EUCARIS

Installation and Operation Manual for the EUCARIS Stand alone web client

Document version	1.5
Document date	05-02-2020
EUCARIS release	7.0
Author	EUCARIS Operations
E-Mail	eucaris2help@rdw.nl

Table of contents

1. Introduction 4
Support 4
1.1 Tools 5
2. Preparation 6
2.1 Hardware requirements 6
2.1.1 Minimum hardware requirements 6
2.2 Network requirements 7
2.3 Database requirements 7
2.4 Software requirements and prerequisites 8
2.4.1 Windows server requirements 8
3. Installation 9
3.1 Initial installation 9
3.1.1 Prerequisites 9
4. Configuration Tool 19
4.1 Wizard Mode (initial installation) 19
4.1.1 Standalone Configuration Tool 19
4.1.2 Configuration Wizard 20
4.1.3 Configuration Tool Preferences 21
4.1.4 Analyse current configuration 21
4.1.5 Local configuration 22
4.1.6 Certificate configuration 23
4.1.7 Checking and finalizing configuration 29
4.2 Advanced Mode 31
4.2.1 User management 31
4.3 System Update mode 32
4.3.1 Configuration 32
4.3.2 Start 33
4.3.3 Overview 34
4.3.4 Details 34
4.3.5 Downloading System Updates 35
5. Installation of Standalone Web client 39
5.1 Install 39
5.2 Configuration 39
5.3 Installation Test 42
5.3.1 Test EUCARIS Web Client 42
6. Security 43
6.1 Authorizations 43
6.2 Setting up SSL for web client 43
6.2.1 IIS configuration - Certificate 44
6.2.2 IIS configuration – Add binding for HTTPS 44
6.2.3 Web.config – Service side 45
6.2.4 Web.config – client side 46
7. Troubleshooting 47
7.1 Application 47
7.1.1 Menu 47
7.1.2 Access Denied 48
7.1.3 Unrecognized attribute ‘Target Framework’ 48
7.2 Internet Information Services 50
7.2.1 Memory usage on the webserver 50
8. Appendix 52

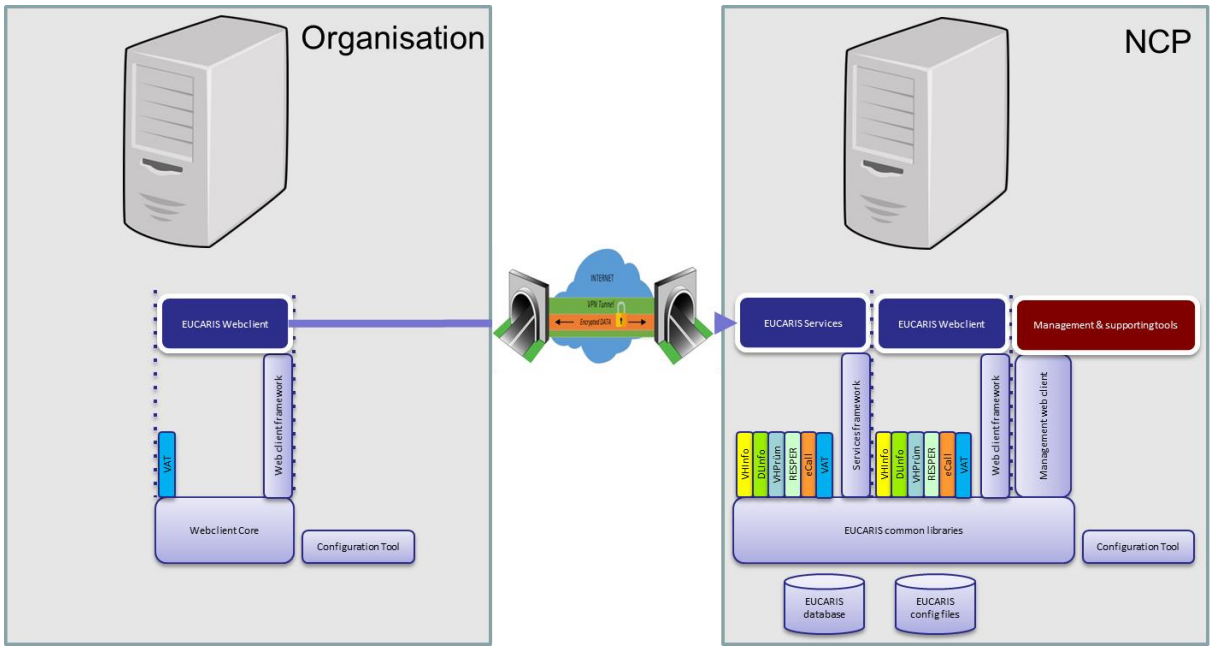
8.1 How To: Install Microsoft .NET Framework 4.7.2 52
8.2 How To: Adding Root and Intermediate certificates via MMC 53
8.3 How To: Manually import a Certificate Revocation List (CRL) 59
8.4 How To: Manually create an EUCARIS service account..... 60
8.5 How To: Manually set the required policies of the EUCARIS service account 61

1. Introduction

This document will describe the installation of the standalone web client. The standalone web client can be used when no autonomous EUCARIS installation is available. Normally the standalone web client will be used by an organization without a direct connection to the Testa network, so this organisation won't be considered to be an NCP (National Contact Point).

The standalone web client however is dependent on the Eucaris installation of the NCP. It will use the NCP's public and internal service to connect to Eucaris. Also the database of the NCP will be used and the standalone web client will be run without its own database.

One important prerequisite for the standalone web client is that the organization running it will have a network connection to the Eucaris services of the NCP. The so called Soap web services of the NCP must be available from the organisation running the standalone web client. Either directly, but preferably secure. Either though a VPN, private network or the Eucaris Secure Tunnel.



For more background information a lot of information can also be found in the EUCARIS – Installation and Operation manual, which is available on request. And for this reason we will not elaborate the Eucaris functionality in too much detail in this document.

Support

For support during installation and operation of the EUCARIS standalone web client you can contact your NCP running Eucaris. If additional support is needed then the installation and development support team of Eucaris can be called by mail via: eucaris2help@rdw.nl and the operation support team can be contacted by mail via: servicedesk@rdw.nl

1.1 Tools

Apart from the standalone web client itself we will use additional tooling to support the distribution of the software packages and to check the prerequisites.

- **Installation**
  The installation application checks most of the prerequisites. To ease the necessary preparations of the server before the EUCARIS application can be installed and configured, the installation application is also able to make some changes to the server, like adding a service account and/or websites in IIS. This tool will be discussed in detail in chapter 3.

- **Configuration**
  To ease the installation of the standalone web client, the application is shipped with a Standalone Configuration Tool. Summarized this tool allows an administrator to install updates issued by *EUCARIS Operations*. This tool will be discussed in detail in chapter 4.

2. Preparation

Before installing and configuring the standalone web client there are a number of hardware and software requirements and prerequisites, which have to be fulfilled.

2.1 Hardware requirements

This section describes the standalone web client hardware requirements.

2.1.1 Minimum hardware requirements

The minimum hardware requirements consist of a (virtual) server with at least the following specifications:

- > 2GHz multi core processor,
- >= 8 GB memory,
- 2 GB free space available (excluding required database space),
- Network connection to the NCP

2.2 Network requirements

Network configuration is not part of this instruction but is essential for connecting the standalone web client to the EUCARIS of the NCP. The following things should be kept in mind when configuring the network:

- **TESTA**
  Only available by the NCP connection directly to Eucaris. When an organisation using the standalone web client does a request to Eucaris. First a call is made to the NCP, only after that the NCP uses the Testa network to inquire other member states.

- **Firewall**
  To allow communication with the NCP the firewall should allow outbound and inbound connections.

- **Security**
  Because the Testa network is not used between the organization running the standalone web client and the NCP it is strongly advised to protect the connection using a private physical network, a VPN or the Eucaris Secure Tunnel.

- **Getting updates**
  Getting updates from the NCP using the Standalone Configuration Tool will require installing a certificate for the signed message requesting the update. This will be discussed in chapter 4.1.6

2.3 Database requirements

No database is necessary. The database of the NCP will be used by calling the Eucaris web services running at the NCP. This is all implemented in the Core functionality of the web client.

2.4 Software requirements and prerequisites

This section describes the standalone software requirements and prerequisites that have to be complied with before installation of the standalone web client of EUCARIS can proceed. The Installation tool can be used to verify part of these requirements and allows configuring the steps to comply with a number of the prerequisites.

2.4.1 Windows server requirements

EUCARIS 7.0 and higher is tested to work correctly on 2012R2 to 2016. This documentation will mainly focus on Windows Server 2016 installation. The following roles and features are required:

Server Roles:

```
 [X] Web Server (IIS)

Web Server Role (IIS)\ Role Services:
 [X] Web Server
    [X] Common HTTP Features
        [X] Default Document
        [X] Directory Browsing
        [X] HTTP Errors
        [X] Static Content
        [X] HTTP Redirection
    [X] Health and Diagnostics
        [X] HTTP Logging
    [X] Performance
        [X] Static Content Compression
    [X] Security
        [X] Request Filtering
        [X] Basic Authentication
        [X] IIS Client Certificate Mapping Authentication
        [X] Windows Authentication
    [X] Application Development
        [X] .NET Extensibility 4.7
        [X] ASP.NET 4.7
        [X] ISAPI Extensions
        [X] ISAPI Filters
 [X] Management Tools
    [X] IIS Management Console
    [X] IIS Management Scripts and Tools
```

Features:

```
 [X] .NET Framework 4.7 Features
    [X] .NET Framework 4.7
    [X] ASP.NET 4.7
    [X] WCF Services
        [X] HTTP Activation
        [X] Message Queuing (MSMQ) Activation
        [X] TCP Port Sharing
    [X] Message Queuing
        [X] Message Queuing Services
            [X] Message Queuing Server
    [X] Windows Process Activation Service
        [X] Process Model
        [X] Configuration APIs
    [X] WoW64 Support
```

NOTE: The installed roles and features can be listed using the PowerShell command 'Get-WindowsFeature'

3. Installation

This chapter describes the installation of the standalone web client of EUCARIS, which starts running the installation tool, checking the prerequisites and installing the Standalone Configuration tool.

Both initial installation and execution of the Configuration tool must be executed by a user with administration privileges.

The descriptions assume the default proposed values for the EUCARIS service account, website folders, website application pool and website names and ports. In case changes to these defaults were made during the Preparation steps it is important to remember to use those values.

NOTE: Use the proposed default values if there is no urgent need to use other than the suggested default

The required installation files can be obtained via EUCARIS Operations at eucaris2help@rdw.nl

3.1 Initial installation

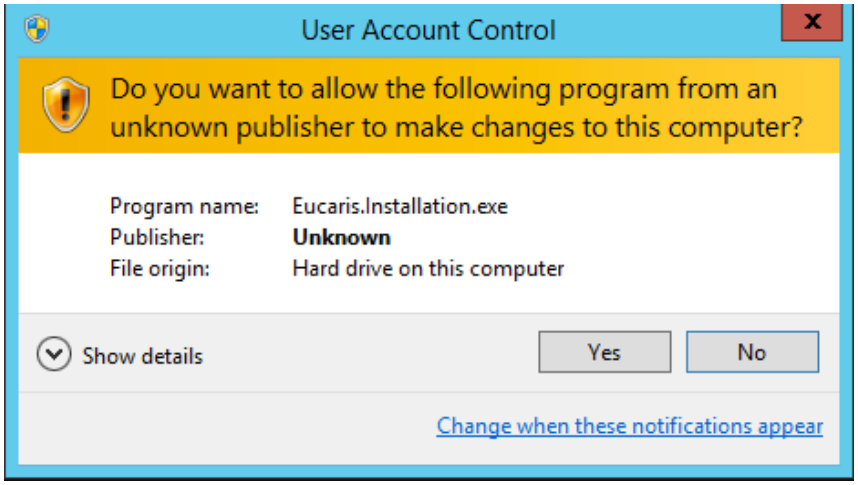
In case of an initial installation of the standalone web client the steps below have to be executed:

- Check prerequisites and install application files
- Install the standalone Configuration Tool
- Install the standalone web client
- Install appropriate plugins (e.g. Vat)
- Configure the standalone web client.

3.1.1 Prerequisites

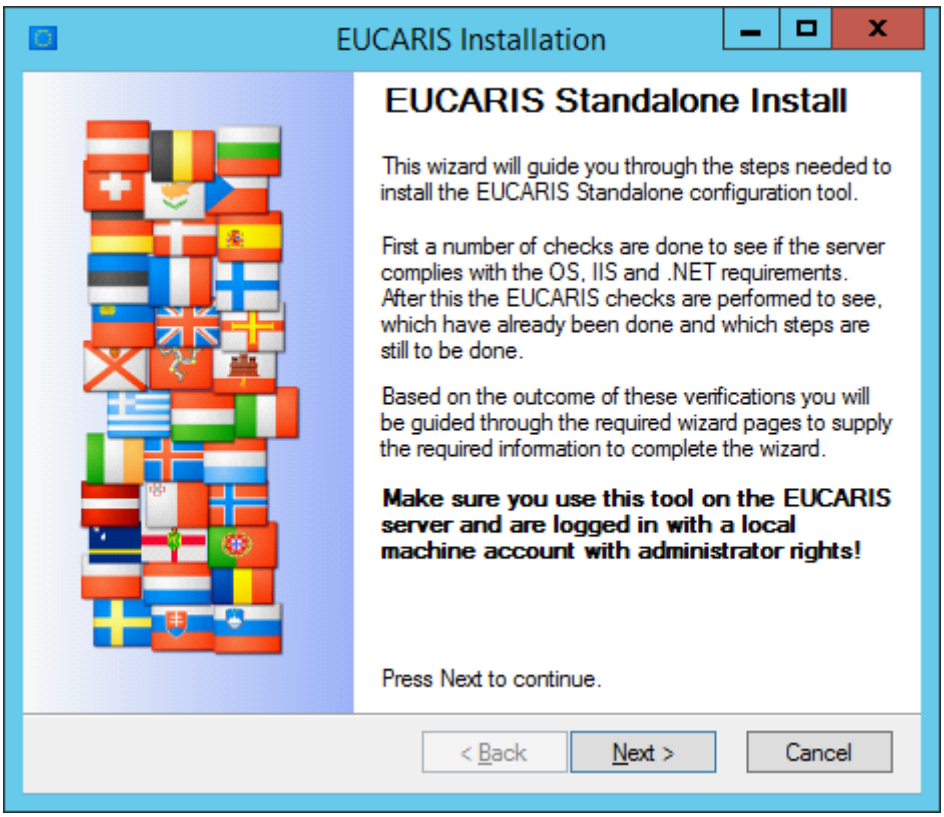
The EUCARIS Standalone Installation tool is used to verify compliance with the requirements and to specify and prepare the prerequisites. The EUCARIS Standalone Installation tool will also install the required files to the designated locations. The following paragraphs will describe how to use the tool. The latest version of the tool can be obtained via EUCARIS operations.

NOTE: The tool must be started with elevated privileges (run as administrator) to function correctly. The UAC (User Account Control) request can and must be answered with 'Yes'



3.1.1.1 Welcome

When the tool is started the following screen is displayed giving an introduction of the tool. After reading the introduction 'Next' can be pressed to continue.



3.1.1.2 Check prerequisites

The tool will automatically check the basic software requirements and prerequisites. The following pre-requisite checks are performed:

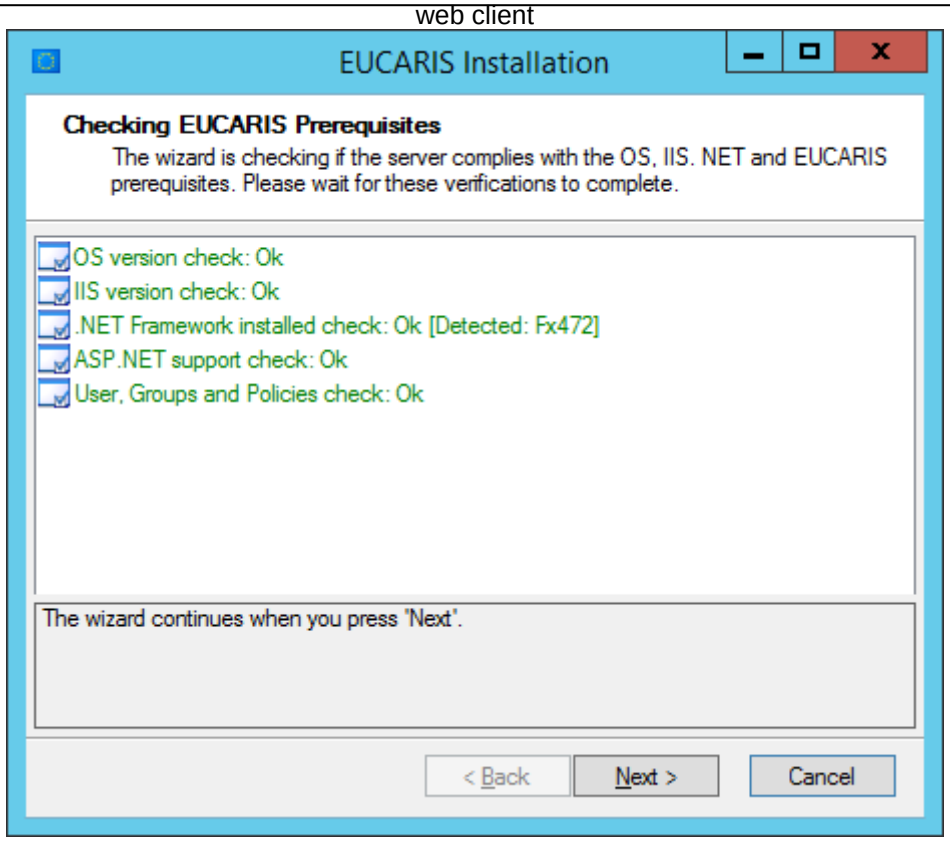
- **OS version check**
  Verifies whether the installed operating system is supported

- **IIS version check**
  Verifies whether the installed IIS version is supported

- **.NET Framework installed check**
  Verifies if the latest version of the .NET Framework 4.7.2 is installed

- **ASP.NET support check**
  Verifies if ASP.NET Runtime 4.0 is correctly installed and configured for IIS

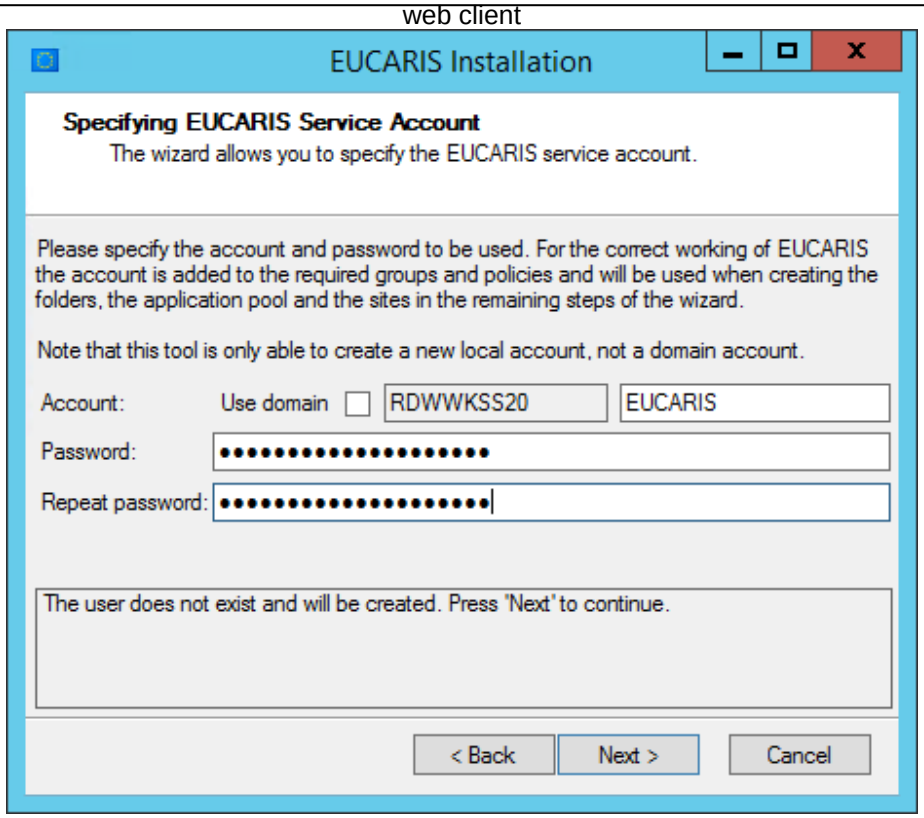
- **User, Groups and Policies check**
  Verifies whether the default proposed EUCARIS service account exists and is added to the required groups and has been added to the required policies



It can be seen above that all software requirements and the prerequisites have been met. Based on the above outcome, the user can press ‘Next’ to continue with the next step.

3.1.1.3 Service account

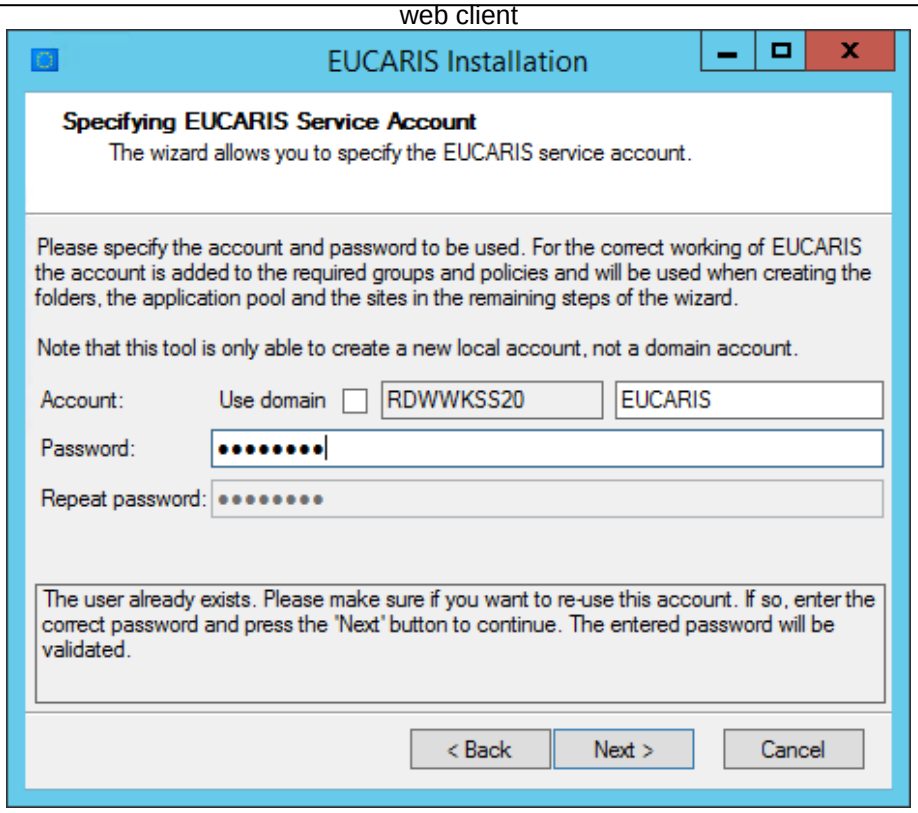
The service account page starts showing the default proposed EUCARIS service account and requires the user to enter the passwords that the user wants to create the service account with. This is shown in the following picture:



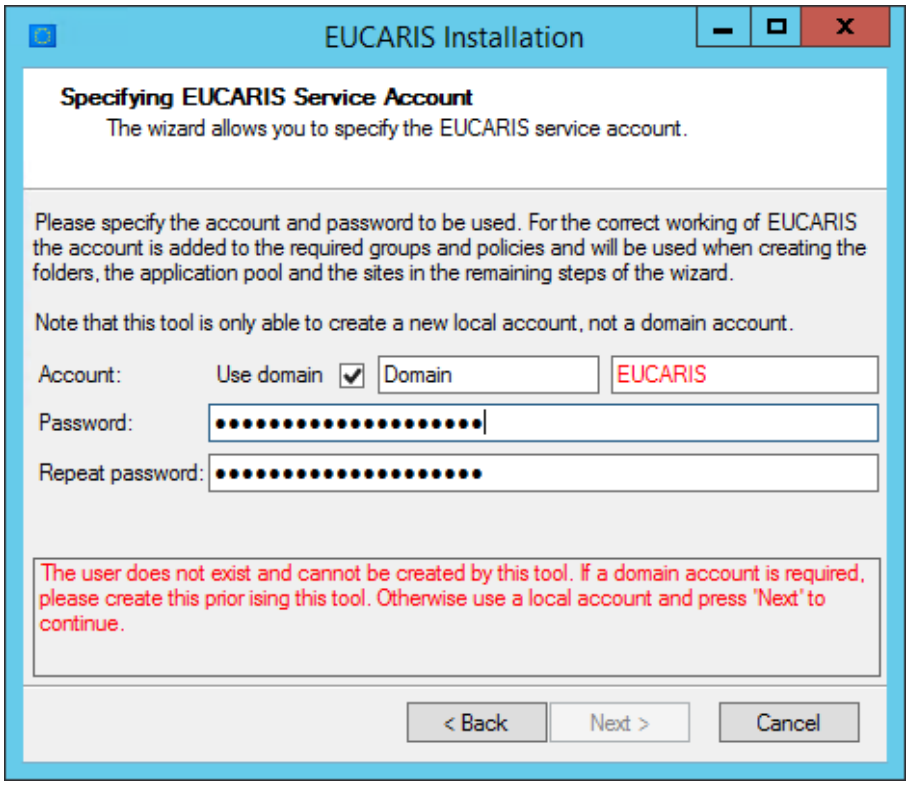
In this scenario, a new local user is created which will serve as service account for all EUCARIS applications.

NOTE: Please make sure to adhere to the local password complexity policy

In case an existing user needs to be used, enter the username and the corresponding password. The username & password combination will be validated as soon as the user presses the 'Next' button:



It is also possible to use an existing domain account as EUCARIS Service account. Please note that you cannot use an account from another domain than the domain you are logged on to during installation. Please also note that the tool is not able to create an account in this EUCARIS domain, so this must be prepared by the domain administrator. The username & password combination will be validated as soon as the user presses the 'Next' button. The tool will show the following error if the domain user does not exist:



NOTE: The Installation Tool will configure this existing user to be a user allowed to run IIS application pools and Windows Services

The user will be added to the following local Windows Groups:

Windows Group	*Description*
Administrators	Local administrators group
IIS_WPG	Replaced by IIS_IUSR on Server 2008 and later
IIS_IUSRS	Built-in group for IIS worker processes

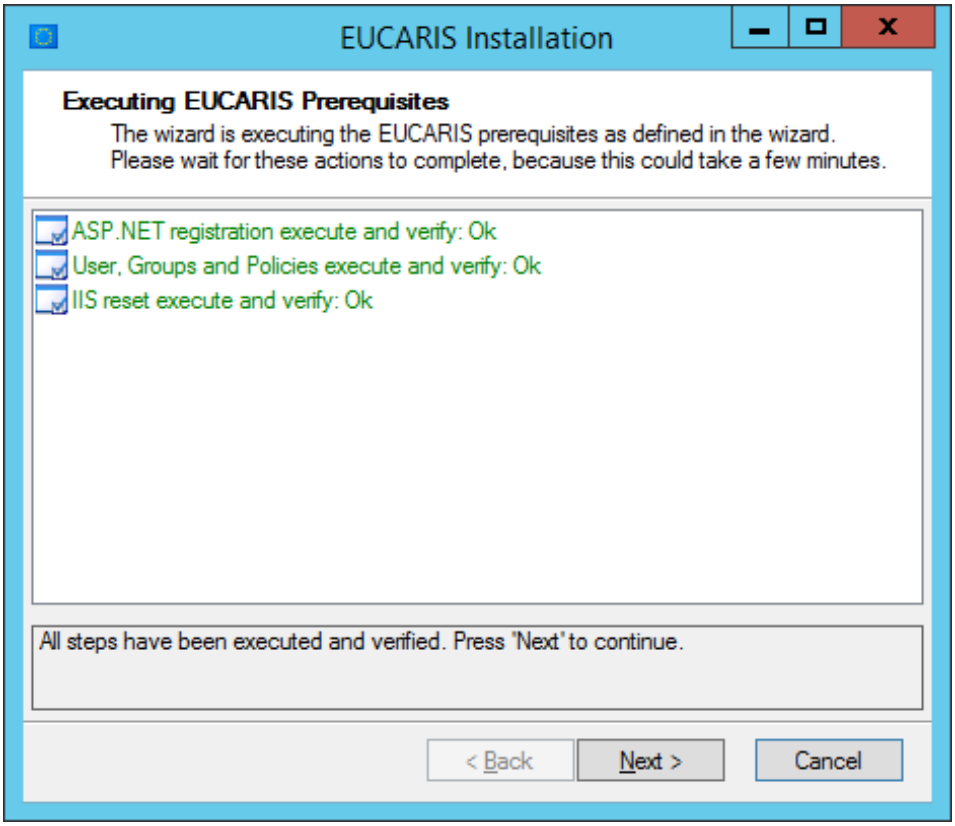
The user will receive the following privileges on the local machine:

Privilege	*Description*
SeAssignPrimaryTokenPrivilege	User Right to replace a process-level token
SeIncreaseQuotaPrivilege	User Right to adjust memory quotas for a process
SeServiceLogonRight	Required for an account to log on using the service logon type

NOTE: The addition of the EUCARIS Service Account to the Administrators group of the local machine should be only temporary needed and only required for analysis and troubleshooting reasons during installation and configuration. It is advised to remove this user from this group as soon as the application is correctly configured and working properly

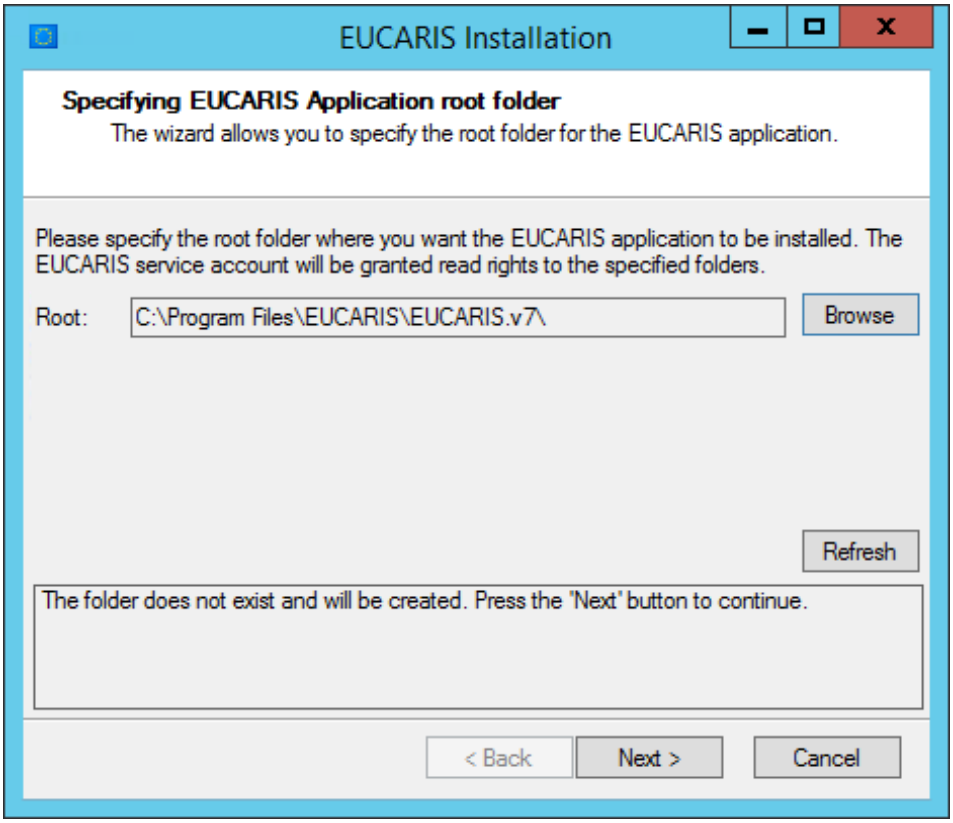
3.1.1.4 Execute EUCARIS Prerequisites

The execute page executes and verifies the required changes. It verifies before and after making the required changes to make sure that manual changes won't interfere with the changes of the tool.



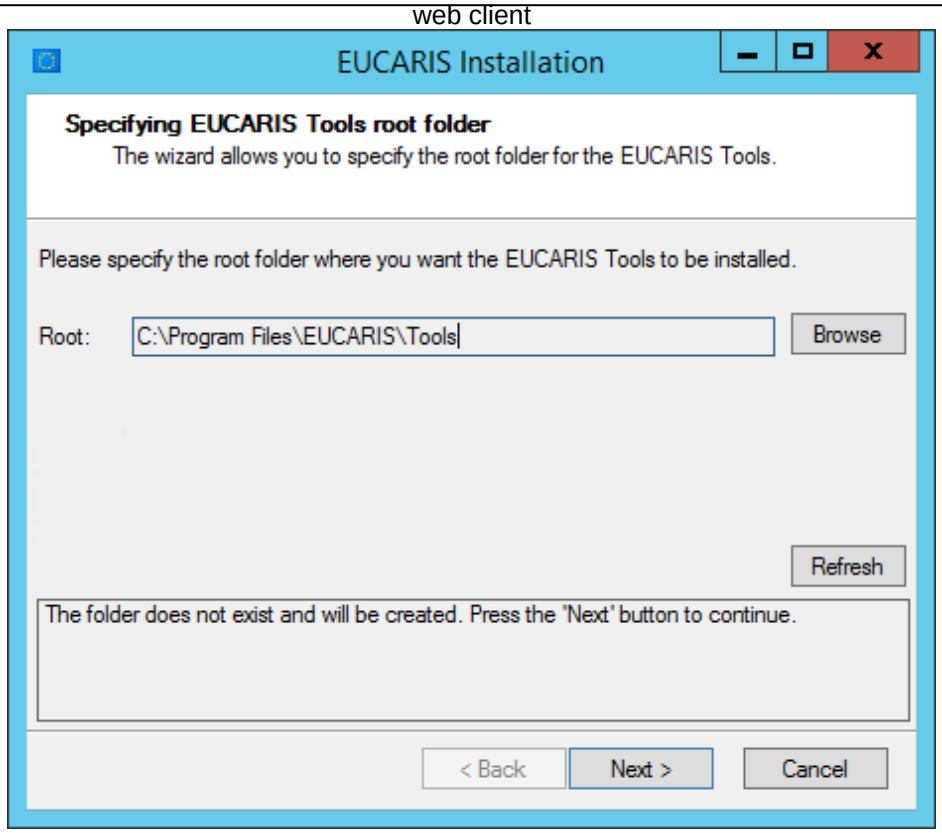
3.1.1.5 Application Root folder

Specify the root folder where the EUCARIS Application files will be installed to.
If you need to change the root folder, press the 'Browse' button to choose a different location.



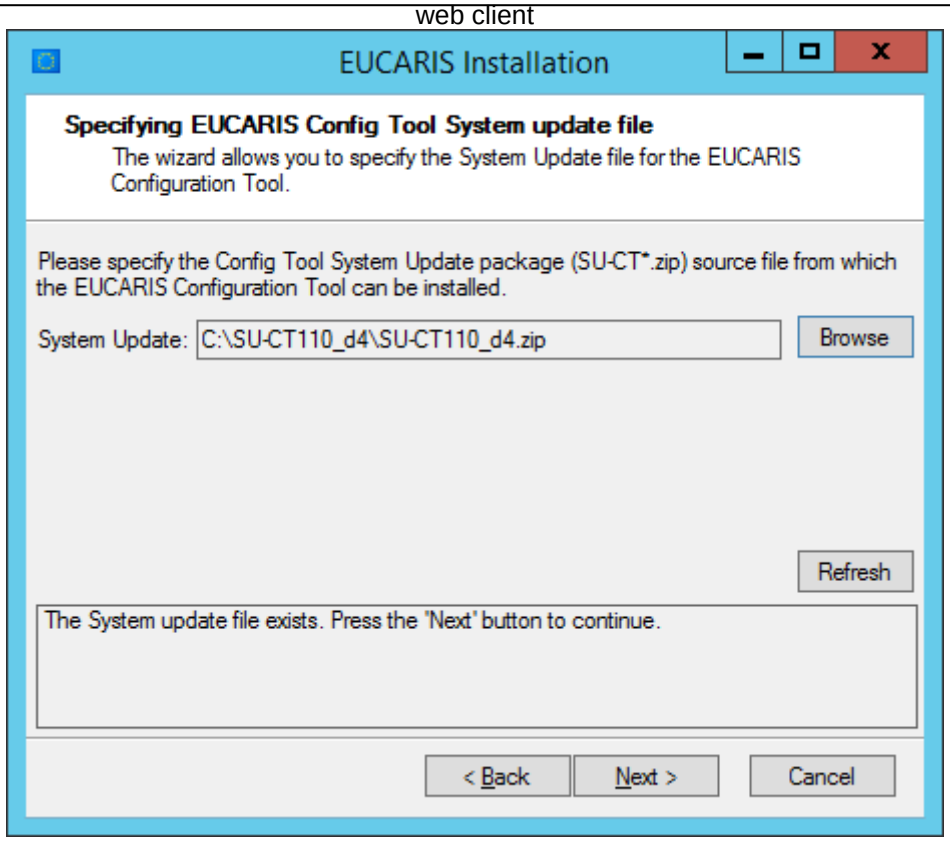
3.1.1.6 Tools root folder

The EUCARIS Application is supported by a number of tools required for configuration, maintenance, reporting and so on. These tools are installed in the root folder which is specified here:



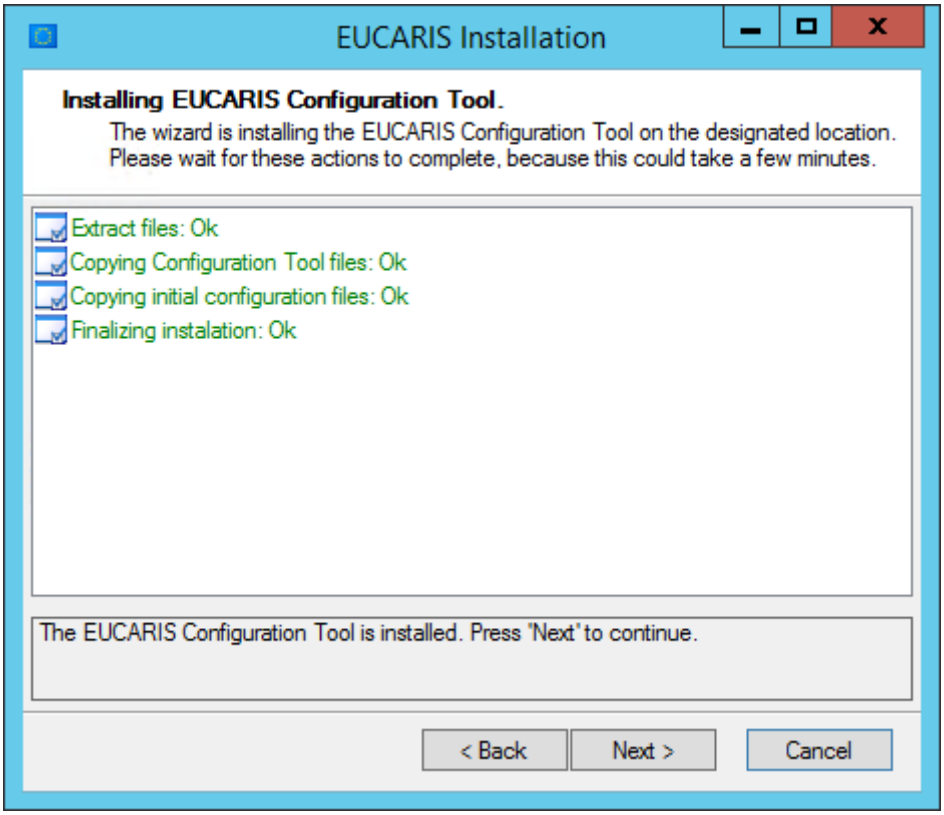
3.1.1.7 Specify Configuration Tool System Update

The installation package contains the latest available *EUCARIS Configuration Tool* System Update (SU-CT110 or higher). The included and required System Update is automatically selected Click ‘Browse’ to select another System Update if required.



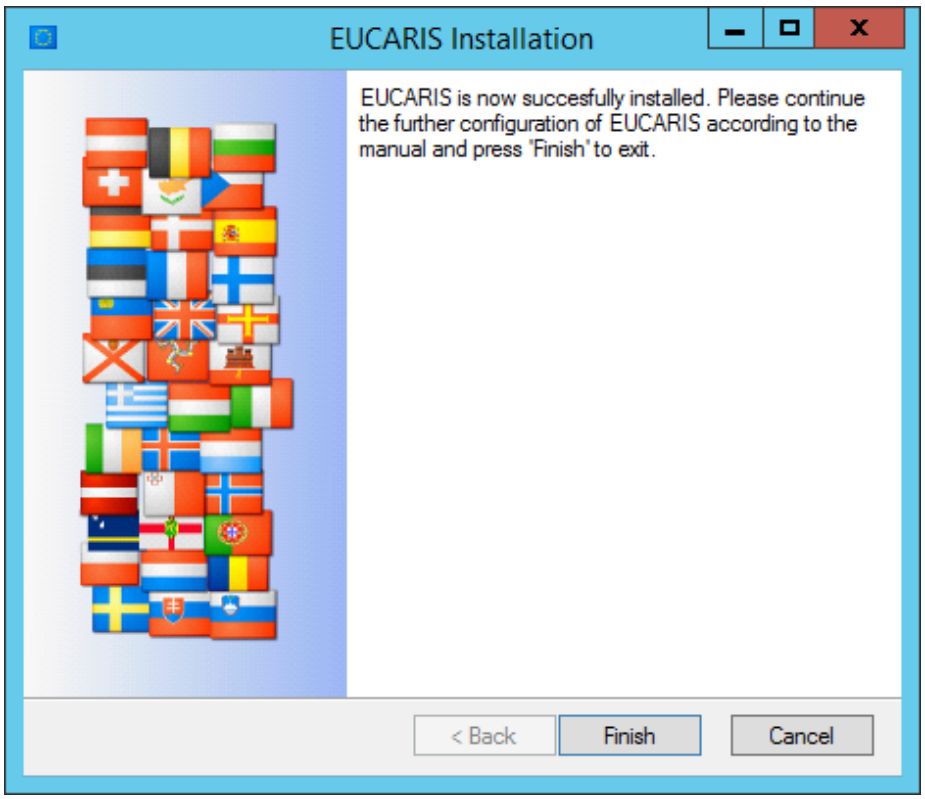
3.1.1.8 Installing EUCARIS Configuration Tool

The installation will now copy the required files to the selected location:



3.1.1.9 Finish

The finish page is the last page of the tool. The required EUCARIS standalone web client files are now installed successfully.



4. Configuration Tool

Before the standalone web client can be used it has to be configured. For this purpose, the Standalone Configuration Tool is created which was installed in the previous chapter. The Standalone Configuration Tool serves the following purposes:

- **Configure a new standalone installation**
  Configuring a new standalone installation is supposed to be done by using the Standalone Configuration Tool in 'Wizard' mode, which leads the user through the required steps to perform

- **Perform system updates issued by *EUCARIS Operations***
  The Standalone Configuration Tool is able to download and install System Updates issued by EUCARIS Operations

The Configuration Tool can run in two modes, respectively 'Wizard' and 'Update' mode. These modes will be discussed in detail in the following paragraphs.

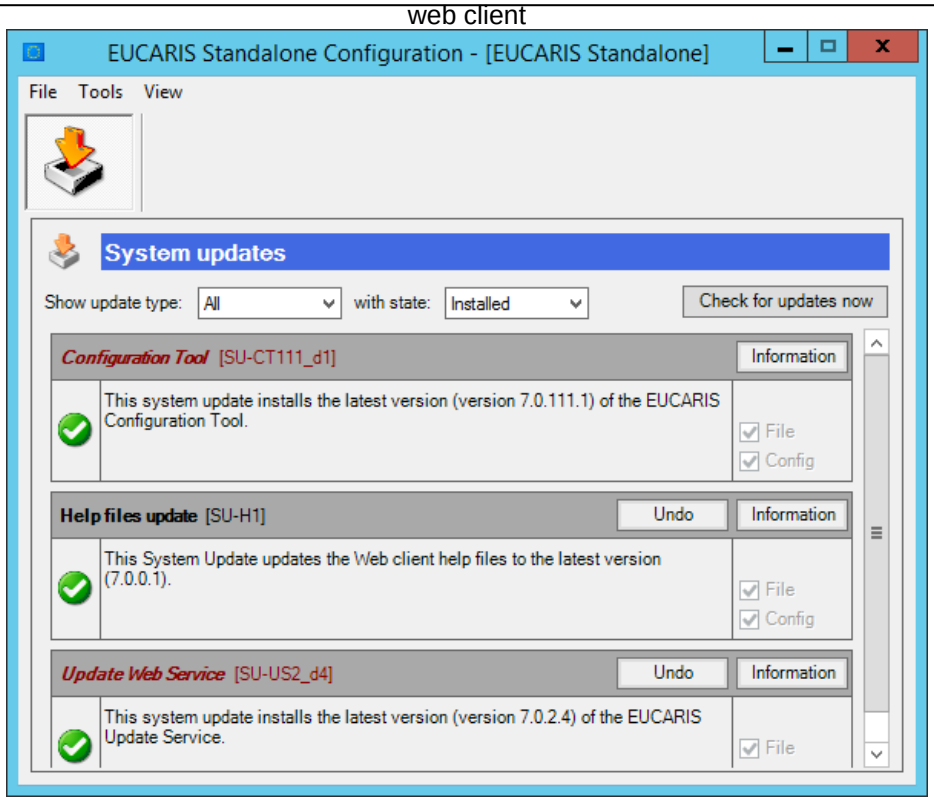
4.1 Wizard Mode (initial installation)

Initial configuration is done using the 'Wizard' mode in which the user is guided through the settings for standalone EUCARIS. In this mode all steps are carried out in the correct order and this mode is used for all standard EUCARIS standalone installations and updates. This paragraph describes the steps required for an initial (new) installation of EUCARIS.

NOTE: After a new installation of EUCARIS it is required to always perform the initial configuration using the EUCARIS Configuration Wizard

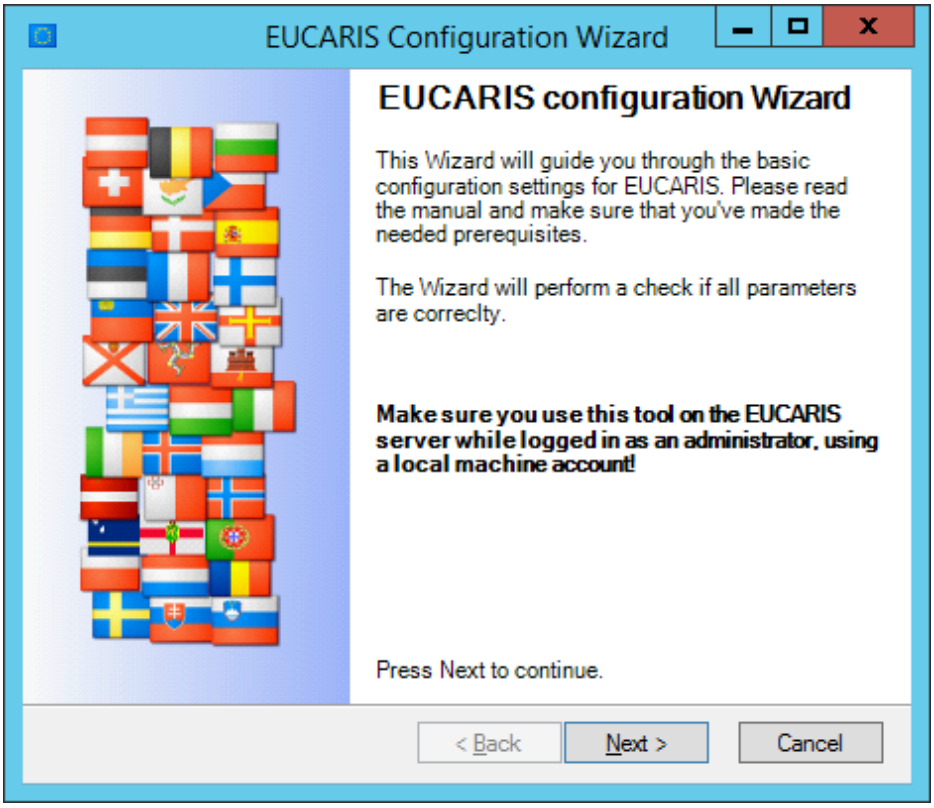
4.1.1 Standalone Configuration Tool

To start the Standalone Configuration Tool use 'Start' > 'All programs' > 'EUCARIS.v7 Tools' > 'EUCARIS.Configuration' > 'Eucaris.Configuration.Standalone'.



4.1.2 Configuration Wizard

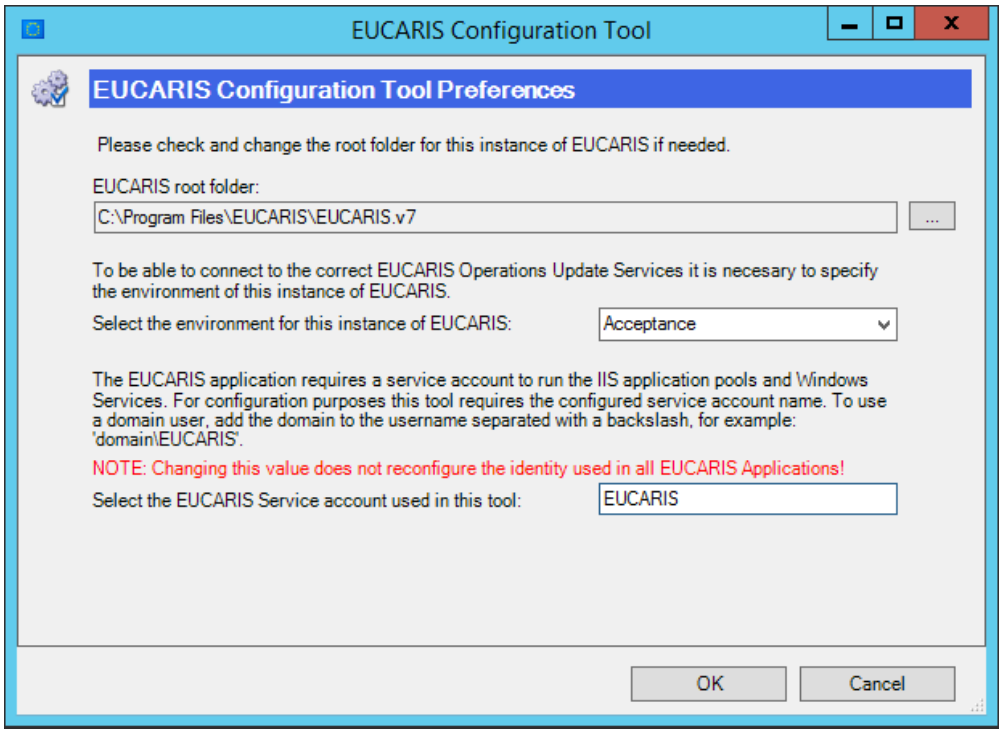
Press 'View' > 'Configuration Wizard' and wait till the following screen is displayed giving an introduction of the tool. After reading the introduction press 'Next' to continue. **For an initial installation it is required to follow all steps in the wizard mode**.



NOTE: The tool must be started with elevated privileges (run as administrator) to function correctly. The UAC (User Account Control) request can and must be answered with 'Yes'

4.1.3 Configuration Tool Preferences

If the Configuration Tool is started for the first time the user must specify the EUCARIS 7.0 application root folder directory, the environment for this specific instance of EUCARIS and the EUCARIS Service account. This has to be the same service account as created (or configured) during the prerequisites and installation as described in paragraph 3.1.1.



NOTE: Make sure to set the correct environment for this instance of EUCARIS (Acceptance/test or Production). This setting is important for connecting to the correct Update Service hosted by EUCARIS Operations

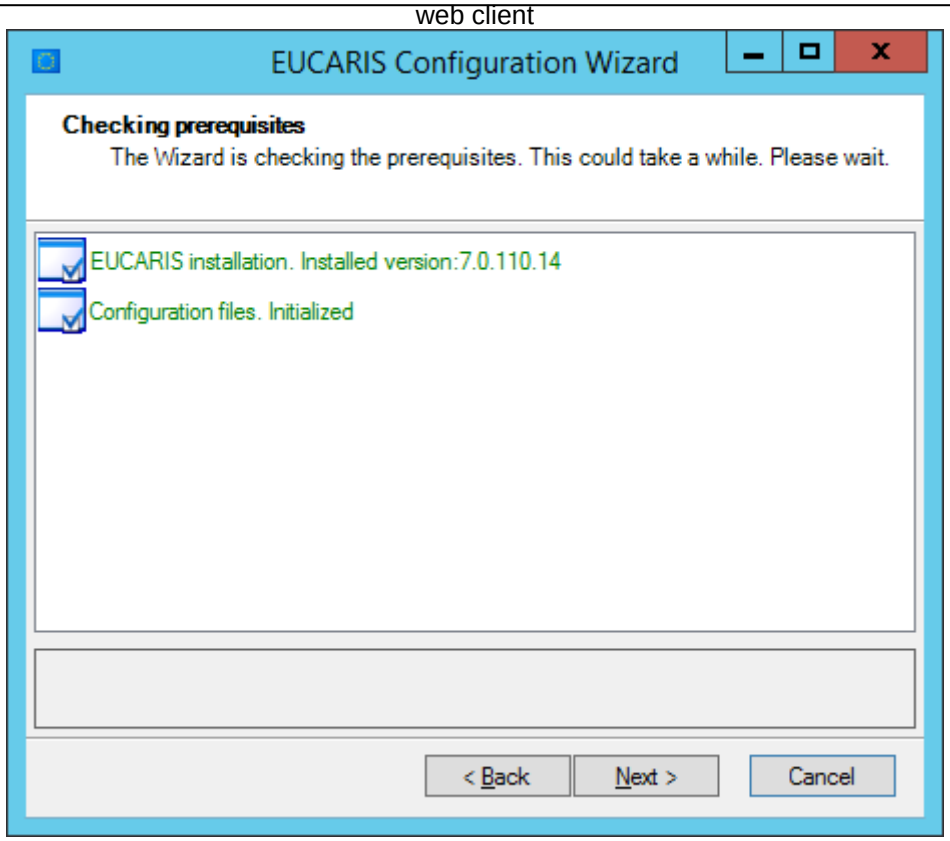
4.1.4 Analyse current configuration

After the selections are made the Configuration Tool continues with the analysis of the following preconditions and won't continue if they are not all met:

- **EUCARIS installation**
  The current version of EUCARIS is verified

- **EUCARIS configuration files**
  The existence of configuration files is checked and they are read and validated

Below is shown what the result of this analysis should be, before the tool can continue:



Press 'Next' to continue to the next step of the wizard.

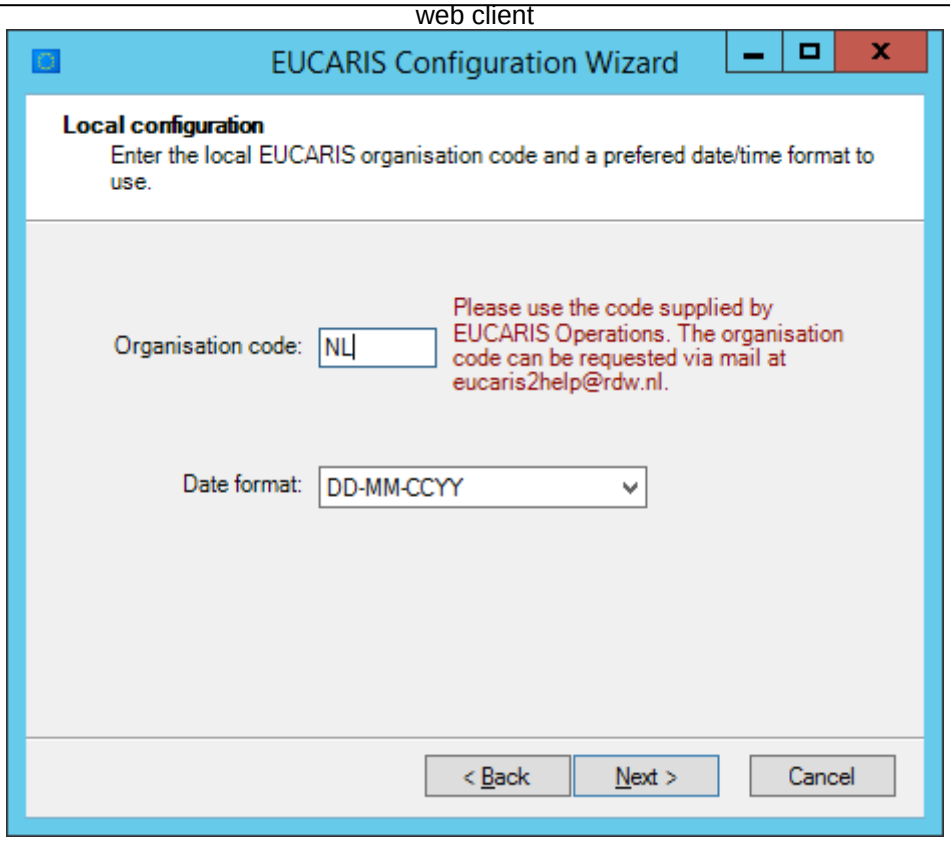
4.1.5 Local configuration

In this step the user must set-up local member state or organisation properties.

The following parameters can be set:

- **Organisation code**
  The organisation code for which to configure EUCARIS. This must be the same code which is used by the NCP you are connecting to.

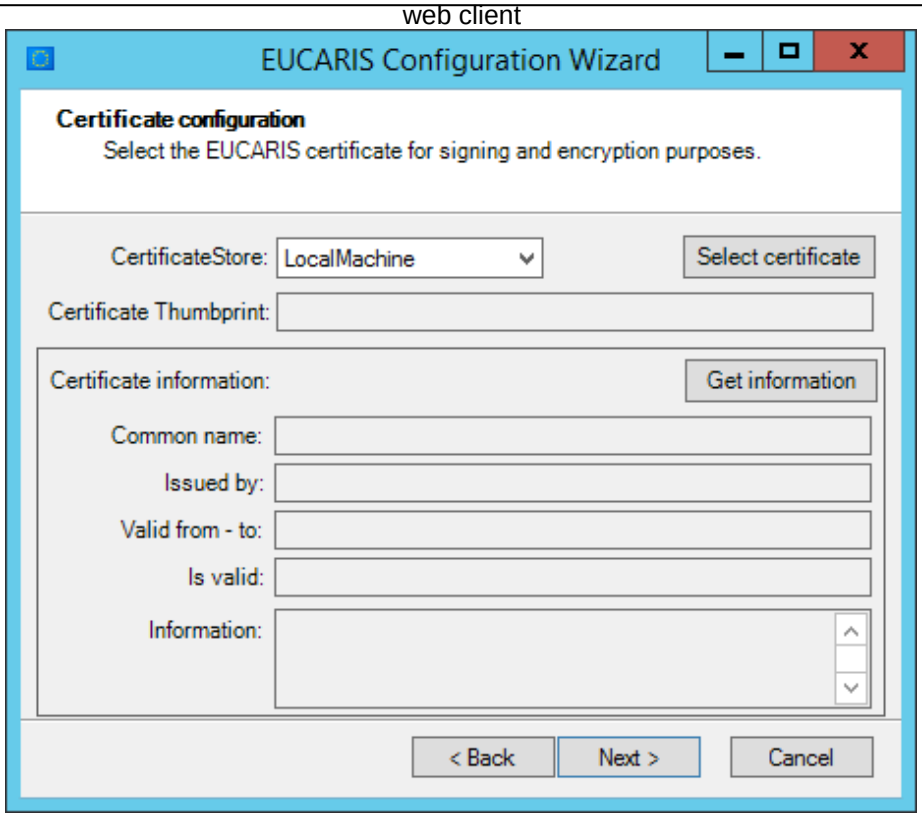
- **Date format**
  The date format that should be used in the EUCARIS web client. All dates will be shown in the format specified here



Press 'Next' to continue to the next step of the wizard.

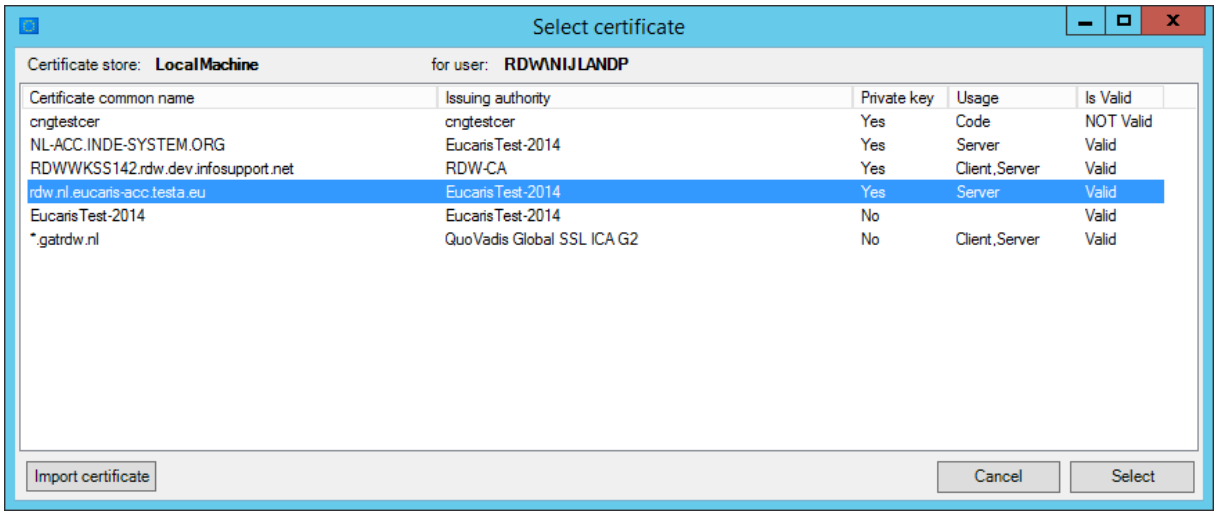
4.1.6 Certificate configuration

In this step, the certificate used for signing and encrypting the EUCARIS messages is selected from the certificate store. If required, a certificate can be imported in case of an initial installation.



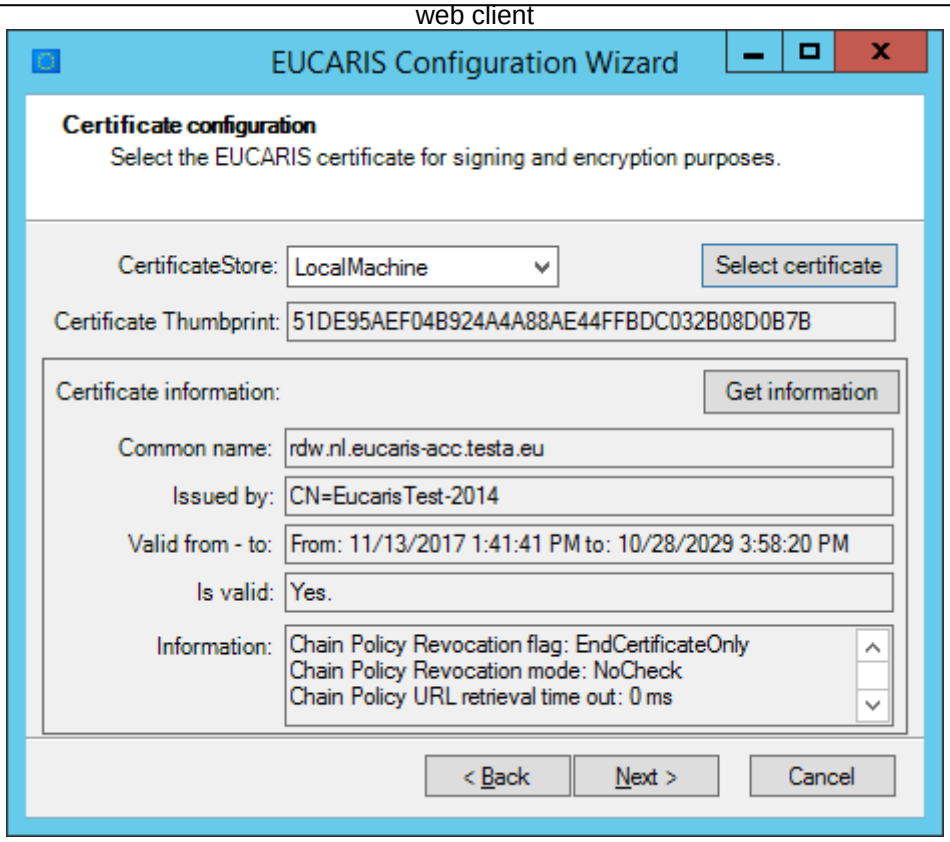
The certificate store to use has to be selected using the selection box which contains a choice between 'LocalMachine' and 'CurrentUser'.
We strongly advise to use the certificates from the 'LocalMachine' store.
Press 'Select certificate' in order to configure the correct EUCARIS certificate.

For the Standalone web client EUCARIS won't supply a certificate. However the configuration tool needs a certificate to sign the calls to the update service of the connecting party. So the root of the chosen certificate should be trusted by the server of the connecting update service.



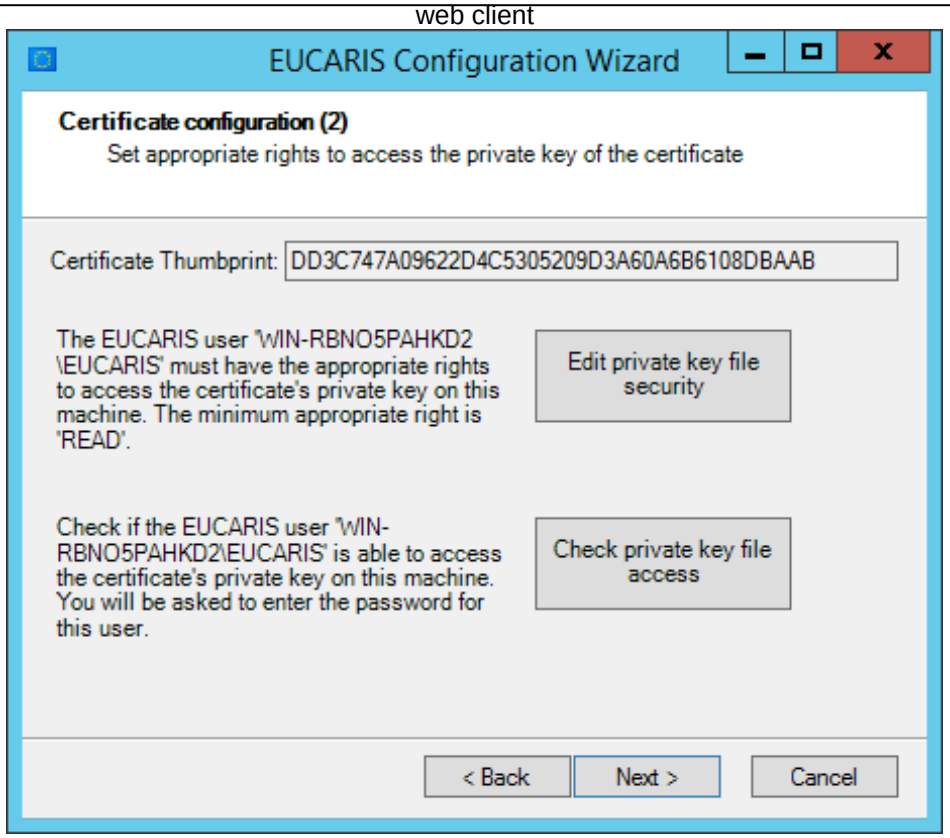
If no valid certificate is available, a certificate can be imported applying the correct System Update.

Select the certificate and press 'Select' to finalize setting the required certificate.

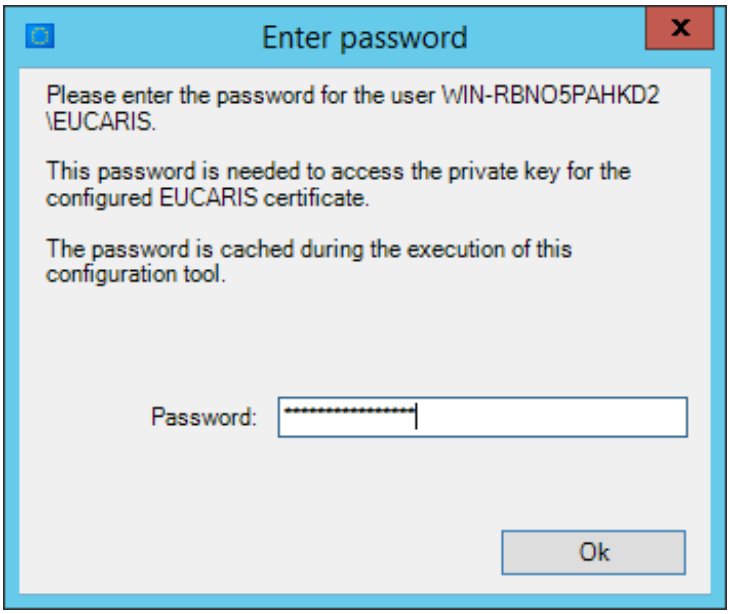


As long as no valid certificate is selected, it is not possible to use Configuration and/or System Update Service and it is not possible to finalise the configuration and installation. An error will be displayed in the finalisation step.

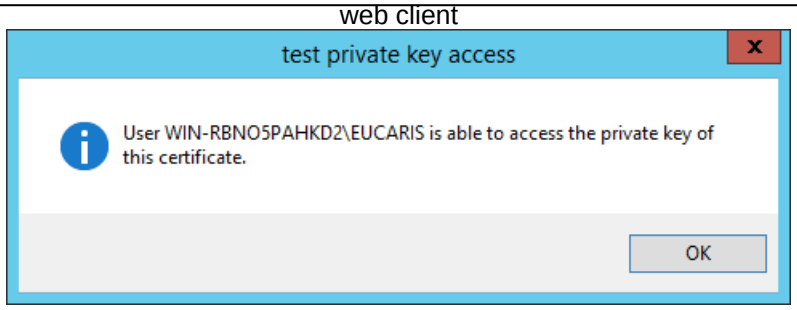
Press ‘Get information’ to view details of the selected certificate and press ‘Next’ to continue to the next Certificate Configuration step of the wizard. The EUCARIS Certificate contains a private key, used for signing and encryption. The EUCARIS Service account must have the appropriate authorisation to access this private key.



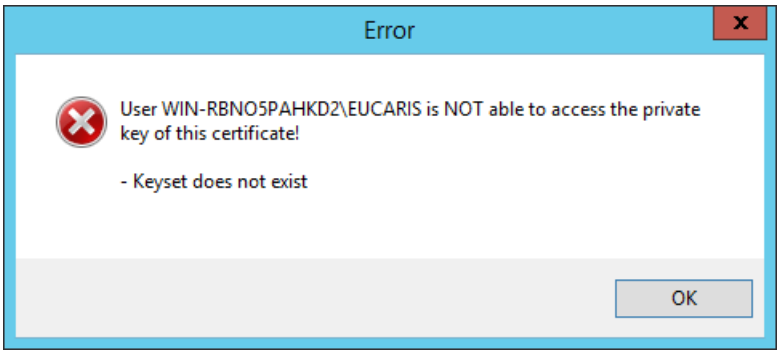
Press 'Check private key file access' to check access to the certificate. The EUCARIS Configuration Tool will check the access using the EUCARIS Service account. To be able to perform this check, the password of the EUCARIS Service account is required.



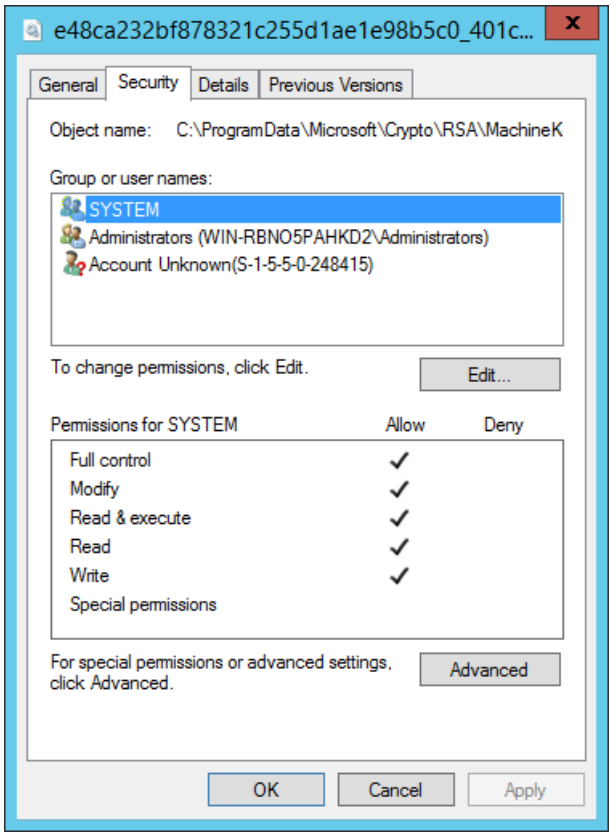
This check can result in one of the next two responses, indicating whether or not the certificate private key is accessible by the EUCARIS service account.



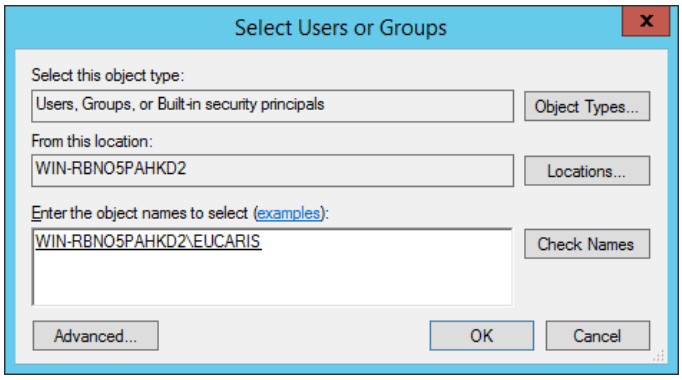
This indicates correct accessibility.
The next Error message displays the situation in which the certificate is not accessible to the EUCARIS service account.



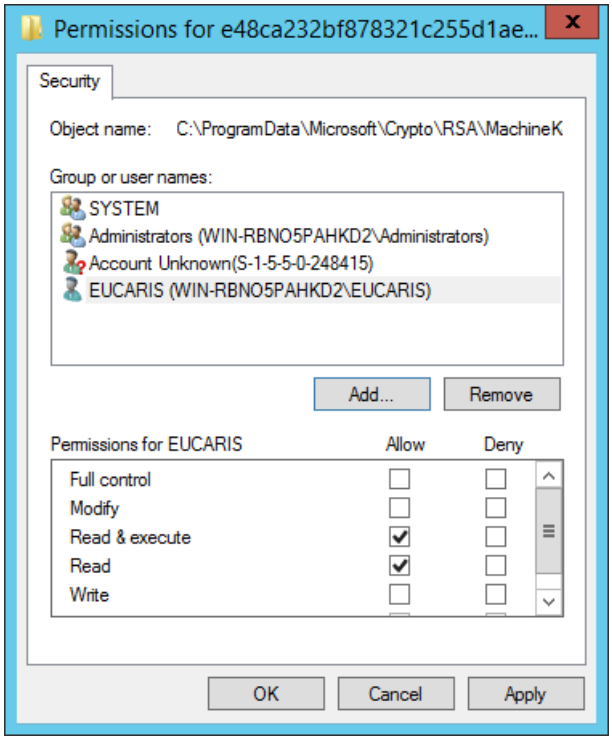
If this Error happens press 'Edit private key file security', which will open a properties dialog and press 'Security' to switch to the security information as shown in the following dialog:



On this dialog use the 'Edit' button to open the permissions dialog and use 'Add…' to add the EUCARIS service account with at least 'Read' and 'Read & Execute' permissions:



When done the permissions dialog adds the default 'Read' and 'Read & Execute' permissions for the EUCARIS Service account. Press 'OK' twice to close the dialogs:



Verify again by using 'Check private key file access' to see if the changes were correct and that the certificate is correctly accessible to the EUCARIS service account.

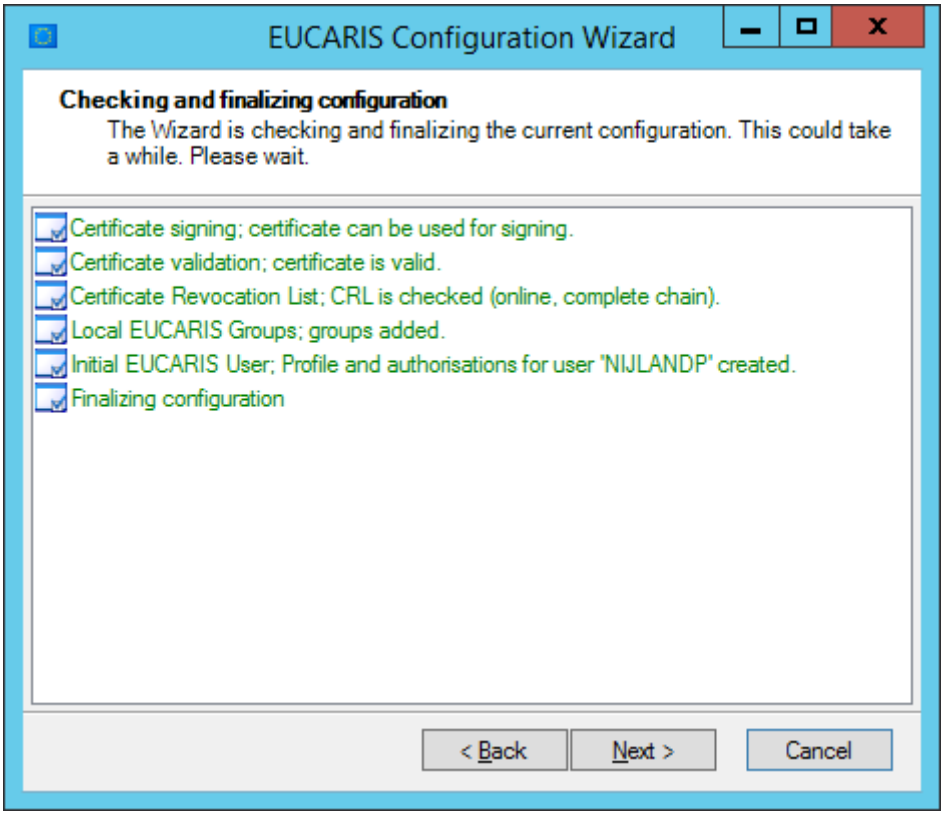
4.1.7 Checking and finalizing configuration

The selected settings for the configuration are checked and finalised. This involves the following:

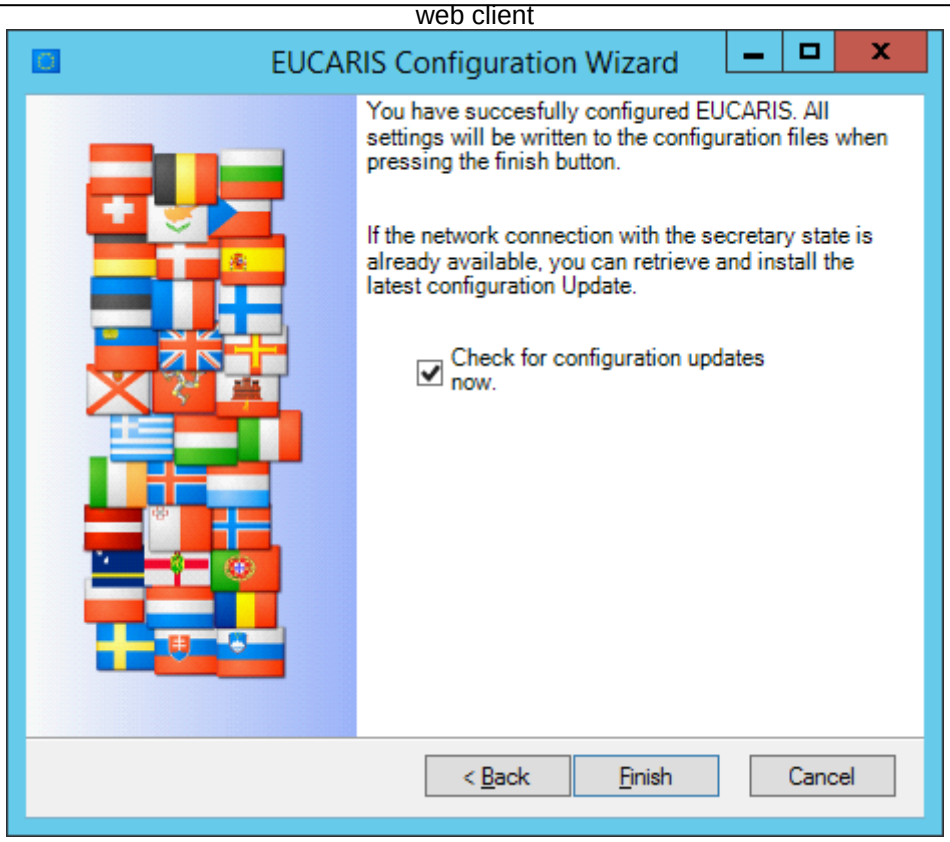
- **EUCARIS Certificate**
  Validates if the chosen certificate is valid. This checks if it can be used for signing EUCARIS messages, if the certificate chain is valid and if the certificate revocation list is valid

- **EUCARIS Groups**
  Adds the required EUCARIS groups

- **EUCARIS User**
  Creates a Web Client profile for the EUCARIS user running the Configuration Tool, with all the required rights. This is done to make sure there is at least one EUCARIS account available that is able to create new profiles in the EUCARIS Web Client



Press ‘Next’ to continue to the next page of the wizard.



By checking or unchecking, the user can either invoke or skip the following steps:

- **Check for Configuration and System Updates now**
  Checks if updates from *EUCARIS Operations* are available by using the EUCARIS Update Service. For details on the EUCARIS Update Service and Configuration- and System Updates, please refer to paragraph 4.3

Press 'Finish' to exit the wizard.

NOTE: After the initial information it is required to update the system with the latest available System Updates first, followed by the latest available Configuration Update.
Updating the system is described in 4.3

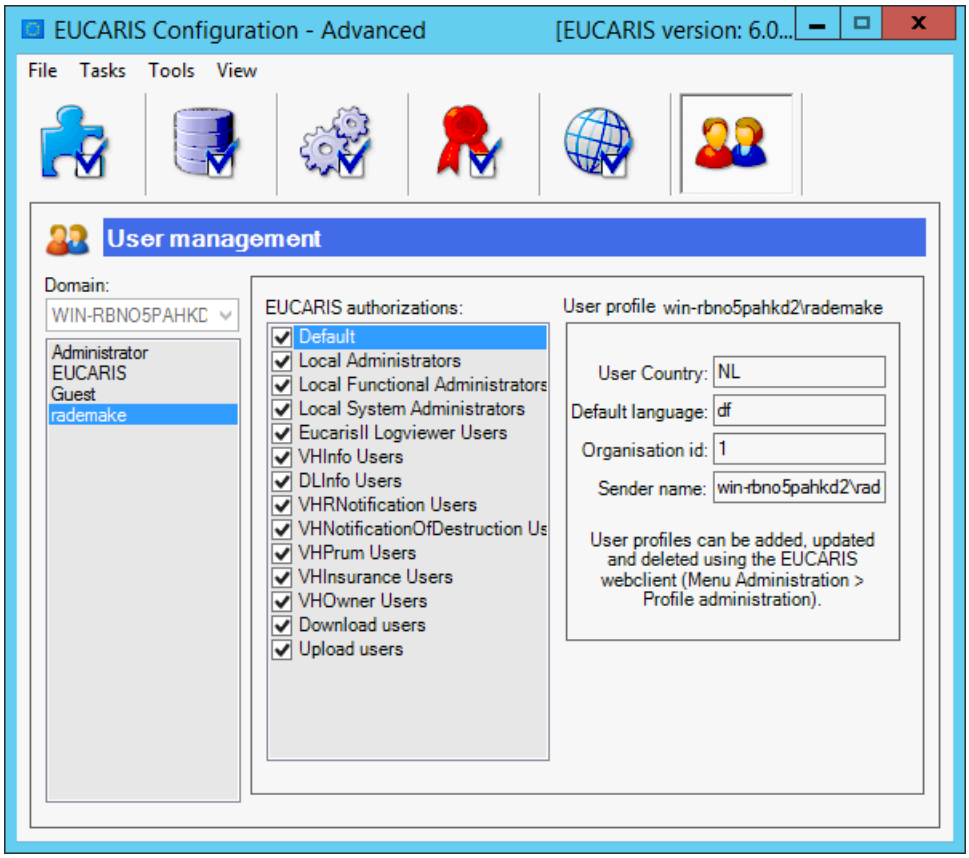
4.2 Advanced Mode

4.2.1 User management

User management is only applicable for the use of the EUCARIS Standalone Web. For a user to be able to use this client at least two requirements have to be met:

1. The user must have a (valid) registered profile in the EUCARIS database of the NCP,
2. The user must be a member of one of the available EUCARIS Windows Groups.

The Configuration Tool offers some basic support for the user management of the Standalone EUCARIS Web Client. This screen allows the user to add one or more users and grant them authorisation:



For users that do not have a EUCARIS profile, a profile will be created of first login.

4.3 System Update mode

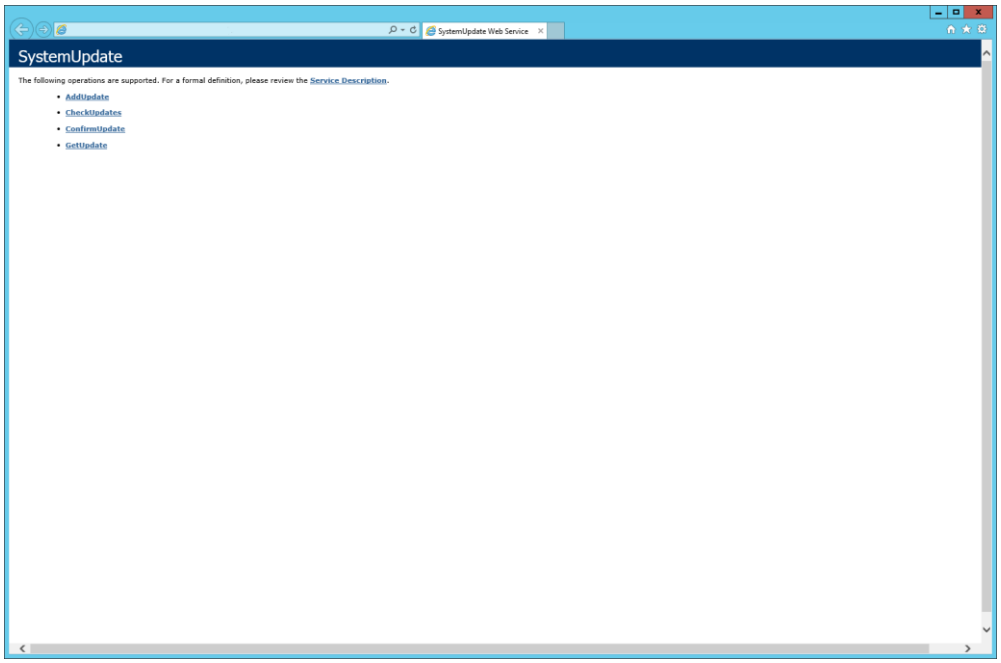
This chapter will first discuss how the System Update Service works and continue with a description how to use the System Update Service with the Standalone Configuration Tool.

4.3.1 Configuration

Before we can get any updates from the NCP we have to adjust the configuration and set the Update Url of the Configuration Tool. The NCP can and must provide this Update Service Url after the have installed the Update service on their own server.

When the NCP provides us with the Update Service Url, it should look something like this:
http://servername:8090/EUCARIS.Update/SystemUpdate.asmx

We can test this Url in the browser to check the connection. It should look like this:

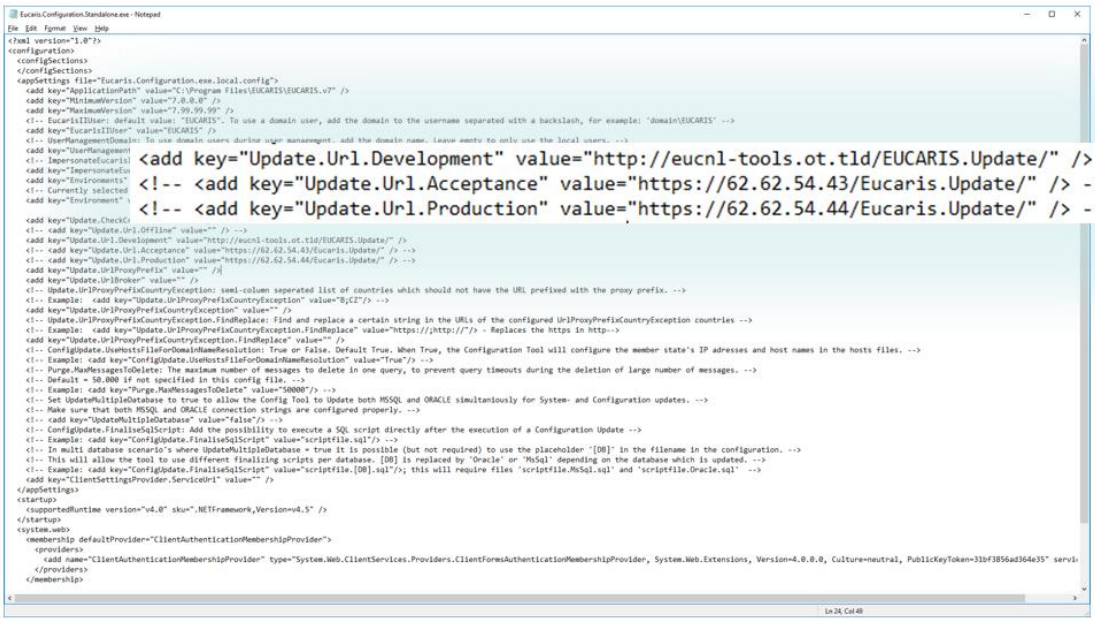


When this is shown correctly we can update the configuration file.

Please use explorer go to the folder configured in: 3.1.1.6, select the folder EUCARIS.Configuration and open Eucaris.Configuration.exe.local with your favourite editor.

Look for the environment chosen in: 4.1.3
And set the Url for this environment without SystemUpdate.asmx!

E.g.



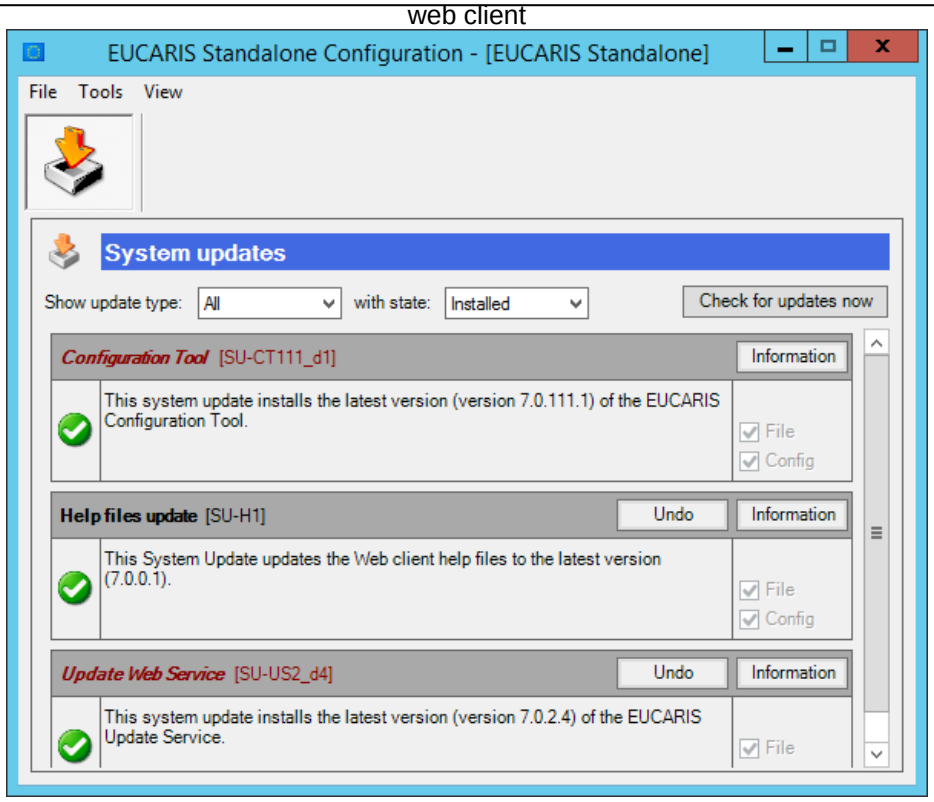
The Update Service on the Eucaris server will use a certificate to sign the System Updates. On the standalone server we need the public part of this certificate to be imported in the certificate store in Personal\Certificates.

Furthermore we have to set the option OverwriteCertificateSubjectnameMustContainlist to contain the subjectname or part of the subjectname of the certificate used by the Update Service. This attribute in the Eucaris.Configuration.Standalone.config of the Standalone Configuration Tool can contain one item, or a list of items separated by a comma.

Also the Standalone server will use a certificate, which root must be trusted by the Eucaris server. This is the certificate of 4.1.6

4.3.2 Start

To start the Standalone Configuration Tool use ‘Start’ > ‘All programs’ > ‘EUCARIS.v7 Tools’ > ‘EUCARIS.Configuration’ > ‘Eucaris.Configuration.Standalone’.



4.3.3 Overview

A published System Update can make a number of changes to EUCARIS, and is system wide, but should be executed on every instance of EUCARIS in case of an out scaled scenario. There are two types of System Update to distinguish:

- Update
- Extension

4.3.3.1 Update

An Update consists of one or more patches that solves one or more problems and/or one or more improvements or functional additions to the web core component. These updates are marked as ‘mandatory’ and must be executed before any available Extension can be installed. An Update is cumulative (the last Update consists of all changes in previous Updates) and updates the web core component.

4.3.3.2 Extension

An Extension consists of a web client plugin, which adds new functionality to the EUCARIS framework. Extensions are optional, but require an updated system (all available and required Updates must have been installed).

4.3.4 Details

A System Update can be downloaded by using the Standalone Configuration Tool. The software components are received via a secure channel and all software is checked for viruses and signed by *EUCARIS Operations*. The Standalone Configuration Tool checks the integrity of the received software components to ensure a safe distribution of these components onto secure environments.

Since a request for System Updates requires secure communications between the Standalone Configuration Tool and the System Update Service, the request for software is signed and encrypted. Therefore the logged in user is required to access the private key of the EUCARIS certificate. Please refer to paragraph 5.2.4 on how to grant a user access to the certificates private key.

A System Update is executed by using the Standalone Configuration Tool and is manually initiated by the system administrator. A single System Update may be regarded as one atomic action: the Update succeeds completely, and if not the System Update is rolled back completely. Both success and failure of a System Update results in a working EUCARIS system. An emergency backup is created before the start of any change, so that the system can be restored if -in exceptional unexpected cases- something fails during installing or rolling back of a System Update. This emergency backup is located at: “C:\ProgramData\EUCARIS\Backup” (W2008) or “C:\Documents and Settings\All Users\Application Data\EUCARIS\Backup” (W2003).

A System Update is a zipped package, which consists of an XML script describing the actions of this System Update and zero, one or more of the following elements:

- EUCARIS related Microsoft .Net libraries (assemblies), scripts, web applications
- EUCARIS XML configuration files
- XSDs

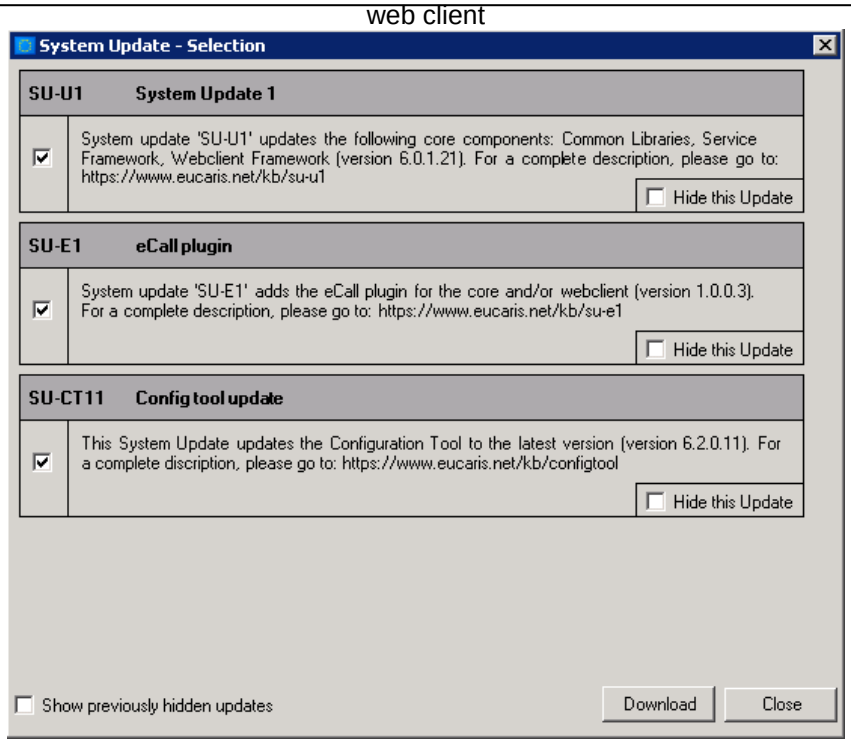
The system administrator is able to fully automatically execute the complete System Update. In case of separate roles for System-, Application- and Database administration it is possible to manually install some or all parts of the update. The actions a System Update performs are divided into the following groups:

- File actions; all copy and replace actions done on files belonging to the EUCARIS application
- Configuration actions; all actions which adapt the EUCARIS configuration files

For each group the System administrator is able to select manual or fully automatic installation and execution of the System Update.

4.3.5 Downloading System Updates

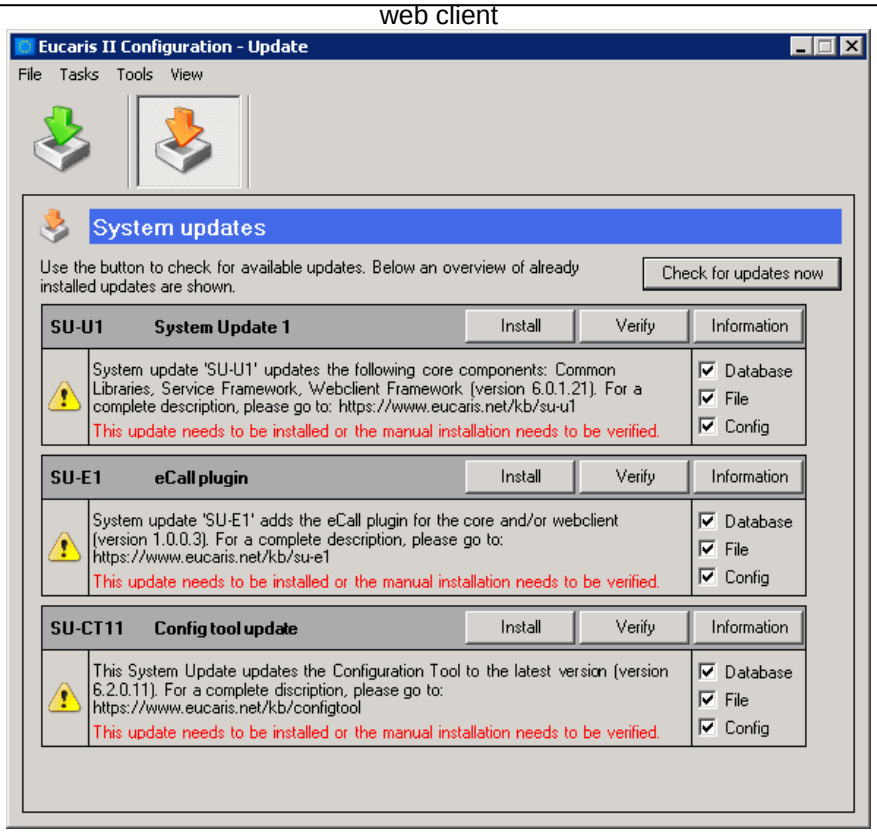
The availability of System Updates is announced via the NCP of your country, after which the administrator starts the Standalone Configuration Tool in the Update mode, selects the System Update screen and press the button “Check for updates now”:



The Configuration Tool retrieves an index of all applicable updates for this instance of EUCARIS. The System Administrator selects the relevant updates to download, or clicks “Hide this update” to suppress this update in the future (note: all suppressed updates are still available and selectable after clicking “Show previously hidden updates”). Updates of the Configuration Tool itself are also distributed via System Updates (denoted as SU-CTxx, where xx is a sequence number)

NOTE: It is advised to always update the Configuration Tool prior to execution of any other System Update.

All selected System Updates will be securely downloaded and extracted after clicking “Download” and the System Update screen will show the downloaded updates as ready to be installed or verified:



Per System Update the System Administrator can perform multiple actions, which are described below.

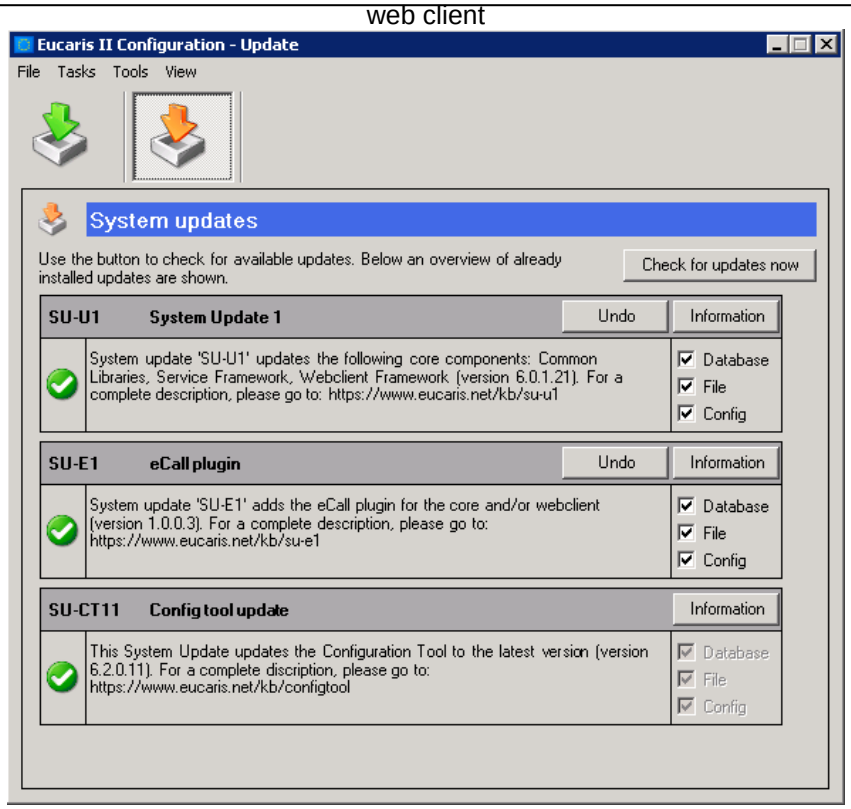
Fully automatic:
When all action groups (File and Config) are selected, the System Update will be installed fully automatic, but only if the current logged on user has the correct privileges to do all actions.

Partly automatic:
Consider to manually run part of the update if the System Administrator does not have the privileges to change application configuration or libraries. Click the button “Information” to get a detailed description of all actions and source files.

NOTE: When performing steps manually, the System Update can only successfully finish after all manual actions have been completed.

Fully Manual:
Click the button “Information” to get a detailed description of all actions and source files and perform the actions manually. After manual installation it is possible to verify this installation by clicking on the “Verify” button. The Configuration Tool gives detailed information if one of the described actions is not executed correctly.

Undo:
The System Administrator is able to undo the System Update in case of problems or on demand. Updates of the core components cannot be removed as long as there are Extensions installed which depend on a minimum core version.



NOTE: It is not possible to undo a System Update that updates the Configuration Tool.

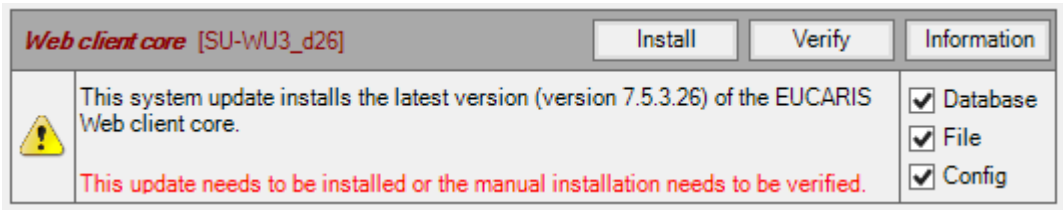
5. Installation of Standalone Web client

For the installation of the Standalone Web client we have to get the right updates from the configuration tool. We need at least the Web Client Core and one or more Web Client Extensions. The Standalone Web Client uses exactly the same package as the regular Web client. The configuration tool will be aware whether a Eucaris Instance is installed or not. If this is not the case the optional database updates will be ignored.

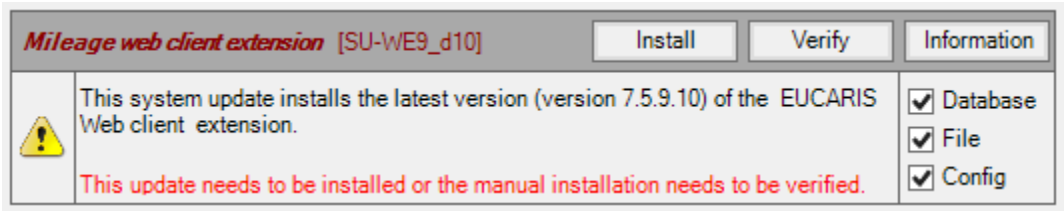
5.1 Install

For this we use the configuration tool as introduced in Chapter 4

First download the Web client Core. It's the update starting with SU-WU



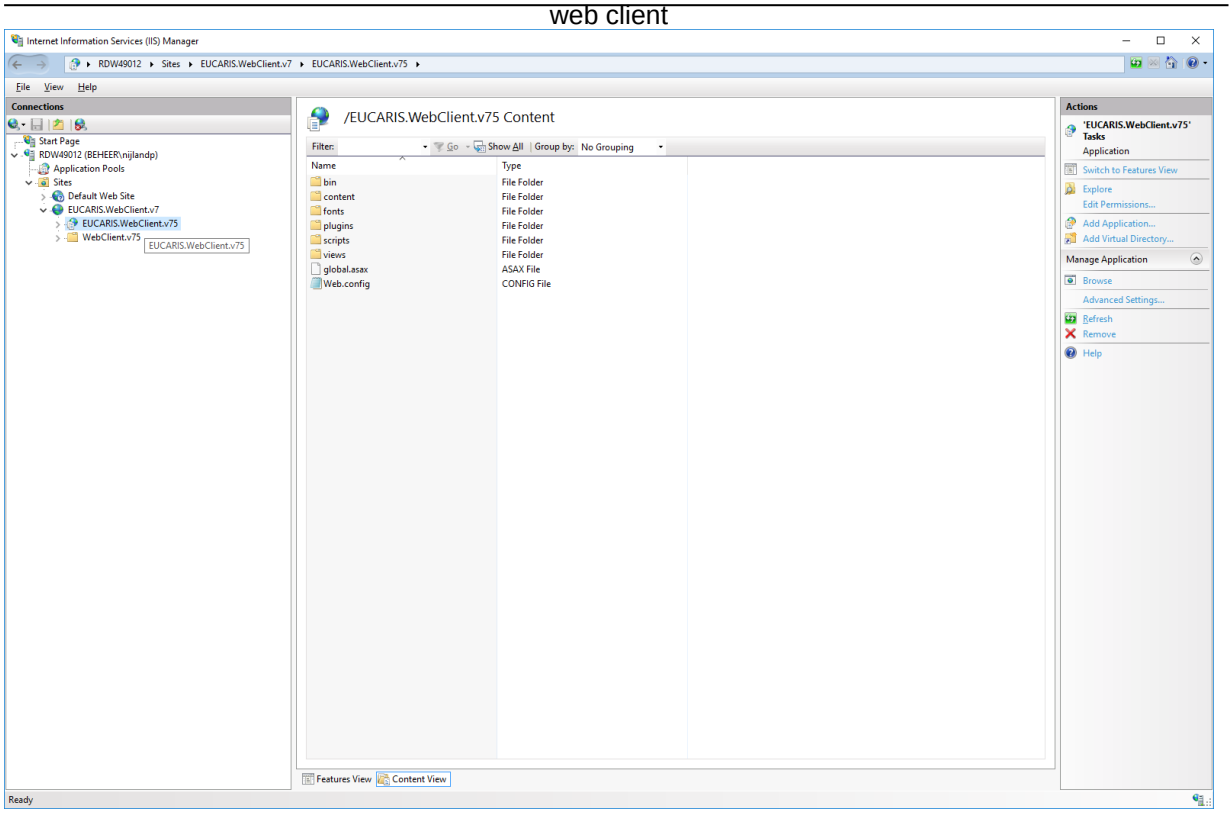
Please press install and follow the onscreen instructions.
After that please download one or more Web Client extensions. (e.g. Mileage).



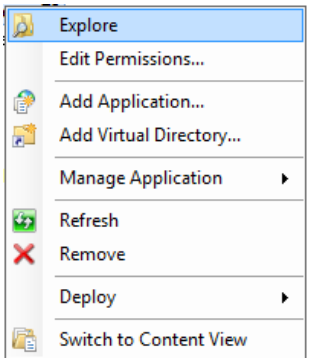
Please press install and follow the onscreen instructions

5.2 Configuration

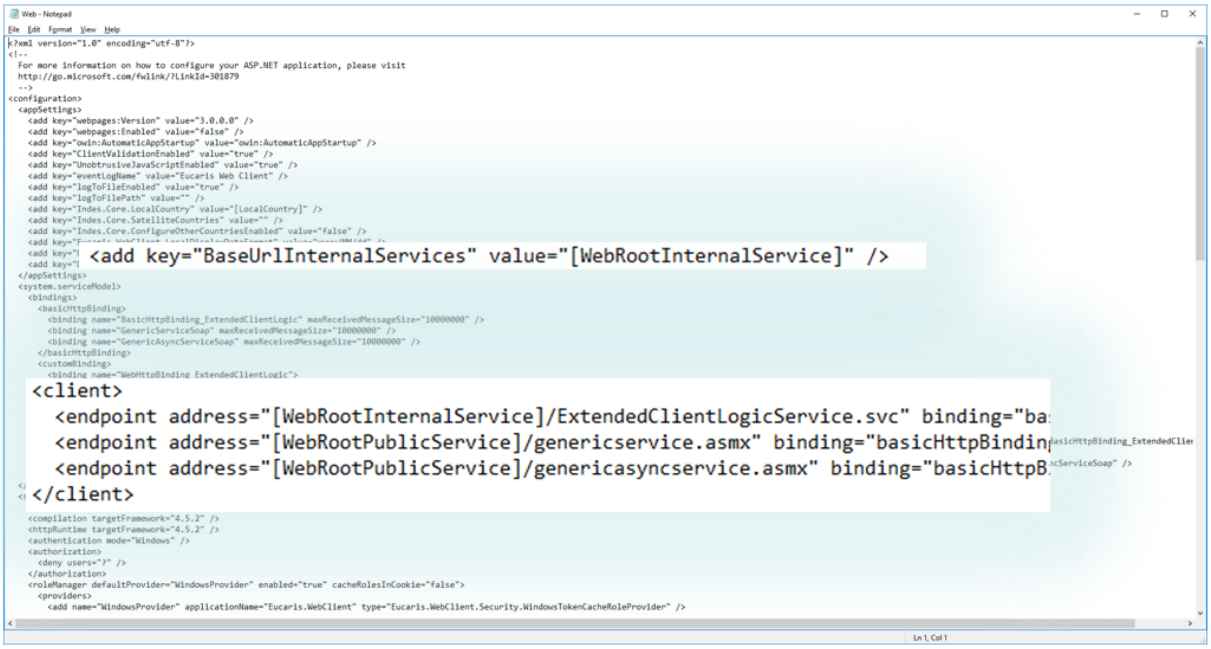
After installation of the Standalone tool we can open IIS and we see the added website:



The last thing we have to do is to change the configuration to use the web services of your NCP. Right click Eucars.Webclient.75 and press explore:



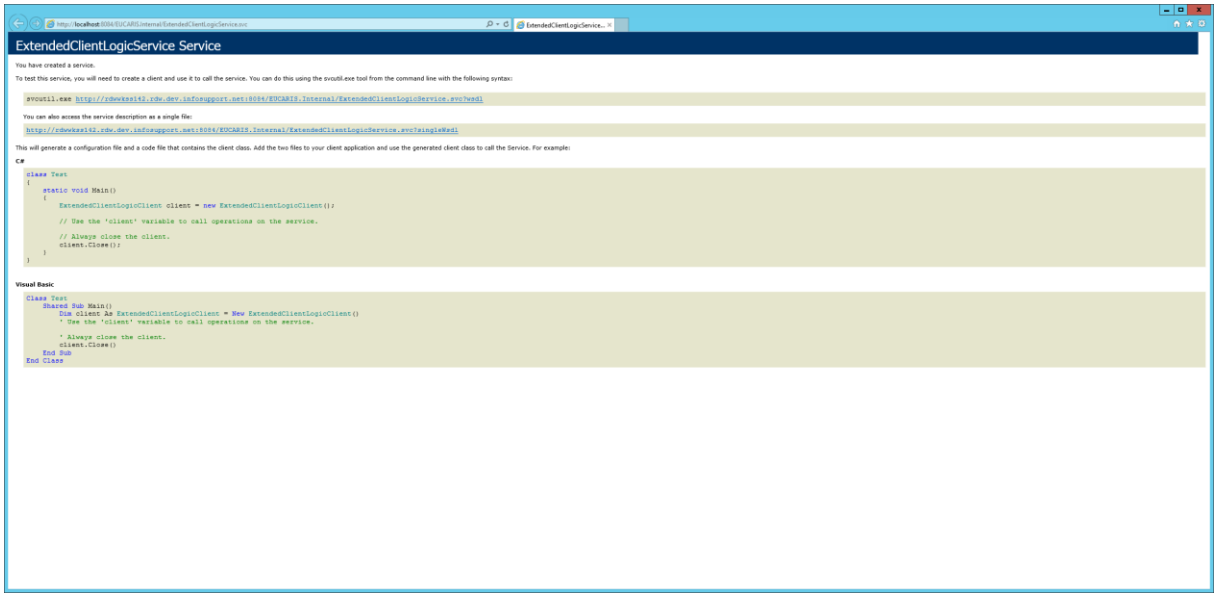
After that select the web.config and open it with an editor (e.g. notepad).



Please adjust the BaseUrlInteralServices and the 3 endpoints according to the information supplied by your NCP. The supplied Url's should look like this:

http://servername:7070/Dev.Eucaris.Internal/ExtendedClientLogicService.svc
http://servername:7070/Dev.Indes.Core.Services.Public/genericservice.asmx
http://servername:7070/Dev.Indes.Core.Services.Public/genericasyncservice.asmx

We can test them in the browser and if the connection is all setup correctly with your NCP, we should have a result like this example:



If this is correct then please use your editor to adjust the web.config and adjust the config on the 4 places as shown:

```
<add key="BaseUrlInternalServices" value="http://servername:7070/EUCARIS.Internal" />
```

Please note, this one is without the **ExtendedClientLogicService.svc**!

And

```
<endpoint
  address="http://servername:7070/Dev.Eucaris.Internal/ExtendedClientLogicService.svc" …
<endpoint
  address="http://servername:7070/Dev.Indes.Core.Services.Public/genericservice.asmx" …
<endpoint
  address="http://servername:7070/Dev.Indes.Core.Services.Public/genericasyncservice.asmx" …
```

For … please leave the rest of the line as is. Only adjust the Url. Please save the web.config.

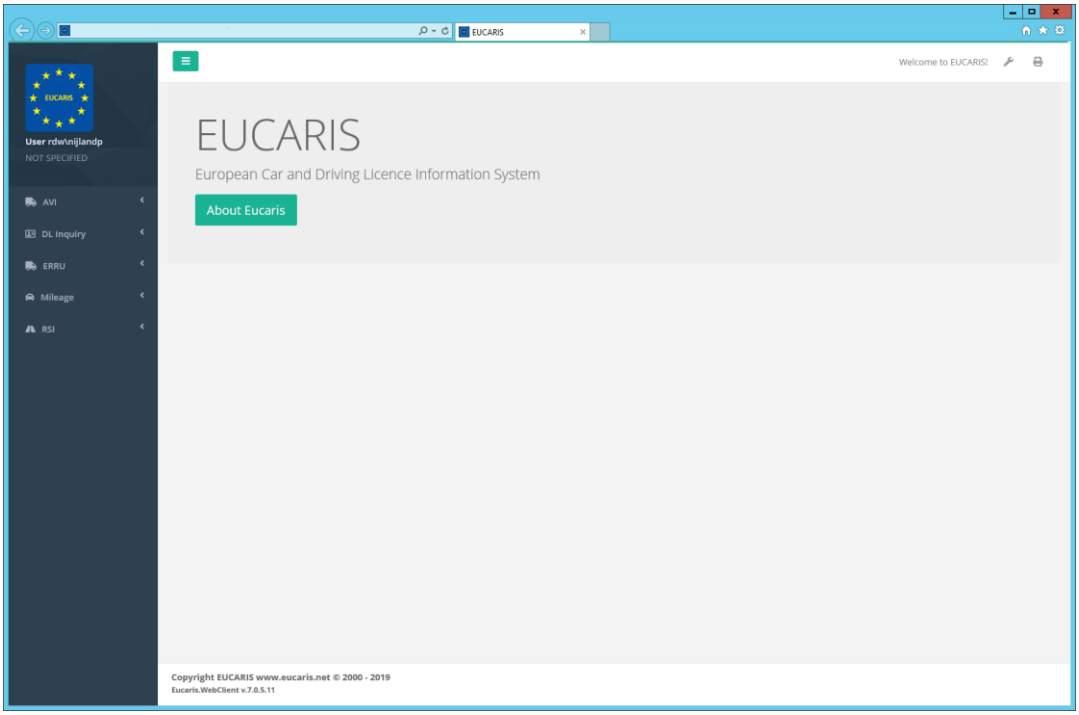
5.3 Installation Test

After all configuration settings are done the member state is ready to use EUCARIS outbound to request information from other countries.

5.3.1 Test EUCARIS Web Client

To verify correct installation of the Web Client browse to the following URL:

http://localhost:80/EUCARIS.WebClient.v75/



6. Security

If everything is working well, the final step is to consider a good security measure to secure the connection from the organisation (you) to the NCP. Eucaris is not responsible for this and cannot even enforce this. However we can you advice and help to accomplish a secure connection.

A possibility is to have a private network or VPN between the NCP and you. Also the Eucaris team has its own solution we can give to you. The so called Eucaris Secure Tunnel. With this option we can communicate with signed and/or encrypted messages between the standalone client and the web services of the NCP. Documentation for this Eucaris Secure Tunnel is available on request.

Furthermore there is a chapter on security in the Eucaris installation and operation manual available to the NCP.

6.1 Authorizations

Once the Standalone webclient is installed, the TAX office can make VAT requests from the VAT webclient, via the EUCARIS instance of the NCP. Very likely, the NCP is capable of performing other types of requests as well. Out of the box the solution presented in this document contains no technical measures that prevent the TAX office from sending requests of such other types, it will simply receive a response from EUCARIS. So, it may request data it is not supposed to.

We advise the NCP to implement means to prevent unauthorised use of services not related to the TAX office. Please note that the EUCARIS Public Services has – by design – no additional authorisation method. The NCP must implement that according to local security patterns or practices. Also note that EUCARIS Operations can advise NCP on how to secure the public service in their local domain. For that, please contact EUCARIS Operations.

6.2 Setting up SSL for web client

The standalone web client connects to the EUCARIS instance running at the NCP through three different endpoints:

- ExtendedClientLogic
- GenericService
- GenericAsyncService

These endpoints are also used by the webclient of the NCP-EUCARIS. The consequence of this instruction is that EUCARIS at the NCP no longer accept non-SSL connections. Therefore we advise to use SSL for the webclient at the NCP as well.

The following instructions explain how to setup the usage of SSL for the Standalone webclient. This involves work on both sides of the communication: the NCP and the TAX office. In short the steps are:

NCP

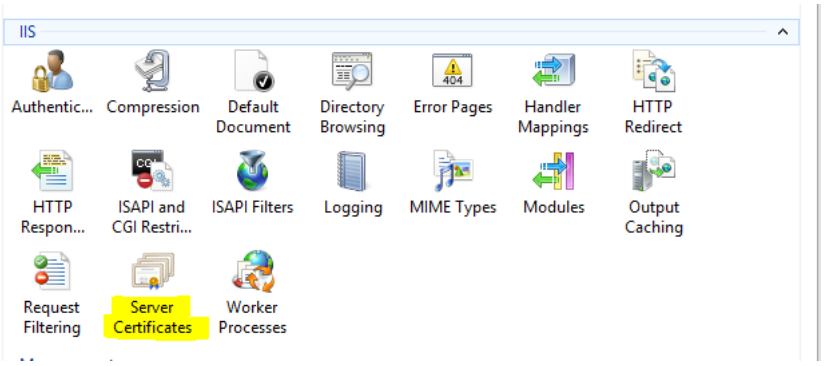
- Make sure there is a certificate (with private key) available that is hostname of the server
- Configure IIS:
    - Add certificate to IIS server certificates
    - Add binding for HTTPS and associate a certificate with it
- Update web.config of web services

TAX office

- Update web.config of the web client

6.2.1 IIS configuration - Certificate

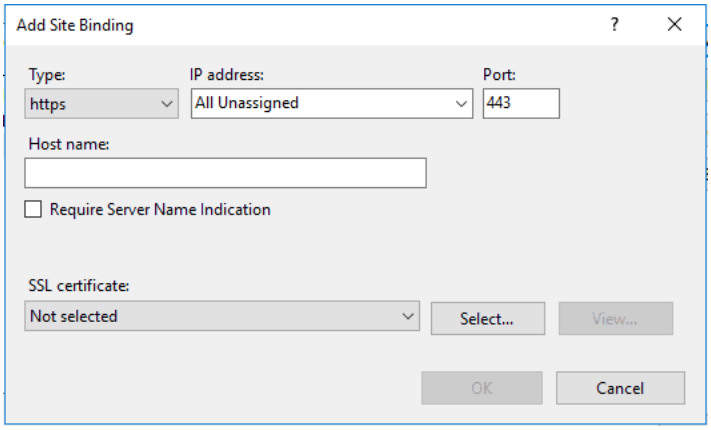
The creation of the certificate is out of scope for this manual; we simply assume it to be available. To install it, in IIS navigate to the server in the left pane and go the item Server Certificates:



The right pane will offer several options to add a certificate to IIS (import from .pfx, create self-signed certificate, …). We will not discuss the details of the options here; they highly depend on your specific situation.

6.2.2 IIS configuration – Add binding for HTTPS

In IIS, in the left pane, navigate to the website EUCARIS.Internal.v7. Right click on it and select “Edit bindings…”.



Apply the following settings:

Setting	Value
Type	https
IP address	All Unassigned
Port	<choose a number>
Host name	<empty>
SSL certificate	Select the certificate from section 6.2.1

Similarly, create a new binding for the website: EUCARIS.External.v7.

6.2.3 Web.config – Service side

In the Web.config file (located in [EUCARIS ROOT]\EUCARIS.v7\Web\Services\Internal), find the following lines:

```
<binding name="ExtendedClientLogicBinding" (…) />
  <security mode="None" />
</binding>
```

Set the security mode to Transport:

```
<security mode="Transport" />
```

Note: there is no service-side configuration required for the GenericService and the GenericAsyncService.

6.2.4 Web.config – client side

In the Web.config file (located in [EUCARIS ROOT]\EUCARIS.v7\Web\Clients\WebClient.v75), make the following replacements:

From:

```
<add key="BaseUrlInternalServices" value="http://host:port/Eucaris.Internal" />
```

To:

```
<add key="BaseUrlInternalServices" value="https://host:port/Eucaris.Internal" />
```

Make sure that the new hostname matches the host name from the certificate and the new port matches the one configured in section 6.2.2.

From:

```
<binding name="BasicHttpBinding_ExtendedClientLogic"
         maxReceivedMessageSize="10000000"/>
```

To:

```
<binding name="BasicHttpBinding_ExtendedClientLogic"
         maxReceivedMessageSize="10000000">
   <security mode="Transport" />
</binding>
```

From:

```
<endpoint address="http://host:port/Eucaris.Internal/ExtendedClientLogicService.svc"
(…) />
```

To:

```
<endpoint address="https://host:port/Eucaris.Internal/ExtendedClientLogicService.svc"
(…) />
```

Again, make sure that the new hostname matches the host name from the certificate and the new port matches the one configured in section 6.2.2.

Repeat the last two replacements for the other two bindings.

This finalizes the SSL configuration for the ExtendeClientLogic, the GenericService and the GenericAsyncService.s

7. Troubleshooting

This chapter will describe tips on how to troubleshoot problems with the EUCARIS installation. If these tips don't solve the problem that the user is experiencing, don't hesitate to contact the EUCARIS support team by email on EUCARIS2help@rdw.nl.

The first place to check for an indication on the problem is checking the windows system and application event logs, which are also used in case of problems by the EUCARIS applications.

More information on Error Messages can also be found at the EUCARIS.net knowledgebase at https://www.EUCARIS.net/kb/error-messages

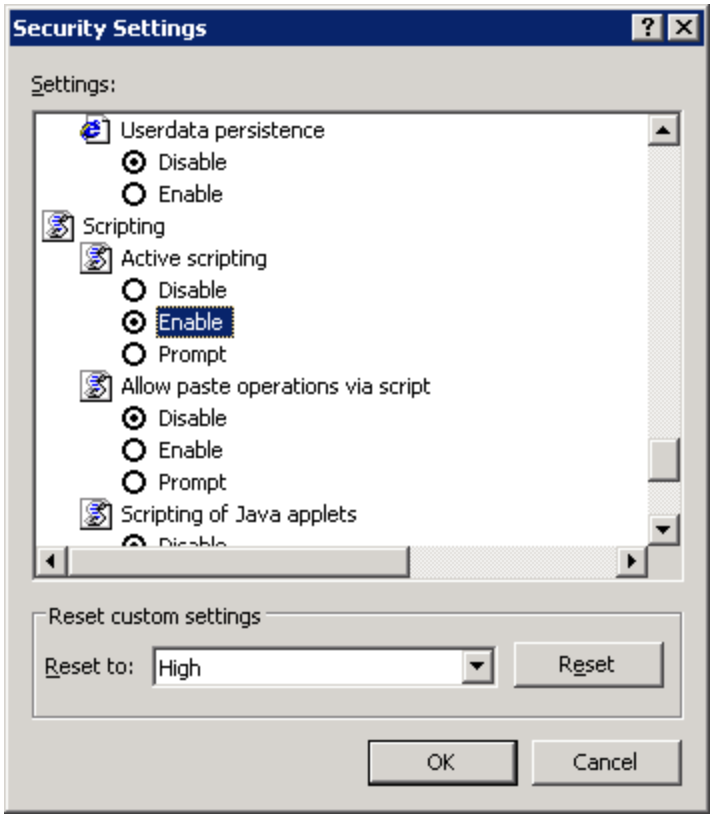
This chapter will further describe tips on troubleshooting the standalone web client and issues with IIS.

7.1 Application

This chapter will discuss multiple problems and solutions that can occur on the EUCARIS application.

7.1.1 Menu

In case the EUCARIS menu appears not to be working, the following has to be executed to fix this. In the web browser use 'Tools' > 'Internet options' and select the 'Security' tab. Select the 'Internet' zone and press 'Custom level…'. On the 'Security Settings' dialog, scroll down to 'Scripting' > 'Active Scripting' and change this to 'Enable'. Close the dialogs and refresh the browser to check if it works.



7.1.2 Access Denied

The error message 'Access Denied' can be caused by several problems, most often related to a wrong configuration of EUCARIS. Although the configuration and usage of the Installation and Configuration Tool is extensively described, below some additional causes are given:

The application is browsed from the server
This might occur just after installation of EUCARIS. Log off and log on again and retry. We advise NOT to use the web client and management client directly on the server.

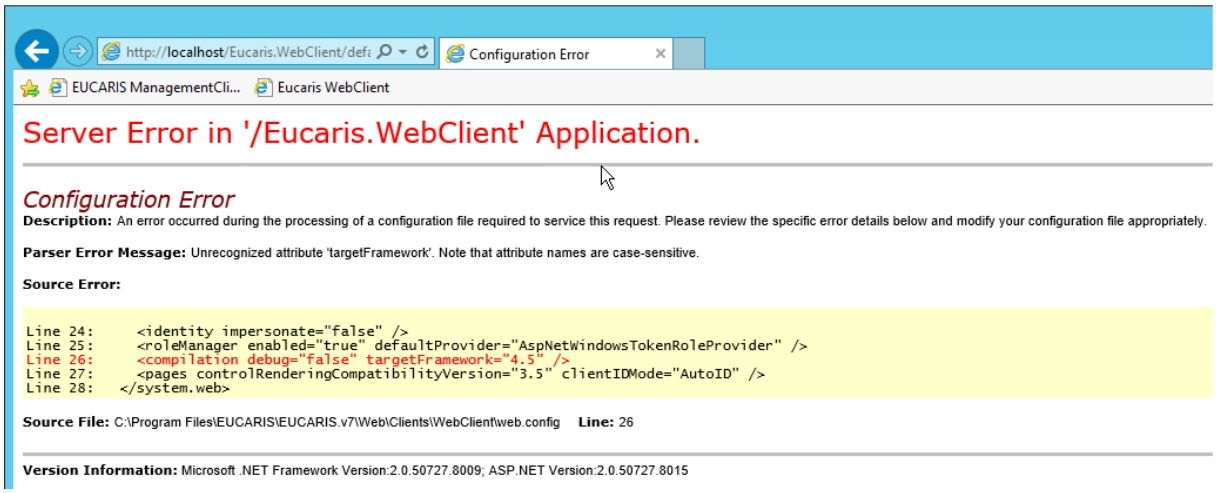
The user is not part of the right user group.
Parts of the application can be accessed by users who are a member of a certain user group. Local users can be setup with the Configuration Tool and domain users have to be added manually to the groups.

The user does not have a user profile in the database.
Each user must have a user profile in the database, which can be created using a script. You can create profiles for local users with the configuration tool. Other user profiles can be created with the Web Client.

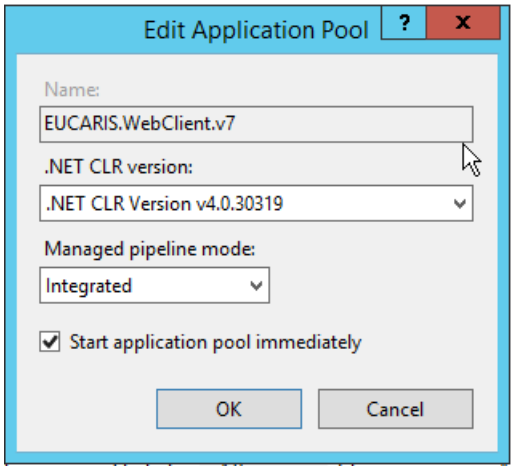
If all configuration settings described above are correct, the problem is probably caused by the database.

7.1.3 Unrecognized attribute 'Target Framework'.

The screenshot shows the appearance of this problem, which is caused by the wrong ASP.NET version being setup for the website.



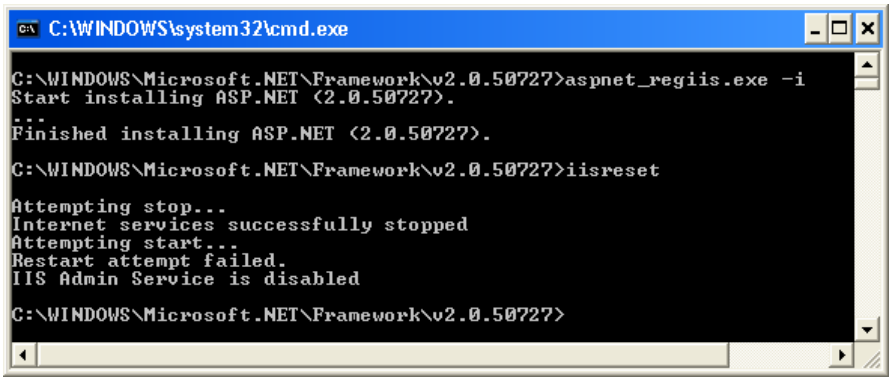
As can be seen in the bottom line of the above screen the .NET Framework 2.0 is used. Assuming the .NET Framework 4.5.x is correctly installed on the server, which is verified by the Pre-Configuration Tool, the EUCARIS sites need to be setup to use the .NET CLR 4.0. This is done by opening the 'Properties' of each EUCARIS site's application pool. On the Edit Application Pool dialog select the '.NET CLR version' dropdown and verify that '.NET version' is set to 4.0.30319.


Edit Application Pool
Name:
EUCARIS.WebClient.v7
.NET CLR version:
.NET CLR Version v4.0.30319
Managed pipeline mode:
Integrated
Start application pool immediately
OK
Cancel

7.2 Internet Information Services

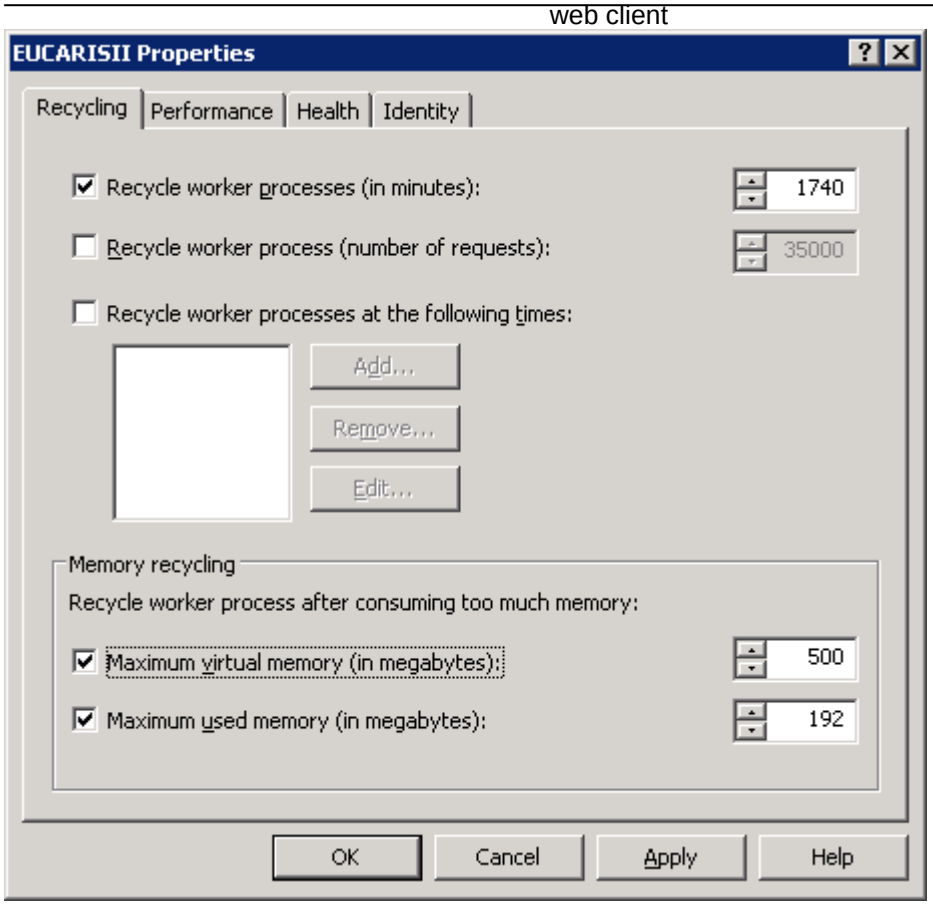
In some cases when browsing to one of the EUCARIS sites a 'HTTP 404 Not Found' or 'The page cannot be displayed' message is shown, which can be caused by multiple problems. The most common problem is a misconfiguration of the .NET framework in IIS. Solution is to reconfigure the ASP.NET installation within Internet Information Service, by running the following command:

'drive:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe –i



7.2.1 Memory usage on the webserver

If you search messages with the log viewer the result set is cached on your webserver. So if you do searches with a large scope you could use up a lot of memory on your server causing the server to stop working. This can be restricted on your server by switching on "memory recycling" on the application pool used for the log viewer. The picture below is an example of this setting:



Of course it is better to narrow your searches on date and time and by using the indexes suggested in section 4.3

8. Appendix

The appendix contains detailed descriptions on how to prepare and configure the server for EUCARIS manually, either in case it is chosen not to use the supplied Pre-Configuration Tool and Configuration Tool or if the unfortunate happens and those tools are not able to execute the steps correctly.

8.1 How To: Install Microsoft .NET Framework 4.7.2

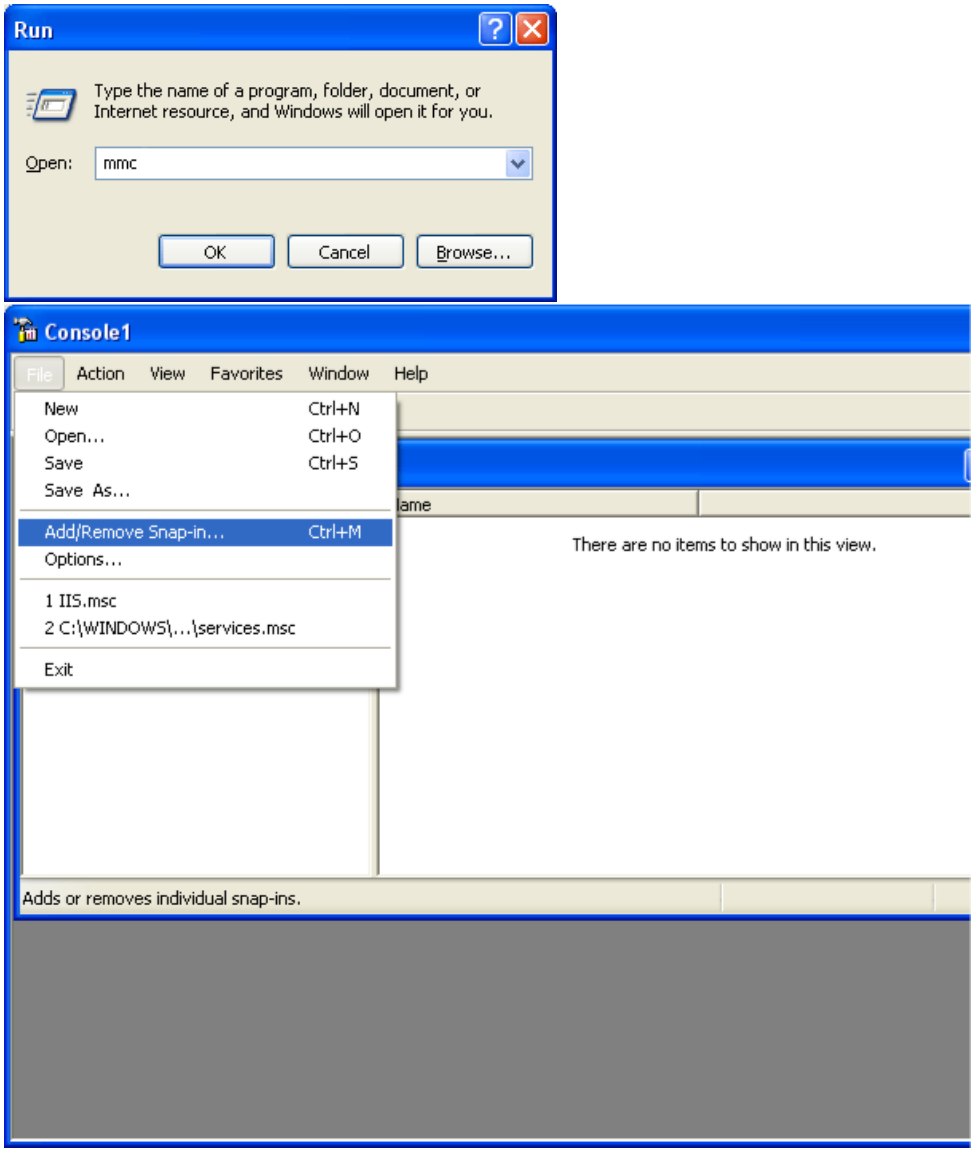
The .NET Framework 4.7.2 offline installer can be downloaded from the Microsoft site (https://www.microsoft.com/en-US/download/details.aspx?id=42642). Follow the associated installation instructions

8.2 How To: Adding Root and Intermediate certificates via MMC

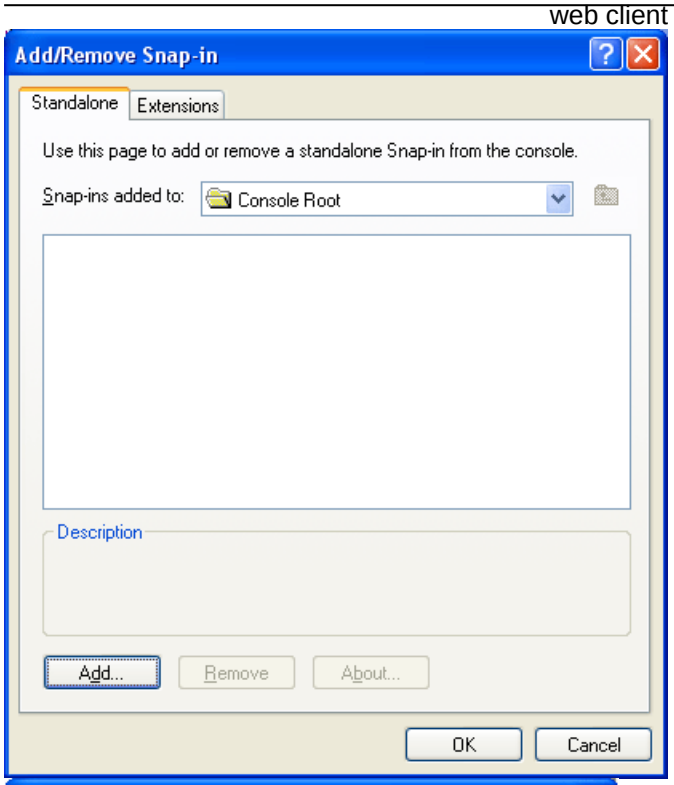
Files to have on hand: Root and/or Intermediate certificate files. If you're unsure which to get or which is which, please contact us at EUCARIS2help@rdw.nl

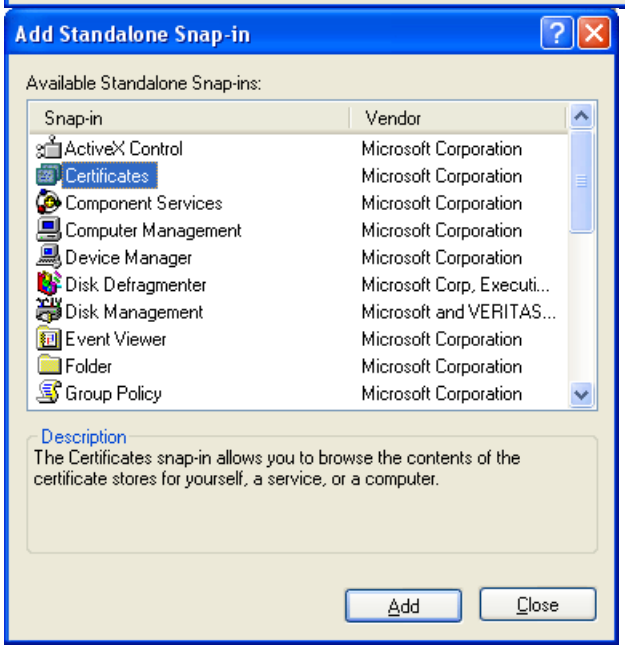
Root and Intermediate Certificate installation via MMC

1. Open up the Microsoft Management Console (MMC)
Start -> Run -> Type "mmc" (without quotes) and Click 'OK' or hit Enter on your keyboard.
2. Open 'Add/Remove Snap-in' Window



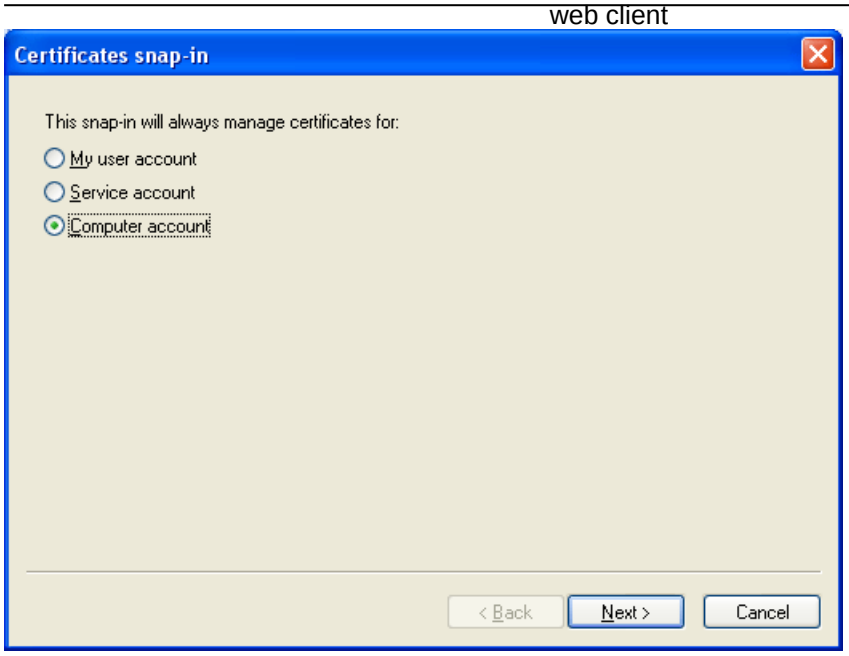
File -> Add/Remove Snap-in 3. Add the Certificates Snap-in





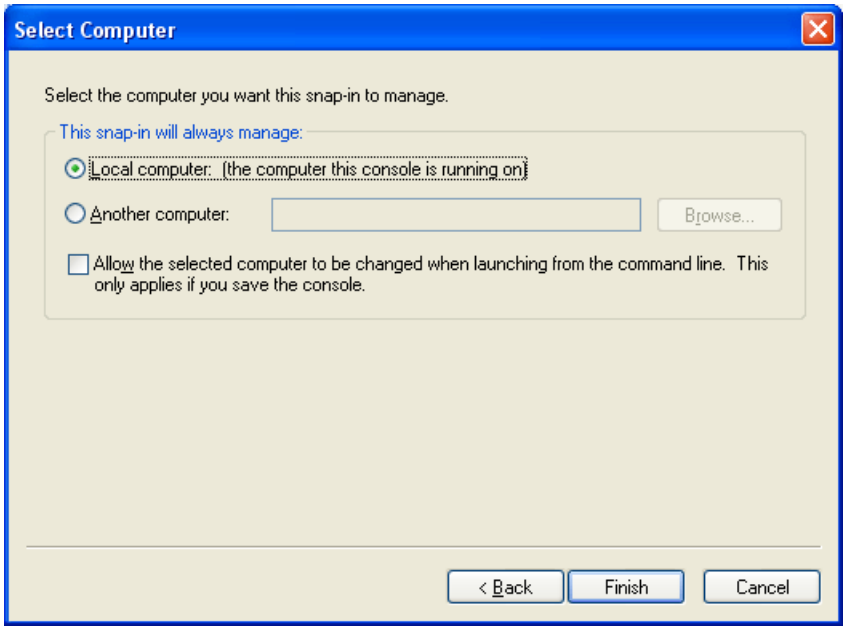
Click 'Add' then double-click 'Certificates'

4. Select 'Computer Account' and click 'Next'



Note: This step is very important. It must be the 'Computer Account' and no other account

1. Select 'Local Computer' and click 'Finish'



6. Close the 'Add Standalone Snap-in' window and click 'OK' in the 'Add/Remove Snap- in' Window.
7. Will now be returned to the MMC.

Install/Import the Root and Intermediates Certificate
**** Procedure for ROOT certificates:***

1. Expand the Certificates section by clicking on the plus (+) sign and turn it to a minus (-) sign to expose the 'Certificates' tree.

2. Import the Root Certificate
Right-click on 'Trusted Root Certification Authorities', select 'All Tasks', then select 'Import'.

Console1
Console Window Help
Console Root
Action View Favorites
Tree Favorites
Name
Console Root
Certificates (Local Computer)
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certificat
Other People
R
REQUEST
SPC
Find Certificates...
All Tasks
New Window from Here
Refresh
Help
Find Certificates...
Import...
Add a certificate to a store
Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

Click 'Next'.

Locate the Root Certificate and click Next. When the wizard is completed, click Finish.

**** Procedure for Intermediate certificates:***

1. Import Intermediate(s)

The process is the exact same except the area of interest is 'Intermediate Certification Authorities' instead of 'Trust Root Certificate Authorities' and the file(s) that are to be imported are the remaining files outside of your domain certificate.

4. Restart EUCARIS Services trough the EUCARIS Configuration Tool.

8.3 How To: Manually import a Certificate Revocation List (CRL)

From command line (with elevated administrator privileges):

```
certutil -addstore ROOT EUCARISTest-2014.crl
```

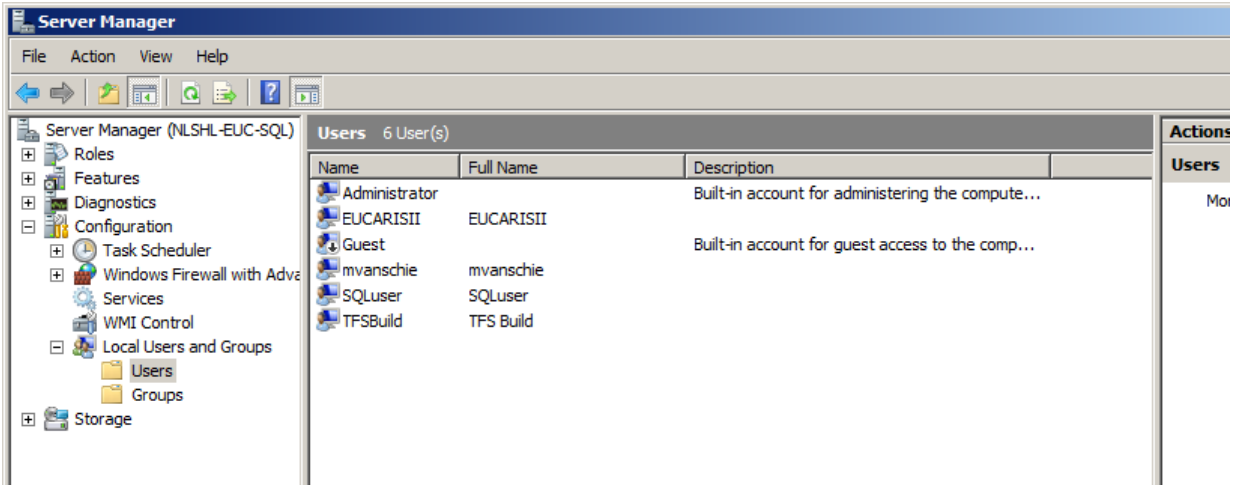
Or from GUI:

Start up the Microsoft Management Console (mmc), and add the Certificates snap-in for the local computer. Select “Trusted Root Certification Authorities” and right-click, select All Tasks and import.

Browse to the folder where you have placed the CRL. Make sure to set the file filter to *.crl, otherwise you won’t see the file. Click import.

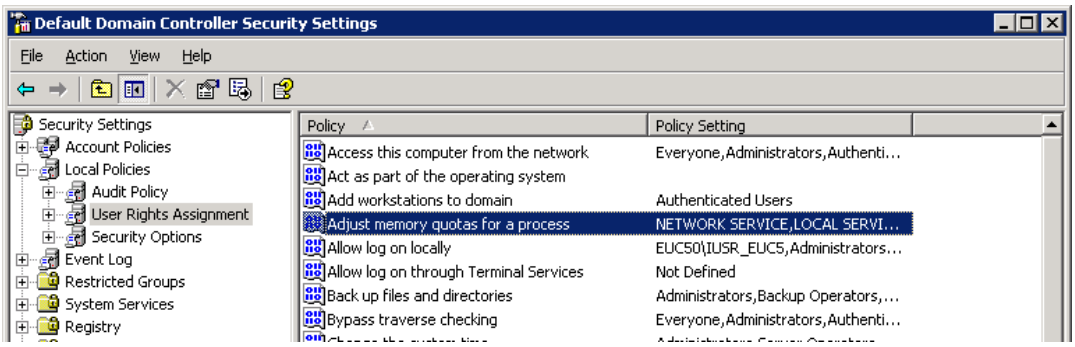
8.4 How To: Manually create an EUCARIS service account

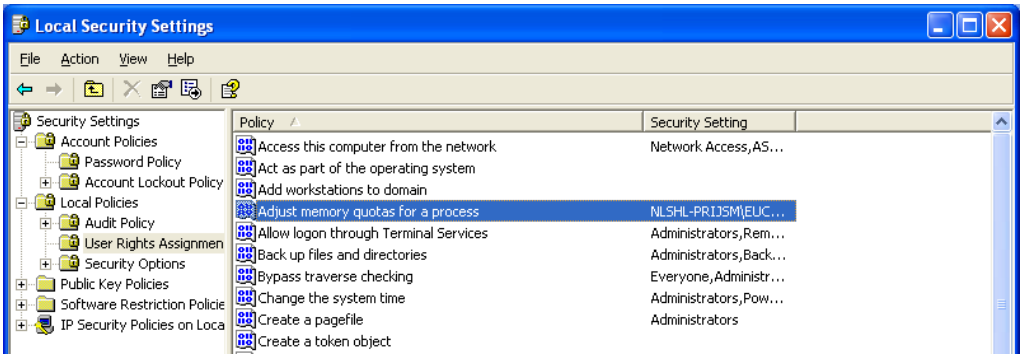
On Windows Server 2008 this is done by opening the 'Server Manager' console and locates the 'Local Users and Groups'. Right-click on the *Users* folder and select *New User*. Create a new user with the user name EUCARIS and apply the policies as described in the next 'How To:'.



8.5 How To: Manually set the required policies of the EUCARIS service account

After the user is created the users has to be added to a number of security policies, to allow using the service account to run an application pool and windows services. Depending if the server is a domain controller the 'Domain Controller Security Policy' or 'Local Security Settings' has to be started from the 'Administrative Tools' as shown below and 'User Rights Assignment' has to be selected:





Locate the following policies and add the EUCARIS service account to these policies, by opening the properties and use the 'Add User or Group' button to add the account:

- Adjust memory quotas for a process
- Log on as a service
- Replace a process level token