultmaker databases may run on (and is advised to run on) Windows Server 2003 (2008 for PP6) 64bit and SQL Server 2005 (2008 for PP6). When running on 64bit the 2GB process limit is removed. The SQL server process and system memory should still be monitored but Resultmaker have no incidents of the SQL server running on Windows Server 2003 (2008 for PP6) 64bit has run out of memory. Monitoring can be used for optimizations though.

14.2.2 Processor load

Platforms with high load which are running smoothly will have a variable CPU load of up to 80% and 100% in peak times. CPU loads of 80% or more for longer periods (minutes) should result in a warning flag. This goes for both application servers and the database servers. If the CPU hits 100% load errors may start to occur for the end users. These errors can be common timeouts or more unexpected errors. In both cases the load should be recorded in such a way that appropriate measures can be taken. It might lead to a requirement of upgrading the CPU of that specific server.

14.2.3 Hard disk space

By far the hard disk space is the biggest reason for system break downs. This often is the case where the system is highly used. Initial allocations are too small and are not reevaluated during operations. The recommendations in this paragraph should be followed to ensure high uptime.

Hard disk space can be divided into two categories, application needs and database needs. The database will increase in size depending on load. The more work flow instances that are made the more space will the databases take up. The space used should be monitored and recorded at least once per day. This recording should be both of the database file and the drive where it resides. If the database cannot expand the database file it will lead to errors. Based on the average increase in space usage a calculation can be made that estimates when the system runs out of space. A warning flag should be raised if this is within three months.

All other servers, the application servers, will not grow in disk space usage in the same way. Only log data and other temporary data will be stored here. The space should still be monitored and a warning flag should be raised if they go under 10 GB free spaces. If a server has less than 1GB of space it is considered critical and actions must be taken. In that case Resultmaker should be consulted or if possible just assign more hard disk space to the system.

14.2.4 SQL Server

Resultmaker uses the Microsoft SQL Server 2005 (2008 for PP60) to store databases. The SQL Server service must be running at all times. Failing this will lead to a fatal break down of the Resultmaker applications. For a more thorough test of the SQL Server periodic queries can be made. The response times for the queries should be logged.

On the PP_OC (OC for ProcessEngine) database this query can be made:

```
SELECT TOP 1 * FROM WorkflowInstances.
```

Optionally all other databases can be monitored using the same procedure. Response times longer than short (below 500ms) should result in a warning flag.

If the build in SQL Server Agent is used for backup this should also be running. Backups should be monitored to make sure that they are executed correctly after schedule. Failure to backup correctly may lead to loss of data.

14.2.5 Network and firewall openings

Communication between the servers in an environment and external systems should always be intact. The internal communication in an environment can be handled by eg. ICMP packets. Even when done with a fair size (like 1000 bytes) the connected server should respond within 1 ms. ICMP packets with larger response for a longer period of time (several periodic tries) should raise a warning flag.

Communication to external systems is very custom and different from platform to platform. This doesn't mean that this should be left out as a part of the monitoring setup as this may critical for the setup. A common way to check if it is possible to make a connection to an external system is by making a *telnet* session. This is done from a command prompt by writing

"telnet HOSTNAME PORTNUMBER"

where the hostname is the domain name/IP address of the external system and port number is the port number. Common port numbers are 80 for http and 443 for https connections. Due to firewall setups at both the platform level and the external system this must be done from the server which is normally performing the requests otherwise this may not show the correct results.

14.2.6 Internet Information Server

The IIS is a critical application for the Resultmaker Process Platform™. Without that working the platform will not work. At all times the IIS must be running and be in full function. Resultmaker applications use ASP.NET which means that the .NET framework must be installed and working. The IIS will be monitored implicit when monitoring the Resultmaker applications as described later in this document.

14.2.7 Mail server

Many of the Resultmaker applications are able to send emails as a part of the error handling system. Furthermore as a part of the customer solution itself it is often very important that mails can be send without problems. In both cases a SMTP server is needed. The basic way to monitor this is to check if the SMTP service is running. The more advanced way and a better way is to periodical send emails through the system. This way delivery time can be measured and if mails are not delivered right away (within a minute) a warning flag should be raised. Doing this might catch some problems in the send mail functionality. Mail sending can be hard to verify since there may be many recipients. A periodical check should be done to see if the STMP server is put on any spam lists. This could be a daily check. A mail server which is put on spam lists can be unable to send mails to any number of recipients and is therefore fatal for the system.

14.2.8 Event Log

The system Event Log can reveal problems with the Resultmaker applications and other operating system issues. Because of this the Event Logs should be monitored. Since the Warnings and Errors which are seen in the Event Log may vary a lot, technical personal should look into each one and clarify if the warning or error should be handled or can be left alone. Based on this Resultmaker can be consulted for further actions. One that needs to be taken seriously is the .NET 2.0 Warnings. These are warnings because it's not a fatal event for .NET but it is probably a fatal event for the application itself. Since many of the Resultmaker applications run under .NET 2.0 these Event Log records should be acted on. The procedure is to collect the error and consult Resultmaker.

15 Monitoring of Applications

This section describes Resultmaker specific applications that need to be monitored. The following tables describe the applications that as a minimum should be monitored. We have divided the applications in three different types, Web services, Web applications and Windows services. For Web services and Web applications the

following can be used in case of an error. The error will probably be the typical “yellow page” .NET error and actions must be taken. Normally the system is set to “CustomErrors=RemoteOnly”, which means that the actual error is not displayed in the response. For .NET 2.0 (or later) applications the error is logged to the EventLog. For .NET 1.1 applications the application must be called from the server itself, which will display the full error.

The tables are divided into ID, Server, Application Path, Depends on and Action.

ID column
ID denotes an identifier for other documents and communication among involved parties.

Server column
The Server column contains what server type on which the application is located. You should refer to customer specific documentation for mapping to what the specific server name is called.

Application Path column
Application Path holds information on where the application is located.

Depends on column
Depends on is displaying what other applications the application is depending on. For most parts a database server has been specified.

When checking if a database server is running the following should be carried out.

1. Verify that SQL server service is running
2. Check server CPU usage (very high usage may lead to timeouts)
3. Check disc space. Do the databases have enough space to expand?
4. telnet from the application server to the database server – use the command prompt “telnet [DBServer] 1433” where [DBServer] is the hostname / IP address of the database server
5. Restart the SQL Server service and recheck 1 through 4

When a FileRep needs to be checked the following procedure should be carried out.

1. Verify that the folder C:\FileRepository exists and contains subfolder with files
2. Make sure that that they are reachable by using e.g. \\localhost\private

If any of the depending application is failing Resultmaker should be contacted for further actions.

Action column
Action describes what actions should be taken in case of a problem. Each action is separated by a comma, and should be carried out in the order in which they are listed. If no specific server or application is mentioned the action should be carried out on the server where the application resides. Before executing any of the actions the Event Log should be viewed to find possible answers to the problem. This information must also be supplied in case of contacting Resultmaker.

We work with four different action types: *AppRestart*, *ServiceRestart* and *ConsultRM*.

AppRestart covers multiple steps. These steps will hopefully result in the web application becoming fully functional again.

1. Recycle the AppPool of which the application is a part of. The associated AppPool is found by entering the IIS manager and choosing properties on the application. The field “Application_pool” in the bottom displays what AppPool the application is running under. The Recycle is done by right clicking the AppPool from the Application Pools overview in the IIS manager and choosing recycle. Please note that recycling is fairly graceful to the system. No end users will be influenced by it.

2. After recycling wait a short while and retry the application again. Make sure that you start a completely new browser before doing this.
3. If the application is still not up, there might be an underlying problem that needs to be resolved. Resolving the problem might need another recycle of the application.
4. If no solution can be found e.g. due to incident happening outside normal working hours an *IISRESET* should be executed. Also if the system is completely down for a majority of end users IISRESET should be executed as well. This is done to avoid extending the environments down time period. IISRESET is done by first stopping the IIS ("iisreset /stop" from a command prompt). You will need to verify that the IIS is actually stopped. This can be done from the IIS manager. In some cases the command need to be executed more than once to stop the IIS. After the IIS has been stopped the IIS can then again be started ("iisreset /start" from a command prompt). Beware that IISRESET will affect all user currently connected to the environment and therefore should not be done without second thoughts.
5. If the above steps do not resolve the problem wait a few minutes and try the steps again.
6. If the application continues to be down, next step will be restarting the server itself.
7. If the application is still down Resultmaker should be consulted.

ServiceRestart is done by opening the services overview and then choosing the restart option of the service in question.
ConsultRM means consult Resultmaker and is put in action in case debugging of the application will demand too much knowledge of the application. Before consulting Resultmaker the problem should be described as well as possible. Common questions that need to be answered are:

1) Who/what discovered the problem
2) When did the problem first occur
3) What error message is returned from the system
4) What was the expected normal behavior
5) How can Resultmaker replicate the error

Failing to describe the above points will make the problem handling process more difficult. Most helpful is to supply a detailed error report to Resultmaker. Problems described as "Error occurred" or "It just doesn't work" is not beneficial for the process.

15.1.1 Web services

ID	Server	Application Path	Depends on	Action	Version
WS1	PPBE	/OC4/OC.asmx	OCDB	AppRestart	All
WS2	PPBE	/ExportServer/Export.asmx	FileRep , OCDB	AppRestart	All
WS3	PPBE	/ExportServerAdminService/ExportServerAdminService.asmx	FileRep , OCDB	AppRestart	All
WS4	PPBE	/PdfServer2/PdfServer2.asmx	FileRep	AppRestart	All
WS5	PPBE	/Resultmaker/Filestore/Server/Download.asmx	OCDB	AppRestart	All
WS6	PPBE	/TokenService/TokenService.asmx	OCDB	AppRestart	All
WS7	PPBE	/SignatureServices/CertificateValidation.asmx		AppRestart	All
WS8	PPBE	/SignatureServices/SignatureValidation.asmx		AppRestart	All
WS9	PPBE	/BlueBox/Transactions.asmx	OCDB	AppRestart	All

Request and response
To check if a web service is up and running use the following format for the URL: http://[Server][Application Path].
All the web services should respond with the standard .NET web service page.

15.1.2 Web applications

ID	Server	Application Path	Depends on	Action
WA1	PPFE	/Resultmaker/Filestore/Client/UploadFile.aspx	[WS6]	AppRestart
WA2	PPFE	/RMFrontend/Default.aspx?userisloggedintovirk=false	FileRep, [WS1]	AppRestart
WA3	PPFE	/DataSelector/Default.aspx?ApplicationName=CPRP_Picker	FileRep	AppRestart

Request and response

To check if a web application is up and running use the following format for the URL: http://[Server][Application Path]. They should all respond with the standard respond code 200.

16 Backup and recovery

An important and often not very complete issue is backup and recovery. For this reason we have gathered recommendations for backup and recovery when operating a Resultmaker Process Platform™.

16.1 Databases

The databases are the most essential part of the platform. This is where all user data resides and for this reason backups should be handled with high priority.

16.1.1 Database Recovery Models

The SQL Server comes with three different type of recovery models; Simple, Full and Bulk-Logged. We recommend using the Full Recovery Model for the Production environment and Simple for all other environments. This will save some maintenance in test and development environments but still ensure that the Production environment has the optimal Recovery Model. This document will not cover in-depth knowledge of Recovery Models.

16.1.2 Database Backup Scheme

For all other environments than Production we recommend making a weekly full backup. This is done outside work hours preferable in weekends. In some cases customers might have a need for having a higher data security on the development environment in order to minimize loss of work. In this case we recommend following the scheme for Production environments.

In Production environments it is highly important that no data is ever lost. As mentioned above the Full Recovery Model is recommended. This gives the possibility for making incremental backups and recovering to a specific time. We recommend making a full backup Sunday morning at 03:00, an incremental backup every night at 03:00 except Sunday. If the platform is under high load hourly backup of the Transaction log can also be used.

Default setup for all databases that comes with Resultmaker Process Platform™ is set to Full Recovery Mode which has the effect that the Transaction log will increase in size over time. If no backup scheme is used at all the Transaction log will eventually take up all disk space leaving the system inoperable.

16.1.3 Process Platform databases

The following databases are installed with Resultmaker Process Platform™ and should all follow the same backup scheme. Please note that every installation might have been altered to match customer demands and might not include all the databases and might include custom databases not listed here.

- AuditTrailSystem or Ats30
- FileStore
- OC
- TokenServiceData
- TransactionData

The databases might be appended with **RM_** or **PP_** for overview purposes in shared database servers.

16.2 File system

To ensure the possibility of disaster recovery parts of the file system needs to be backed up. In a default installation of Resultmaker Process Platform™ the following folders on all servers except database server needs backup

- C:\FileRepository
- C:\Inetpub\wwwroot
- C:\Program Files\Resultmaker
- C:\Deployments

- C:\Logs

All the folders except Logs will only change as a part of a software or content deploy to the environment while the Logs folder may change all the time during usage of the environment. We recommend using a nightly backup of the changes in all the folders.

16.3 Verifying the backup

In all cases of backup it is important to periodical verify that the backup is working as it is supposed to. Failing to do this might lead to data loss. We recommend doing this at least once after the backup schemes have been set up fully and doing it again if the backup schemes changes.

17 Where do we go now

Depending on the purpose of the installed server different ways to go may be at hand.

If it's a demonstration server cloning the server might be a solution for fast redeploy for the next demonstration. If it's a test or development server starting to think about scaling the production environment might be a good idea.

Firstly more content should be developed though. As we say in Resultmaker pushing the software to the limit is one of the goals of a Business Process Architect. The server holds all the software needed to make a simple form or to make very complex workflows with hundreds of decision points and activities and multiple roles.

If you are a Technical Consultant and you are *just* installing the server you might not care much of this. But you should be aware that heavy usage on the server will need attention when it comes to monitoring disk space and trying to handle any problems that the Business Process Architects might encounter.

You should also familiarize yourself with the new applications of the server. There is a numerous number of web sites and windows services installed. They all need to be running for server to be working properly.

Before you start changing the configuration settings on your own please take a backup as Resultmaker cannot support any manual changes to the configurations.

Good luck with Resultmaker Process Platform™!

18 Consulting Resultmaker

18.1 In case of an error

Before consulting Resultmaker with a problem, describe it as precise as possible. Common questions that need to be answered are:

1) Who/what discovered the problem
2) When did the problem first occur
3) What error message is returned from the system
4) What was the expected normal behavior
5) How can Resultmaker replicate the error

Failing to describe the above points will make the problem handling process more difficult. Most beneficial way is to give a detailed error to Resultmaker. Problems described as "Error occurred" or "It just doesn't work" is not beneficial for the process.