CPR BROKER

Installation and setup

MAGENTA aps

Last Updated: 12 July 2013

TABLE OF CONTENTS

INTRODUCTION

This document will describe how to install CPR Broker.

CPR Broker includes two parts, the CPR Broker and the Event Broker. The installation package installs both.

Before you begin, please make sure you have the requirement listed in the chapter Requirements and also the information in chapter Needed information

Next, you can see the chapter Installing CPR Brokerfor details.

After the installation finishes, some configuration steps are necessary. See the chapter *Configuring CPR Broker* for details.

1REQUIREMENTS

1.1System requirements

- Windows 2003 or Windows 2008 with IIS installed. Windows XP/Vista/7 with IIS installed will work for demonstration purposes but not for production due to the 10 concurrent connections limit these operating system impose.

  For Windows 2008 you need to make sure that you have the *IIS 6 Management Compatibility* Role Service for *Web Server (IIS)* Role installed, as well as - of course - the *Web Server (IIS)* Role itself. You should also install the *.NET 3.5.1* Feature via *Server Manager.*

- SQL Server 2005 or higher (Express version is OK).
- .NET Framework version 3.5 SP1.

Any computer capable of running the above software will also be capable of running CPR Broker.

Extra requirements for Person Master

- .NET Framework 4.0
- IIS 6 or higher is a must.

If your system meets all these requirements you don't need to read chapter 2. On the other hand if your system is lacking something it might be a good idea to have a look at that chapter.

1.2Data requirements

As of **version 2.2** the CPR Broker sports historical data features - ie. performing periodical lookups (lookup over a historical timespan). In order to take advantage of these historical data features a **subscription to historical data extracts from the CPR office is a prerequisite**.

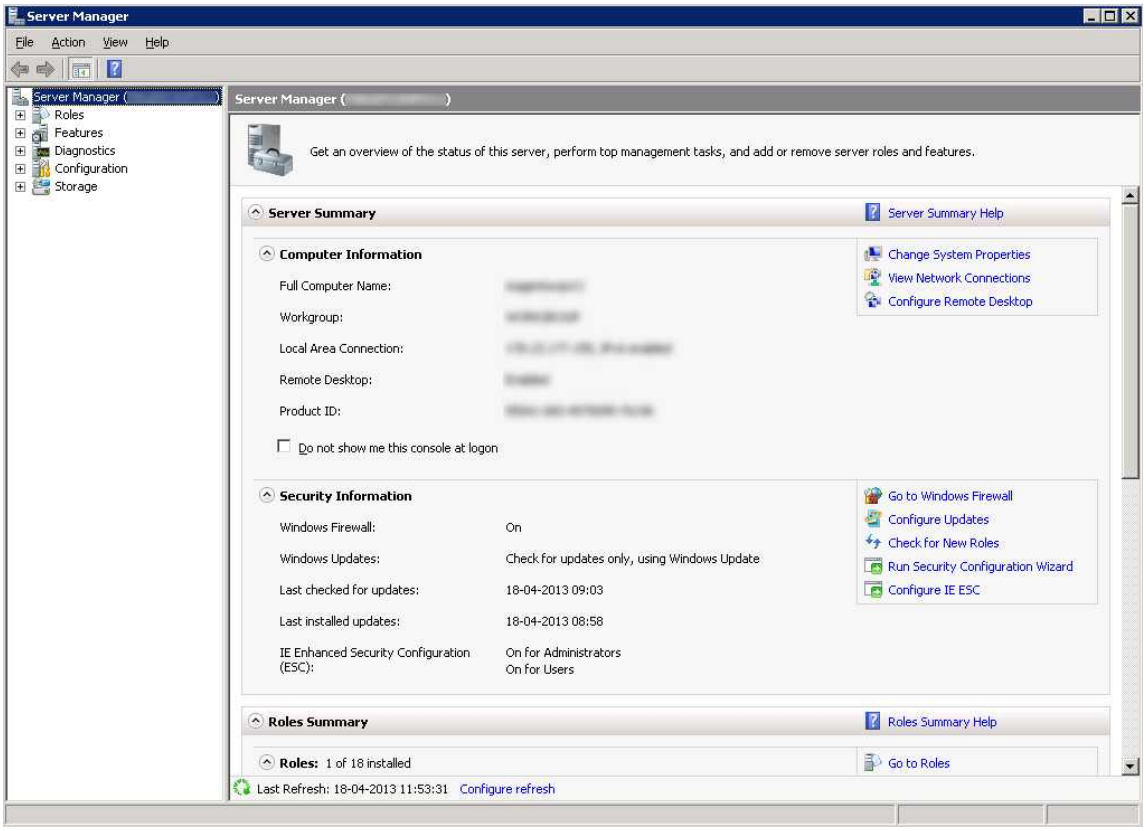
2PREPARING THE SYSTEM

In this section we will describe how to set up your server to meet the CPR Broker requirements.

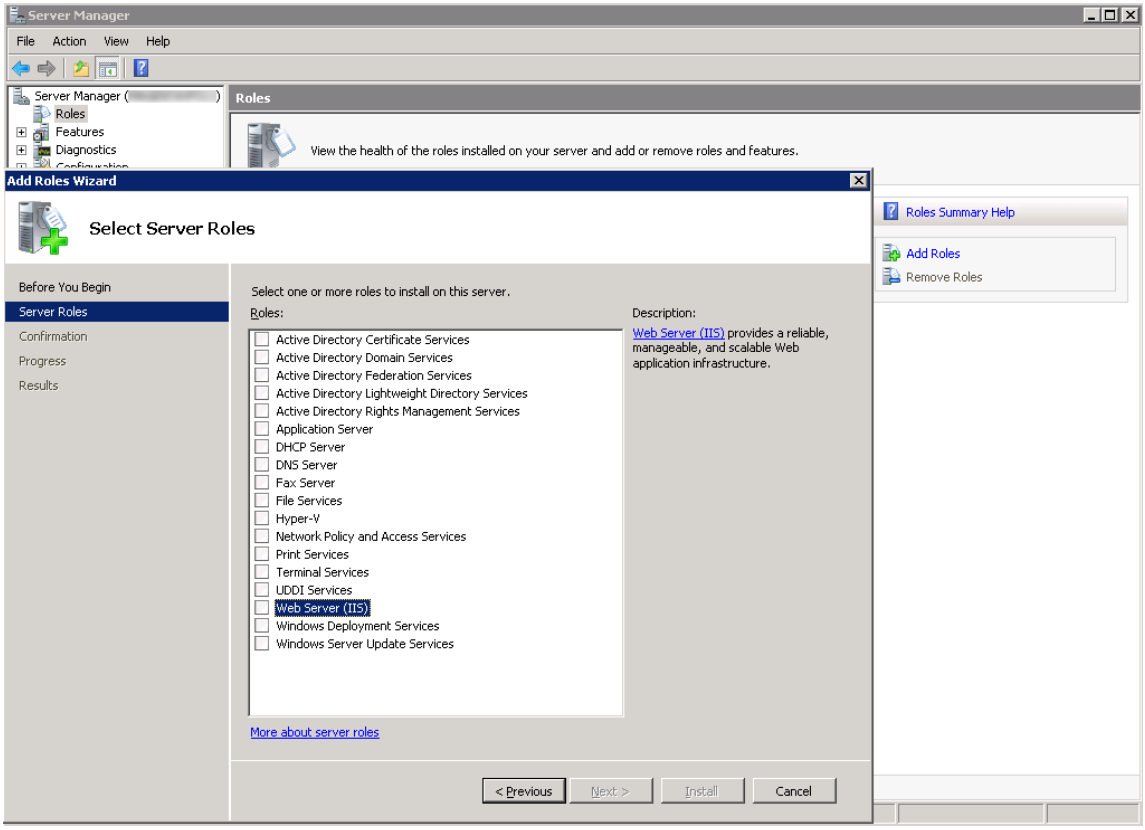
2.1Installing IIS

As the CPR Broker is a web service it relies on a web server. On Microsoft platforms Internet Information Server is the most common web server and therefore this has been the choice.

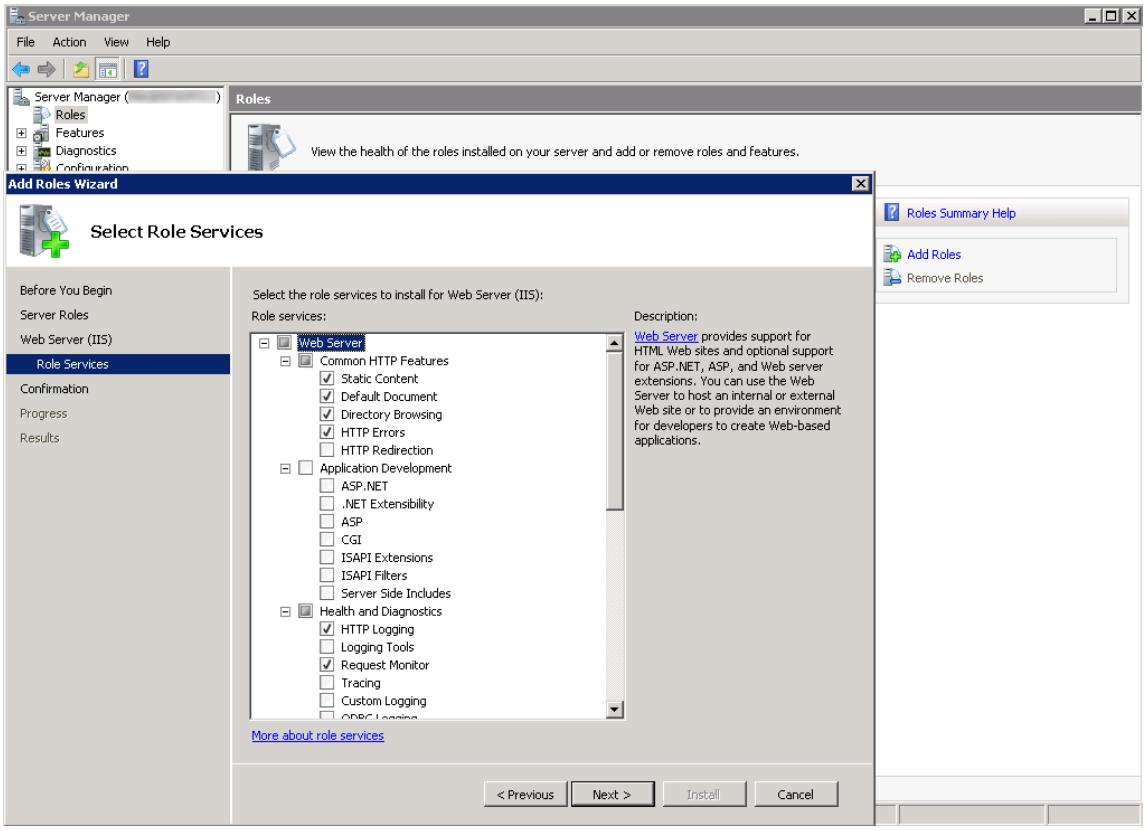
Go into Server Manager:



Then go into 'Roles', select 'Add Roles' and choose 'Server Role':



In this dialog select the 'Web Server (IIS)' option and new options will appear on the left:



As mentioned in the requirements in the previous chapter, you should check the 'IIS 6 Management Compatibility' option – make sure to check all sub-items.

Click 'Next' and afterwards 'Install'. Now IIS is being installed.

2.2Installing .NET 3.5.1

Again in the 'Server Manager', select 'Features' in the left-hand menu. Select 'Add Features' and look for a point named '.NET 3.5.1 Features'. Expand the option and select '.NET 3.5.1'. You might get a pop-up stating that you need to add additional roles – click the 'Add Required Role Services' and then confirm and install.

If you do not see the '.NET 3.5.1 Features' in the list, please check if it is actually already installed. Sometimes it is installed, but does not appear in the list. Check the path: C:\Windows\Microsoft.NET\Framework64\ and see if the folder '3.5' exists. If it does, you already have the framework installed.

If you do not see the framework in either place, then you should download it from the Microsoft website and install it. Just do the default installation.

2.3Installing .NET 4

The same steps counts for this part as for 3.5.1.

2.4Installing Microsoft SQL Server

It is recommended, performance-wise, to install a full version of SQL Server, but SQL Server Express will also do.

You will need to (purchase and) download it from the Microsoft website. Follow the default instructions and you should be good.

3NEEDED INFORMATION

You will need to have some information before you install CPR Broker. You will also need to make a few decisions for the names of database and web server entries.

3.1Windows

You will need a windows account that have administrative rights on the machine you are installing on.

3.2Web

CPR Broker can be installed as a root site (on Windows 2003 and 2008 only) or as a virtual directory to an existing root site. You need to decide on names for CPR Broker and Event Broker web sites (or virtual directories).

If you want to install CPR Broker as a root site (which is what is recommended) you must prepare a DNS record to point to the web server before beginning the installation. The installation program does not create this DNS record for you. You can do that locally by editing the hosts file, usually located at *c:\WINDOWS\system32\drivers\etc\hosts*

3.3Database

You need to know the machine name and server instance of the SQL Server instance that you plan to use for the broker. You need to have access to instance. The account you use must be a member of the sysadmin role (used only during the installation to create the database).

You need to decide the database names that you plan to use. The suggestion is CprBroker and EventBroker, but you can use whatever names you want.

You should also determine the login information that you want the broker to use in order to access the database. The installer can create it for you.

3.4Data providers

To configure CPR Broker after installation, you need information about how to connect to its data providers. Please refer to the section Data Providers for more details.

4INSTALLING CPR BROKER

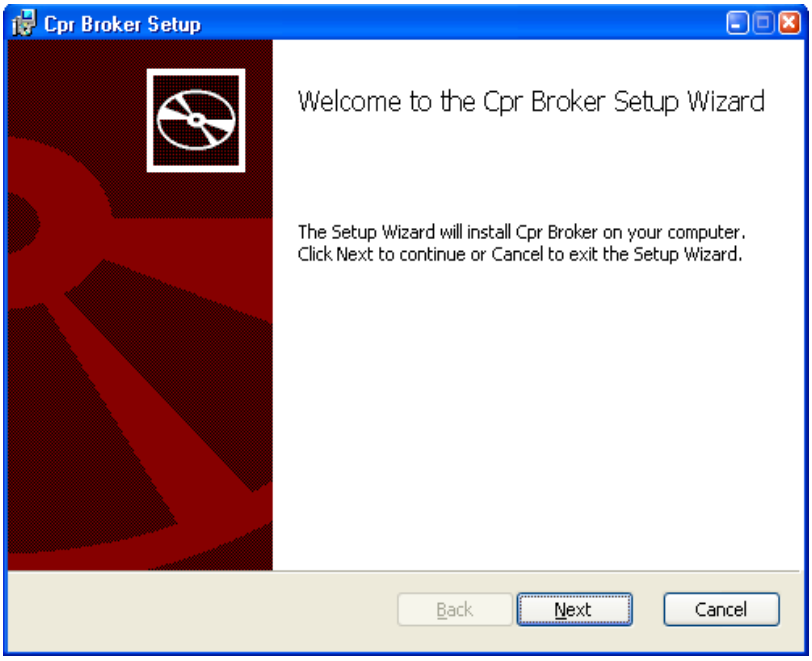
Copy the installer zip package to the computer with *IIS* installed. Unzip the package if needed.

You can install CPR Broker using a wizard, or -if you know what you are doing- by a silent installation via the command line.

4.1Using the installation wizard

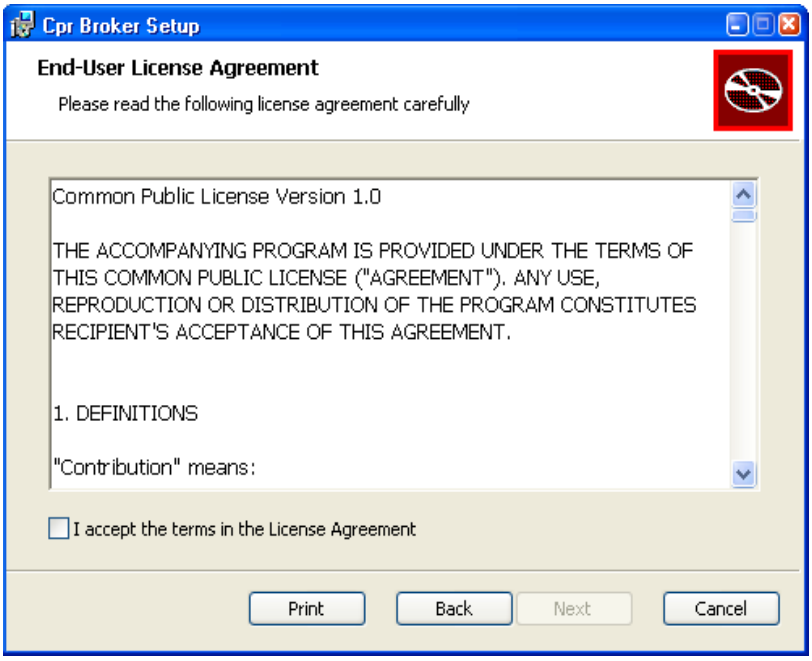
Double-click CprBroker.exe to launch.

Please note: On a computer with *User Account Control (Vista/2008/ 7)*, the program will ask you to use elevated privileges. If you are comfortable with it, allow it to elevate.

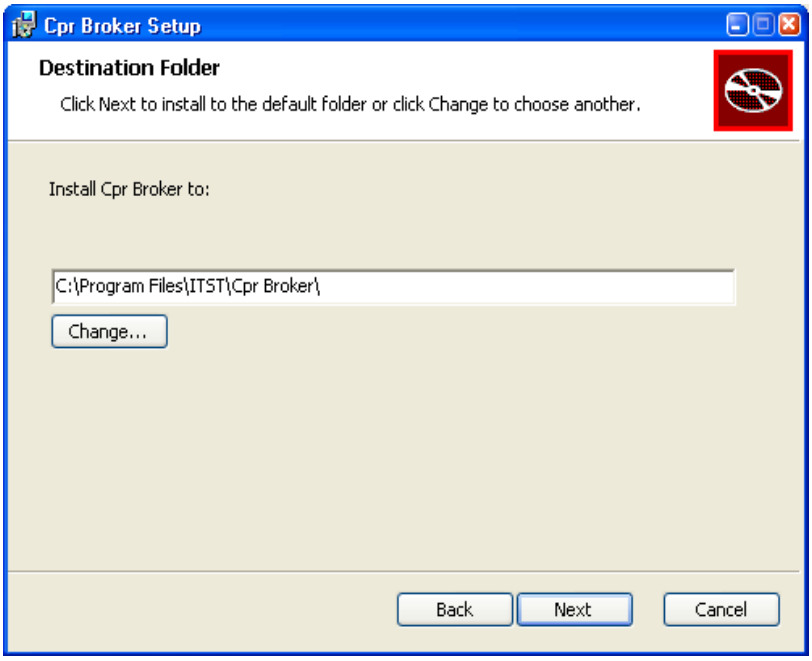


Click *Next* to continue.

The next screen will show the license terms. Accept and click *Next*.

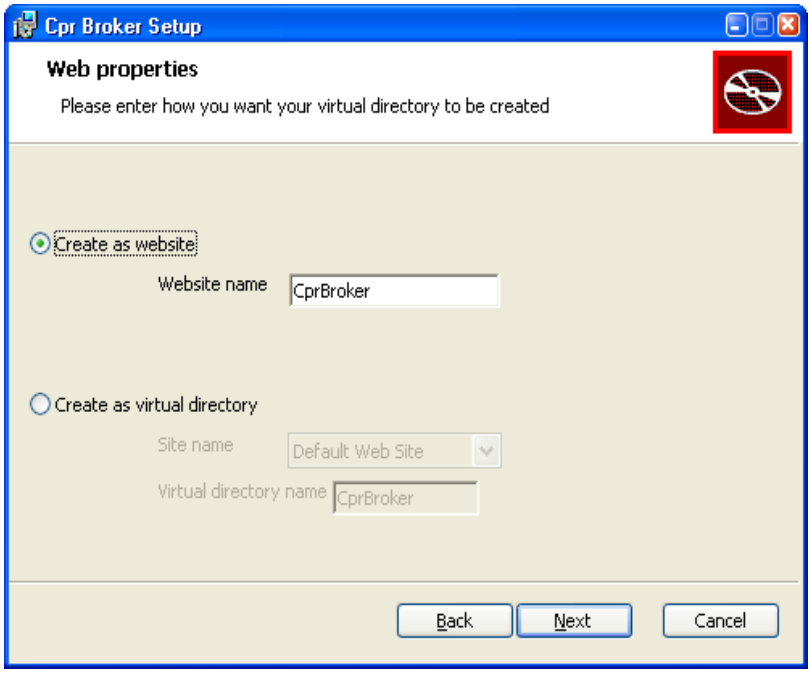


Now you will see this screen.



Choose where to install the files for CPR Broker. The default selection will most likely be a perfect fit. Click *Next*.

The installer now needs information on the CPR Broker web site should be installed



If your IIS can have multiple sites (on e.g. Windows 2003 and 2008), type the name of the website to be created. The default name is fine.

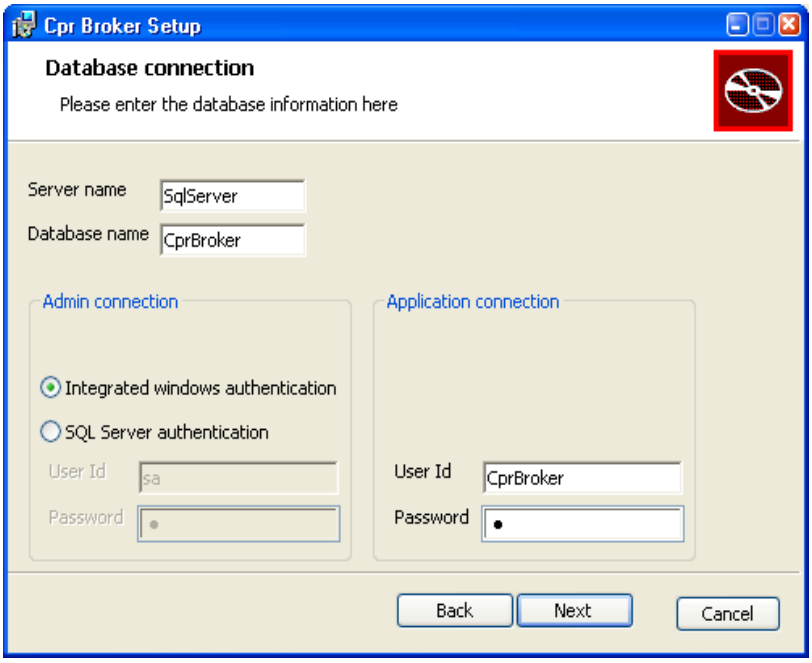
You can also choose to install as a virtual directory in an existing website. Choose the website from the list and type the name for the virtual directory. Default name is fine.

If you are installing on e.g. Windows XP you only have the option of installing as a virtual directory to the Default Web Site. The *CprBroker* application name will be okay for most purposes.

Click *Next*.

The installer now needs information necessary to create the database in which it stores copies of CPR -information.

The *Server name* is the name or IP-address of the computer on which the SQL Server resides. It could be *localhost* if the SQL Server resides on the same computer as the web site. If the server has multiple instances, type [ServerName]\[InstanceName]. Example is localhost\SQLEXPRESS



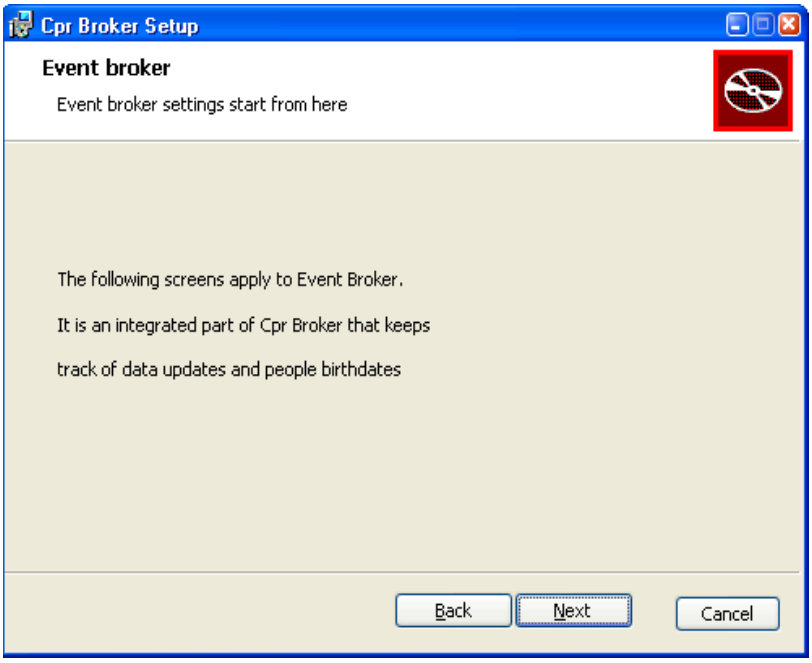
Database name is the name of the database. *CprBroker* would be a well chosen default name. If the database already exists, you will be given a warning message. If you accept it, the database will be used as it is. Please note that you will have to re configure the data providers because of encryption issues. Refer to the section “Data Providers” for details on how to do that.

Admin login is used for logging into the SQL Server and creating the database with the necessary tables etc. Whether you should use *Windows authentication* or *SQL Server authentication* depends very much on your setup. If the SQL Server is on the same computer as the web site you should most likely use *Windows authentication*.

Application login is used by the web site and services to connect with the database. The credentials needed for this purpose do not need to have as many privileges as the *Admin login*. Type the *User Id* and *Password* that you want the broker to use. If the user exists as a login, the password has to be the correct user's password. If not, the installer will create a new SQL login for you. In all cases, the user will be added to the db_owner role in the database.

When you are satisfied with your settings, click *Next*. The installer will test the information you have provided. You will see an error message if the information is invalid. Please check the information and click Next again in this case.

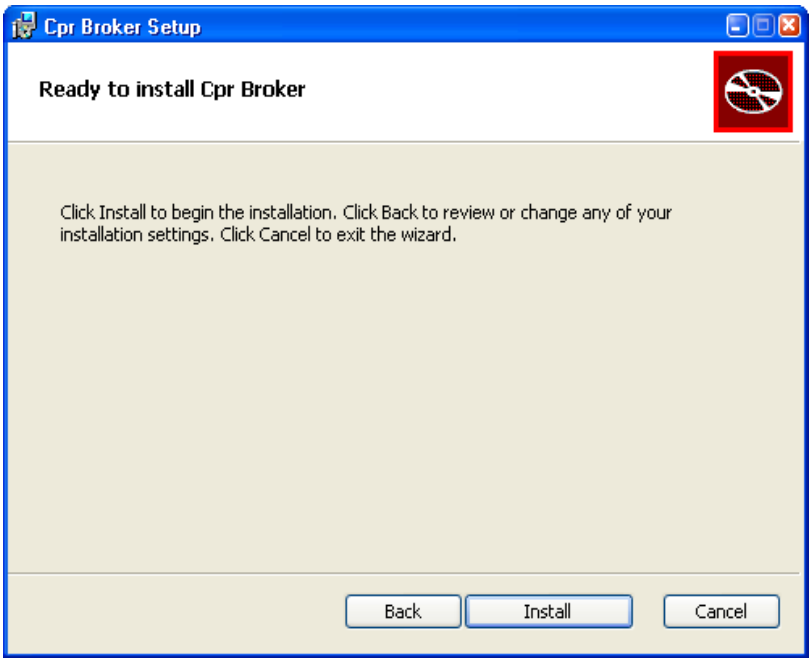
Now we have configured the web and database for the CPR Broker feature of the CPR Broker product. From this point, we will start entering the information for the Event Broker feature. The next screen will give you a warning.



Click *Next*.

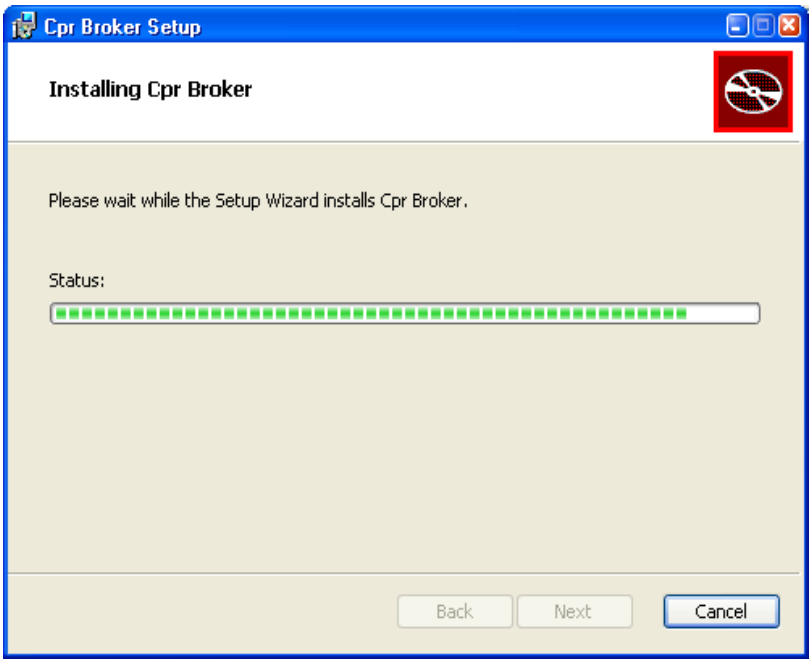
Now you will be prompted to enter the information for the web site and database of Event Broker. Please fill them as you did previously. Please make sure the web/database names you enter here are different from what you entered previously (for the CPR Broker feature).

After you are finished, you will see this screen.

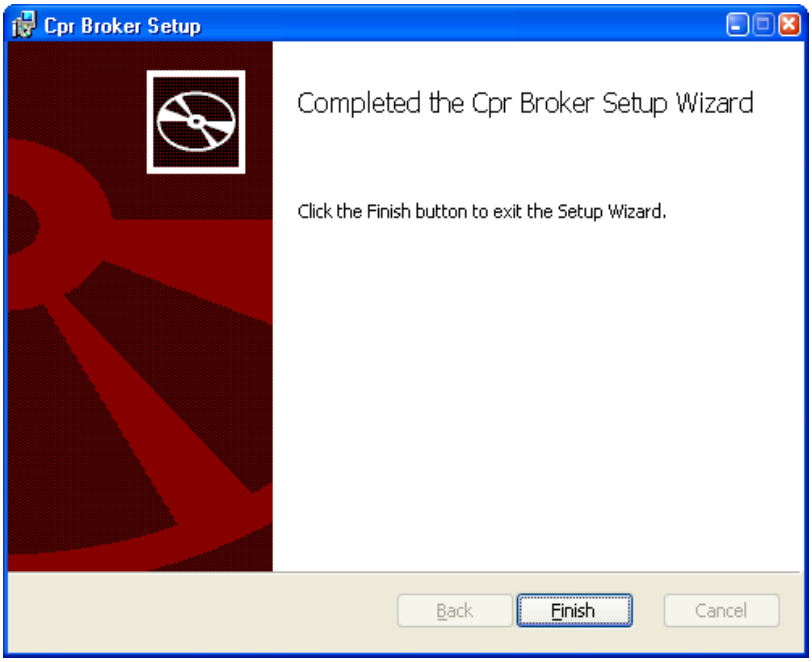


Now click Install to start the installation process.

You will see the progress screen



Wait until the process is finished. Then you will see this screen



Now everything is OK. Click *Finish* to close the wizard.

Done!!

4.2Silent installation

If you are the type of people who prefer to use command line interfaces, then you can also do a (semi) silent installation of CPR Broker.

If you are installing on an operating system that has user account control, please make sure you run the command as *Administrator*.

The command to use is

msiexec /qb /i CprBroker.msi /lv* SilentInstall.log [PROPERTY=VALUE,.....]

The following tables describes the parameters in details.

4.2.1Parameters belonging to windows installer

<table>
<tr><th>Parameter</th><th>Description</th><th>Example</th></tr>
<tr><td>/qb</td><td>Specifies user interface level. Could be<table><tr><td>/qn</td><td>Completely silent installation</td></tr><tr><td>/qb</td><td>Basic user interface. With progress dialogs</td></tr><tr><td>/qr</td><td>Reduced user interface</td></tr></table></td><td>/qb</td></tr>
<tr><td>/i</td><td>Path to msi package</td><td>/i CprBroker.msi</td></tr>
<tr><td>/lv*</td><td>File to use as a log (optional)</td><td>/lv* SilentInstall.Log</td></tr>
</table>

4.2.2Parameters specific to CPR Broker

These parameters are used to pass values for public properties. They are used in the form PROPERTYNAME=value

If the value contains a space, you need to enclose it in double quotations

PROPERTYNAME=”value with space”

Property	Description	Example value
WEB_CREATEASWEBSITE_CPR	To create CPR Broker feature as a website. ”True” means create as website, anything else means ”False”	True
WEB_SITENAME_CPR	Name of CPR Broker website. If WEB_CREATEASWEBSITE_CPR = True, this property has to be the name of an existing IIS website.	CprBroker
WEB_VIRTUALDIRECTORYNAME_CPR	Name of CPR Broker virtual directory. Only needed if WEB_CREATEASWEBSITE_CPR is false	CprBroker
DB_SERVERNAME_CPR	Name or IP address of database server on which to install CPR Broker database	SqlServer
DB_DATABASENAME_CPR	Database name for CPR Broker	CprBroker
DB_ADMININTEGRATEDSECURITY_CPR	If admin connection to SQL server uses integrated windows authentication. True or False.	True
DB_ADMINUSERNAME_CPR	User Id for admin connection (only if DB_ADMININTEGRATEDSECURITY_CPR <> True)	sa
DB_ADMINPASSWORD_CPR	Password for admin connection (only if DB_ADMININTEGRATEDSECURITY_CPR <> True)	<SqlPassword>
DB_APPSAMEASADMIN_CPR	Whether to use the same admin info for application login. Always set to False	False
DB_APPUSERNAME_CPR	User Id to be used by CPR Broker to connect to the database	CprBroker
DB_APPPASSWORD_CPR	Password for above user	<password>
WEB_CREATEASWEBSITE_EVENT	To create Event Broker feature as a website. ”True” means create as website, anything else means ”False”	True
WEB_SITENAME_EVENT	Name of CPR Broker website. If WEB_CREATEASWEBSITE_EVENT = True, this property has to be the name of an existing IIS website.	EventBroker
WEB_VIRTUALDIRECTORYNAME_EVENT	Name of Event Broker virtual directory. Only needed if WEB_CREATEASWEBSITE_EVENT is false	EventBroker
DB_SERVERNAME_EVENT	Name or IP address of database server on which to install Event Broker database	SqlServer
DB_DATABASENAME_EVENT	Database name for Event Broker	EventBroker
DB_ADMININTEGRATEDSECURITY_EVENT	If admin connection to SQL server uses integrated windows authentication. True or False.	True

DB_ADMINUSERNAME_EVENT	User Id for admin connection (only if DB_ADMININTEGRATEDSECURITY_EVENT <> True)	sa
DB_ADMINPASSWORD_EVENT	Password for admin connection (only if DB_ADMININTEGRATEDSECURITY_EVENT <> True)	<SqlPassword>
DB_APPSAMEASADMIN_EVENT	Whether to use the same admin info for application login. Always set to False	False
DB_APPUSERNAME_EVENT	User Id to be used by Event Broker to connect to the database	CprBroker
DB_APPPASSWORD_EVENT	Password for above user	<password>

For example, this command will install CPR Broker to CprBroker and EventBroker websites, create CprBroker and EventBroker databases on SQL server SqlServer, using integrated windows authentication, and the installed sites will use CprBroker and EventBroker users to connect to the databases.

msiexec /qb /lv* SilentInstall.log /i CprBroker.msi WEB_CREATEASWEBSITE_CPR=True WEB_SITENAME_CPR=CprBroker DB_SERVERNAME_CPR=SqlServer DB_DATABASENAME_CPR=CprBroker DB_ADMININTEGRATEDSECURITY_CPR=True DB_APPSAMEASADMIN_CPR=False DB_APPUSERNAME_CPR=CprBroker DB_APPPASSWORD_CPR=pwd WEB_CREATEASWEBSITE_EVENT=True WEB_SITENAME_EVENT=EventBroker DB_SERVERNAME_EVENT=SqlServer DB_DATABASENAME_EVENT=EventBroker DB_ADMININTEGRATEDSECURITY_EVENT=True DB_APPSAMEASADMIN_EVENT=False DB_APPUSERNAME_EVENT=EventBroker DB_APPPASSWORD_EVENT=pwd

5INSTALLING PERSON MASTER

Person master is an essential data provider for CPR Broker. CPR Broker relies on it to map CPR numbers to UUID's. This makes CPR Broker useless unless it is connected to at least one Person Master instance.

The installation procedure for Person Master is similar to CPR Broker. However, it is more simple. The differences are

- Person Master has only one database and one website.
- It can only be installed as a website (This means it must be installed on IIS 6 or higher)

5.1Needed information

As you did we CPR Broker, we need to prepare similar stuff. The difference is that the DNS record and database name are now for Person Master

In addition, you need to prepare

- A strong encryption key (just make one up) to be used by Person Master. It should be at least 8 characters long, contain lower and upper case characters, contain at least one digit and at least one non alphanumeric character.
- A domain name to be used in the database. Any string like “pm” (without quotes) would work.

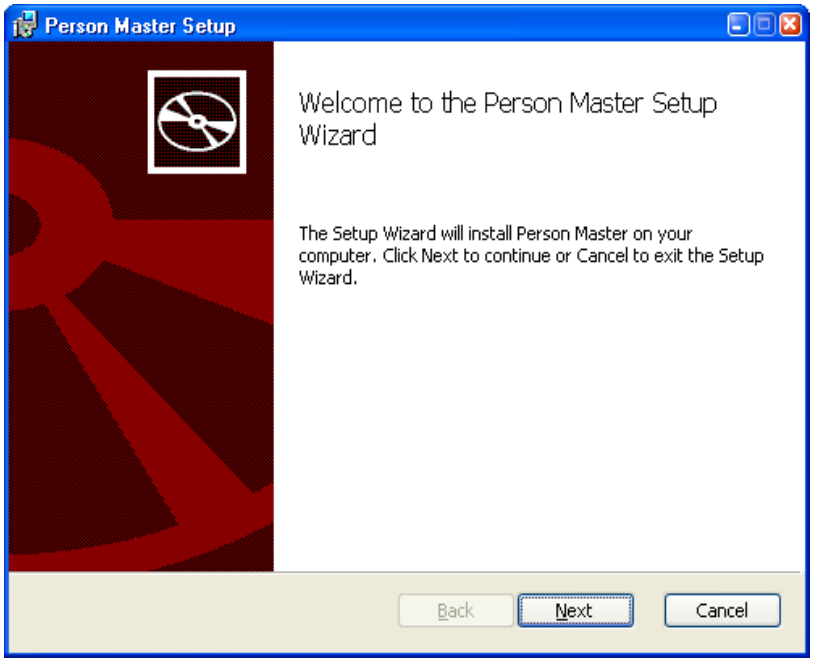
5.2Using the installation wizard

Double click the file PersonMasterInstaller.exe.

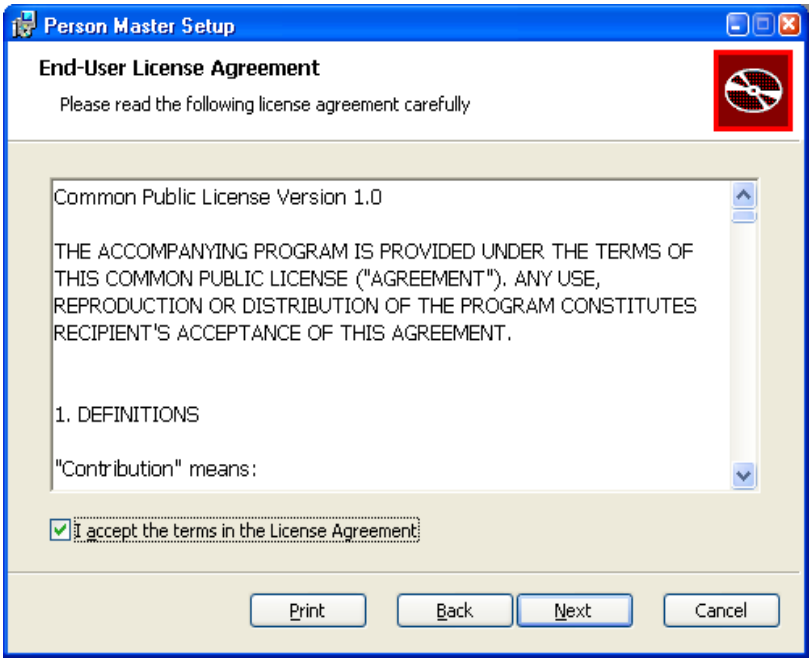
If the installer complains: 'This application requires IIS version 7. Please install IIS 7 and then run the installer again' it is due to [explain what causes this and how to fix it].

On a computer with *User Account Control (Vista/2008/ 7)*, the program will ask you to use elevated privileges. If you are comfortable with it, allow it to elevate.

You will see this screen

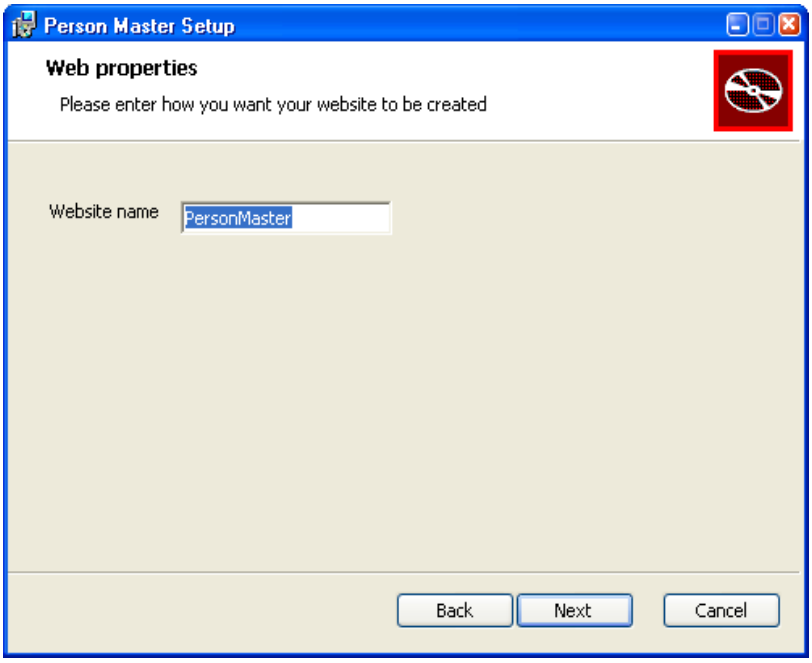


Click *Next*.

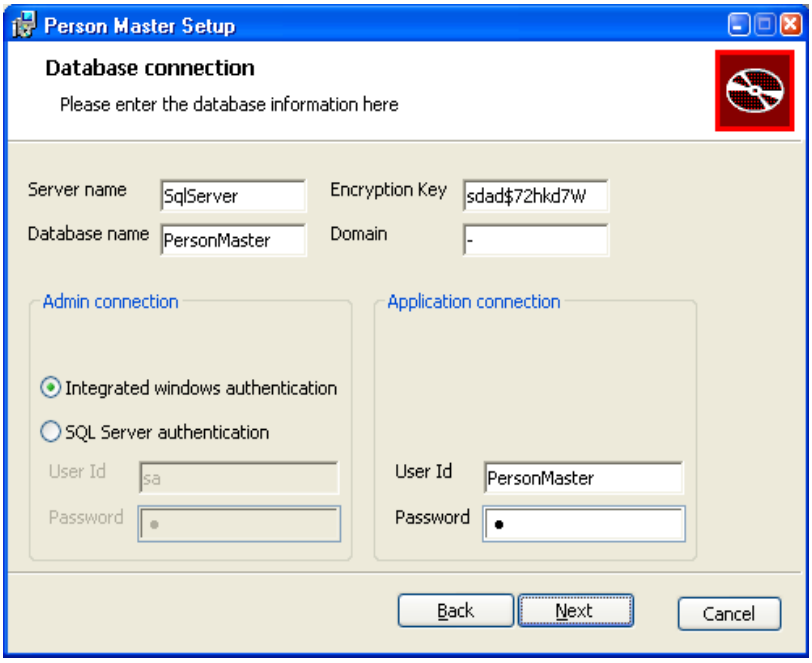


Accept the license terms and click *Next*.

Select the destination folder –the default value is OK- and then click *Next*.

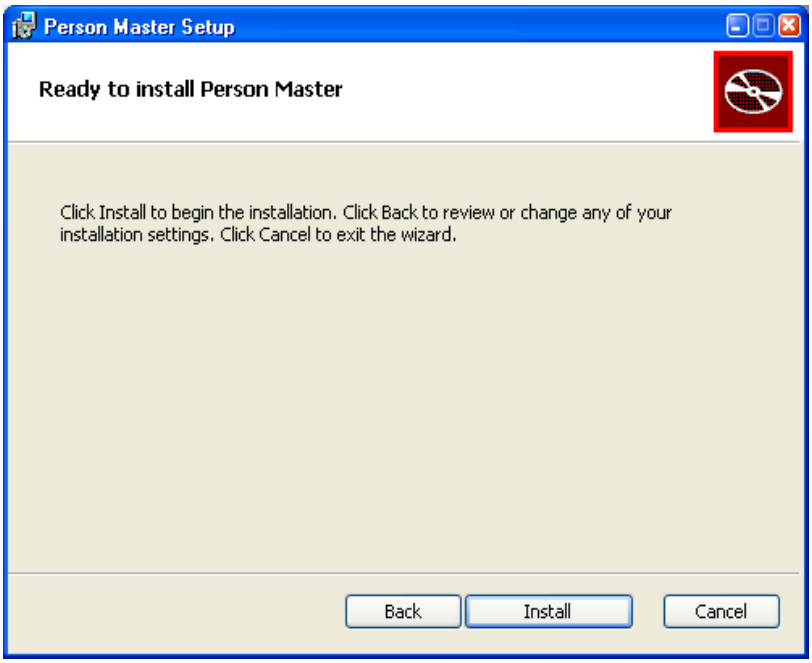


Type the name you want for the created website and click *Next*.

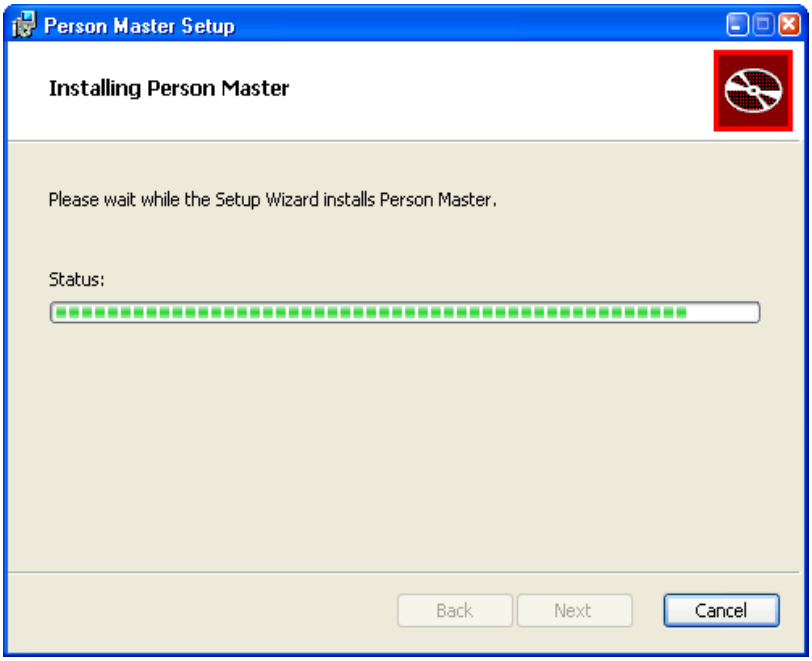


Type how you want to create the database. You can also use an existing database (in case you have previously installed PersonMaster manually). The installer will only guarantee access to the database, but will not create any database objects.

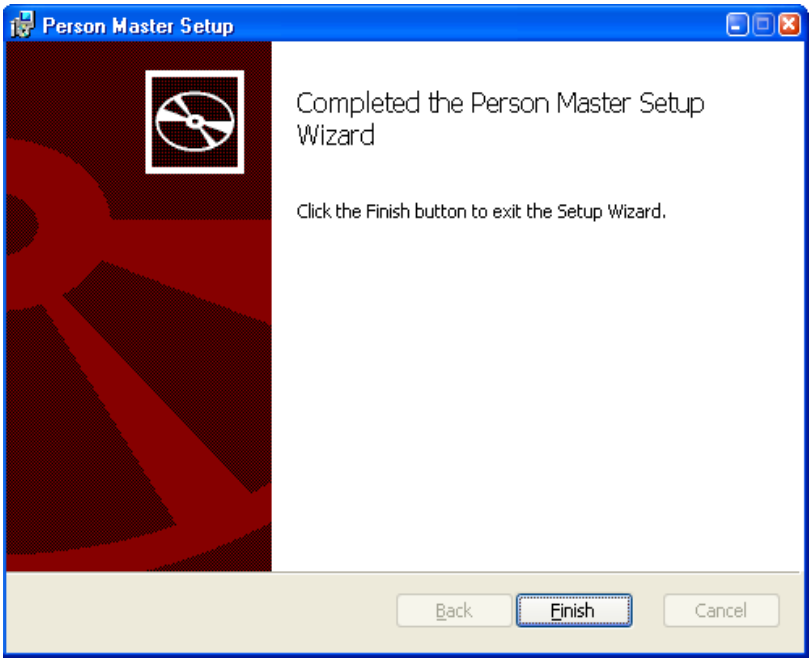
Click *Next*.



Now you have finished input of the needed information. Click *Install* to start the installation process. You will see the following window.



Wait until the installation is complete, and then you will see this:



Click *Finish* to close the wizard.

Done!!

5.3Silent installation

Just like CPR Broker, Person Master can be installed from the command line.

Again, if you are installing on a system with user account control, run the command prompt as *Administrator*.

The command to use is

msiexec /qb /i PersonMasterInstaller.msi /lv* SilentInstall.log [PROPERTY=VALUE,.....]

The properties are similar to CPR Broker, Except

- Installation must be as a website
- The property suffix is _PM (not _CPR or _EVENT). Since we have only one database and one website, we can skip the _PM suffix and just something like

  DB_SERVERNAME=SqlServer

5.3.1Parameters specific to Person Master

The following table gives more details

Property	Description	Example value
WEB_SITENAME	Name of CPR Broker website.	PersonMaster
DB_SERVERNAME	Name or IP address of database server on which to install Person Master database	SqlServer
DB_DATABASENAME	Database name for Person Master	PersonMaster
DB_ENCRYPTIONKEY	The symmetric key to be created and used to encrypt data. Enclose this in double quotes because the command line interprets non alphanumeric characters as a word separator.	“hdgueS^22”
DB_DOMAIN	String value that identifies the system.	pm
DB_ADMININTEGRATEDSECURITY	If admin connection to SQL server uses integrated windows authentication. True or False.	True
DB_ADMINUSERNAME	User Id for admin connection (only if DB_ADMININTEGRATEDSECURITY <> True)	sa
DB_ADMINPASSWORD	Password for admin connection (only if DB_ADMININTEGRATEDSECURITY <> True)	<SqlPassword>
DB_APPUSERNAME	User Id to be used by Person Master to connect to the database	PersonMaster
DB_APPPASSWORD	Password for above user	<password>

For example, this command will install Person Master to PersonMaster website, create PersonMaster database on SQL server SqlServer, using integrated windows authentication, and the installed site will use PersonMaster user to connect to the databases.

msiexec /qb /lv* SilentInstall.log /i PersonMasterInstaller.msi
WEB_SITENAME=PersonMaster DB_SERVERNAME=SqlServer
DB_DATABASENAME=PersonMaster DB_ENCRYPTIONKEY=<key>
DB_DOMAIN=”<domain>” DB_ADMININTEGRATEDSECURITY=True
DB_APPUSERNAME=PersonMaster DB_APPPASSWORD=pwd

5.4Upgrading Person Master

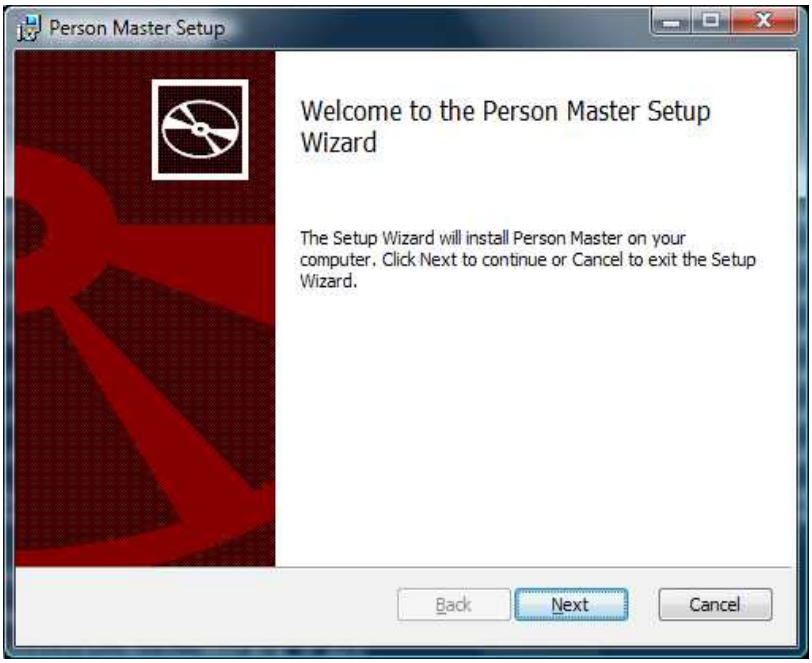
To upgrade Person Master from an older installed version, simply run the new installer.

As usual, on a computer with user account control (2008/7/Vista), please run the from an

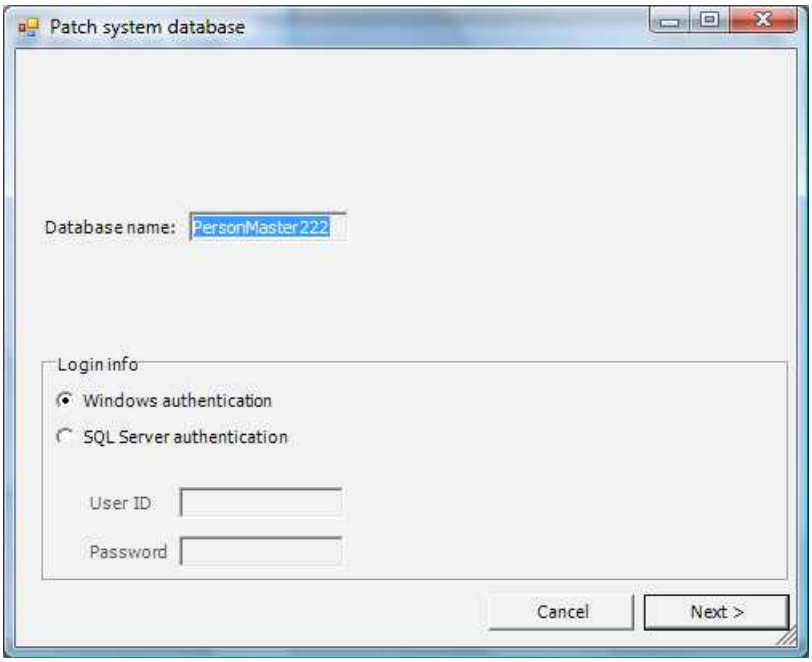
administrator command prompt.

msiexec /i PersonMasterInstaller.msi /lv* Install.log

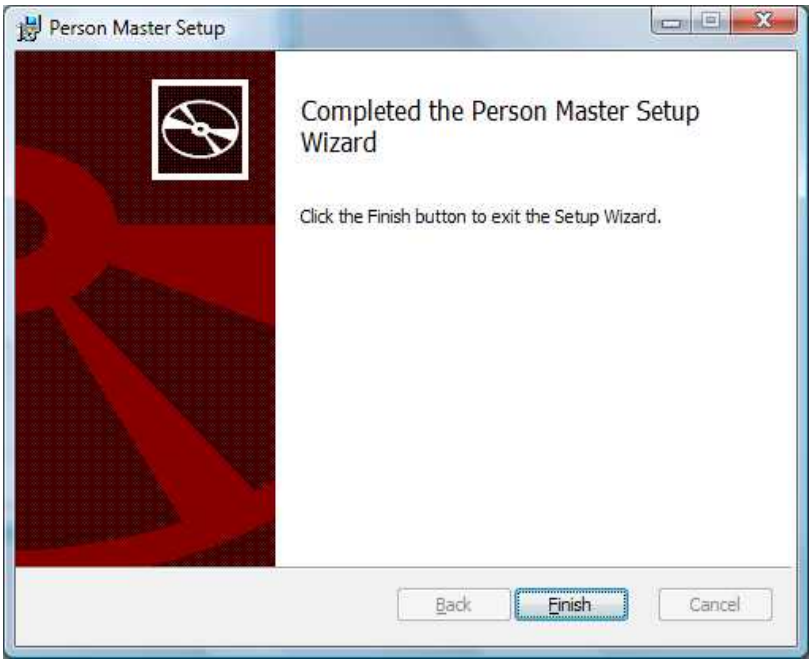
You will see the normal welcome screen.



You do not need to pass database and web information to the command. If the new version contains database upgrades, you will be asked to input a database admin connection.



Follow the wizard as usual until it is finished.



Done !!

5.5Uninstalling Person Master

To uninstall Person Master, run this command as an **administrator**:

msiexec /x PersonMasterInstaller.msi /lv* Uninstall.log

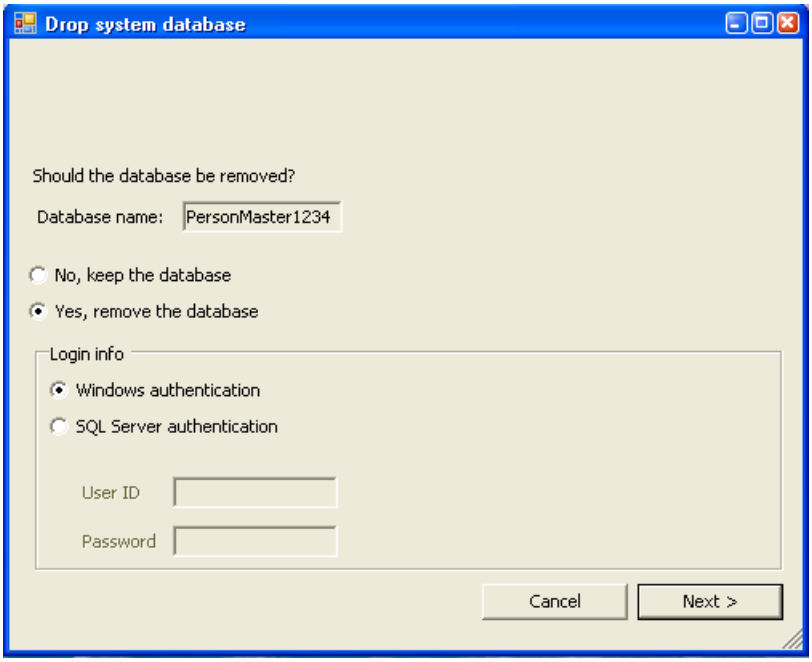
Alternatively, if you know the product code

msiexec /x <product code> /lv* Uninstall.log

The following table shows the product codes of Person Master so far.

Version	Product code
Up to 1.2.0	{DDB79617-A985-4841-9626-22779DED8D13}
1.2.1	{1F607476-879D-4931-B75E-048925C1272C}
2.0.0	{C66AD53A-395C-4471-A4DA-7D69F689F832}
2.1.0	{9980A898-4BB5-459C-B107-67335139FDD8}

You will be asked if you want to drop the database. If yes, you may need to provide a user account that is a member of sysadmin role in order to delete the database.

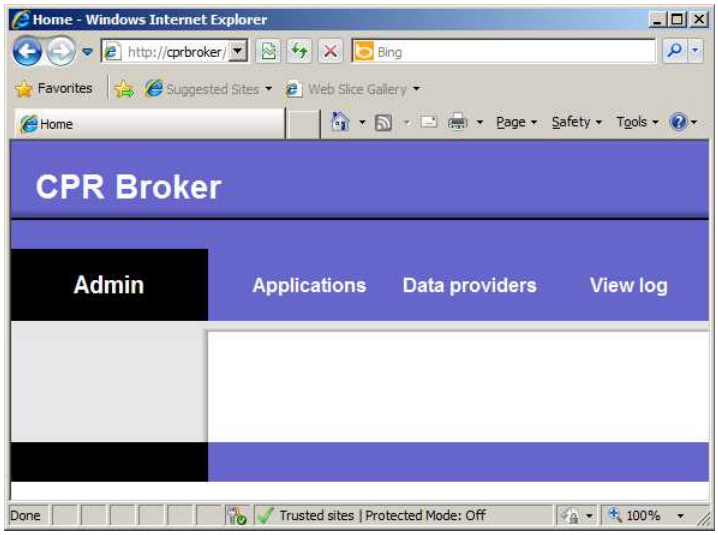


Click *Next*.

Now wait for the wizard to end, and Person Master is removed from your system.

6CONFIGURING CPR BROKER

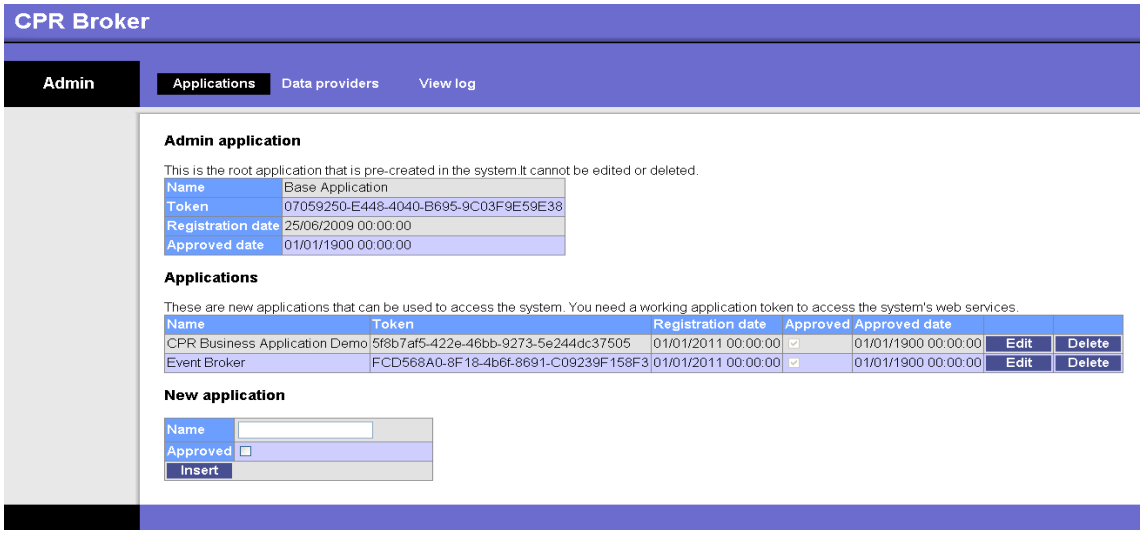
Open up a browser and point it to *http://localhost/CprBroker/Pages/Applications.aspx* (or wherever you chose to install it) to see whether your installation was successful



This is a basic interface but it does get the job done.

6.1Applications

Now click *Applications*:



For a client application to be able to use the broker, it needs to use an application token that uniquely identifies the application. This is modelled by the concept of *Application* in the broker.

An application has a unique name and a unique token. The name is a user friendly string

that can be seen in the log entries identifying relevant log entries. The token is a unique key sent with all web service requests to tell the broker which application is making the call. The token is an auto generated GUID (Globally Unique Identifier) by default, but it can be changed to be any string that uniquely identifies the application. The application needs to be approved before it can be used.

Applications can be created through the Applications page and also through web services. Name and token can be changed through the user interface (only), but they still have to be unique.

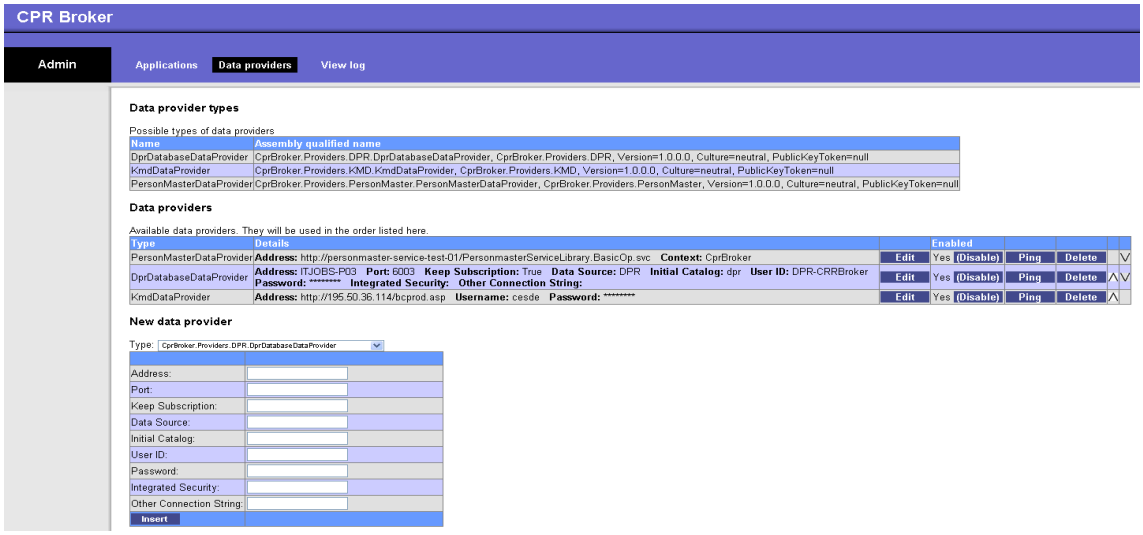
The system comes with three pre approved applications. The *Admin application* is a built-in name for an application that is allowed to work with the administrative parts of the CPR Broker. The other two applications are the event broker and the demo application. Please leave these two applications untouched.

To approve an application, simply click *Edit* for the application in question and check the *Approved* check box. Then click *Update* (only shown after *Edit*).

To create an application, simply give it a *Name* and whether it should be initially approved (it probably should). Then click *Insert*. The application is now listed under *Applications*.

6.2Data Providers

Now click *Data Providers*:

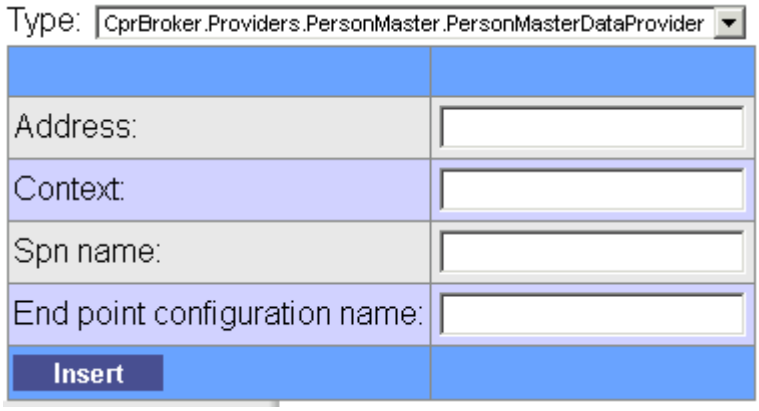


A *Data Provider* is a connector that provides the broker with information. CPR Broker itself does not produce data, but rather queries other systems for data.

To setup any of these connections you need an account and connection information from the provider. Then choose the appropriate provider type, enter the information and click *Insert*. You now have a Data Provider.

In order for the broker to be usable, it must be told where to get people's data from. There are two groups of data providers:

6.2.1Person master data providers



Used to assign UUID's to CPR Numbers. It gets UUIDs from the specified person master service.

Address is the address of the service (http://.../PersonmasterServiceLibrary.BasicOp.svc).

Context is any arbitrary string that identifies the broker instance.

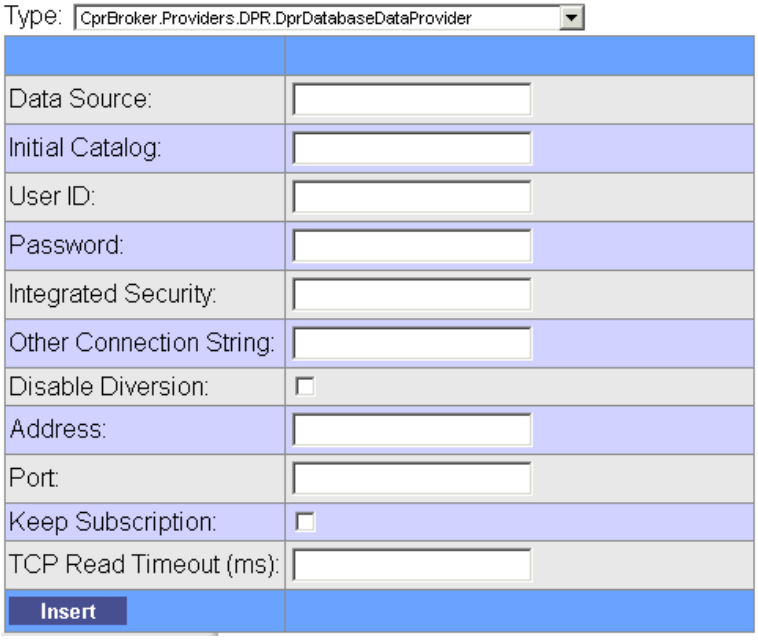
Spn name is a parameter used by the service that you should get from the administrator, or by checking the WSDL file of the actual service instance. You can find the WSDL file by following the link in Person masters default page (<Person master URL>/Default.htm).

6.2.2CPR data providers

These data providers are the ones that retrieve the detailed information of persons. There are currently a few data providers that are implemented, described below.

6.2.2.1DPR

Address and *Port* are TCP address and port of the DPR forwarding (DPR Viderestilling) service.

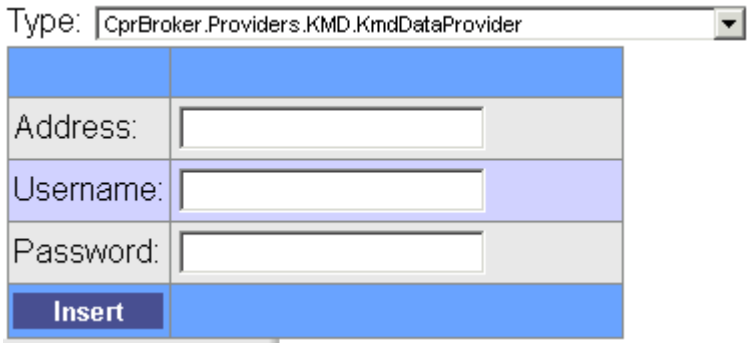


Keep Subscription tells the instance whether to set a subscription when requesting data from DPR forwarding in case data is not already in DPR. It can be either *True* or *False*.

Disable Diversion disables the usage of DPR forwarding altogether (in case you want to save money).

The rest of the parameters are used to build an *SQL Server* connection string that points to the DPR database. Let the database properties point to the DPR database. 'Data Source' is the sever name, 'Initial Catalog' is the name of the database. [Integrated security is...?]

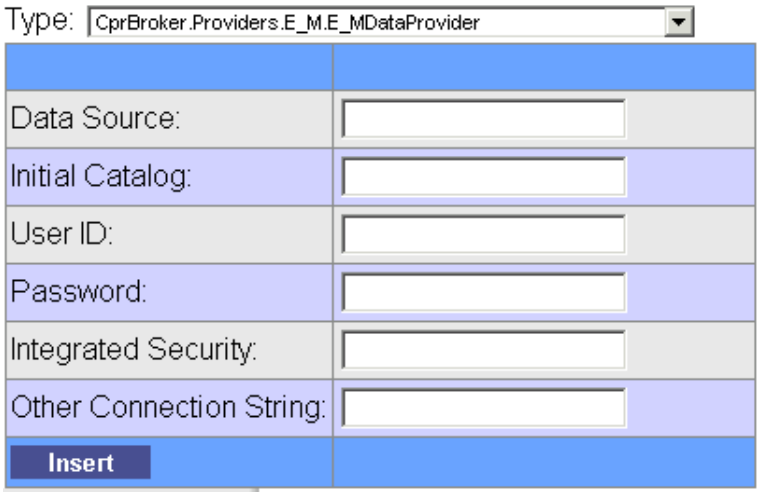
6.2.2.2P-Data (KMD)



Address is the web service base address (http://their.domain/kmd/pData). The broker will add the parameter zservice=AN08002 (or whatever service) when actually calling the web services.

Username and *Password* are sent with the requests.

6.2.2.3E&M

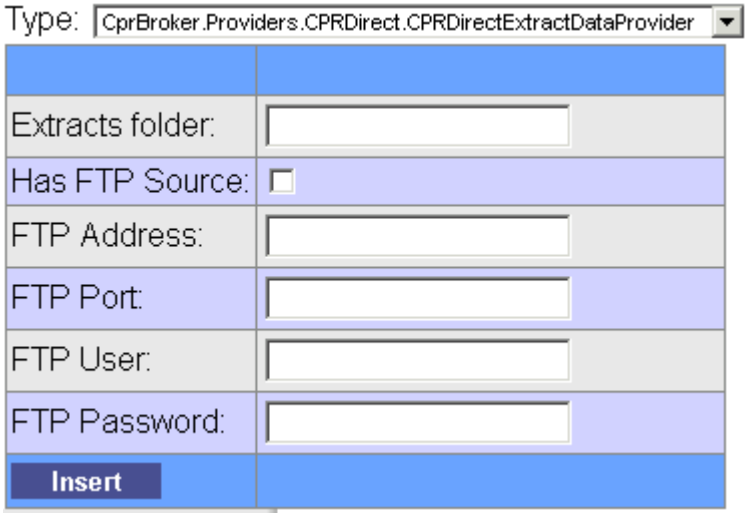


The configuration properties are used to connect to the E&M database. It is preferable not to use integrated windows authentication.

6.2.2.4CPR Direct

There are two types of data providers for CPR Direct

CPR Direct Extract

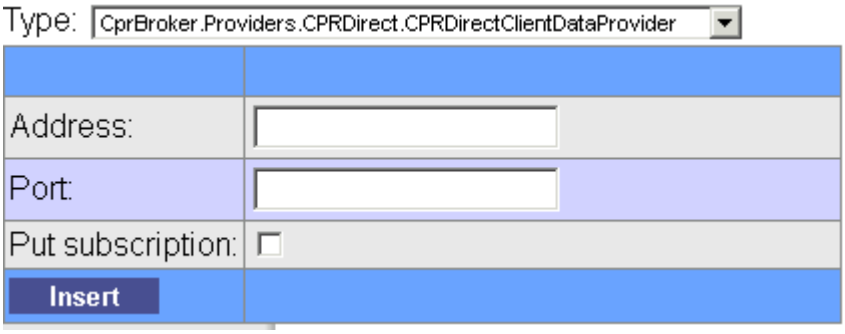


This data provider looks for change extract files at a configurable location on the server/network. It is very important that the user 'Network service' has full access to the path, otherwise it will not work. The field 'Extracts folder' should contain the path to the folder in which the extracts go.

It is also possible to get the files from an FTP location. It takes parameters for the folder

location for files and also how to access the FTP site (if needed).

CPR Direct Client



This data provider calls a TCP/IP interface provided by CPR Direct Client service. The service should be installed on the local network. This provider gets parameters for address, port, and whether a subscription to be put on the person.

It is strongly recommended to configure it with 'Put Subscription = True'

7CONFIGURING SECURITY

7.1Restricting access to the website

CPR Broker is installed with default to allow access to everybody as long as they can access the server on which it is installed via HTTP.

In real life, this is not exactly how you want things to be. This section describes how to limit access to CPR Broker admin pages. The following sub sections will describe two examples of the configuration on **Windows Server 2008 R2** and **Windows 7**.

Please note that PersonMaster is built using a different technology stack and hence requires some different steps. It has been modified, though, so that it can be configured very similarly to the other two components.

7.1.1Add necessary software and Configure IIS

7.1.1.1Production environment

This section assumes that the server is a member of a domain and that the DNS entries for the website have been correctly put into the DNS. The exact steps are for **Windows Server 2008 R2**

- Install Windows Authentication (if not already installed):

  Start → Server Manager → Roles → Web Server (IIS) → Role Services → Add Role Services → Web Server → Security → Windows Authentication
  Make sure it is checked and press OK.

- Start → Internet Information Services (IIS) Manager → Sites → <your CPR broker site> → Authentication
  Anonymous Authentication → Disable
  Windows Authentication → Enable

7.1.1.2Test/Development environment

This section assumes that the machine is not a member of a domain and that the host name for the site has been manually added to the hosts file (C:\Windows\System32\drivers\etc\hosts). The exact steps are for **Windows 7 SP1**

- Install Windows Authentication (if not already installed):

  Start → Turn Windows Features on or off → Internet Information Services → World Wide Web Services → Security → Windows Authentication.

Make sure that it is checked and press OK.

- Start → Internet Information Services (IIS) Manager → Sites → <your CPR broker site> → Authentication
  Anonymous Authentication → Disable
  Windows Authentication → Enable

- Start → regedit.exe → HKEY_LOCAL_MACHINE → SYSTEM → CurrentControlSet → Control → Lsa → MSV1_0
  Create a new value
  Type: Multi String
  Name: BackConnectionHostNames
  Value: <your cpr broker site name>

7.1.2Edit the site's configuration file

This is an XML file where you can configure the website. It should be usually located at "C:\Program Files (x86)\ITST\Cpr Broker\CprBroker\Website\web.config"

- First, look for node <authentication> under <system.web>. Make sure it looks like:
  ```
  <authentication mode="Windows" />
  ```

- Add this section under <configuration> node:
  ```
  <location path="Pages">
   <system.web>
   <authorization>
   <allow users="<domain>\<user name>"/>
   <allow users=".\<local user name>"/>
   <allow roles="<<domain>\<role name>"/>
   <deny users="*"/>
   </authorization>
   </system.web>
  </location>
  ```

  Please replace the text text marked with <> with actual values from your environment. For example:
  <domain>\<user name> → mydomain.dk\myuser

7.1.2.1Services

If you want to apply this also to web services, do the same, but then put a different path

```
<location path="Services">
..
</location>
```

In general, you can do the same for any virtual path within the website

Note
In case you restrict access to something under path 'Services', then any client applications using CPR broker will have to run as a user that is matched in the <allow> elements.

7.1.2.2Person Master related

When setting SSL for PM remember to change from 'httpGetEnabled' to 'httpsGetEnabled'.

7.2Backend service

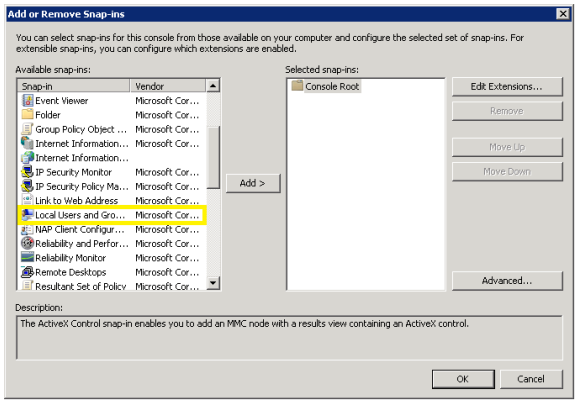
The backend service is, on install time, set to run as 'NT Authority\Network Service'. As this could create a posible security hole if the broker is exposed to the outside of the domain, it is advisable to create a new user by whom the service can be run.

7.2.1Run the backend service as a local user

7.2.1.1Creating a local user

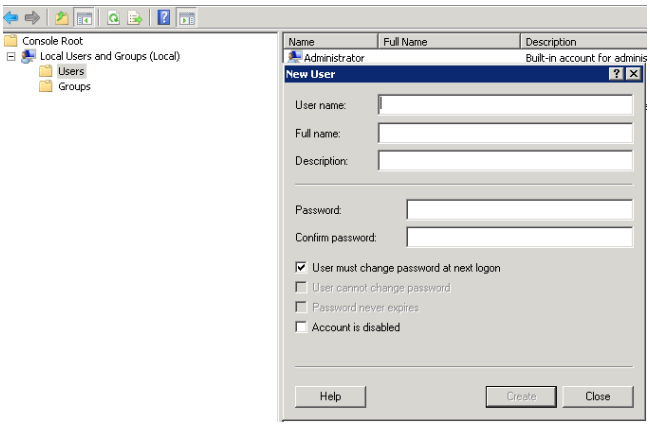
First we must add a local user on the server. On Windows Server 2008 R2 that is done in the Microsoft Management Console (MMC). You can enter the MMC by typing 'mmc' in the search field from the start menu.

In the MMC select File->Add/remove Snap-in. Then select 'local users and groups' and click the 'Add' button. Finish by clicking 'OK'.



Now right click in the central area and choose 'New user'. Type in the credentials for the new user. Remember that the password must be CaMeL case and must containt both

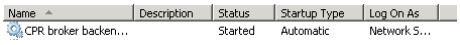
numbers and special characters.



When that is done you can close the MMC.

7.2.1.2Changing the user of the backend service

Open the services dialog (eventually by typing 'services' in the search field of the start menu). Navigate to the service called 'CPR Broker Backend' and right click it.



Firstly select 'Stop' and secondly select 'Properties' and choose the tab 'Log On'. Now, click the 'Browse' button and type in the name of the newly created user and click 'OK'. Then fill in the password, click 'Apply' and finally 'OK'.

Right click the service again and select 'Start'. Now it should all be done and the service should be run as the new user.

7.2.1.3Changing the user of the websites

In IIS Mangement Studio go to 'Application Pools' in the left-hand menu. Right click a website and select 'Advanced Settings...'. In the dialog, locate the row beginning with 'Identity'. When you click it a button with 3 dots appears (). Click it and select 'Custom Account' and click 'Set...'. In the dialog, specify the credentials of the new user and click 'OK'.

Now, do the same for all the wbsites.

7.2.1.4Allowing access for the local user

If you have restricted access to any of the components of the broker, you will also have to allow the local user access to these components. Thus add an 'allow' element for the user under the 'authorization' element, as stated in section 7.1.2.

7.3Using SSL

As extra security measures for your website, you can also enable usage of SSL in the website. In order to do this, you need to create a certificate and link it to the website. The steps are described in the following sub sections.

7.3.1Note

Please not that if you apply SSL to EventBroker then you will also have to change the URL setting EventsServiceUrl section in the configuration file 'CprBroker.EventBroker.Backend.exe.config' (usually stored in 'C:\Program Files (x86)\ITST\Cpr Broker\EventBroker\Website\bin'):

```
<CprBroker.Config.Properties.Settings>
    <setting name="EventsServiceUrl" serializeAs="String">
      <value><YOUR_HTTP_URL_TO_EVENTBROKER></value>
    </setting>
</CprBroker.Config.Properties.Settings>
```

Here you will content of the value field to the HTTPS URL.

7.3.2Creating a certificate

There are several ways to do this, depending on the actual need for SSL.

7.3.2.1Domain certificates

This is usually the most common way to use. If you have a domain controller, you can create a domain certificate. This certificate will usually be trusted by default within your Intranet.

Start → Internet Information Services (IIS) Manager → Server Certificates → Create Domain Certificate → (Fill fields) → Next → (Select certificate authority) → OK

7.3.2.2Self Signed certificates

If your client applications will all run locally, then you probably only need to encrypt communication to/from CPR broker without the need of clients to validate the site's identity. If this is the case, you can create a self contained certificate as follows:

Start → Internet Information Services (IIS) Manager → Server Certificates → Create Self-Signed Certificate → (Enter name) → OK

Note
If you follow this way, usually the client applications need to be changed so that they accept the certificate. This way is only recommended for development and testing environments.

7.3.3Configuring HTTPS bindings

CPR broker is installed with HTTPS bindings so we only need to select the certificate to be used with the binding.

Start → Internet Information Services (IIS) Manager → Sites → <your CPR broker site> → Edit Bindings → (select the one with https) → Edit → SSL certificate → (select your certificate) → OK → Yes

Note
If needed, you can delete the HTTP binding to force SSL communication to the website.

7.4Person Master

While CPR Broker and Event Broker are build as ASP.NET web pages and services, Person Master is built as a Windows Communication Foundation (WCF) service. This means that it requires different procedures for securing the service.

Typically, you will need to:

- Adjust the site settings in IIS Manager as you did for CPR Broker and/or Event broker
- Configure <system.serviceModel> / <bindings> / <wsHttpBinding> / <binding> elements
  You will change the list of elements based on your scenario
- Configure <system.serviceModel> / <service> / <endPoint> elements
  You will change the list of elements based on your scenario
- Leave/Remove mex end point (under <system.serviceModel> / <service> / <endPoint>)based on your scenario

```
<endpoint binding="mexHttpBinding" name="mex" contract="IMetadataExchange"
/>
```

7.4.1Scenarios

There are tons of options to configure WCF services. We have chosen a few simple scenarios, taking into consideration compatibility with CPR broker.

The settings in IIS need to be paired with settings in the configuration file. We have come up with three possible scenarios that you can choose from based on your requirement for security and compatibility with CPR Broker.

If you use one of these modes, CPR broker will decide which one to use based on whether the address URI scheme (http/https).

This table summarizes what needs to be done:

Section	Insecure only	Secure only	Both
Description	This is the "implicit" default for Person Master. Compatible with all versions of CPR broker.	Supports transport level security for communication with CPR broker.	Allows secure communication while keeping backwards compatibility with older versions of CPR broker
Enabled authentication methods in IIS	Anonymous only	Windows only	Anonymous and Windows
<binding> elements	<binding name="insecure"> <security mode="**Message**"> <message clientCredentialType="Windows"/> </security> </binding>	<binding name="secure"> <security mode="**Transport**"> <transport clientCredentialType="Windows"/> </security> </binding>	(Both binding elements)
<endPoint> elements	<endpoint address="PersonMasterService12" binding="wsHttpBinding" bindingConfiguration="insecure" name="wsBasicHttpInSecure" contract="PersonmasterServiceLibrary.IBasicOp" />	<endpoint address="PersonMasterService12" binding="wsHttpBinding" bindingConfiguration="secure" name="wsBasicHttpSecure" contract="PersonmasterServiceLibrary.IBasicOp" />	(Both endPoint elements)
'mex' end point	Can exist	Must be removed	Can exist
URI Schemes	Http	Https	Http/Https
Compatible CPR Broker versions	Any	2.1.1 or above	Any for insecure 2.1.1 or above for secure

7.4.1.1Custom end points

If you are really a WCF guru, you can customize the end points in Person Master as you wish. The exact details are out of the scope for this document, but an overview is listed

below:

- Create endPoint element(s) in Person Master configuration file
- Create endPoint element(s) in CPR Broker configuration file.
- Set the “End point configuration name” attribute for the person master data provider to the name of the end point that you have created.
- Clear all other attributes for person master data provider.

Note
This option is available in CPR broker version 2.1.1 and above

7.4.2Limiting access to the service

Limiting access of WCF service to specific users or roles is more complex than regular ASP.NET sites. We have chosen the approach of creating a custom class that inherits ServiceAuthorizationManager, and then write its code to decide what to allow or deny.

7.4.2.1Creating a custom authentication manager

- Create a new .NET Dll, based on .NET Framework version 4
- Add a class that inherits from ServiceAuthorizationManager. Code should be something like this

```
using System;
using System.Collections.Generic;
using System.Linq;
using System.Text;
using System.ServiceModel;
namespace Authorization
{
    public class PersonMasterServiceAuthorizationManager:
      ServiceAuthorizationManager
    {
        protected override bool CheckAccessCore(OperationContext
      operationContext)
        {
            //TODO: Replace this with your code
            return base.CheckAccessCore(operationContext);
        }
    }
}
```

7.4.2.2Editing the site's configuration file

- Under the “behavior” element corresponding to the end point, add this `<serviceAuthorization principalPermissionMode="UseWindowsGroups" serviceAuthorizationManagerType="<Type name>" >`
- Replace the value of attribute “serviceAuthorizationManagerType” with the type name of the class that you have created. This could be something like “Namespace.ClassName, AssemblyName”.

8SETTING UP LOGGING

CPR Broker can log to file, Windows Event Log, to the Database and to email.

There place to setup logging: In the *loggingConfiguration.config* file for CPR Broker web service. The default position for this is *C:\Program Files\ITST\CPR Broker(Event Broker)\Web\Config*

Additional location for Event Broker: in *the CprBroker.EventBroker.Backend.exe.config* file for the Backend service. The default position for this is *C:\Program Files\ITST\Event Broker\Web\bin*.

The procedure is the same for both files. Locate the `< loggingConfiguration>` tag in the specific config file. Under the `<listeners>` tag you will find four `<add` tags. The `"CprDatabase"` as well as the `"EventLog"` should be left untouched in all cases.

In `"FlatFile"` you should look for the `fileName` attribute. This should be set to the full path and name of the where to put the log file. By default, the path is“[InstallDir]CprBroker\Website\CPR Broker.log”. The installer will create the file and give CPR Broker the necessary permissions to write to it.

In `name="Email"` there are more settings. The ones most likely to be adjusted are: `toAddress`, `fromAddress`, `smtpServer` and perhaps `smtpPort`.

Please note: If you change FlatFile, you need to make sure that the ‘NT AUTHORITY\NETWORK SERVICE’ account has sufficient access rights to the destination.

You have now adjusted the settings for each type of logging, but you have yet to set what types of logging are *active*. You now look for the `<specialSources>/ <allEvents>` tag. In this you will another `<listeners>` tag. Per default `"CprDatabase"` is active, which can be seen from the fact that it is not commented out like e.g. `<!--add name="EventLog" /-->` is.

To enable a specific listener simply remove the `<!--` and `-->` characters from the line. And to disable a listener simply put them back in.

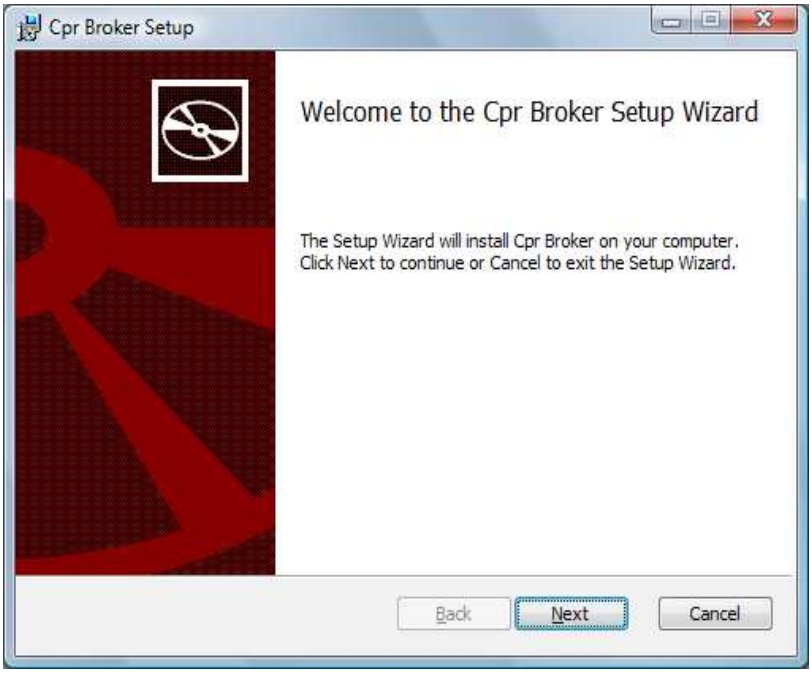
9UPGRADING CPR BROKER

To upgrade CPR Broker from an older installed version, simply run the new installer.

As usual, on a computer with user account control (2008/7/Vista), please run the from an administrator command prompt.

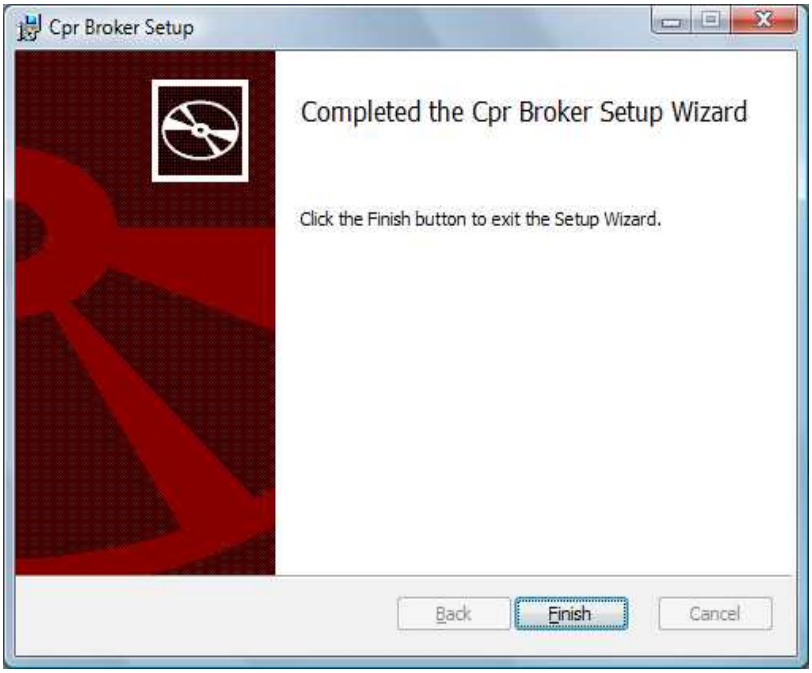
msiexec /i CprBroker.msi /lv* Install.log

You will see the normal welcome screen.



You do not need to pass database and web information to the command. If the new version contains database upgrades, you will be asked to input a database admin connection. There are no database upgrades so far, so you will not be asked for it at the moment.

Follow the wizard as usual until it is finished.


Cpr Broker Setup
Completed the Cpr Broker Setup Wizard
Click the Finish button to exit the Setup Wizard.
Back
Finish
Cancel

Done!!

10UNINSTALLING CPR BROKER

To Uninstall CPR Broker, run this command as an **administrator**:

msiexec /x CprBroker.msi /lv* Uninstall.log

Alternatively, if you know the product code

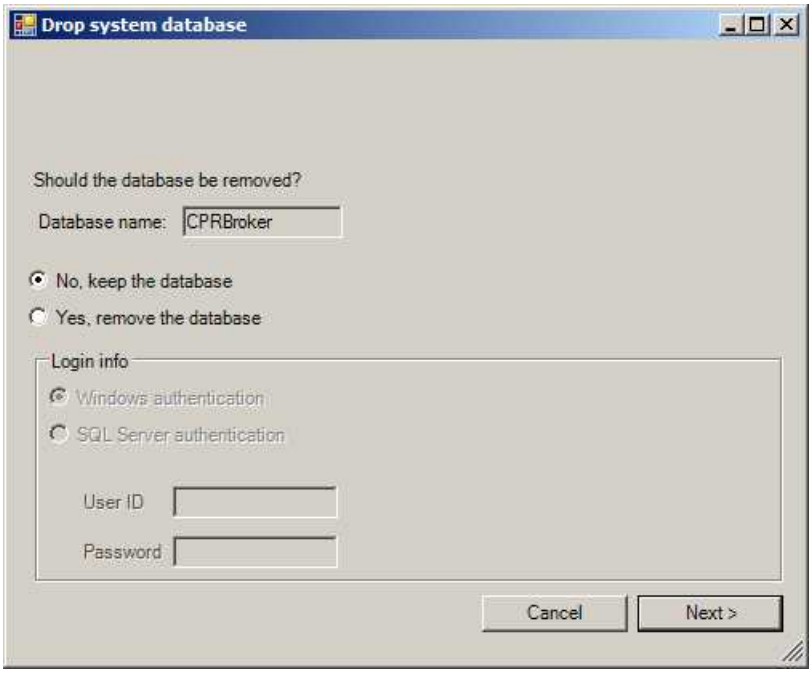
msiexec /x {product code} /lv* Uninstall.log

The following table shows the product codes of CPR Broker so far. The code of interest is the version of the latest version that you have installed.

Version	Product code
Up to 1.1.1	{30875D64-A423-4CCD-A929-5DD556A90EDD}
1.1.2	{509416EA-BD78-42ED-BD9C-C2557E2D5872}
1.2.0	{0570C9B9-0BED-4F6E-BE96-999A7C904DCC}
1.3.0	{929977A9-19B9-4F37-BFDD-46FD5E86FAC0}
1.3.1	{8EDC4FA8-83CD-4997-9E76-F0EA2D08038D}
1.3.2	{83D6E13C-3BD6-4DC2-B375-4272390C1F4C}
1.4.0	{49822D46-27B2-4340-9BCC-AEB9C4470E6F}
2.1.0	{DEBB9B03-91B6-490B-B21A-55B1DF5BBA01}
2.1.1	{8FD4F5C5-C8C0-4077-BE4D-4180E0627078}
2.2.0	{B7B04971-4A23-4387-8C78-1702FAEE9D72}

You will be asked twice if you want to drop the database. First time is about CPR Broker database and second is about Event Broker database.

If you choose to drop the database(s), you may need to provide a user account that is a member of sysadmin role in order to delete the database(s).



Click *Next*.

Now wait for the wizard to finish, and then CPR Broker is removed from your system.

11INSTALLING A TEST SERVER

It is sometimes needed to create a sandbox installation so that developers can use it to test code without dealing with real data.

You will need

- Access to CPR broker admin interface, usually at
  http://cprbroker/Pages/Applications.aspx
  and
  http://cprbroker/Pages/DataProviders.aspx
- Administrator access to the server where CPR broker is installed
- Server should have SQL server management studio installed. You should also have 'sysadmin' access to an instance of SQL server
- Get the files for BatchClient, DPR test database ('DPR_TEST20110616.bak'), and CPR Direct sample extract (U12170-P opgavenr 110901 ADRNVN FE)

The steps needed are a follows:

11.1CPR Broker/Person Master

- Install CPR broker as usual
- Install a test instance of Person Master (or use an existing one).
- Create a new data provider of type Person Master, let it point to the test instance of Person Master (please refer to the 'Person Master' section for details).
  Note: Please make sure not to configure a test instance of CPR broker to use a production instance of Person Master.

11.2CPR Direct

- Create a folder somewhere on the server, something like C:\CPRDirectExtracts
- Set the security of the folder so that everyone has full access to it.
- Put the file 'U12170-P opgavenr 110901 ADRNVN FE' in the folder.
- Add a CPR Direct Extract data provider (please refer to the 'CPR Direct' section for details), with 'Extracts Folder' pointing to your folder, and 'Has FTP Source'=False.
- If the installation is OK, the file should be automatically imported and moved to '\Processed' folder under the folder you have created.

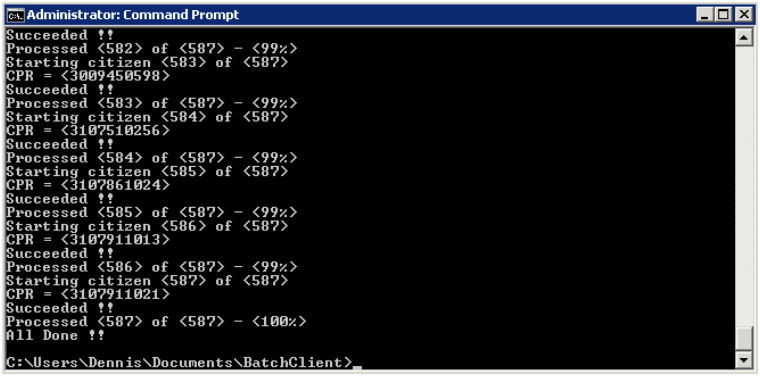
11.3DPR

- Create an empty database called DPR (or whatever) in SQL server.
- Restore the file 'DPR_TEST20110616.bak' to the DPR database
- Create an SQL login / user with membership in 'db_owner' role in the DPR database
- In the DPR database, run this command
  SELECT PNR FROM DTTOTAL
  Copy the result in a text file and save it somewhere, say 'C:\DPR-PNRs.txt'
- In the applications page, create a new application called 'Batch Client'. Set approved = true.

  The important part is to note the application token:

- In CPR Broker's DataProviders.aspx page, create a new provider of type DPR (refer to the 'Data providers' section). Set DisableDiversion=True. Let the database properties point to the DPR database you previously created and 'Integrated Security' should be set to 'false'.
- In a command prompt, run batch client as follows:
  BatchClient.exe /envType "BatchClient.RefreshData, BatchClient" /source "C:\DPR-PNRs.txt" /partUrl "http://cprbroker/Services/Part.asmx" /appToken "133b16df-37e0-4849-9957-70b09a60500a" /userToken MyUser

  Please replace values for /source, /partUrl, and /appToken with the actual values for file with the CPR numbers from DPR, URL of Part service in CPR broker, and the application token created for BatchClient application.
- Let the process run for a few minutes and make sure that successful conversion is the most common case. It should look something like this:



MAGENTA aps

adresse
Studiestræde 14, 1.
1455 København K

email
info@magenta-aps.dk

telefon
(+45) 33 36 96 96