



EUCARIS

Installation and Operation Manual

Document version	11
Document date	19-01-2023
EUCARIS release	7.64
Author	EUCARIS Operations
E-Mail	eucaris2help@rdw.nl

Table of contents

1.	Introduction.....	5
1.1	Structure	5
1.2	Support	5
2.	Overview.....	6
2.1	Context.....	6
2.2	Structure	7
3.	Preparation.....	9
3.1	Hardware requirements	9
3.1.1	Minimum hardware requirements	9
3.1.2	Recommended hardware requirements.....	9
3.1.3	Database.....	9
3.1.4	Test and production requirements	9
3.2	Network requirements	10
3.3	Database requirements	10
3.4	Software requirements and prerequisites.....	11
3.4.1	Windows server requirements	11
3.4.2	TLS1.2 requirements	12
4.	Installation.....	13
4.1	Initial installation.....	13
4.1.1	Prerequisites and application files.....	13
4.1.2	Welcome	14
4.1.3	Check prerequisites	14
4.1.4	Service account.....	15
4.1.5	Website Folders.....	17
4.1.6	Website Names, Ports and Application Pools	18
4.1.7	Execute EUCARIS Prerequisites	20
4.1.8	Application Root folder	20
4.1.9	Installing EUCARIS Core.....	21
4.1.10	Tools root folder	21
4.1.11	Installing EUCARIS Configuration Tool	22
4.1.12	Install or re-use EUCARIS Database	23
4.1.13	Finish.....	35
5.	Configuration (initial installation)	36
5.1	Wizard Mode (initial installation).....	36
5.1.1	Welcome	36
5.1.2	Configuration Tool Preferences.....	37
5.1.3	Analyse current configuration	38
5.1.4	Local configuration	38
5.1.5	Certificate configuration (initial installation)	39
5.1.6	Checking and finalizing configuration	45
5.2	Advanced Mode	48
5.2.1	Basic configuration analysis	49
5.2.2	Create Analysis Report.....	50
5.2.3	Database configuration	52
5.2.4	Logging configuration	54
5.2.5	Application configuration.....	55
5.2.6	Certificate configuration	57
5.2.7	Network analysis.....	60
5.2.8	User management	62
5.2.9	Export and Import Settings	64

5.2.10	Tasks.....	65
5.2.11	Tools.....	68
5.3	Update mode	69
5.3.1	Configuration Update Service.....	70
5.3.2	System Update.....	80
5.4	Broker configuration mode.....	84
5.5	Installation test.....	84
5.5.1	Test EUCARIS Web Clients.....	85
5.5.2	EUCARIS Test Tools	86
6.	Security.....	87
6.1	Securing External Services	87
6.2	Securing Public Services.....	87
6.2.1	IP and Domain Restrictions	88
6.2.2	Client Certificate Mapping	89
6.3	Securing Internal Services.....	90
6.4	Support for Malware detection.....	91
6.4.1	General configuration	92
6.4.2	Configuration per extension.....	92
6.4.3	Malware application specific configuration	93
6.4.4	Malware detected.....	93
6.5	Setting up SSL for web client.....	94
6.5.1	IIS configuration - Certificate.....	94
6.5.2	IIS configuration – Add binding for HTTPS	95
6.5.3	Web.config – EUCARIS service side	95
6.5.4	Web.config – web client side	96
7.	Performance and scaling	97
8.	Operation.....	98
8.1	Management.....	98
8.2	Statistics.....	99
8.3	Maintenance	99
8.3.1	Database.....	99
8.3.2	Backup.....	99
8.3.3	Configuration updates	99
9.	Troubleshooting.....	101
9.1	Network	101
9.2	Certificates.....	102
9.3	Database	102
9.4	Application	103
9.4.1	Access Denied.....	103
9.4.2	Unrecognized attribute ‘Target Framework’	103
9.5	Internet Information Services	105
9.5.1	Memory usage on the webserver.....	105
10.	Appendix.....	107
10.1	How To: Adding Root and Intermediate certificates via MMC	107
10.2	How To: Manually import a Certificate Revocation List (CRL)	112
10.3	How To: Manually create an EUCARIS service account	113
10.4	How To: Manually set the required policies of the EUCARIS service account	118
10.5	How To: Manually set SSL authentication for External application on IIS.....	119
10.6	How To: Manually add a client certificate to legacy service connections	120
10.7	How To: Install a Certificate using System Updates	127
10.7.1	Online.....	127
10.7.2	Offline.....	128

- 10.8 How To: configure a satellite country in EUCARIS.....129
 - 10.8.1 Outbound configuration.....129
 - 10.8.2 Inbound configuration131
- 10.9 How To: Install the EUCARIS Update Service132
 - 10.9.1 Installing the update service132
 - 10.9.2 Exposing updates.....132
 - 10.9.3 Configuration.....132
 - 10.9.4 Certificate configuration133
- 10.10 How To: get remote support on the EUCARIS server134
 - 10.10.1 Installation procedure.....135
 - 10.10.2 Enable EUCARIS Remote Desktop.....137
 - 10.10.3 Disable EUCARIS Remote Desktop138

1. Introduction

This chapter introduces the structure of the installation and operation manual and how to contact the EUCARIS support teams.

1.1 Structure

This document contains all the information that is needed to install and operate EUCARIS in a member state. The following chapters are included in the document:

Chapter 1 – Introduction	: Describes the document structure and support for EUCARIS.
Chapter 2 – Overview	: Describes EUCARIS on a global level.
Chapter 3 – Preparation	: Describes how to prepare for EUCARIS installation.
Chapter 4 – Installation	: Describes how to install EUCARIS.
Chapter 5 – Configuration	: Describes how to configure EUCARIS.
Chapter 6 – Performance and sizing	: Describes the scenarios for performance and sizing.
Chapter 7 – Operation	: Describes how to operate and maintain EUCARIS.
Chapter 8 – Troubleshooting	: Describes how to troubleshoot EUCARIS.
Appendix	: Contains detailed ‘How To:’ descriptions

1.2 Support

For support during installation and operation of EUCARIS, the member states can contact the support teams of the Nominated Party for Operations (called “*NPO*” or “*EUCARIS Operations*”). The *NPO* is just like any other participating member state but has additional responsibilities. These additional responsibilities consist of informing, supporting and accepting the other member states and reporting to the other member states. Currently this role is assigned to the RDW in the Netherlands. The *NPO* is denoted as *EUCARIS Operations* in this document.

The member states can contact the installation and development support team by mail via EUCARIS2help@rdw.nl

2. Overview

This chapter introduces EUCARIS on a global level to clarify the context EUCARIS is used in and what the basic structure of EUCARIS is and which supporting tools are available.

2.1 Context

EUCARIS is used by a large number of European countries for the cross-border exchange of transport related information. The application has been developed by the EUCARIS organisation, originally aiming to support the registration authorities of the participating countries in their fight against vehicle crime and fraud, within the legal framework of the EUCARIS Treaty.

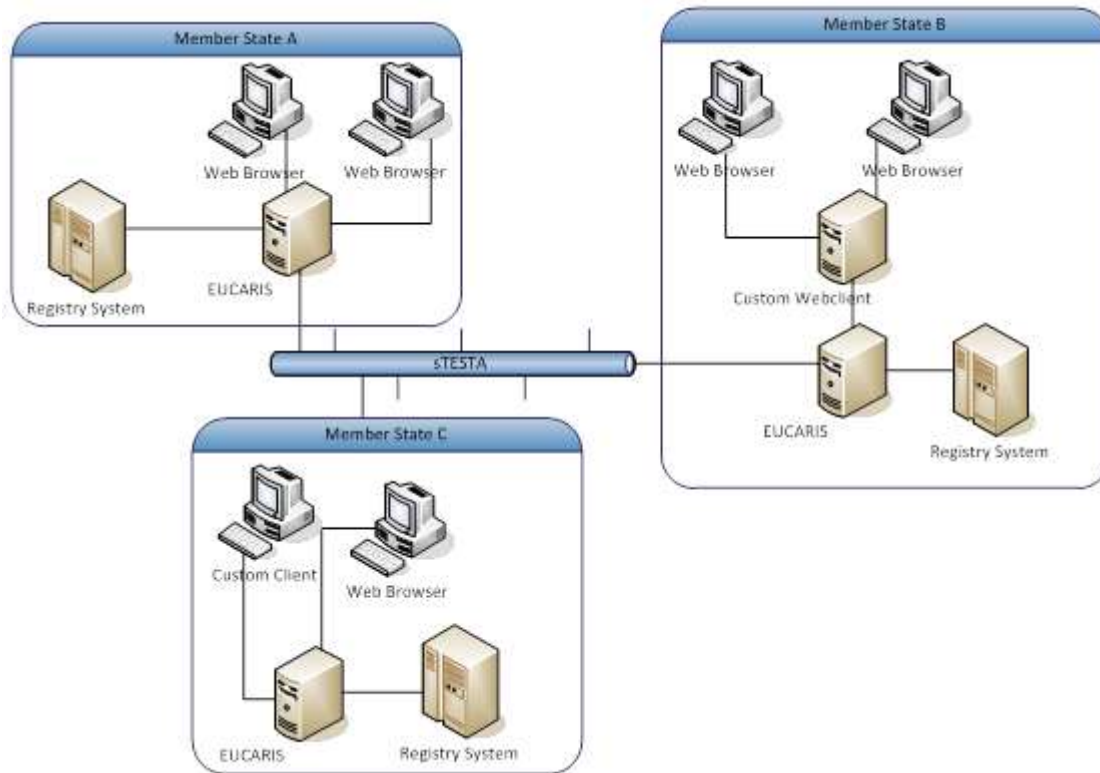
Each member state is responsible for its own vehicle (and related) registration. EUCARIS merely connects these registrations and is responsible for routing, logging and securing the international part of the communication. Each member state is responsible for the security within the domestic domain of the member state.

In recent years EUCARIS has become available for other parties as well. Police organisations use EUCARIS within the framework of the Prüm Council Decisions to exchange information on insurances, vehicles and their owner/holders. Recently several European projects has sought co-operation with the EUCARIS organisation in order to communicate vehicle- and driver's license information between authorities. Currently EUCARIS supports a large number of data exchanges which includes:

- CBE, Cross-Border Enforcement,
- eCall, Harmonised eCall European Pilot (HeERO),
- ERRU, European Register of Road Transport Undertakings,
- EUCARIS (treaty),
- IVI, Initial Vehicle Information,
- Mileage, vehicle mileage registration,
- Prüm (EU Council Decision 2008/615/JHA),
- RESPER, RESeau PERmis de conduire,
- TACHO, Tachograph card information exchange,
- VHOH, Bilateral Vehicle owner/holder exchange
- VAT, Value added tax
- Toll-EETS, European Electronic Toll Service
- ProDriveNet, Professional Drivers Network

2.2 Structure

EUCARIS has a peer-to-peer structure, implying that each member state has its own EUCARIS server. This allows for any to any communication between member states without depending on a central message broker and the availability of all member states. See below for an example:



EUCARIS is built around a number of web applications, each with its own purpose, which are:

- **The EUCARIS Core services**
A set of web services responsible for receiving and processing inbound requests, applying message validation, security, logging and routing. The core services consists of the following components:
 - **External web services**
This set of services is the endpoint for the other member states to request data from the local server
 - **Public web services**
When a custom client for EUCARIS –or other legacy application integration- is to be build, this set of services can be used to send requests to all connected (and authorised) member states

- **Web Client applications**
EUCARIS includes a default web clients to support data requests or application management:
 - **EUCARIS Web Client**
A web application which can be used for most of the available data exchanges
 - **EUCARIS Management Client**
A web application for basic application management

The communication from and to EUCARIS is based on standard XML and SOAP. To ensure secure connection and communication between member states, a number of security measures are taken, which are:

- **Dedicated channel**
Connection can only be established via TESTA (Secured Trans European Services for Telematics between Administrations).
TESTA is a private, highly-secured closed network for public administrations in Europe
- **Encryption**
EUCARIS uses Transport Layer Security (TLS) between member states so the data is encrypted between the EUCARIS instances of the Member States
- **Signing**
EUCARIS messages are signed using an X509 certificate. Each participating member state receives a unique certificate issued by *EUCARIS Operations*

The communication between EUCARIS and the domestic/local services can be secured using commonly used (Windows) security. EUCARIS supports both TLS and Client Certificate security.

Apart from the already described EUCARIS web applications, EUCARIS also includes a number of supporting tools. These are the following tools:

- **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 4.
- **Configuration**
To ease the installation and configuration of EUCARIS, the application is shipped with a Configuration Tool. Summarized this tool allows an administrator to configure and modify an EUCARIS installation, export configuration and translation information and install updates issued by *EUCARIS Operations*. This tool will be discussed in detail in chapter 0 and 5.

3. Preparation

Before installing and configuring EUCARIS there are a number of hardware and software requirements and prerequisites, which have to be fulfilled before EUCARIS can be installed.

3.1 Hardware requirements

This section describes the EUCARIS hardware requirements. Furthermore some advice is given about combining a test and production environment on one hardware platform.

3.1.1 Minimum hardware requirements

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

- > 2GHz multi core processor,
- \geq 8 GB memory,
- 20 GB free space available (excluding required database space),
- Network connection to *TESTA (secured Trans European Services for Telematics between Administrations)*

The above hardware is sufficient as a starting point for EUCARIS, but it is important to keep in mind that the configuration depends on the number of active users and the expected message volume. Scaling might be needed if the number of users or message volume increases, see also chapter 7.

3.1.2 Recommended hardware requirements

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

- > 2GHz multi core processor,
- \geq 16 GB memory,
- 20 GB free space available (excluding required database space),
- Network connection to *TESTA (secured Trans European Services for Telematics between Administrations)*

3.1.3 Database

If the database is running on the same server we would advise to at least double the memory. The Eucaris database can grow significantly in time due to the logging and the obligation to keep certain logging for a period of time. We have automatic purging on logging, but the purging is aware of the retention dates of the logging.

It is also advised to set the database size to auto grow.

3.1.4 Test and production requirements

We advise to create a permanent and separate environment for testing. This test environment should be used to test the client functionality of the EUCARIS application in combination with the permanent test environment of *EUCARIS Operations* and to test the integration with the local register.

NOTE: For the test and production environment separate TESTA IP addresses are required

3.2 Network requirements

Network configuration is not part of this instruction but is essential for using EUCARIS with other member states. The following things should be kept in mind when configuring the network:

- **TESTA**
EUCARIS uses the TESTA closed user group network so the user should arrange a connection to this network. Please send the TESTA IP addresses to EUCARIS2help@rdw.nl as soon as available
- **Firewall**
To allow communication with other member states the firewall should allow outbound and inbound connections. A list of IP addresses can be obtained via eucaris2help@rdw.nl
- **URLs and IP addresses**
The URLs and IP addresses of other member states are distributed via the EUCARIS configuration update mechanism. EUCARIS does not use a DNS system, therefore the IP addresses of other member states must be stored in the hosts file of the server, and if applicable on a local DNS system. For more details on the configuration update mechanism please refer to paragraph 5.3

3.3 Database requirements

Database installation is not part of the installation and operation manual, but it is essential for EUCARIS to work correctly. Currently EUCARIS supports the following databases and database versions:

Microsoft SQL Server 2014 SP2 – 2022 (all editions)

For each of these SQL Server editions also free Express editions are available, but keep in mind that there are technical restrictions for these editions. The most important restriction to mention here is the maximum size of the database, which differs for each Express version. Furthermore it is advised to install using a default instance, mixed authentication and of course the most recent service pack available for the chosen edition.

Oracle 19C – 21C (all editions)

For some editions there are express (XE) editions available, which can be used as well, but also here some restrictions apply regarding the number of supported databases. Also for Oracle it is advised to install the latest service packs available. Installation of an Oracle Client on your EUCARIS server is required for a EUCARIS connection to your Oracle database. Make sure to use the 64 bit client for Oracle on a 64 bit Server.

The appendix describes details on how to install the free and advised SQL Express 2012.

3.4 Software requirements and prerequisites

This section describes the EUCARIS software requirements and prerequisites that have to be complied with before installation of EUCARIS can proceed. The Pre-Configuration tool can be used to verify these requirements and allows configuring the steps to comply with the prerequisites.

3.4.1 Windows server requirements

EUCARIS 7.0 and higher is tested to work correctly on 2012R2 to 2022. This documentation will mainly focus on Windows Server 2019 installation. The following roles and features are required:

Server Roles:

Web Server (IIS)

Web Server Role (IIS)\ Role Services:

Web Server

- Common HTTP Features
 - Default Document
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - HTTP Redirection
- Health and Diagnostics
 - HTTP Logging
- Performance
 - Static Content Compression
- Security
 - Request Filtering
 - Basic Authentication
 - IIS Client Certificate Mapping Authentication
 - Windows Authentication
- Application Development
 - .NET Extensibility 4.7
 - ASP.NET 4.7.2
 - ISAPI Extensions
 - ISAPI Filters

Management Tools

- IIS Management Console
- IIS Management Scripts and Tools

Features:

- .NET Framework 4.7.2 Features
 - .NET Framework 4.7.2
 - ASP.NET 4.7.2
 - WCF Services
 - HTTP Activation
 - Message Queuing (MSMQ) Activation
 - TCP Port Sharing
 - Message Queuing
 - Message Queuing Services
 - Message Queuing Server
- Windows Process Activation Service
 - Process Model
 - Configuration APIs
- WoW64 Support

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

3.4.2 TLS1.2 requirements

Since June 2018 TLSv1.0 and TLSv1.1 are officially deprecated on TESTA. Since October 2018 this is enforced by only supporting TLSv1.2 by services on TESTA. Therefore the EUCARIS server needs to be configured to be able to handle TLS1.2 traffic.

When using Microsoft Windows Server 2012R2 (or lower) and/or Microsoft .NET framework version 4.6.2 or lower (in any combination) additional settings are required.

Please check if the following keys and values are present and set accordingly in the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"AspNetEnforceViewStateMac"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\.NETFramework\v4.0.30319]
"AspNetEnforceViewStateMac"=dword:00000001
"SchUseStrongCrypto"=dword:00000001
```

When using Microsoft Windows Server 2016 (or higher) and/or Microsoft .NET framework version 4.7.2 or higher

Please check if the following keys and values are present and set accordingly in the Windows Registry:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\.NETFramework\v4.0.30319]
"SystemDefaultTlsVersions"=dword:00000001
"SchUseStrongCrypto"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server]
"DisabledByDefault"=dword:00000000
"Enabled"=dword:00000001
```

4. Installation

This chapter describes the installation of EUCARIS, which starts with the initial base installation of EUCARIS release 7.x, and additional System Updates to get the most recent software version.

Both initial installation and execution of System Updates must be executed by a user with administration privileges and 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 the following url:
<https://www.eucaris.net/download/eucaris-installation-package-v7/>

Valid credentials are needed to download the file and can be obtained by sending an email to eucaris2help@rdw.nl

4.1 Initial installation

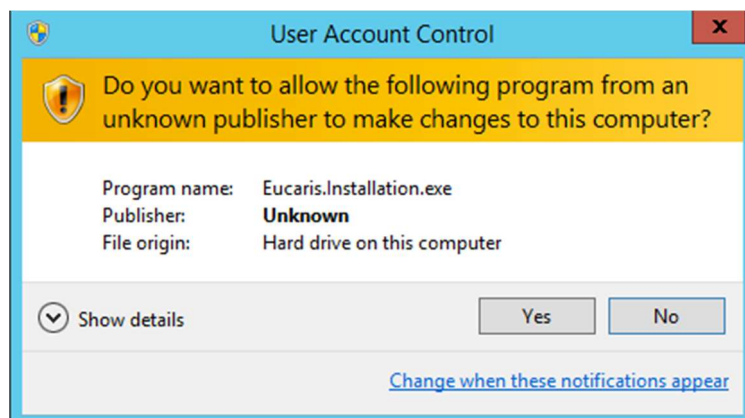
In case an initial installation of EUCARIS is needed the steps below have to be executed:

1. Check prerequisites and install application files
2. Install EUCARIS and Configuration Tool
3. Create or select the EUCARIS database

4.1.1 Prerequisites and application files

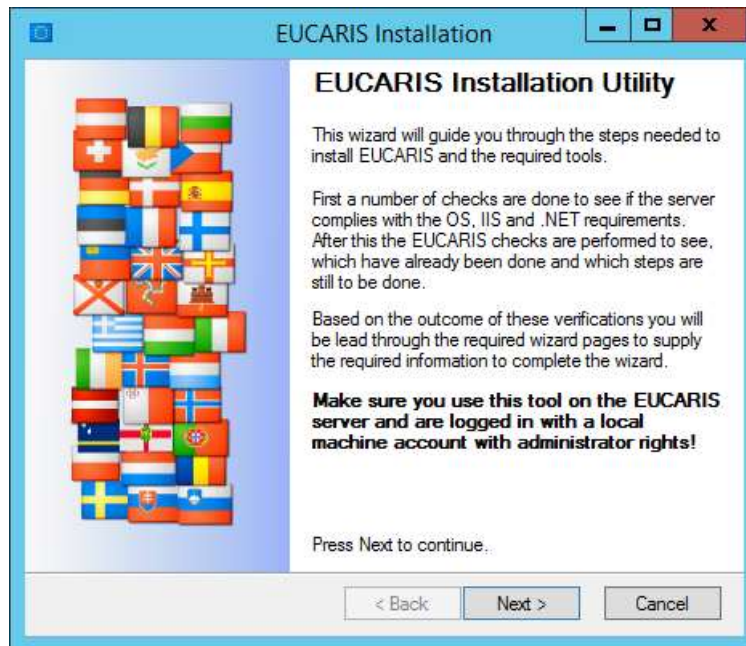
The EUCARIS Installation tool is used to verify compliance with the requirements and to specify and prepare the prerequisites. The EUCARIS Installation tool will also install the required files to the designated locations. The following paragraphs will describe how to use the tool. The latest version 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'



4.1.2 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.

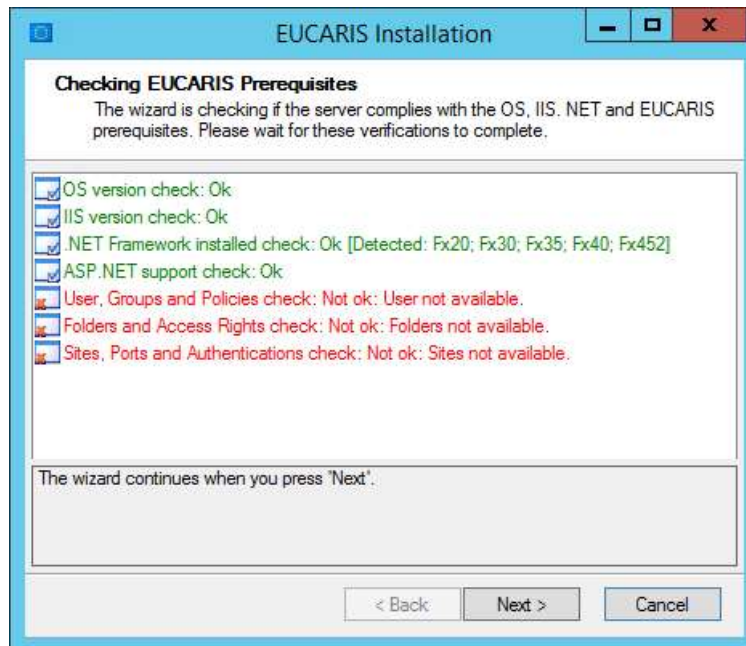


4.1.3 Check prerequisites

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 version 4.7.2 or higher of the .NET Framework is installed
- **ASP.NET support check**
Verifies if ASP.NET Runtime 4.0 is correctly installed and configured for IIS

If any of the above checks fail, the tool can't continue, but if the tool is started on a correctly installed server that never ran EUCARIS software the tool will show the following screen:



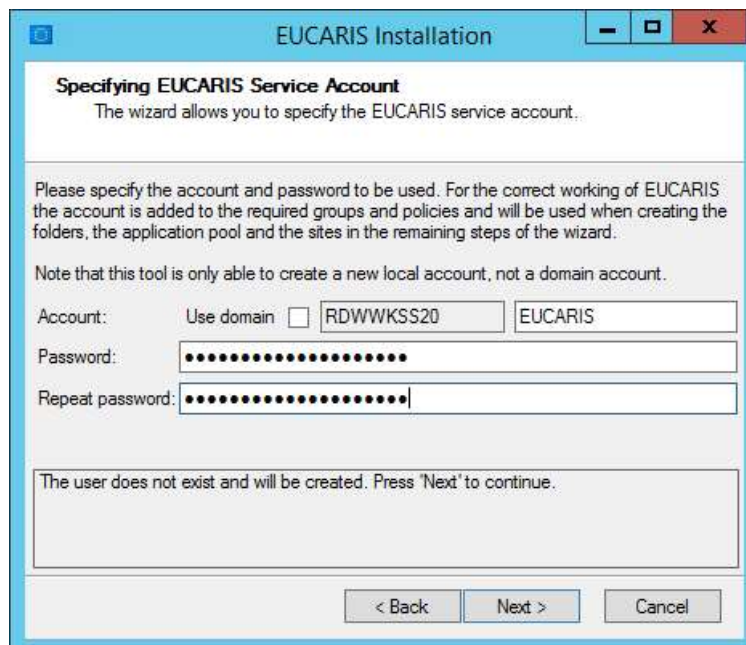
It can be seen above that all software requirements have been met and that the prerequisites have not been met yet, which is to be expected on a new server or installation. The checks indicated in red are the following verifications:

- **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
- **Folders and Access Rights check**
Verifies whether the default proposed EUCARIS folders are available and if the EUCARIS service account has the required access rights
- **Sites, Ports and Authentications check**
Verifies whether the default proposed website names and ports are available and not used

Based on the above outcome, the user can press 'Next' to continue with the next step.

4.1.4 Service account

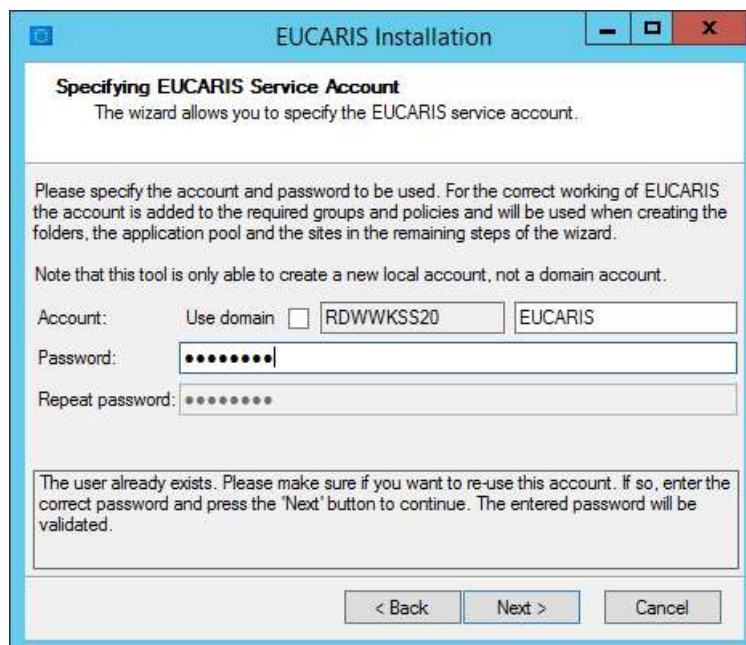
The service account page starts showing the default proposed EUCARIS service account and requires the user to enter the passwords that the user wants to create the service account with. This is shown in the following picture:



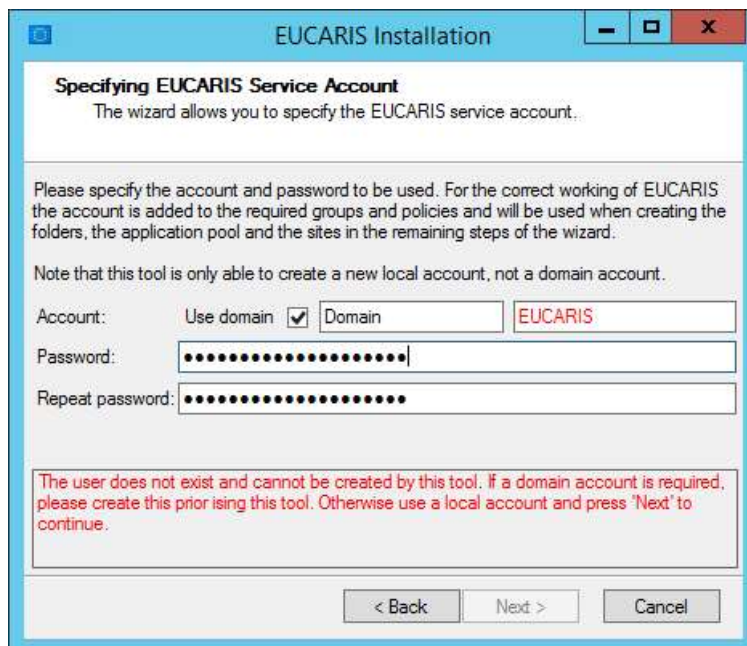
In this scenario, a new local user is created which will serve as service account for all EUCARIS applications.

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 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:

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

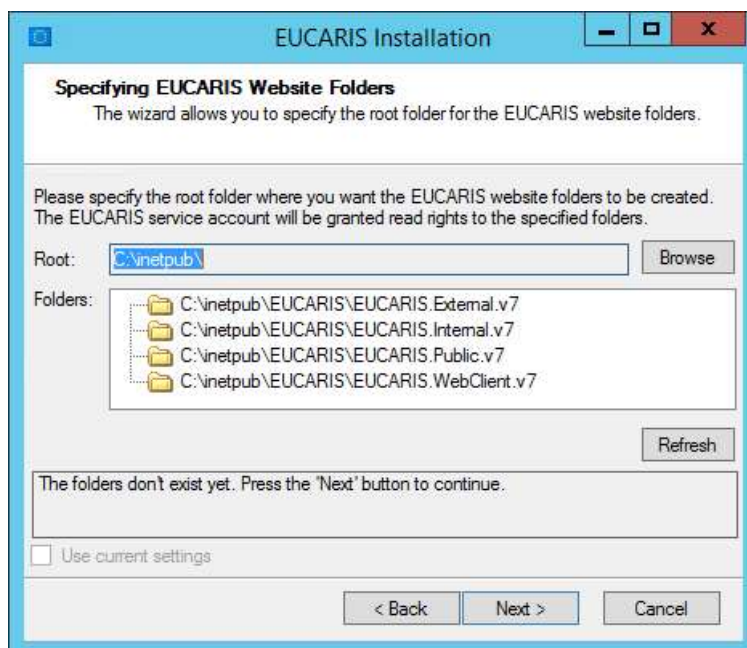
The user will receive the following privileges on the local machine:

<i>Privilege</i>	<i>Description</i>
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

4.1.5 Website Folders

The website folder page shows the default proposed root folder and the related subfolders that will be created. If the user decides to use a different location for the website folders a new root folder can be selected by pressing the 'Browse' button.

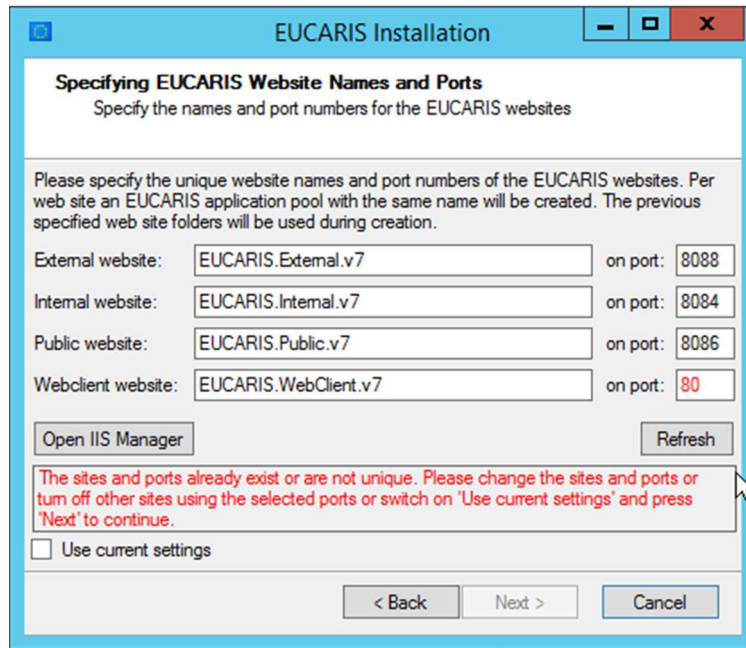


NOTE: The website root folders will not contain the actual application, but serve as root-folder for the websites hosting the EUCARIS application. The actual application files will be installed to the application root folder which can be set later on

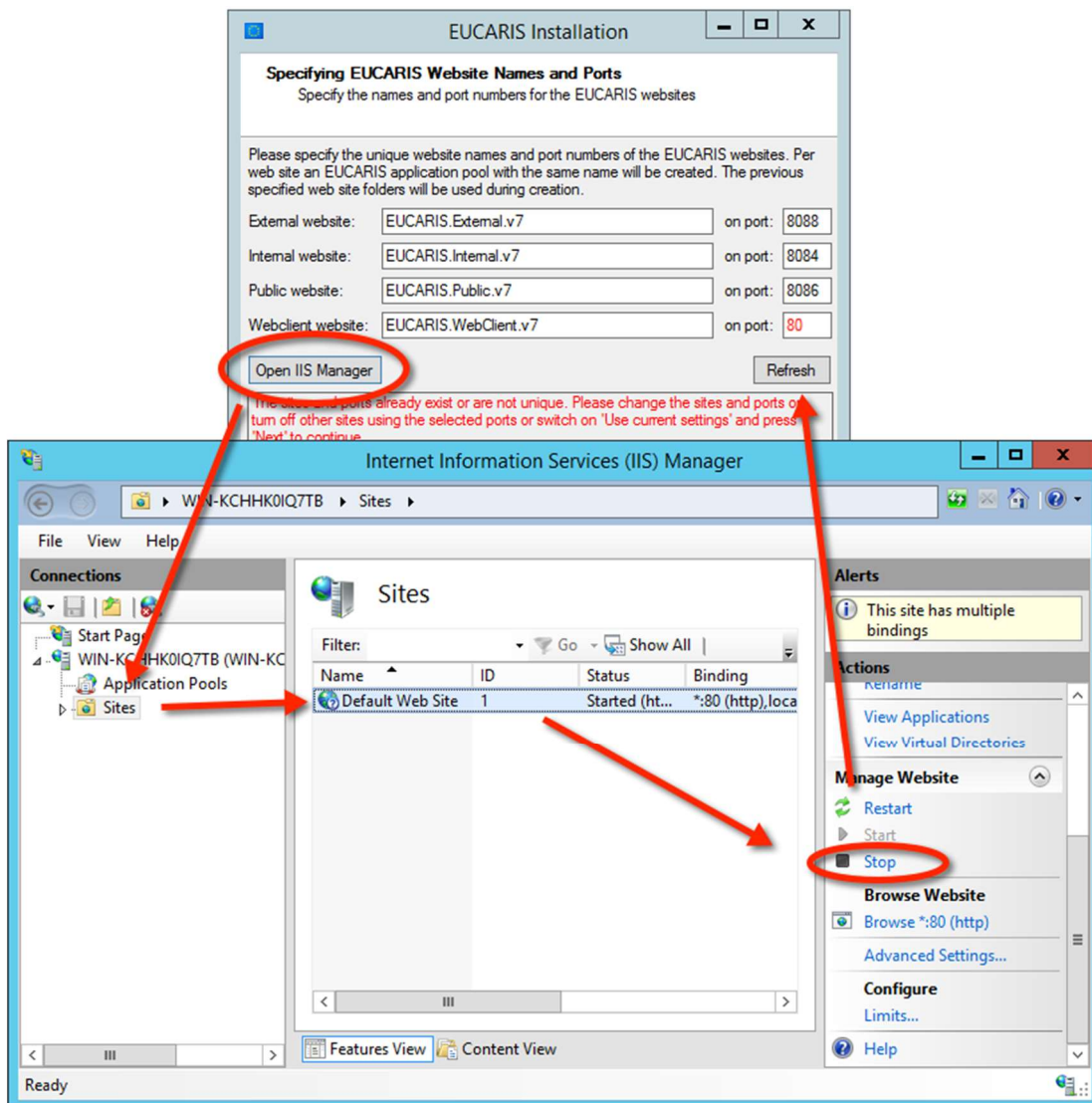
4.1.6 Website Names, Ports and Application Pools

NOTE: Windows Firewall may show a pop-up requesting access for some features of the EUCARIS.Installation.exe application. Select 'Private networks' and click 'Allow Access'

The website names and ports page shows the default proposed names and ports that will be created. If the user decides to use different names or ports this can be entered, but keep in mind that all entered information is required to be unique. In case the chosen values already exist it will be indicated in red, which can be overridden using the 'Use current checkbox' or by selecting different values. On a clean installation it is advised to turn off the 'Default Web Site', because it is configured by default to use port 80.

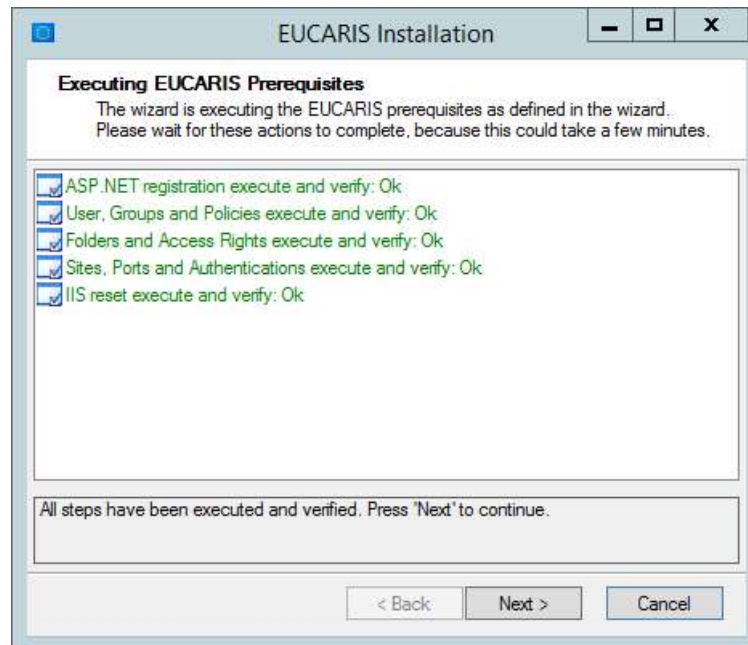


Disable the existing default website:



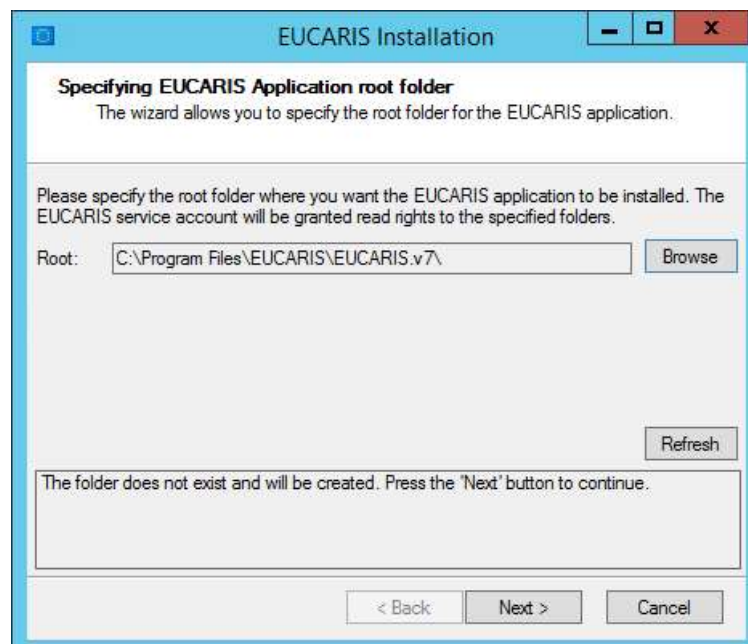
4.1.7 Execute EUCARIS Prerequisites

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.



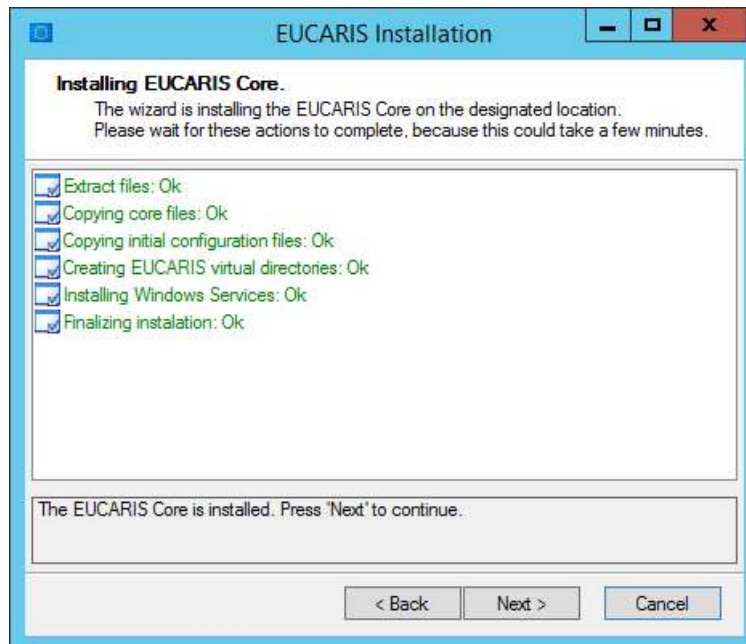
4.1.8 Application Root folder

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.



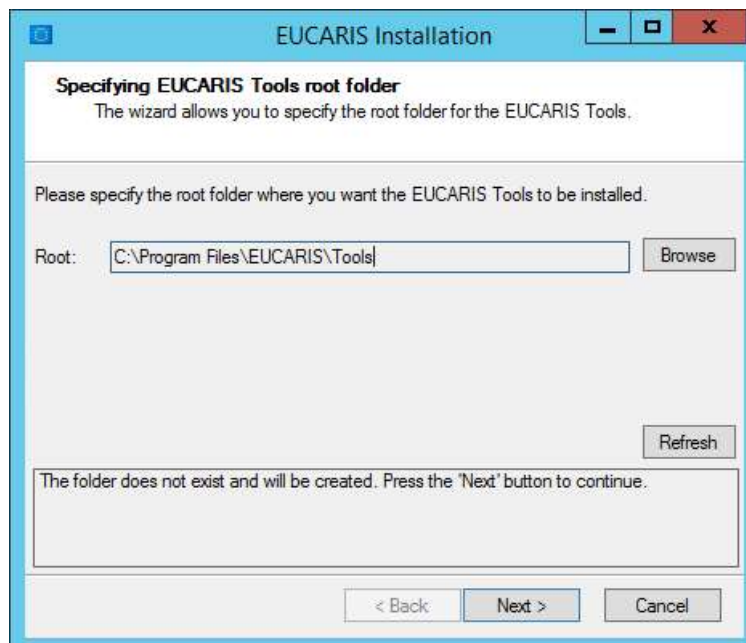
4.1.9 Installing EUCARIS Core

The installation will now copy the required files to the selected location, create virtual directories in IIS and create Windows Service instances on the local machine:



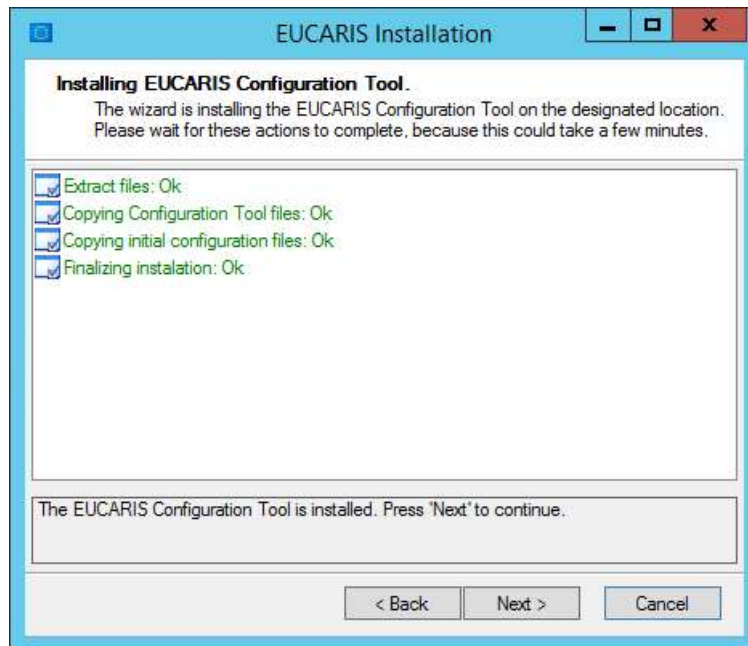
4.1.10 Tools root folder

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:



4.1.11 Installing EUCARIS Configuration Tool

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

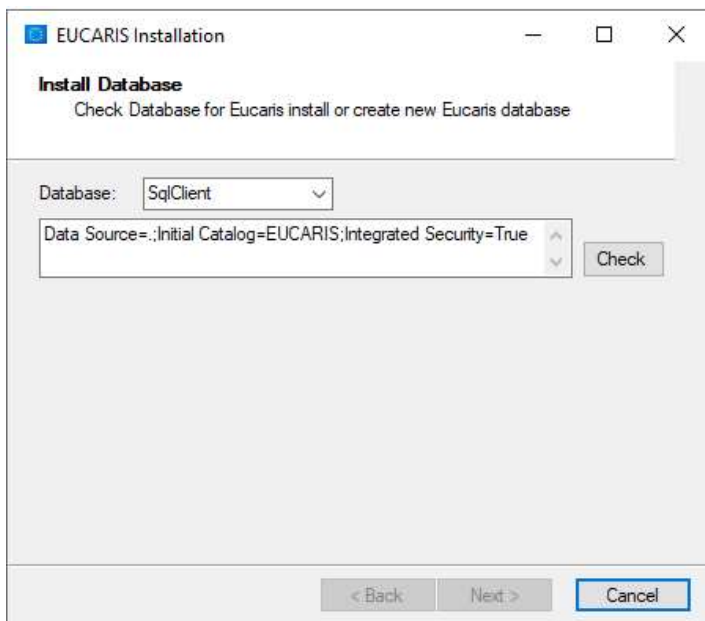


4.1.12 Install or re-use EUCARIS Database

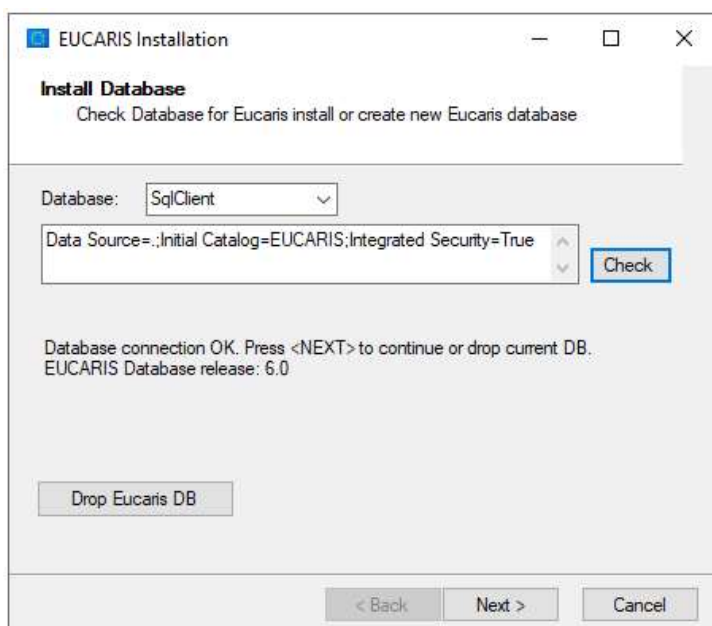
The next step in the installation process is to select a current EUCARIS database or creating a new EUCARIS database. The different scenarios are elaborated below. Please choose the scenario that is applicable in your situation.

4.1.12.1.1 Re-use a current EUCARIS Database

If your EUCARIS database remains the same and this installation is only used for installing EUCARIS on a new application server, it is possible to enter the current connection string in this screen. Depending on the database, a choice can be made between SqlClient and OracleClient. Enter the proper connection string.



After entering the correct connection string, the button “Check” can be clicked to check if a valid connection can be made.



4.1.12.2 Create a new EUCARIS Database (empty EUCARIS Database available)

When it is needed that a database should be created by your database administrator, you follow the next steps. If you have enough rights to create a database, please continue with paragraph 4.1.12.3.

Prerequisite: Please let a database administrator create an empty database with the name EUCARIS before moving on with the install wizard. The database must have the name EUCARIS otherwise the scripts won't work.

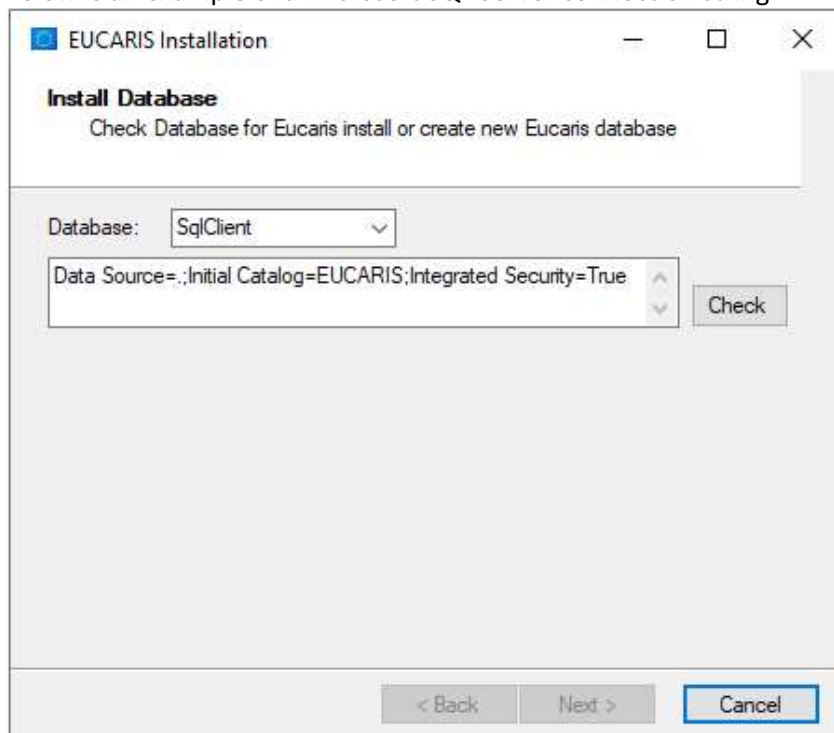
Depending on the database, a choice can be made between SqlClient and OracleClient. Enter the proper connection string.

- **Datasource**
The name given to the connection set up to the database
- **User ID**
Username of the preferred EUCARIS user of the database.
- **Password**
Password of the preferred EUCARIS user of the database.

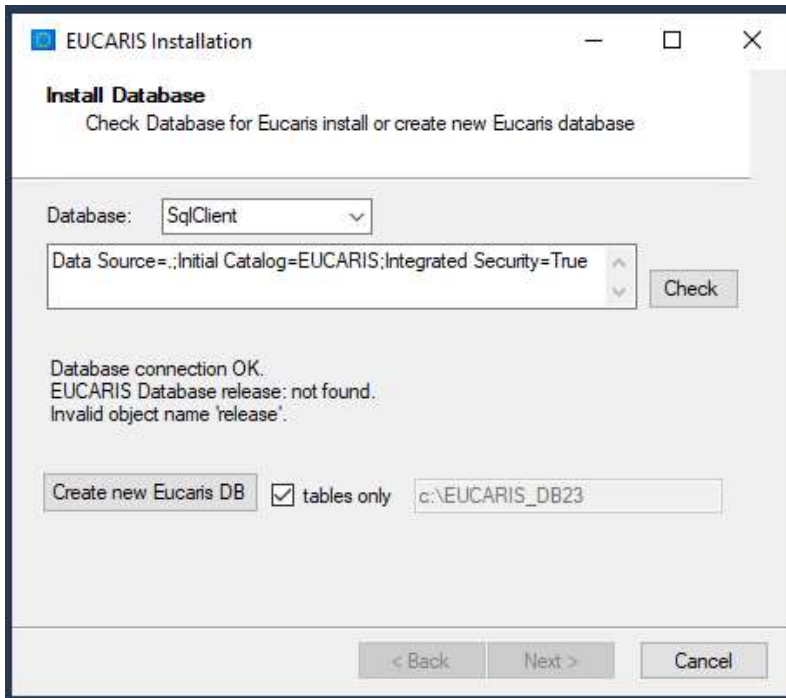
NOTE: When using Windows Integrated Security, please make sure that both the EUCARIS Service account and the local user have appropriate authorisations (minimal: read, write, optional: create & modify for System Updates) on the database

MS SQL

Below is an example of a Microsoft SQL Server connection string

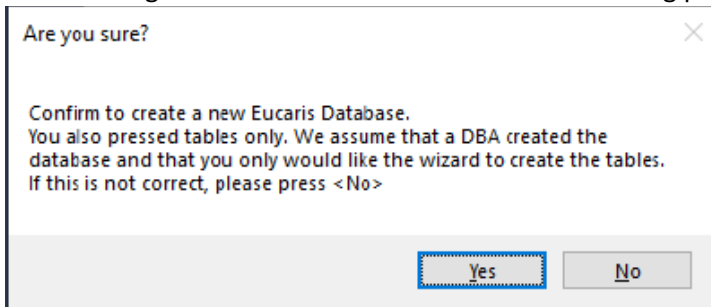


Press 'Check' after entering the connection string, to verify if the connection string is correct.



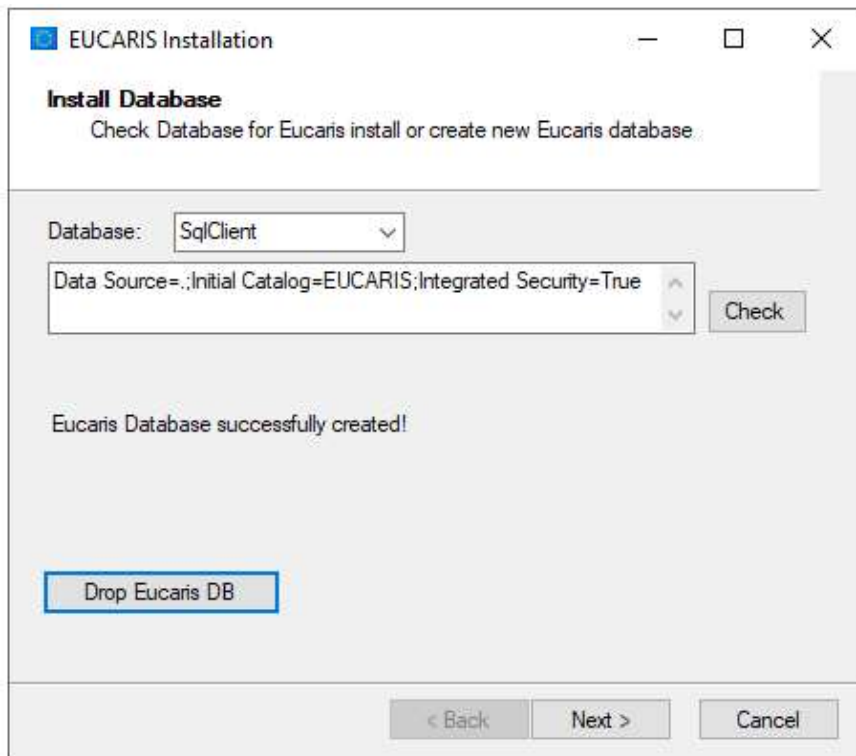
When a database connection is established, and a filled EUCARIS database cannot be found, check the checkbox “tables only”.

After clicking on “Create new EUCARIS DB” the following popup appears:



When you click “Yes” the EUCARIS tables will be created in the EUCARIS database.

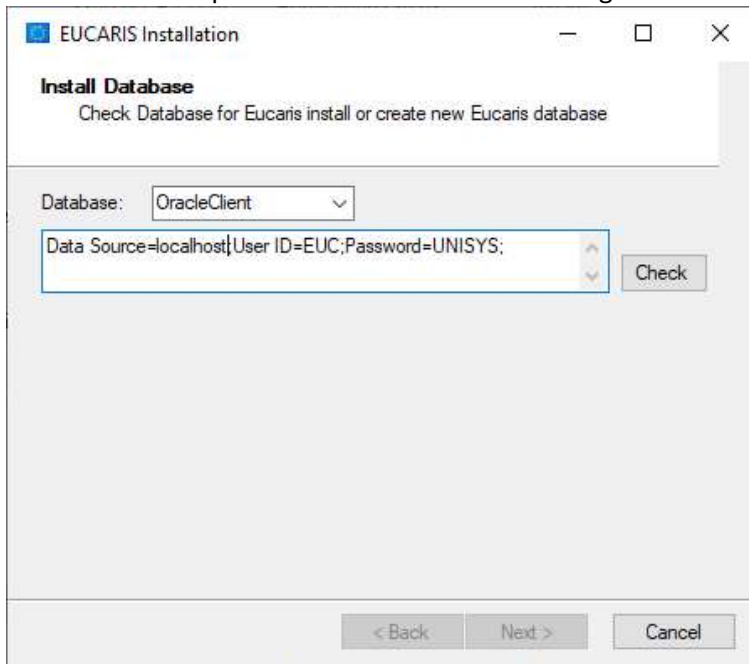
The EUCARIS database will now be created.



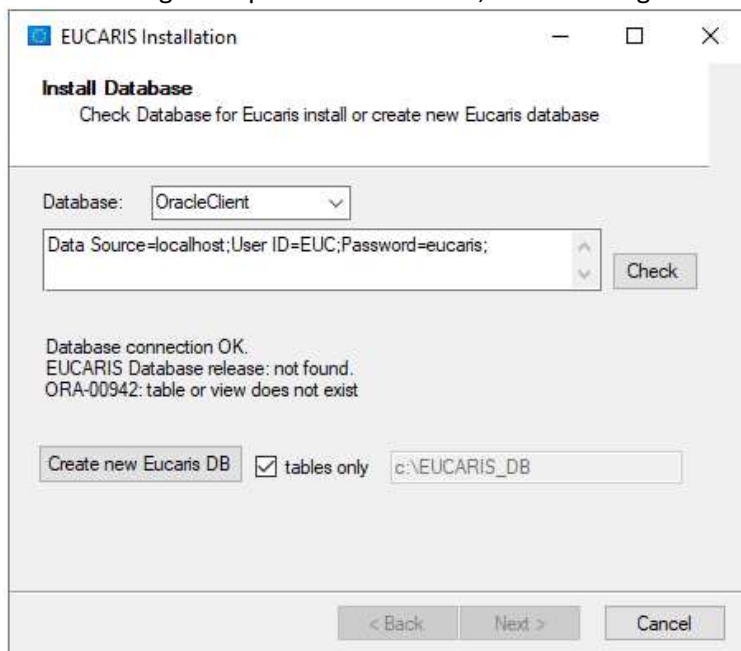
Press 'Next' once the database has been successfully created. The database can also be removed, if an error has been made. Select 'Drop Eucaris DB' to remove the database and repeat the previous steps.

Oracle

Below is an example of an Oracle connection string

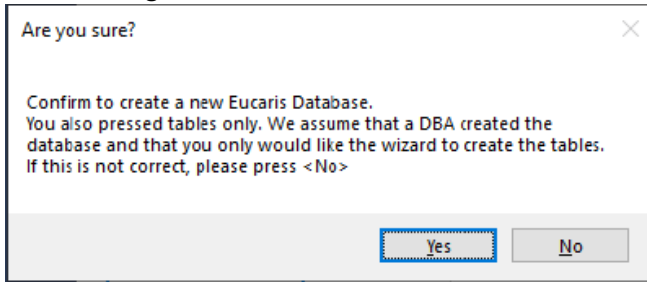


Press 'Check' after entering the connection string, to verify if the connection string is correct. After checking if the password is correct, the following screen will show:

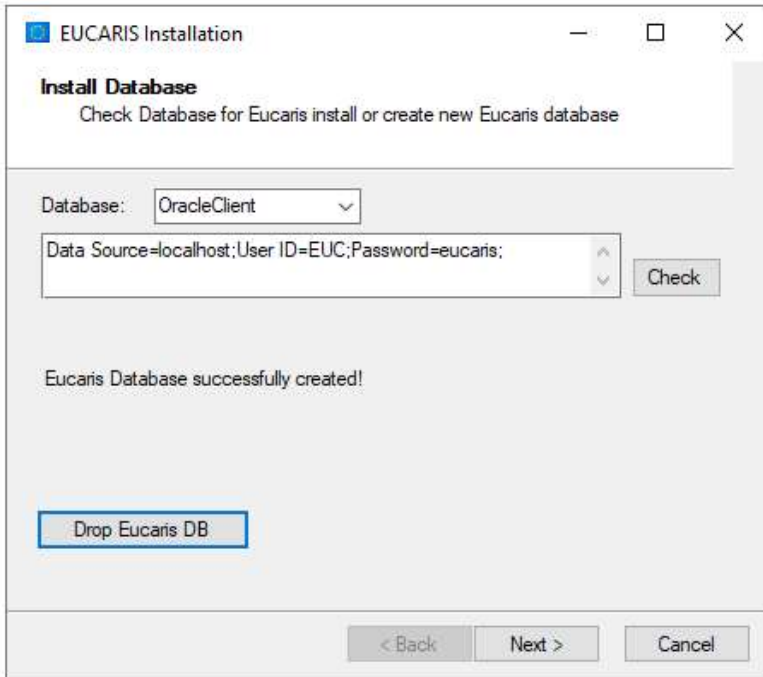


When a database connection is established, and a filled EUCARIS database cannot be found, check the checkbox "tables only".

After clicking on “Create new EUCARIS DB” the following popup appears:



When you click “Yes” the EUCARIS tables will be created in the EUCARIS database.



Press ‘Next’ once the database has been successfully created. The database can also be removed, if an error has been made. Select ‘Drop Eucaris DB’ to remove the database and repeat the previous steps.

4.1.12.3 Create a new EUCARIS Database (EUCARIS Database does not exist)

Please make sure that a database instance has been installed and is running. This can be either Microsoft SQL Server or Oracle.

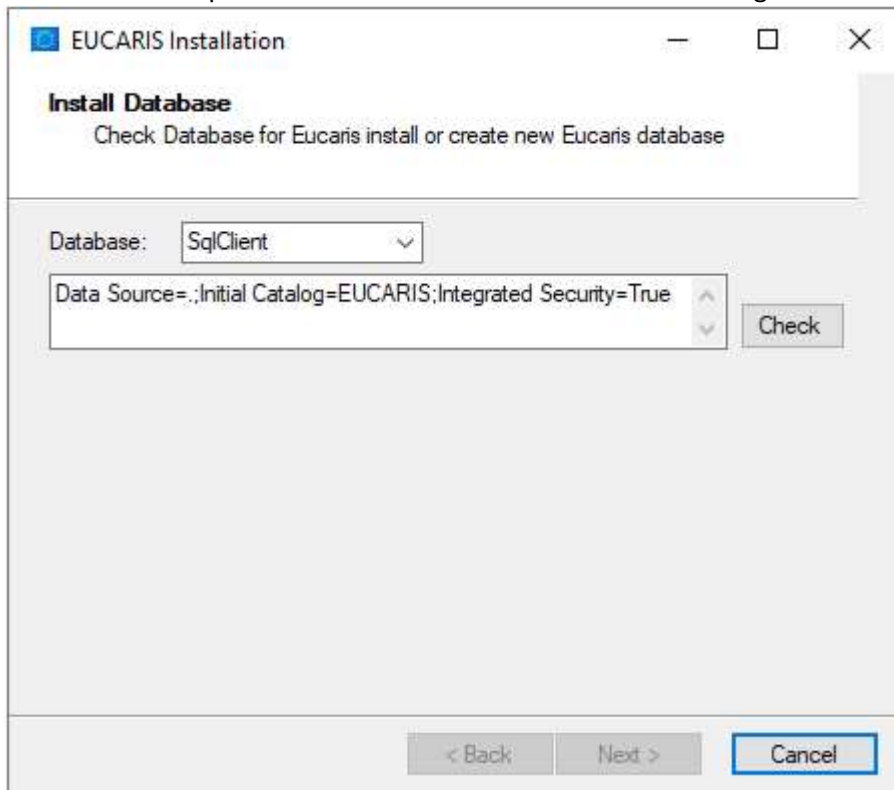
Depending on the database, a choice can be made between SqlClient and OracleClient. Enter the proper connection string.

- **Datasource**
The name given to the connection set up to the database
- **User ID**
Username of the preferred EUCARIS user of the database.
- **Password**
Password of the preferred EUCARIS user of the database.

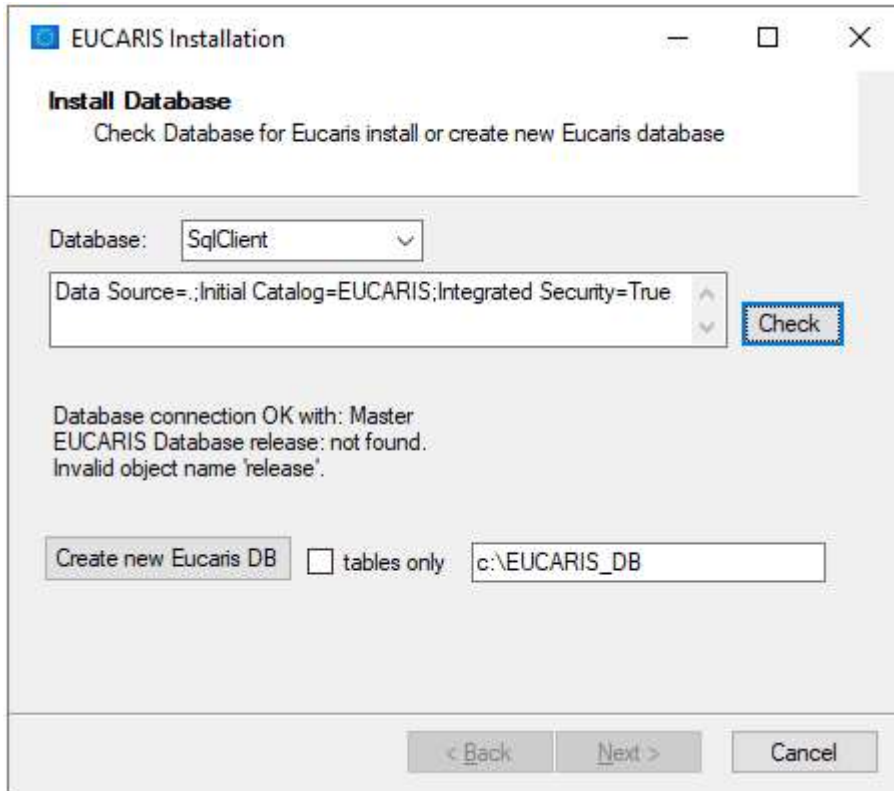
NOTE: When using Windows Integrated Security, please make sure that both the EUCARIS Service account and the local user have appropriate authorisations (minimal: read, write, optional: create & modify for System Updates) on the database

MS SQL

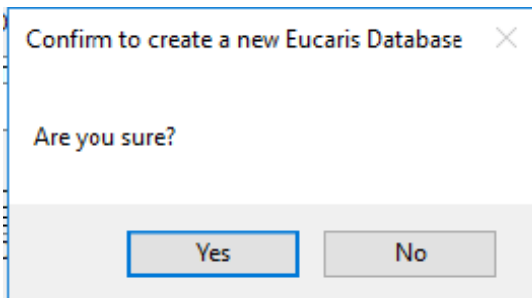
Below is an example of a Microsoft SQL Server connection string



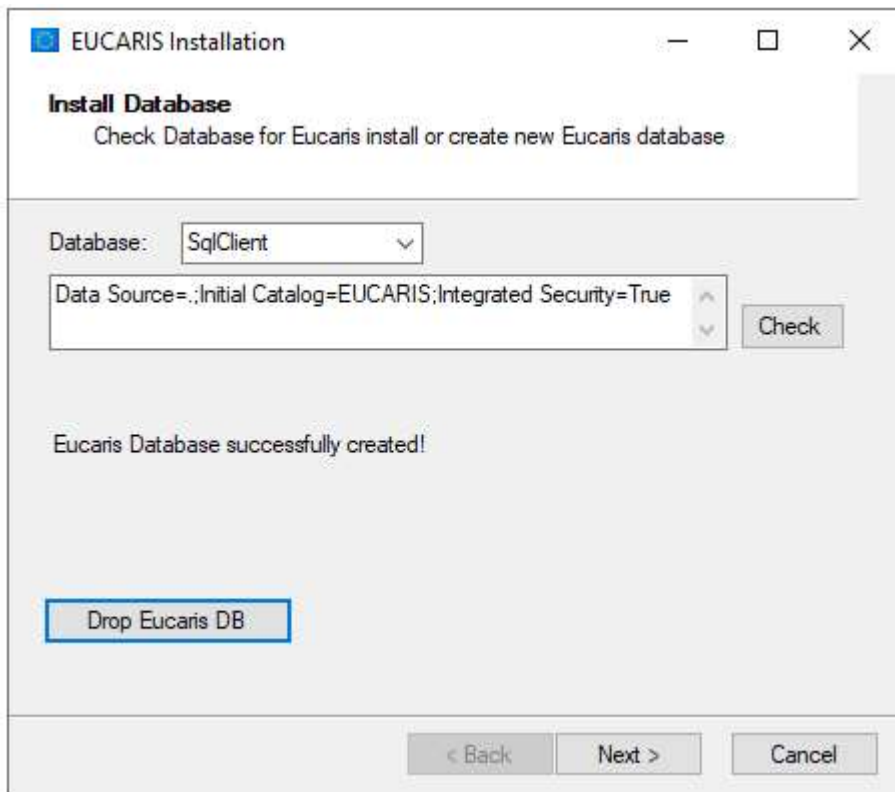
Press 'Check' after entering the connection string, to verify if the connection string is correct.



Please select the location in which the database file is stored. In this case it is c:\EUCARIS_DB. Press 'Create new Eucaris DB' afterwards and confirm with 'Yes' in the pop up.



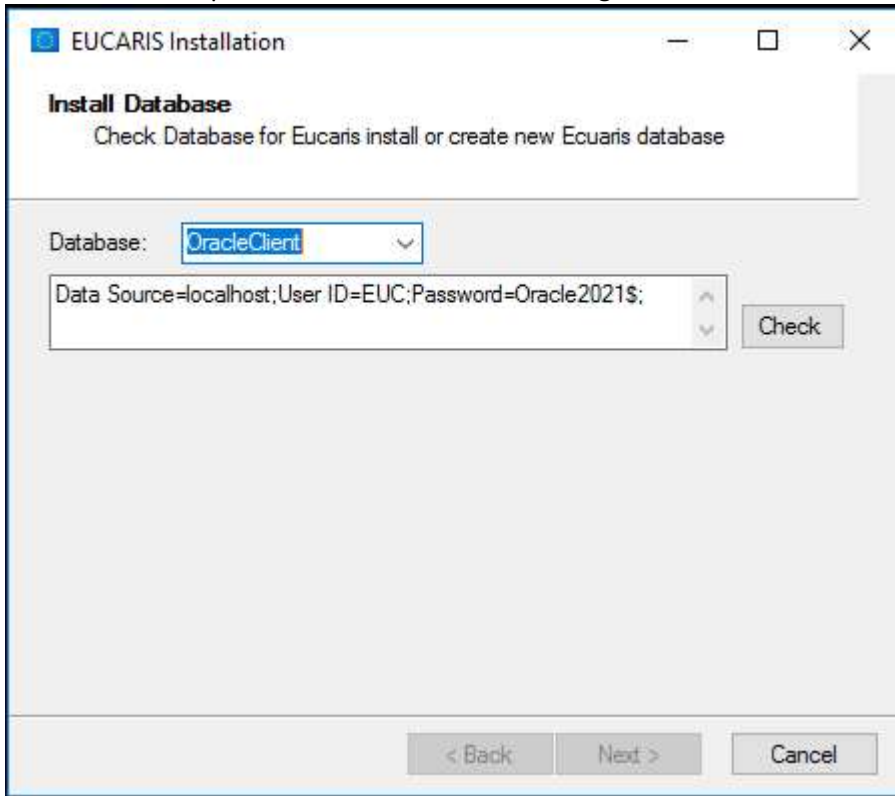
The EUCARIS database will now be created.



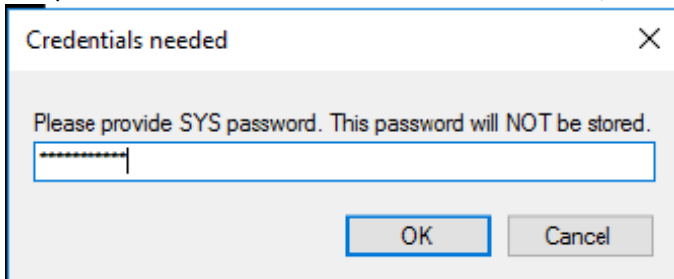
Press 'Next' once the database has been successfully created. The database can also be removed, if an error has been made. Select 'Drop Eucaris DB' to remove the database and repeat the previous steps.

Oracle

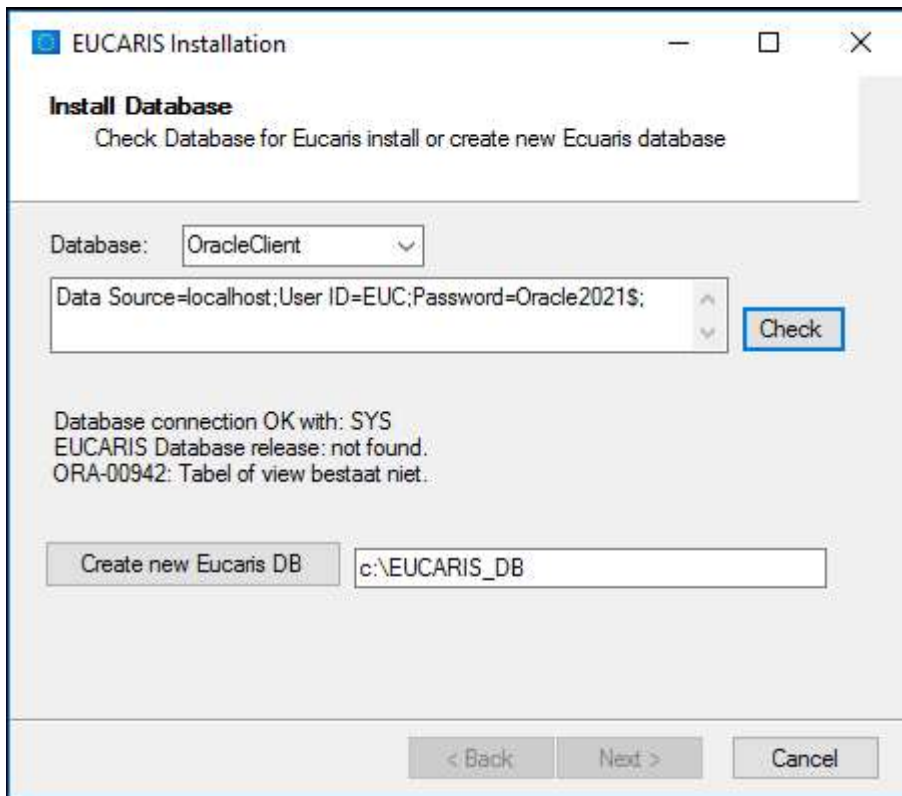
Below is an example of an Oracle connection string



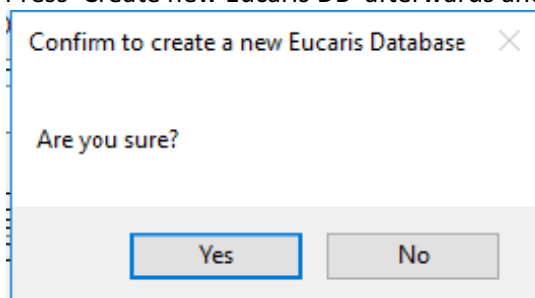
Press 'Check' after entering the connection string, to verify if the connection string is correct. The password of the SYS user needs to be entered, if the User ID is unknown:



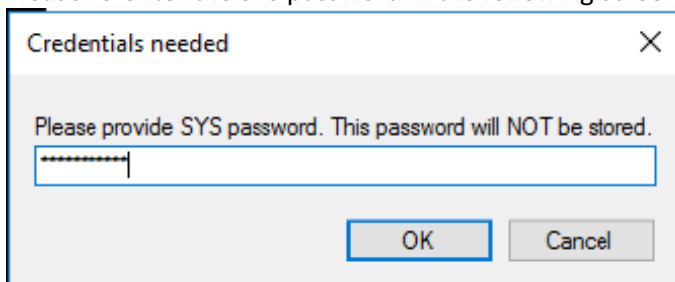
After checking if the password is correct, the following screen will show:



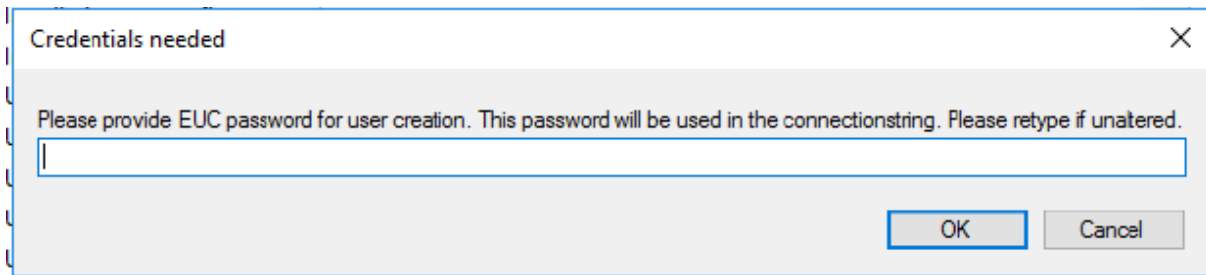
Please select the location in which the database file is stored. In this case it is c:\EUCARIS_DB. Press 'Create new Eucaris DB' afterwards and confirm with 'Yes' in the pop up.



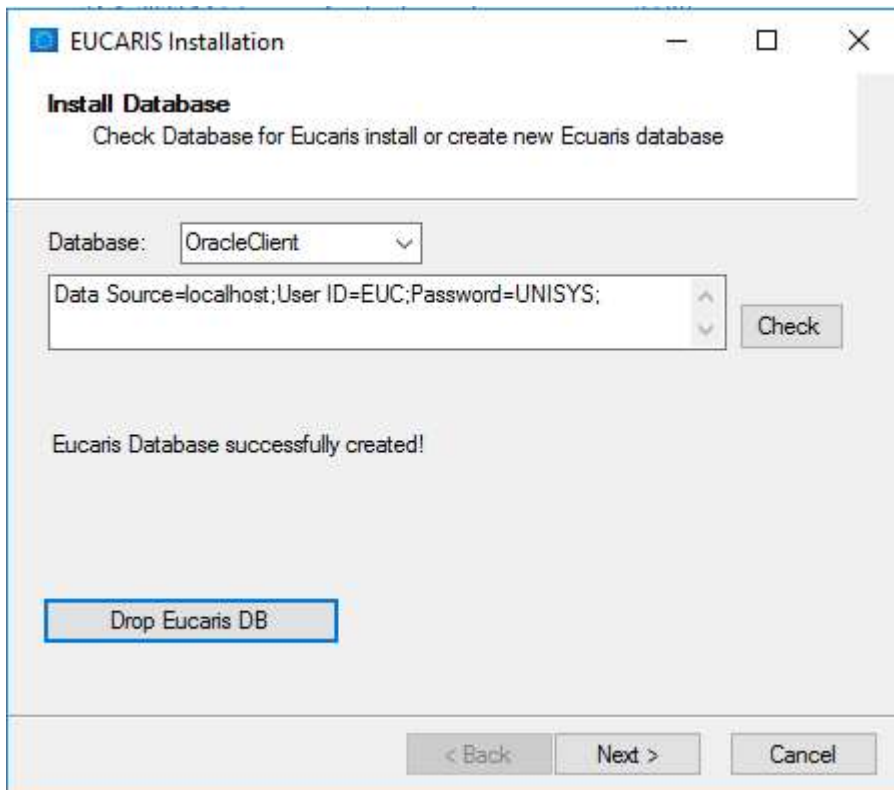
Please re-enter the SYS password in the following screen.



Also, the password of the EUCARIS-user of the database needs to be entered.



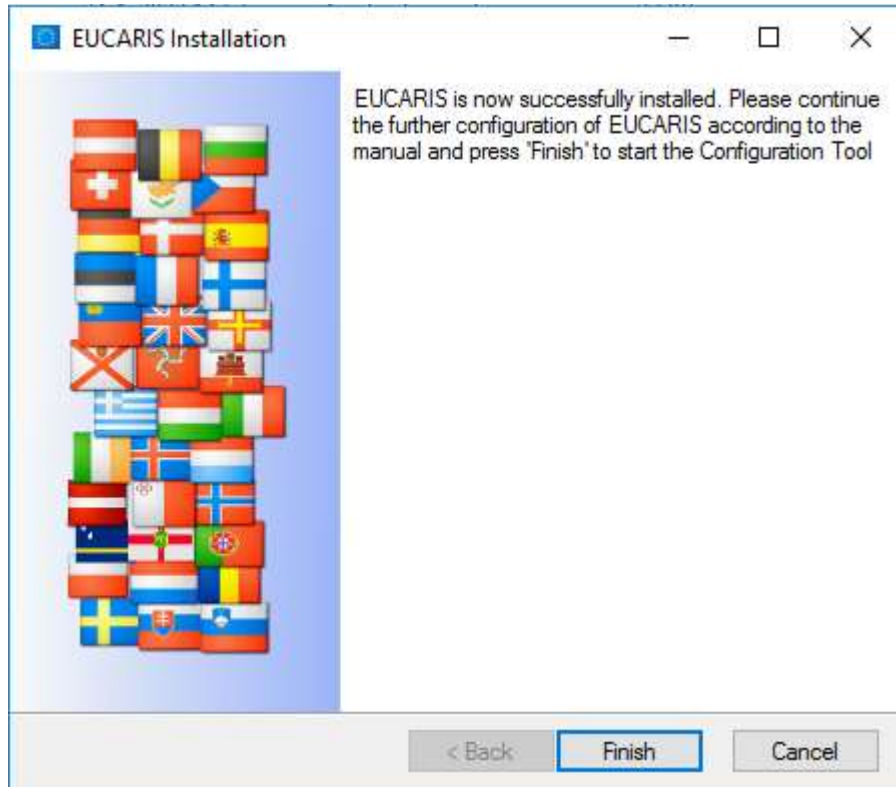
The EUCARIS database will now be created.



Press 'Next' once the database has been successfully created. The database can also be removed, if an error has been made. Select 'Drop Eucaris DB' to remove the database and repeat the previous steps.

4.1.13 Finish

The finish page is the last page of the tool. The required EUCARIS application files are now installed successfully. The last step in installation of EUCARIS is the configuration, which is described in chapter 5. The configuration wizard will start automatically after pressing 'Finish'.



5. Configuration (initial installation)

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

- **Configure a new EUCARIS installation**
Configuring a new EUCARIS installation is supposed to be done by using the Configuration Tool in 'Wizard' mode, which leads the user through the required steps to perform
- **Modify an existing EUCARIS installation**
Modifying an existing EUCARIS installation is supposed to be done by using the Configuration Tool in 'Advanced' mode, which allows the user to perform the steps that need modification
- **Export and import EUCARIS configurations and translations**
Exporting and importing EUCARIS configurations and translations are supposed to be done during a backup, configuring of horizontally scaled EUCARIS servers or transporting translations to other staged environments
- **Perform configuration updates issued by EUCARIS Operations**
The configuration of EUCARIS regarding URLs, IP addresses and authorisations of other member states is distributed in Configuration Updates. The Configuration Tool is able to obtain this Configuration Update at the Update Service hosted by EUCARIS Operations
- **Perform system updates issued by EUCARIS Operations**
Since release 6 EUCARIS is based on a 'pluggable framework architecture'. This means that the functionality of EUCARIS can be easily extended or adapted. The Configuration Tool is able to download and install System Updates issued by EUCARIS Operations

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

5.1 Wizard Mode (initial installation)

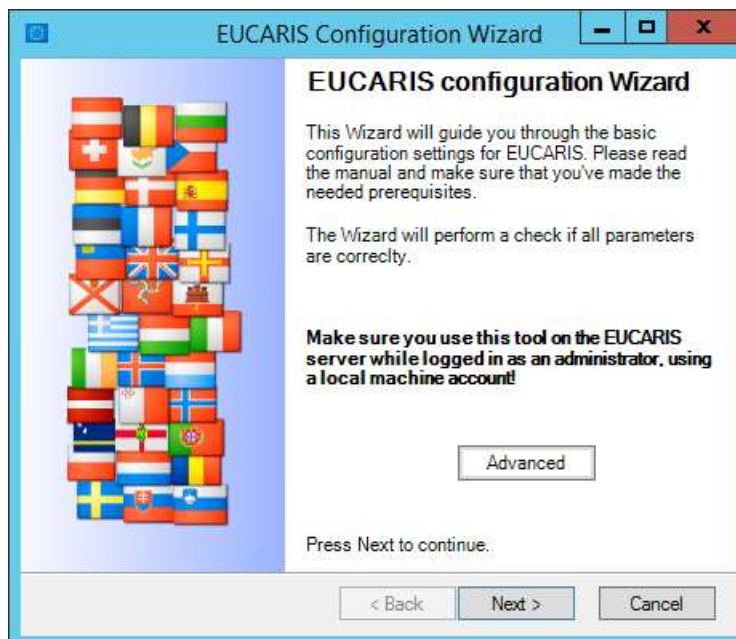
Initial configuration is done using the 'Wizard' mode in which the user is guided through the settings for EUCARIS. In this mode all steps are carried out in the correct order and this mode is used for all standard EUCARIS installations and updates. This paragraph describes the steps required for an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

5.1.1 Welcome

The tool will be started automatically after pressing 'Finish' in step 4.1.2.2.

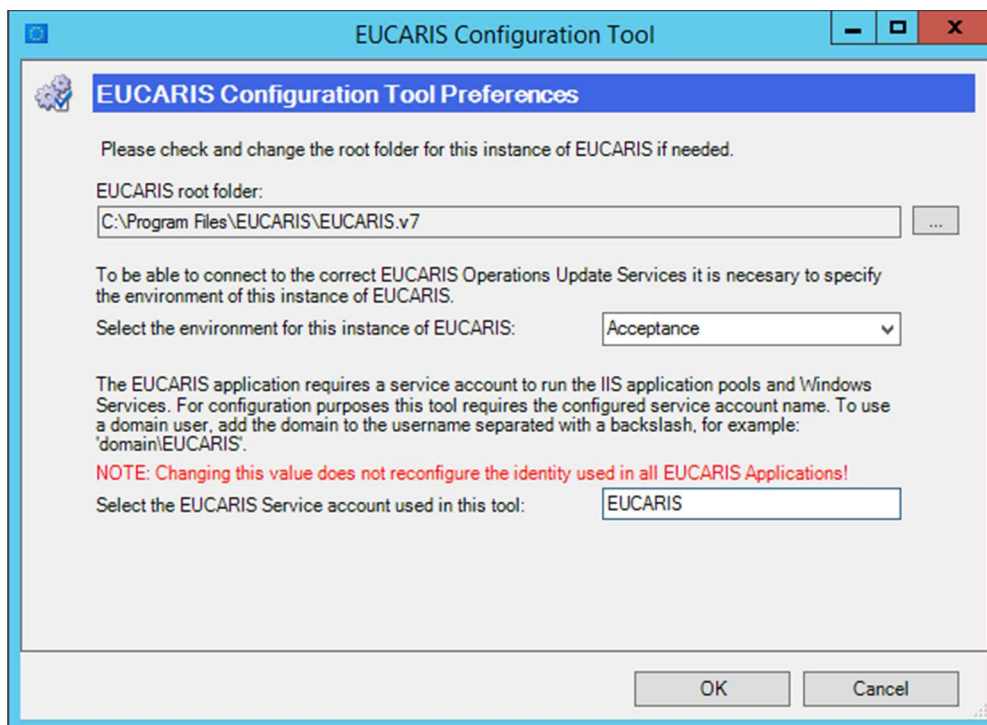
The tool can be started manually by using 'Start' > 'All programs' > 'EUCARIS.v7 Tools' > 'EUCARIS.Configuration Wizard' and wait till the following screen is displayed giving an introduction of the tool. After reading the introduction press 'Next' to continue or press 'Advanced' to directly switch to the 'Advanced' mode. **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'

5.1.2 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 4.1.1 or **Fout! Verwijzingsbron niet gevonden..**



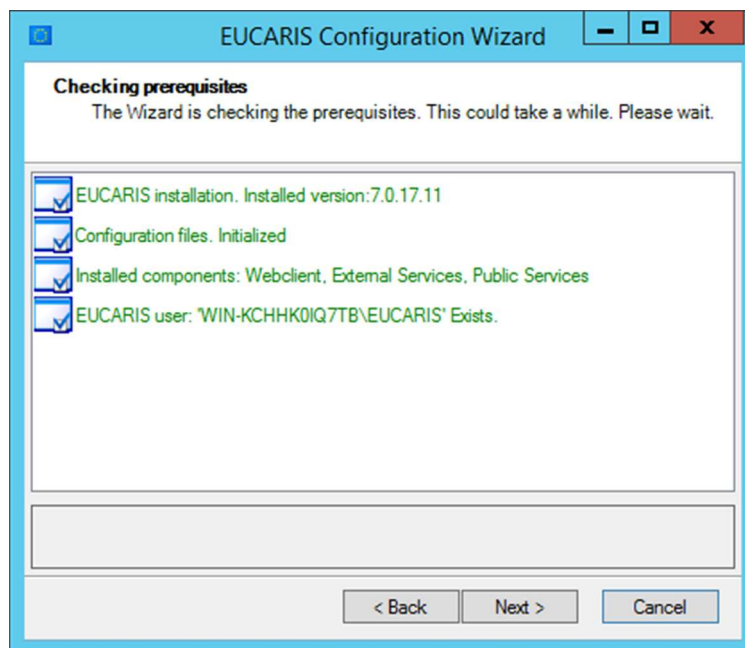
NOTE: Make sure to set the correct environment for this instance of EUCARIS (Acceptance/test or Production). This setting is important for connecting to the correct Update Service hosted by EUCARIS Operations

5.1.3 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
- **EUCARIS components**
The installation status of different parts of EUCARIS are verified
- **EUCARIS user**
The existence of the EUCARIS service account is verified

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.

5.1.4 Local configuration

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

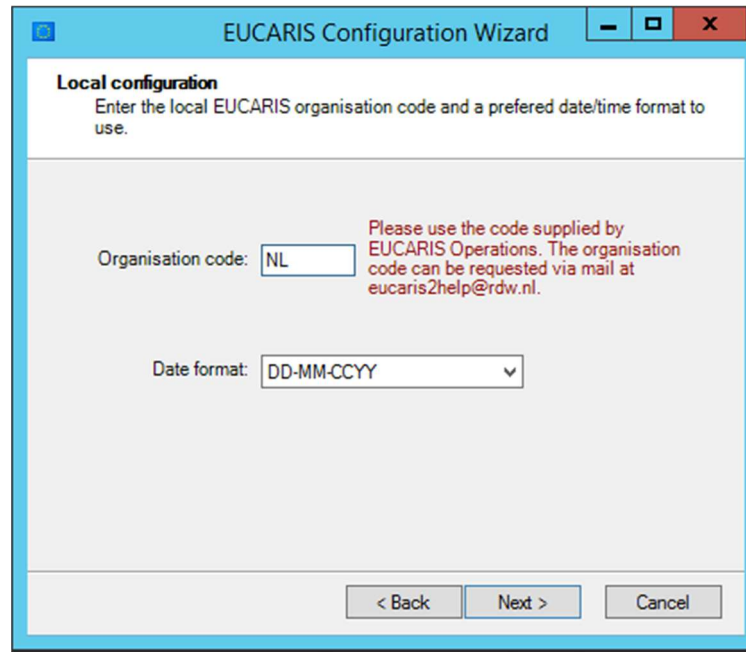
The following parameters can be set:

- **Organisation code**
The organisation code for which to configure EUCARIS

NOTE: Please use the code supplied by EUCARIS Operations. The organisation code can be requested via mail to the installation and implementation Servicedesk at EUCARIS2help@rdw.nl

- **Date format**

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

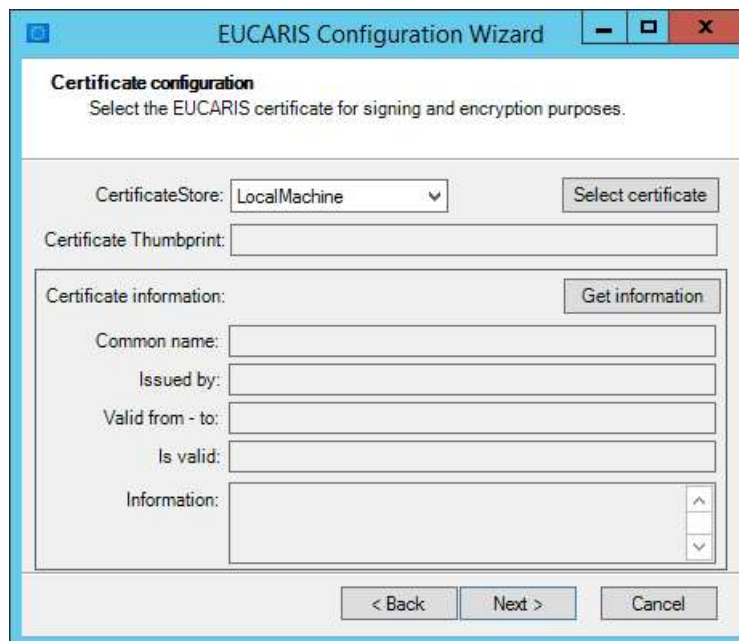


The screenshot shows a window titled "EUCARIS Configuration Wizard" with a "Local configuration" section. The instructions state: "Enter the local EUCARIS organisation code and a preferred date/time format to use." There are two input fields: "Organisation code:" with a text box containing "NL" and "Date format:" with a dropdown menu showing "DD-MM-CCYY". A red note on the right says: "Please use the code supplied by EUCARIS Operations. The organisation code can be requested via mail at eucaris2help@rdw.nl." At the bottom are buttons for "< Back", "Next >", and "Cancel".

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

5.1.5 Certificate configuration (initial installation)

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. Please contact *EUCARIS Operations* if using the 'Local Machine' store is not possible due to restrictions or policies. Press 'Select certificate' in order to configure the correct EUCARIS certificate.

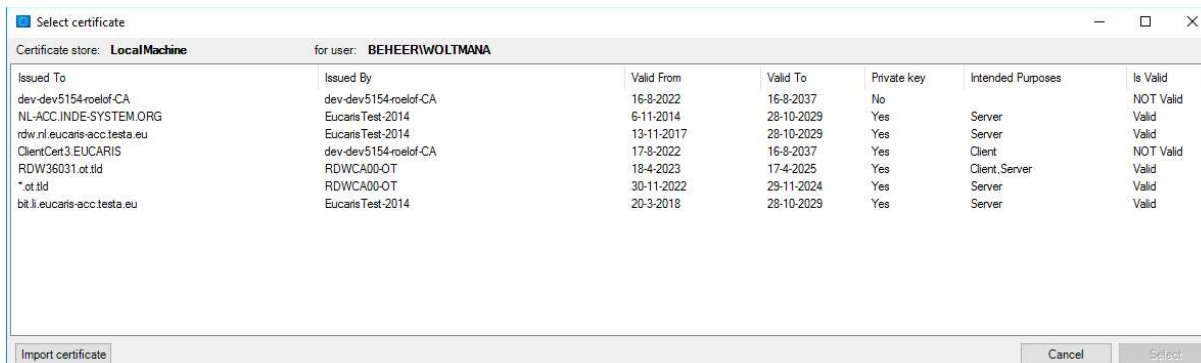
The EUCARIS certificates for both the acceptance as well as the production environment can be obtained by requesting them from the *EUCARIS Operations* at EUCARIS2help@rdw.nl.

NOTE: Since the introduction of the TESTA PKI (early 2018), EUCARIS System Updates are used in the distributing and installation of EUCARIS certificates. Since the end of 2023 certificates no longer derived from via the TeleSec PKI (offered by the EC), new certificates now are derived from the QuoVadis PKI (contracted by EUCARIS Secretariat).

Please review paragraph 5.3.2 System Update for more information on System Updates, and paragraph 10.8, How To: Install a Certificate using System Updates

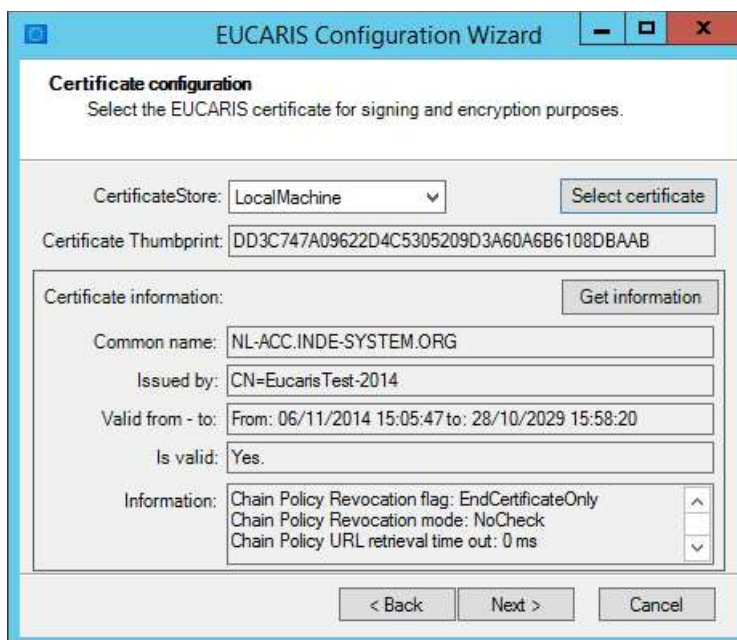
NOTE: Although EUCARIS will accept any X509 certificate with key usages: Digital Signature, Non-Repudiation, Key Encipherment and Data Encipherment, both acceptance and production certificates for use in the EUCARIS infrastructure are supplied by EUCARIS Operations. Please contact EUCARIS2help for more information about the certificate request procedure

NOTE: during the import of an EUCARIS certificate also the certificates of the intermediate- and root Certificate Authorities are imported to ensure a complete trusted chain



If no valid certificate is available, a certificate can be imported applying the correct System Update (please review paragraph 10.8, How To: Install a Certificate using System Updates).

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.

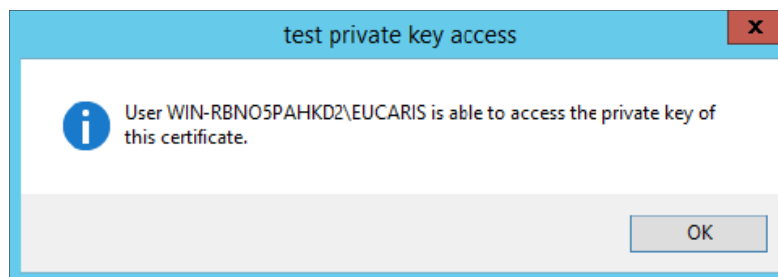
Press 'Get information' to view details of the selected certificate and press 'Next' to continue to the next Certificate Configuration step of the wizard. The EUCARIS Certificate contains a private key, used for signing and encryption. The EUCARIS Service account must have the appropriate authorisation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

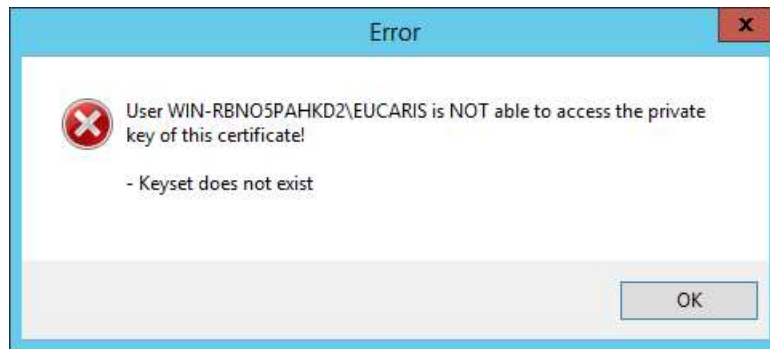


This check can result in one of the next two responses, indicating whether or not the certificate private key is accessible by the EUCARIS service account.

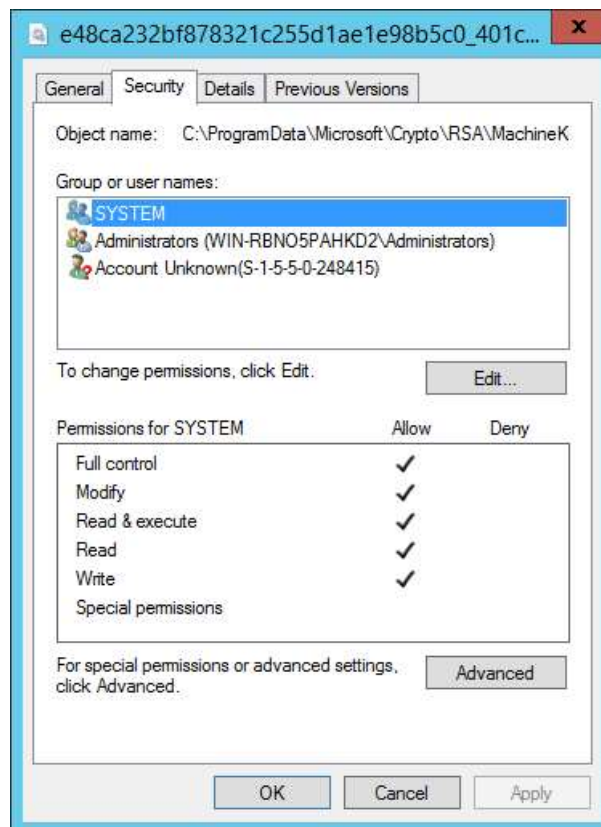


This indicates correct accessibility.

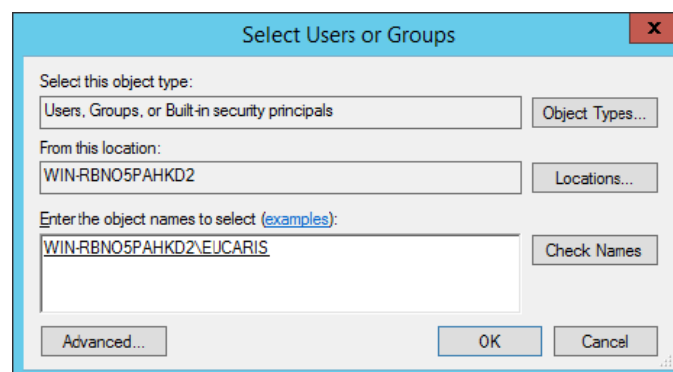
The next Error message displays the situation in which the certificate is not accessible to the EUCARIS service account.



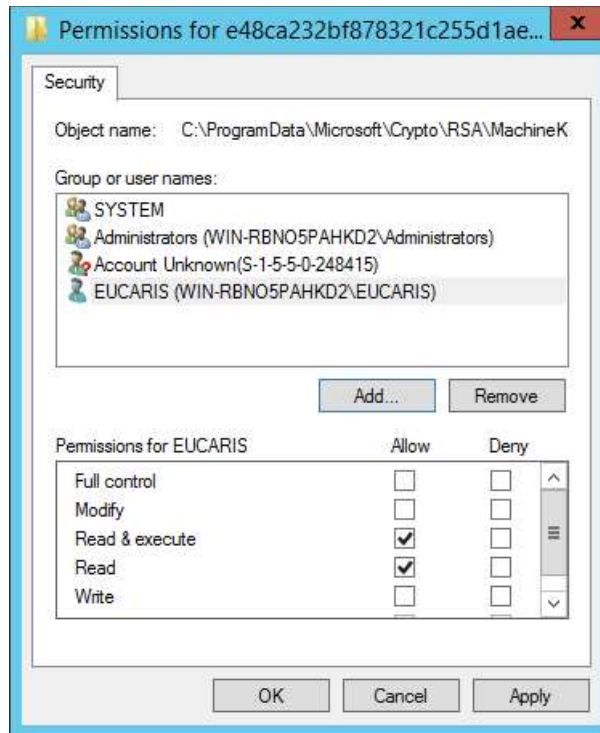
If this Error happens press 'Edit private key file security', which will open a properties dialog and press 'Security' to switch to the security information as shown in the following dialog:



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:

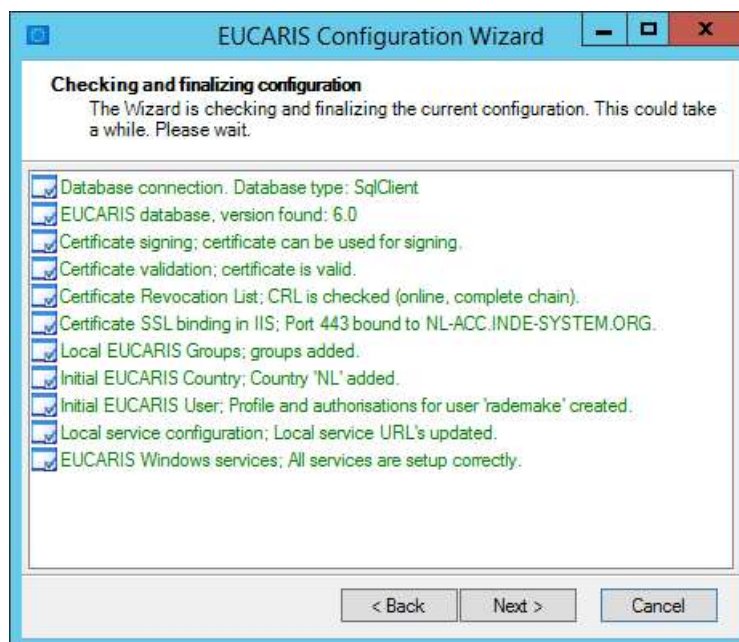


Verify again by using 'Check private key file access' to see if the changes were correct and that the certificate is correctly accessible to the EUCARIS service account.

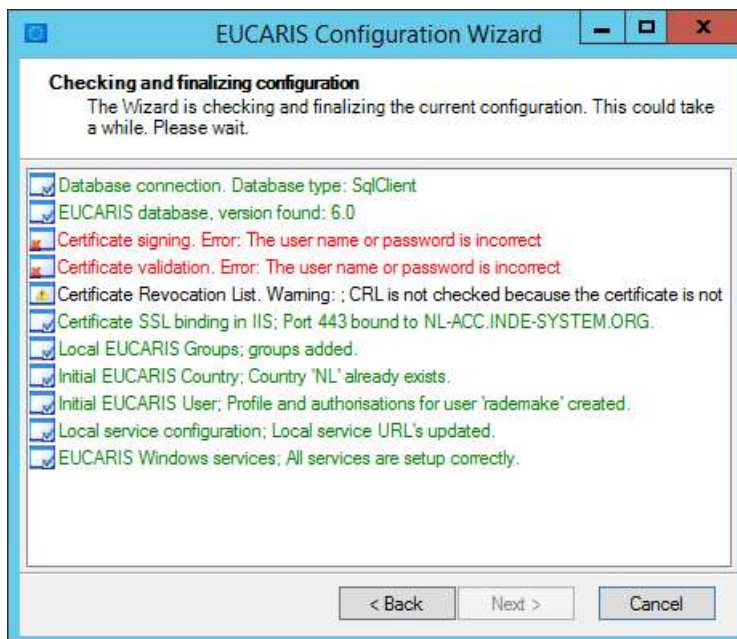
5.1.6 Checking and finalizing configuration

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

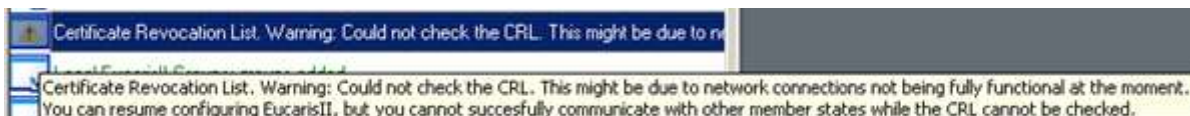
- **EUCARIS Database**
Verifies the database can be connected and if it has the correct version
- **EUCARIS Certificate**
Validates if the chosen certificate is valid. This checks if it can be used for signing EUCARIS messages, if the certificate chain is valid and if the certificate revocation list is valid
- **EUCARIS Groups**
Adds the required EUCARIS groups
- **EUCARIS Country**
Adds the configured member state
- **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
- **EUCARIS Services**
Verifies if the required EUCARIS Windows services are setup correctly



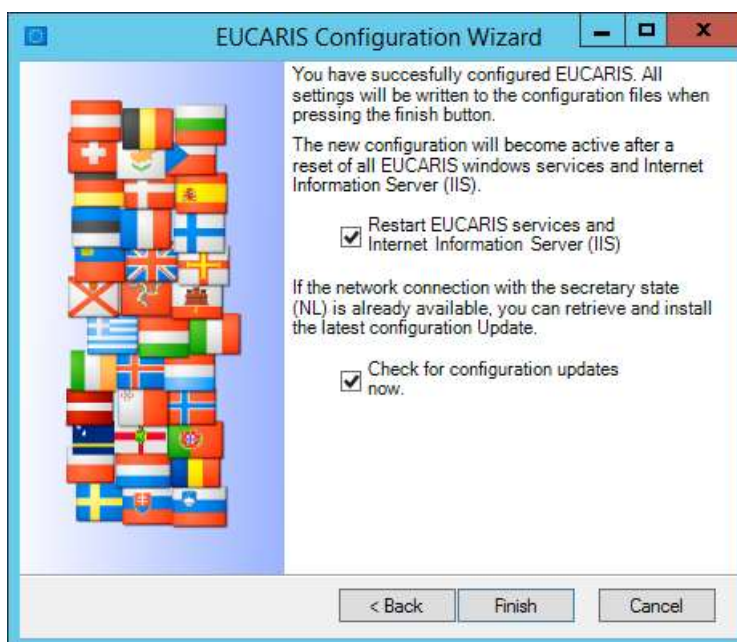
In case of errors it is not possible to proceed and finish the configuration. See below for an example:



If no errors occur the configuration can be finished. A warning might be shown for the Certificate Revocation List (CRL) check, in case no network connection with *EUCARIS Operations* is available yet. Although blocking for the correct functioning of EUCARIS the wizard is allowed to continue. Check paragraph 9.2, Certificates troubleshooting.



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 System Updates now**

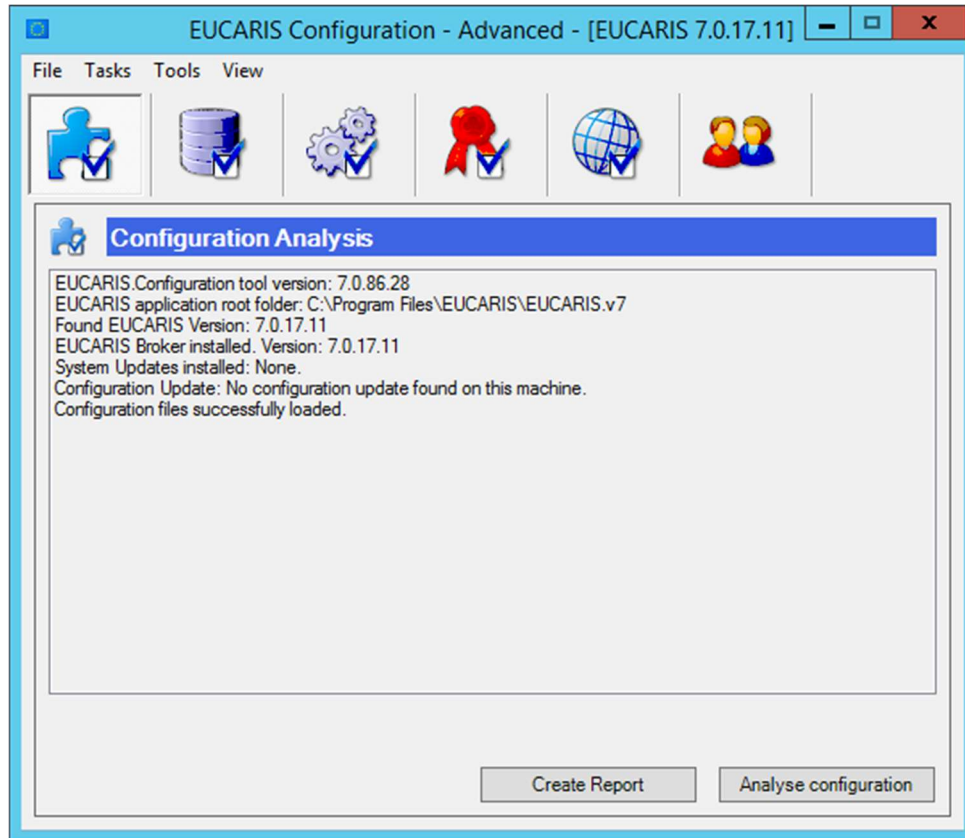
Checks if updates from *EUCARIS Operations* are available by using the EUCARIS Update Service. For details on the EUCARIS Update Service and Configuration- and System Updates, please refer to paragraph 5.3

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 5.3

5.2 Advanced Mode

The Configuration Tool has an advanced mode, allowing the user to verify or modify the settings. The order in which steps are carried out is free and more details are shown compared to the wizard. It also allows to configure and test networks and can be used for a non-standard EUCARIS installation, for troubleshooting the current configuration and for operational management.



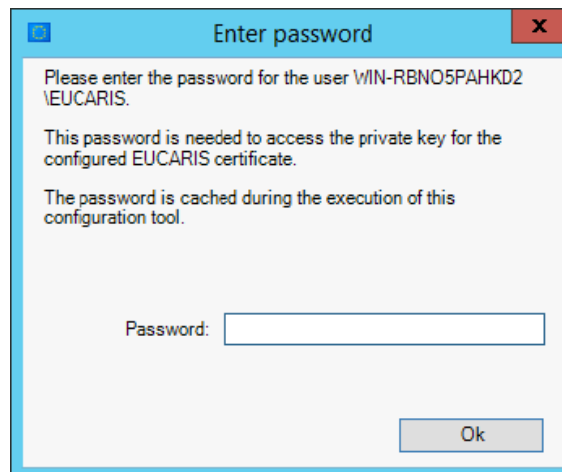
5.2.1 Basic configuration analysis

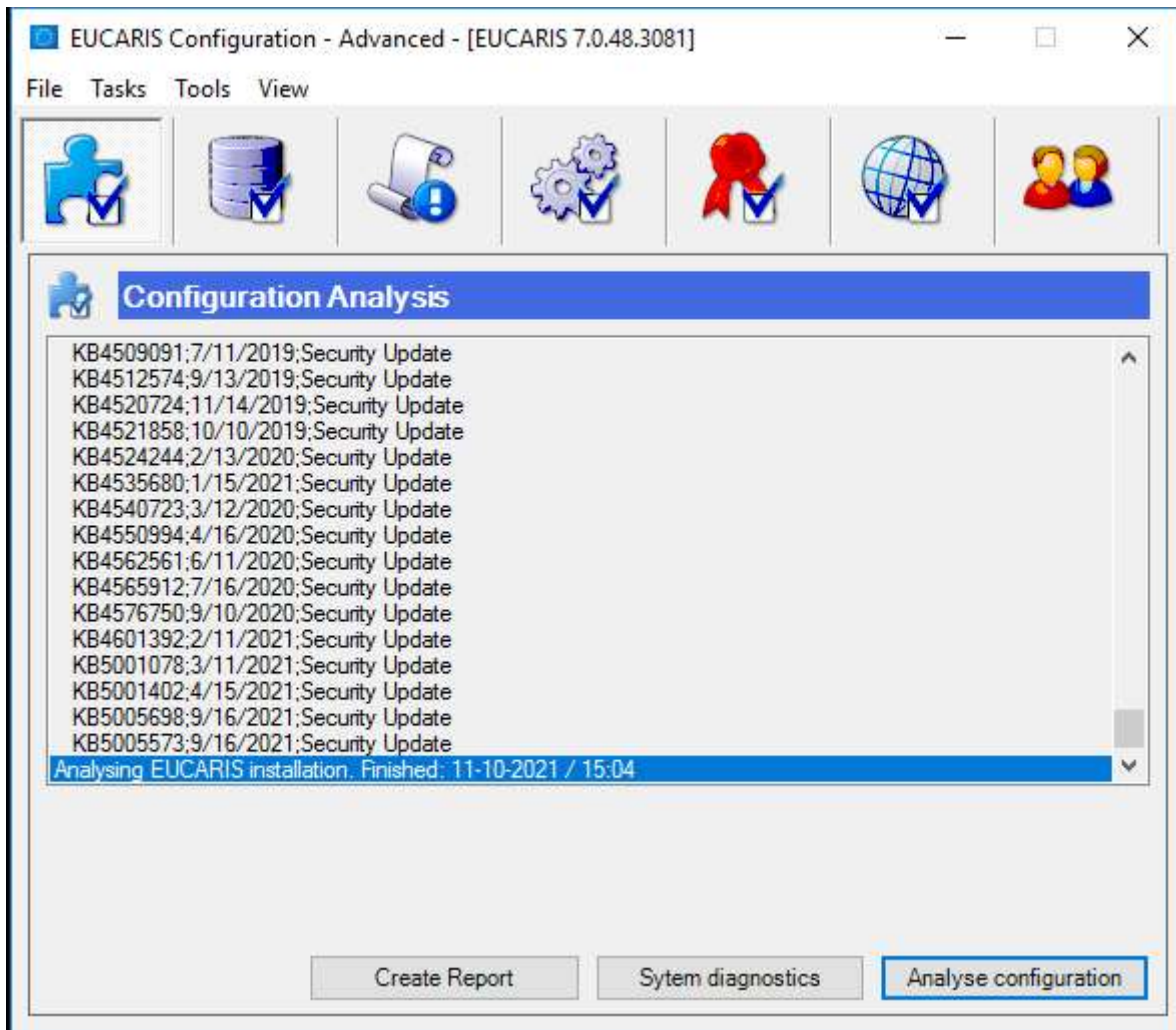
In this screen the following items are checked:

- **Version and root folder**
Determines and checks the current version of EUCARIS, tools and components and displays the application root folder configured
- **EUCARIS System Updates**
Determines and checks the installed System Updates and their versions
- **EUCARIS Configuration update**
Determines and checks the latest Configuration Update version, installation date and status

To analyse the configuration in more detail, press the button 'Analyse configuration'. This analysis might take up to a minute to complete.

NOTE: for some checks and operations the password of the EUCARIS service account is required. In such case the dialog below is shown, stating the reason for the usage of the password. The password is cached in memory during the execution of the EUCARIS Configuration Tool (unless the password is incorrect)





The following additional items are checked:

- **EUCARIS user**
Determines the existence of the EUCARIS service account
- **EUCARIS database**
Determines the existence, connection and version of the EUCARIS database
- **EUCARIS certificate**
Determines if the certificate is valid for use with EUCARIS
- **EUCARIS websites**
Determines if the websites can be accessed
- **EUCARIS services**
Determines if the EUCARIS services are setup correctly

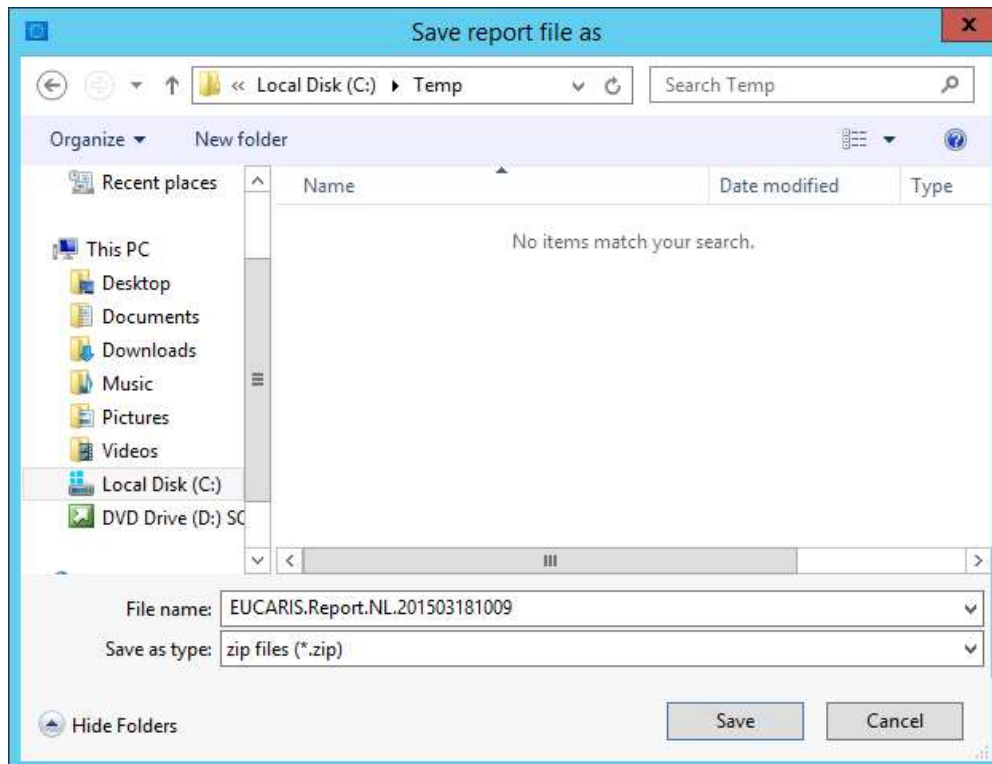
5.2.2 Create Analysis Report

For advanced troubleshooting and analysis it is possible to create an even more detailed report of the EUCARIS system, installation and configuration by pressing the 'Create Report'.

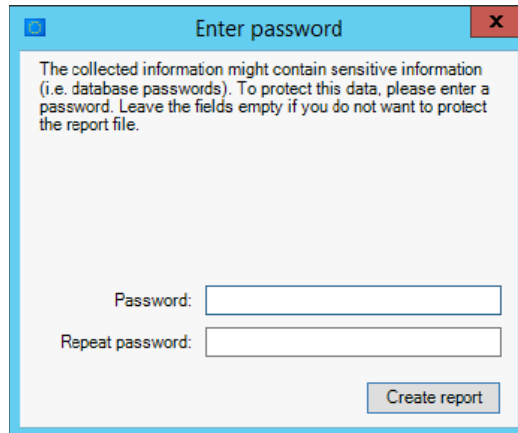
The analysis involves an analysis of the network configuration. If no network parameters are available, the user will be notified and if this analysis needs to be included these network parameters need to be provided (for details see 5.2.7). The user can choose to skip the network analysis.



The report and all applicable files will be collected and added into a zipped archive. Select a folder for this archive. The EUCARIS Configuration Tool suggest a filename, containing the configured EUCARIS Country Code and timestamp of the analysis. It is advised not to change this suggested filename.



This report can optionally be secured with a password since it might contain sensitive system data from e.g. a production environment. Leave the password fields empty if the report does not have to be protected.



The following items are collected when the 'Create Report' is pressed:

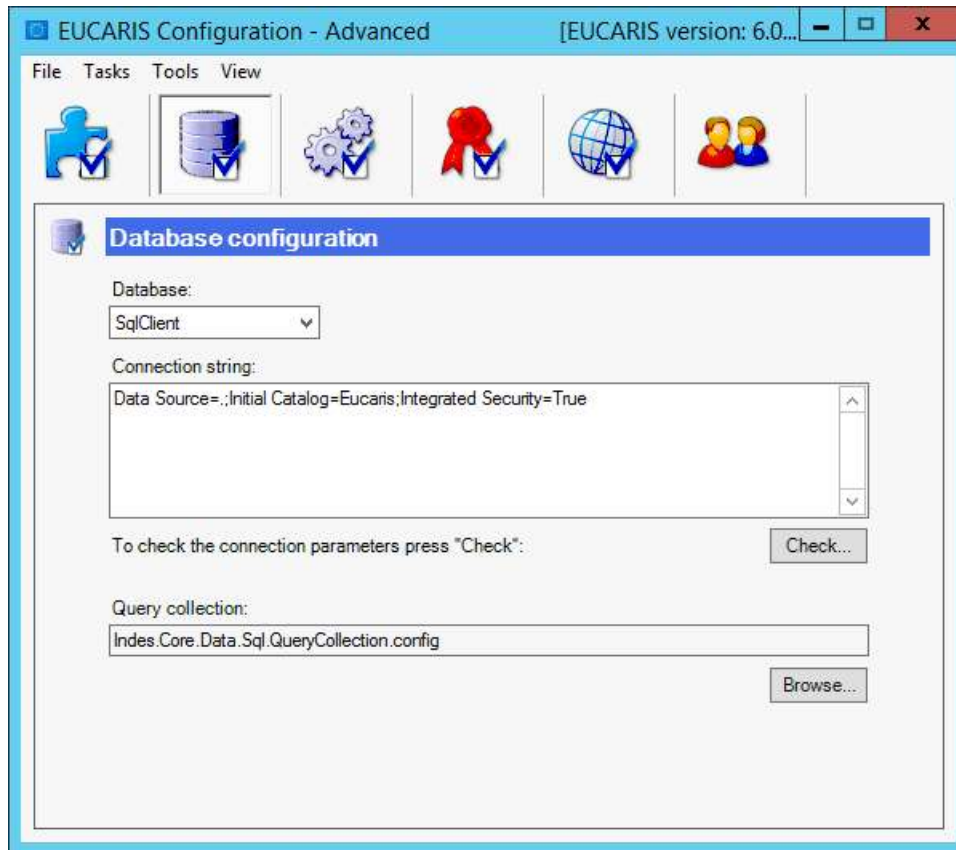
- **Configuration analysis report**
The output of the configuration analysis
- **Hosts file**
The hosts file of the current server
- **Configuration files**
The configuration files of EUCARIS and installed components
- **.NET assembly versions**
The versions of the EUCARIS .NET assemblies
- **Application log**
The application log entries of the last 24 hours
- **System log**
The system log entries of the last 24 hours
- **Network analysis report**
The output of the network analysis report (if performed)
- **Service configuration**
The configuration of the EUCARIS services
- **Logging configuration**
The configuration of the logging of EUCARIS

5.2.3 Database configuration

In this screen the user can configure the database to use for EUCARIS. Either a Microsoft SQL Server or an Oracle database can be chosen. Furthermore the connection can be modified and the specified connection can be verified.

The EUCARIS application uses fairly basic SQL queries for its operations, and require no specific DBMS features or stored procedures. The required SQL queries are stored in "query collections".

And although the query collections can be selected by using the 'Browse' button it is strongly advised not to modify this value nor the contents of the query collections.



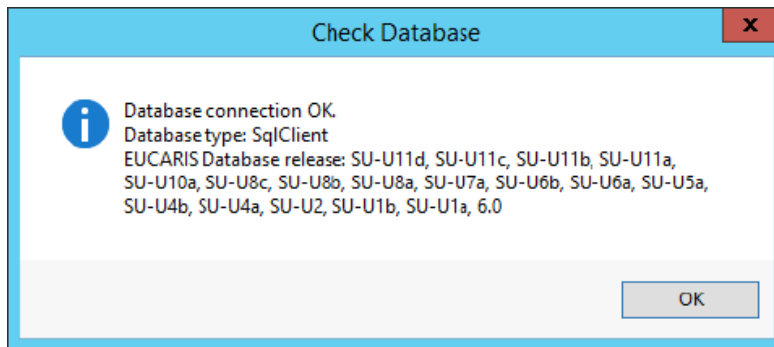
The configured connection string will be used for the following operations:

1. Default operations performed by the EUCARIS application (services and web client), requiring SELECT, INSERT and UPDATE permissions on the EUCARIS database,
2. Configuration Updates performed by the Configuration Tool during the execution of a Configuration Update, requiring SELECT, INSERT and UPDATE permissions,
3. System Update operations performed by the Configuration Tool during the execution of System Updates, requiring SELECT, INSERT, UPDATE, CREATE and MODIFY/ALTER permissions on the EUCARIS database.

By default, the EUCARIS Service Account is added to the database role EUCARISII, which grants database owner (DBO) permissions to the EUCARIS database.

NOTE: When using Integrated Security, please make sure that the database permissions of both the EUCARIS Service account and the local administrator are set correctly!

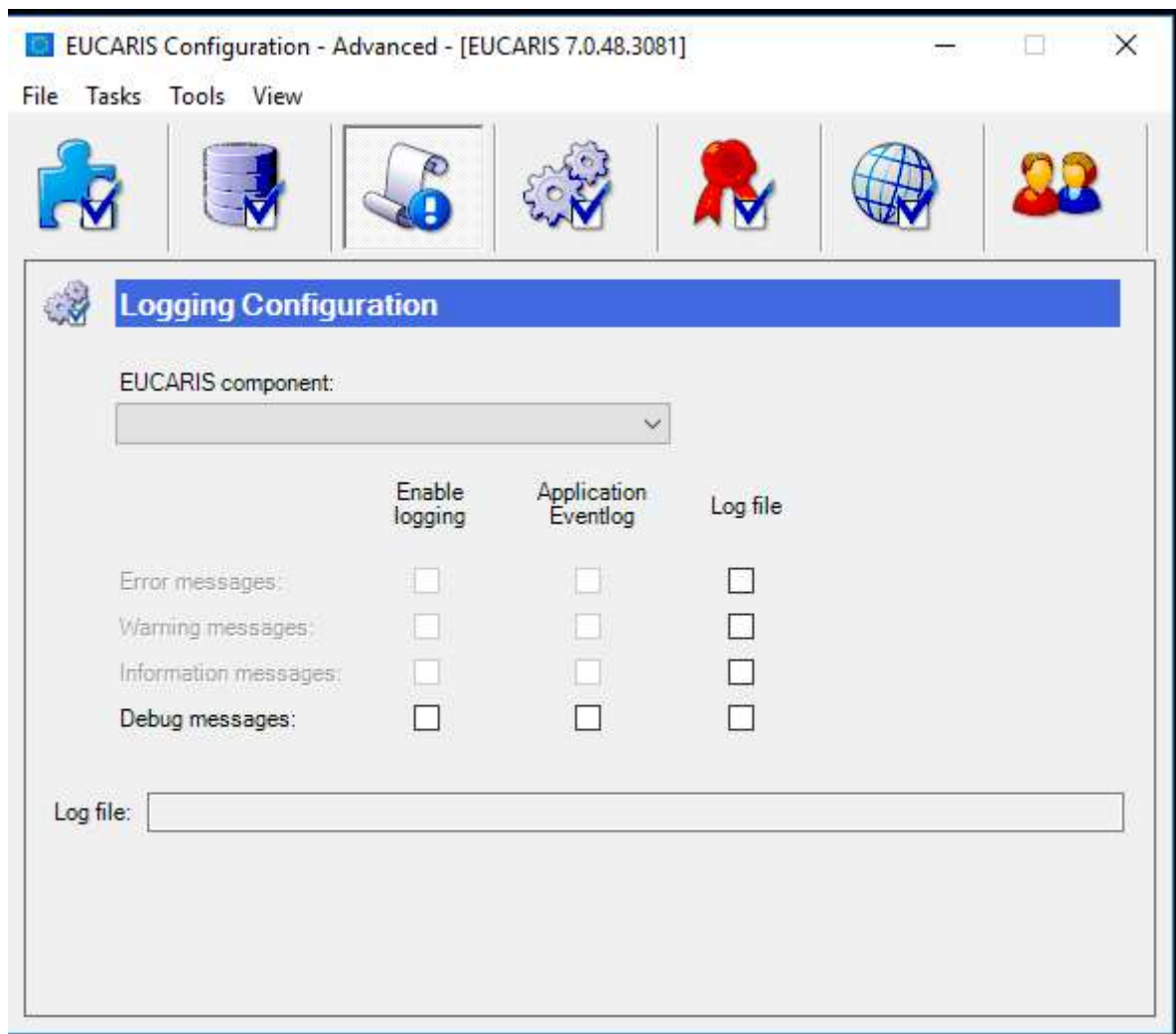
To check the current configured connection string Select 'Check' to verify the connection parameters:



If configured correctly, the dialog will contain EUCARIS version information of the current connected database. The noted EUCARIS database release identifiers relate to the System Update containing the specific database updates.

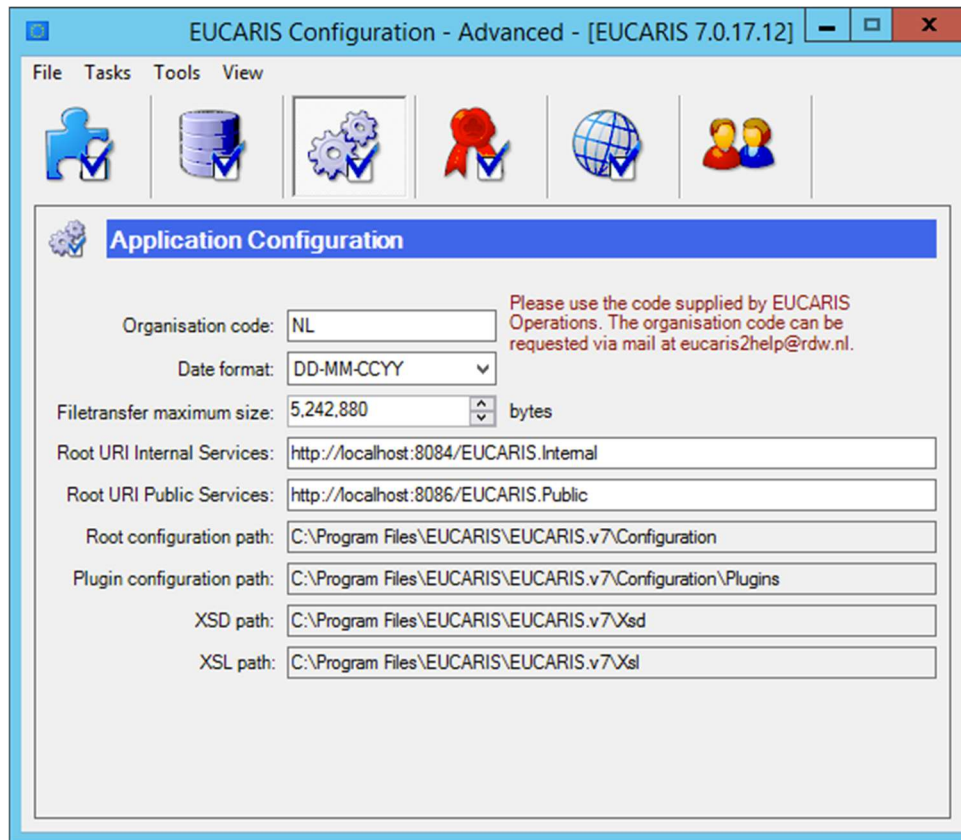
5.2.4 Logging configuration

The user can specify per Eucaris component which type of messages could be logged in a Log file. In case of debug messages, there's also the option to enable the logging and to show them in the Application Eventlog.



5.2.5 Application configuration

In this screen the user can set for which member state or organisation the EUCARIS installation is set up. Normally, after configuring for a specific member state or organisation, this value needs no changes later. However it might be needed for testing purposes to configure another member state organisation code.



The following parameters can be set:

- **Organisation code**
 The organisation code for which to configure EUCARIS. Please use the code supplied by *EUCARIS Operations*

NOTE: Please use the code supplied by EUCARIS Operations. The organisation code can be requested via mail at EUCARIS2help@rdw.nl.
- **Date format**
 The date format that should be used when presenting dates in the EUCARIS web client. All dates will be shown in the format specified here
- **File transfer maximum size in bytes**
 The maximum file size that can be sent by EUCARIS, attached in asynchronous messages. It is advised to set this value to 5,242,880 bytes. EUCARIS will produce an error when it receives an asynchronous message bigger than the defined maximum. Please keep in mind that the maximum message size also depends on both the local infrastructure and network capacity and the infrastructure and network capacity of the other member states that files are exchanged with

- **Root URI Internal Services**

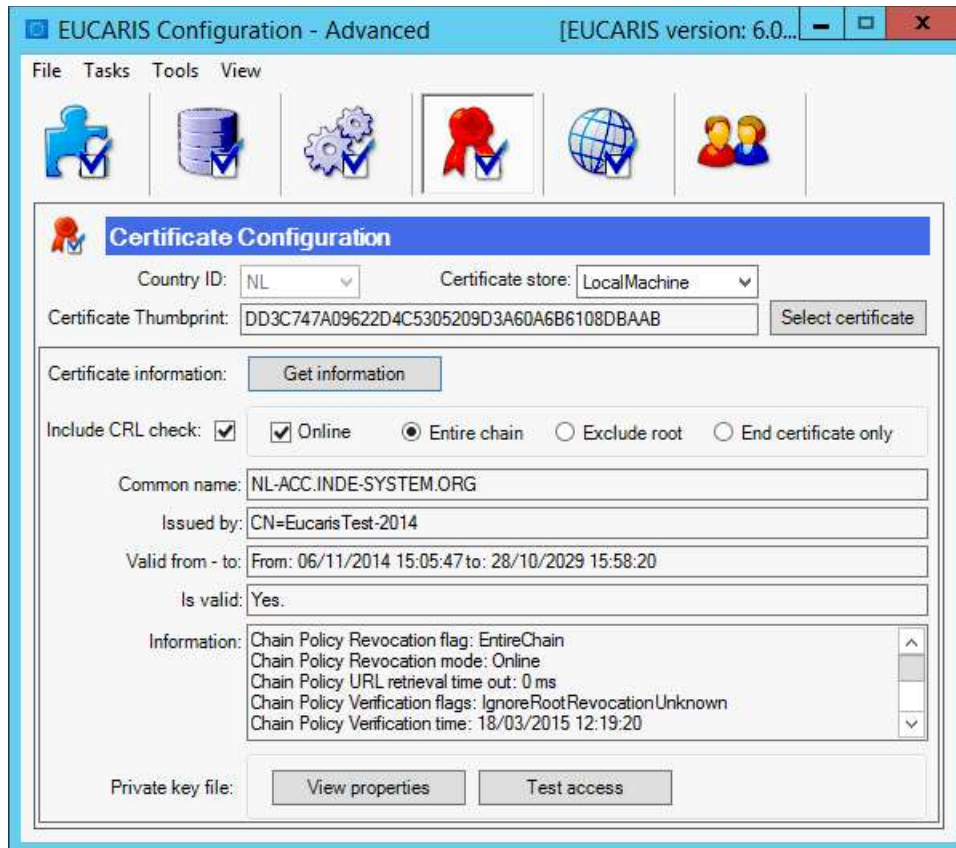
The EUCARIS applications requires the correct root URI of the EUCARIS Internal Services. This URI is set during the initial configuration and should contain the correct default value. In some circumstances (in specific deployment scenarios) it is required to validate and change this value to the correct one

- **Root URI Public Services**

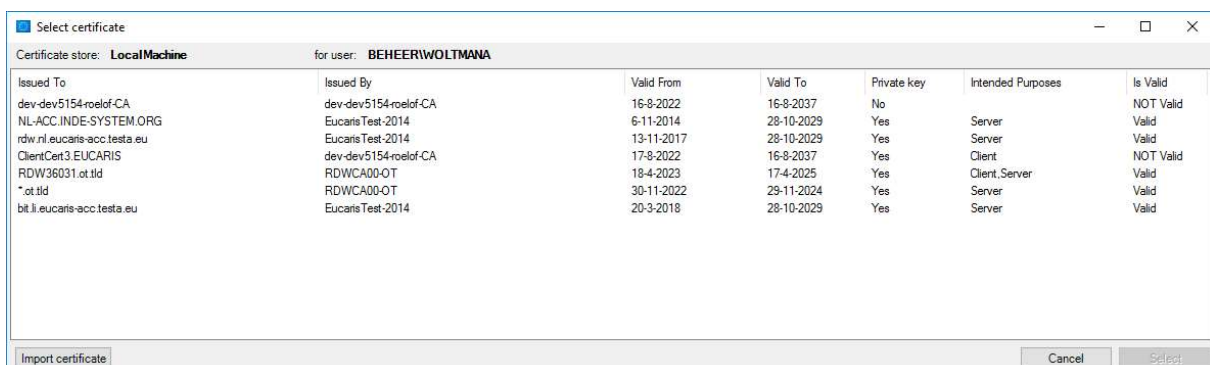
The EUCARIS applications requires the correct root URI of the EUCARIS Public Services. This URI is set during the initial configuration and should contain the correct default value. In some circumstances (in specific deployment scenarios) it is required to validate and change this value to the correct one

5.2.6 Certificate configuration

This window is used to configure the certificate used for signing and encrypting of the EUCARIS messages. The validity of the certificate can be checked, as well as the access to the private key by the EUCARIS service account.



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. Please contact *EUCARIS Operations* if using the 'Local Machine' store is not possible due to restrictions or policies. Press 'Select certificate' in order to configure the correct EUCARIS certificate.

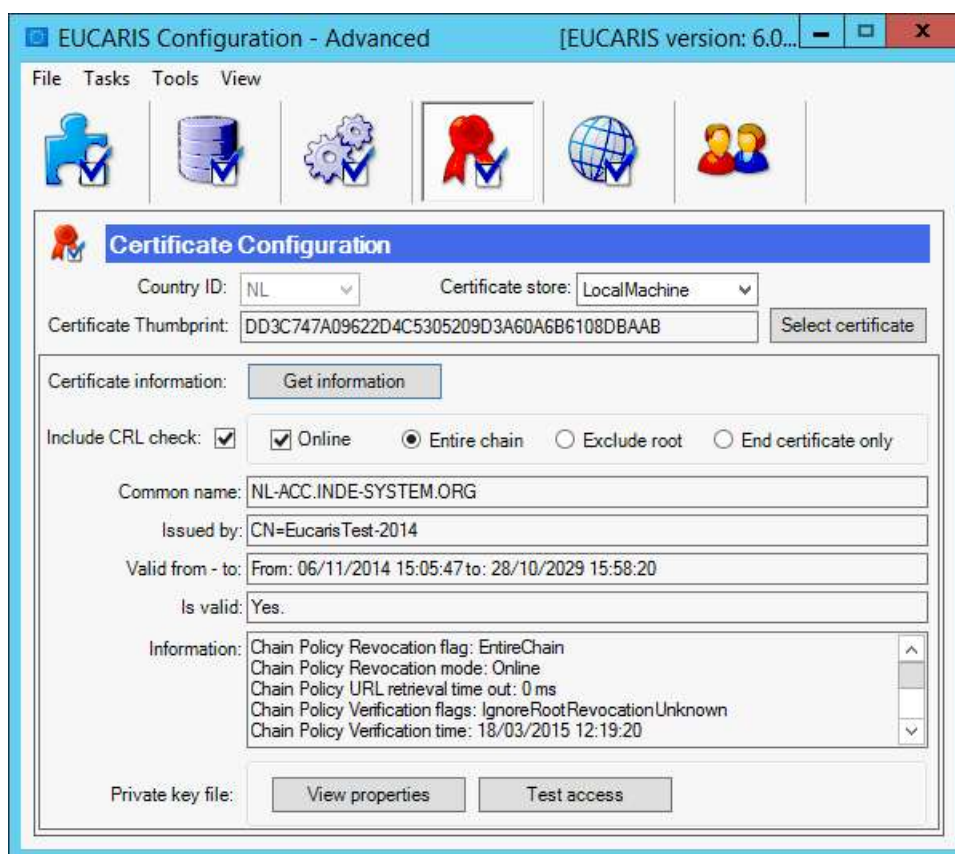


The EUCARIS certificates for both the acceptance as well as the production environment can be obtained by requesting them from the *EUCARIS Operations* at EUCARIS2help@rdw.nl.

NOTE: Since the introduction of the TESTA PKI (early 2018), EUCARIS System Updates are used in the distributing and installation of EUCARIS certificates. Since the end of 2023 production certificates no longer are derived from the TeleSec PKI (offered by the EC), since then new certificates are derived from the QuoVadis PKI (contracted by EUCARIS Secretariat). Please review paragraph 5.3.2 System Update for more information on System Updates, and paragraph 10.8, How To: Install a Certificate using System Updates

NOTE: Although EUCARIS will accept any X509 certificate with key usages: Digital Signature, Non-Repudiation, Key Encipherment and Data Encipherment, both acceptance and production certificates for use in the EUCARIS infrastructure are supplied by EUCARIS Operations. Please contact EUCARIS2help for more information about the certificate request procedure

NOTE: during the import of an EUCARIS certificate also the certificates of the intermediate- and root Certificate Authorities are imported to ensure a complete trusted chain



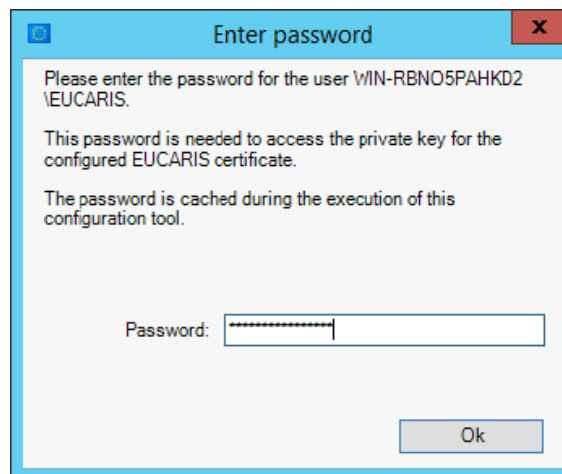
As long as no valid certificate is selected, it is not possible for EUCARIS to communicate to other instances of EUCARIS.

Press 'Get information' to validate the certificate, with or without the checks on the Certificate Revocation List (CRL). Whether or not the validation of the certificate is including the CRL check can be controlled by selecting the 'Include CRL check'. If this is selected 'Online' can be used to do the CRL check online and the level of validation can be controlled using 'Entire chain', 'Exclude root' and 'End certificate only'.

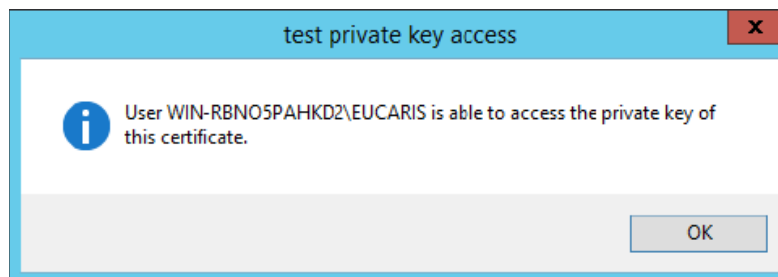
NOTE: Both the intermediate certificate uses and the peer certificates use a Certificate Revocation List (CRL) which is hosted on the Internet by the Certificate Authority (QuoVadis). EUCARIS Operations republishes this CRL so that they are available for you via the TESTA network. Downloading and installing the latest available Configuration Update should be sufficient to configure the local system to use the republished CRL on TESTA

The certificate contains a private key, and any user (including the EUCARIS service account) which must be able to use this private key must be explicitly authorised in Windows.

Press 'Test access' to check if the EUCARIS service account is able to access the certificate's private key. The application will ask for the password of the EUCARIS service account to verify accessibility.



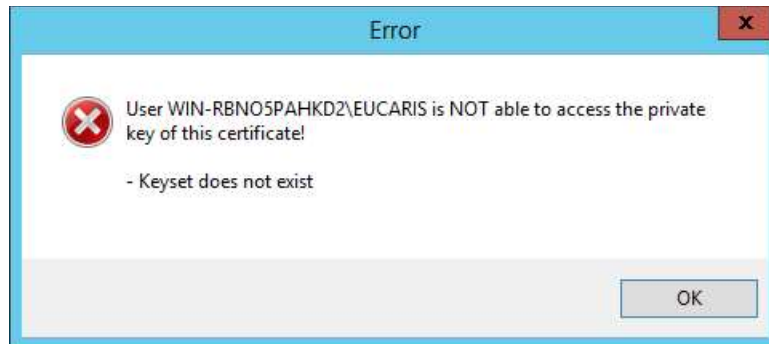
This check can result in one of the next two responses, indicating whether or not the certificate private key is accessible by the EUCARIS service account.



This indicates correct accessibility.

The configuration now can be saved via 'file' and selecting 'Save current configuration'

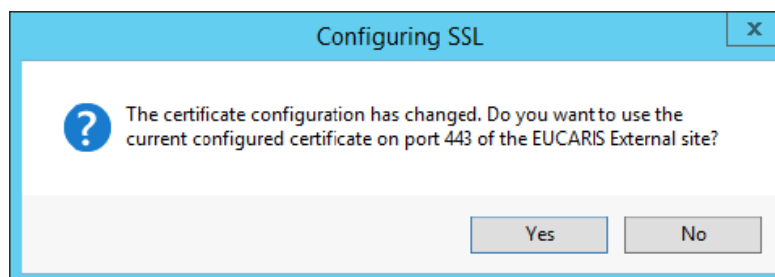
The next Error message displays the situation in which the certificate is not accessible to the EUCARIS service account.



If this Error happens press 'View properties', which will open a properties dialog and press 'Security' to switch to the security information. Using the 'Edit' button opens the permissions dialog and 'Add...' has to be used to add the EUCARIS service account with at least 'Read' permissions. When done 'Test access' can be retried to verify the certificate is correctly accessible to the EUCARIS service account.

If the certificate now is accessible to the EUCARIS service account, save the configuration via 'file' and selecting 'Save current configuration'.

The EUCARIS certificate is also being used for the Transport Layer Security (TLS, https). The TLS can be configured to terminate on the EUCARIS Server (on the EUCARIS.External website in IIS), or on a component in the infrastructure e.g. a Firewall. If the certificate configuration has been changed, the Configuration Tool will ask if the current configured certificate should be installed as TLS certificate on the EUCARIS.External website in IIS:

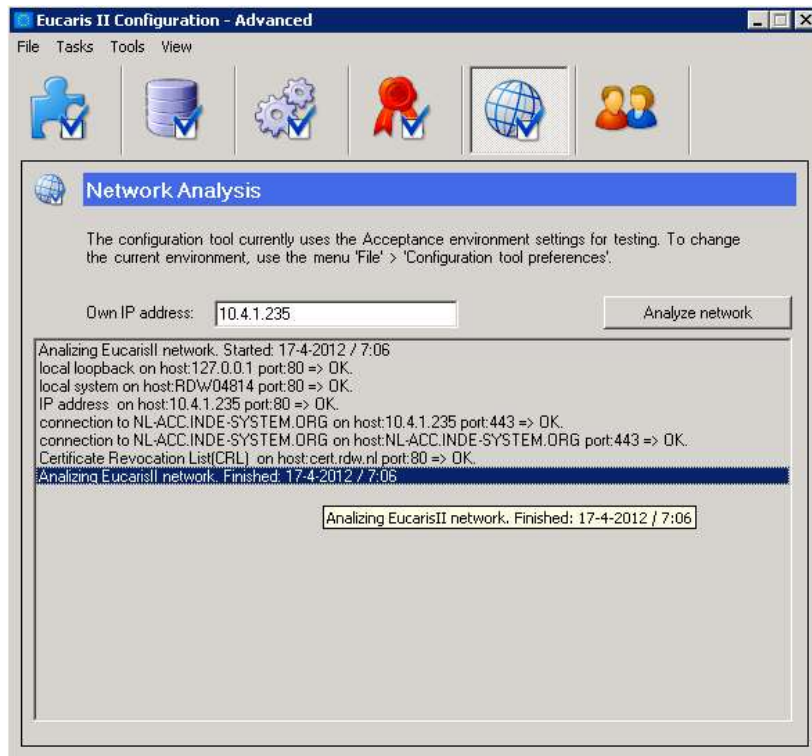


NOTE: If the TLS is by design not established by IIS, then do not forget to install the certificate on the network appliance that terminates the TLS

5.2.7 Network analysis

In this screen the network configuration can be analysed based on the supplied parameters and whether a connection to *EUCARIS Operations* is possible. The IP Address of the server must be entered to perform some local tests.

Pressing 'Analyse network' tries to connect to *EUCARIS Operations* and, in this case success is shown:



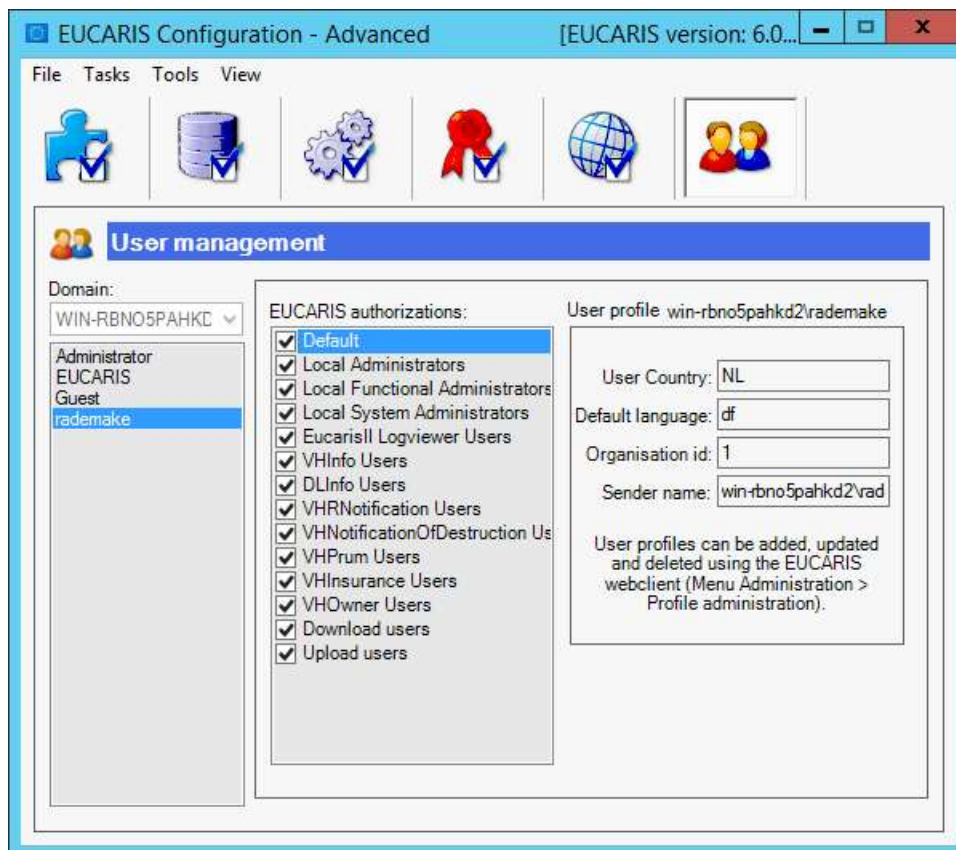
5.2.8 User management

User management is only applicable for the use of the EUCARIS Web Client of the EUCARIS Management Client. For a user to be able to use one of these clients at least two requirements have to be met:

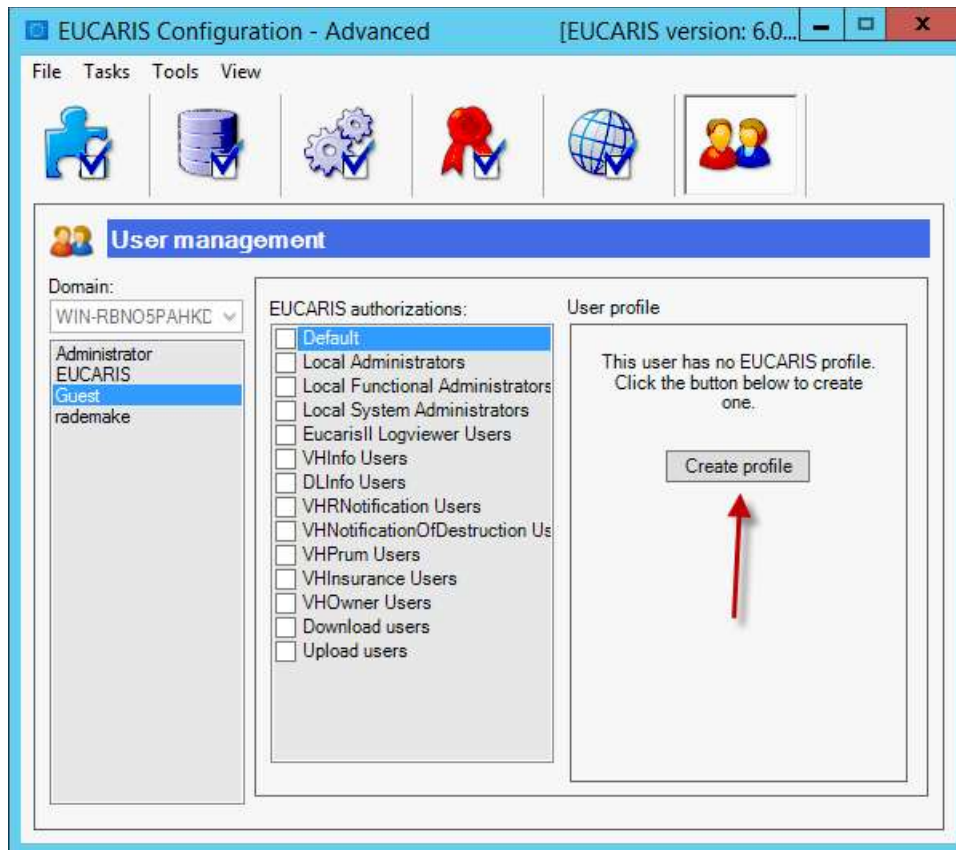
1. The user must have a (valid) registered profile in the EUCARIS database (table UserProfile),
2. The user must be a member of one of the available EUCARIS Windows Groups.

Please review paragraph **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** for more information on the authentication methods of the EUCARIS Web Client and EUCARIS Management Client.

The Configuration Tool offers some basic support for the user management of the EUCARIS Web Client and Management 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 can be created:



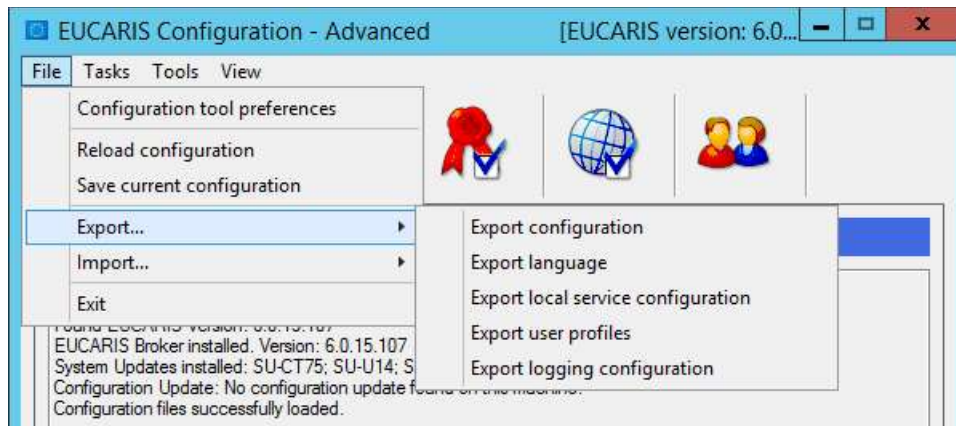
It is possible to select users from an active directory using this tool. If users from another domain needs to be added, close the Configuration Tool and locate and open the EUCARIS.Configuration.exe.config file (default located at C:\Program Files\EUCARIS\Tools\EUCARIS.Configuration). Change the following key:

```
<add key="UserManagementDomain" value="domain" />
```

NOTE: Every EUCARIS Web client or Management client user should be added in the 'Default' user group

5.2.9 Export and Import Settings

The Configuration Tool offers functionality to export EUCARIS settings and import them in another version or another environment. The exported settings are stored in different XML files.



Choose 'File' > 'Export' > 'Export configuration' to export a configuration.

Choose 'File' > 'Export' > 'Export language' to export a language after verifying access to the databases and retrieving the available languages, the user can choose each language to export.



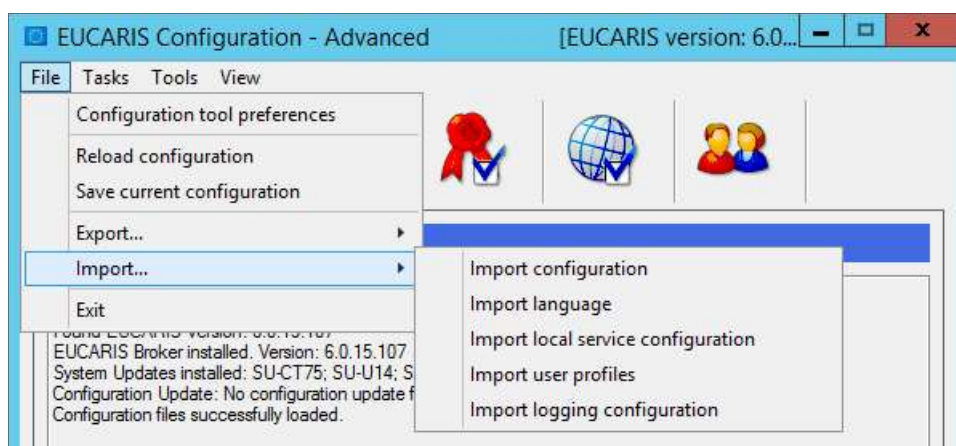
Choose 'File' > 'Export' > 'Export local service configuration' to export the local service configuration.

Choose 'File' > 'Export' > 'Export user profiles' to export the user profiles.

Choose 'File' > 'Export' > 'Export logging configuration' to export the logging configuration.

For all exports a file dialog is presented to select the location where to store the exports.

To import the following menu is available:



Choose 'File' > 'Import' > 'Import configuration' to import a configuration.

Choose 'File' > 'Import' > 'Import language' to import a language after verifying access to the databases and retrieving the available languages, the user can choose each language to import.



Choose 'File' > 'Import' > 'Import local service configuration' to import a local service configuration.

Choose 'File' > 'Import' > 'Import user profiles' to import user profiles.

Choose 'File' > 'Import' > 'Import logging configuration' to import a logging configuration.

For all imports a file dialog is presented to select the location of the file to use for import.

Apart from 'Import configuration', all imports directly update the database, so it is up to the user to verify the imported configuration is correct and press 'File' > 'Save current configuration' to save the configuration.

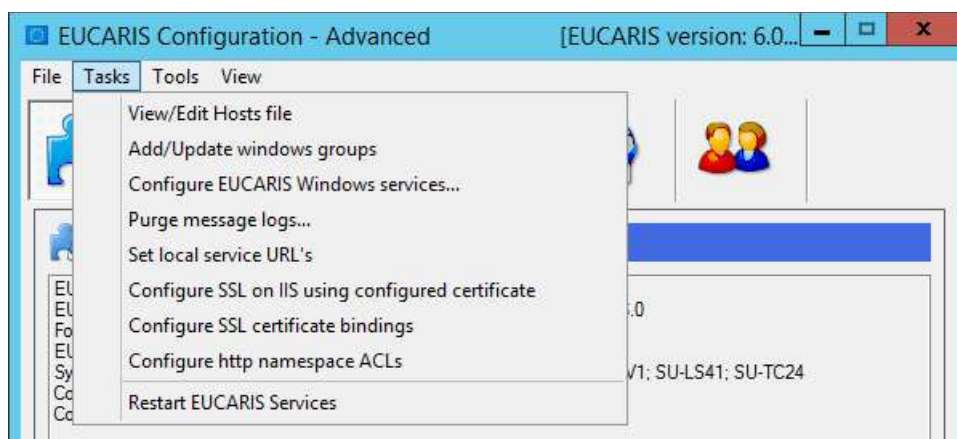
Configuration changes only become active after all EUCARIS services are restarted. The Configuration Tools asks the user if the services should be restarted now. Click 'Yes' to restart now or restart all EUCARIS services later by using 'Tools' > 'Restart EUCARIS Services'.

NOTE: In case the user decides to restart the services manually it is important to keep in mind that the new configuration will only be reloaded in case all services are stopped before starting them again. Therefore, it is advised to restart the services using the Configuration Tool

NOTE: Restarting also includes a reset of Internet Information Services (IIS), causing all web applications and web services to be stopped and started automatically. If the server is hosting other websites also this should be kept in mind

5.2.10 Tasks

The EUCARIS Configuration Tool offers a number of specific tasks which may be needed to properly configure and/or analyse the EUCARIS Configuration:



5.2.10.1 View/Edit hosts file

The EUCARIS network infrastructure does not utilize the TESTA DNS. Instead of DNS, EUCARIS uses the local Windows Hosts file to make the translation from an TESTA IP address to the EUCARIS host names. EUCARIS Host names follow the syntax: [organisationcode].[countrycode].Eucaris.Testa.Eu for the production environment and [organisationcode].[countrycode].Eucaris.Testa.Eu for the acceptance environment. The task “View/Edit host file” allows to easily check the contents of this hosts file.

NOTE: The Hosts file is maintained centrally by EUCARIS Operations and this file is adapted by means of Configuration Updates. Therefore, it is advised to not make changes within the marked EUCARIS section.

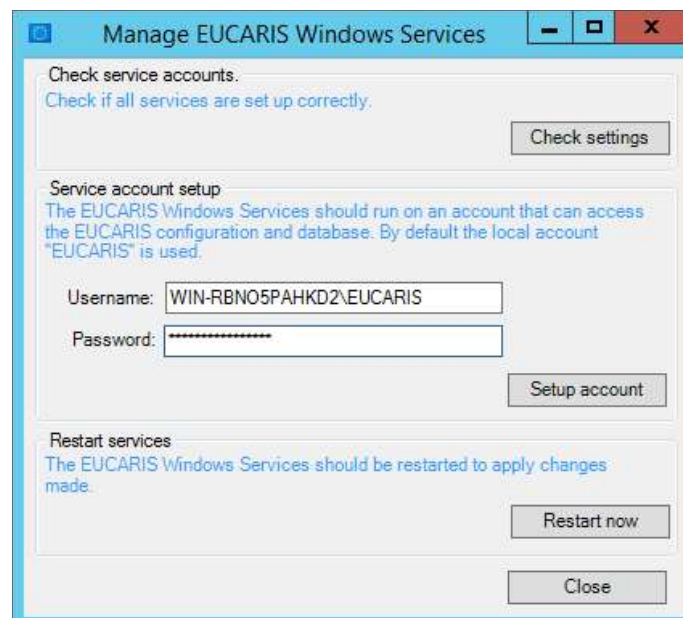
5.2.10.2 Add/Update windows groups

The ‘Tasks’ > ‘Add / update windows groups’ allows the user to create or update the required windows groups for the EUCARIS Web client and the EUCARIS management client. This will not change existing groups, but only adds new groups that are required.

NOTE: This task should not be used in normal operation. Required Windows groups will be created by the applicable System Update.

5.2.10.3 Configure EUCARIS Windows services

The ‘Tasks’ > ‘Configure EUCARIS Windows services...’ is used to check and configure the EUCARIS related Windows Services to start automatically and run under the EUCARIS service account. In the dialog the username and password of the EUCARIS service account can be entered. Press ‘Setup account’ to setup the EUCARIS services according the specified and required settings and press ‘Check settings’ to verify the current settings. ‘Restart now’ can be used to restart the services after the update.

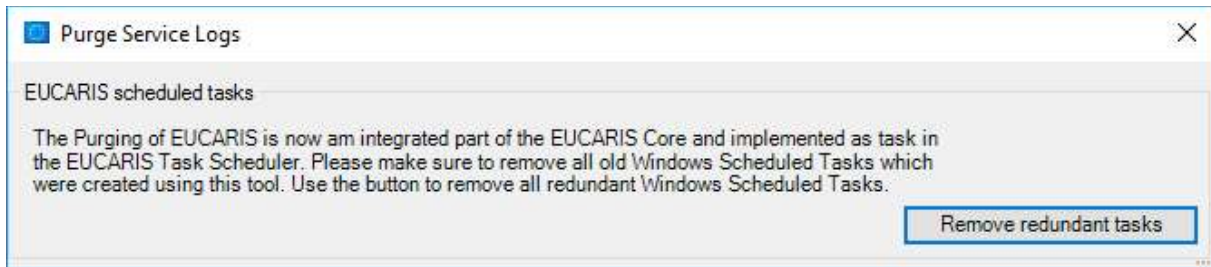


NOTE: The EUCARIS Windows Services can be identified by the name, starting with “EUCARIS”.

5.2.10.4 Purge message logs

Messages that have been exchanged by EUCARIS are stored in the message log (table: ServiceLog). Each treaty, framework or bilateral agreement must define data retention rules on how long a message must and may be persisted in a local system. To support these data retention rules of specific treaties, EUCARIS has a task scheduler which runs as a windows service.

In the past the EUCARIS Configuration tool was able to configure and schedule tasks to automatically purge the service log daily using the “Purge message log”. Currently it shows the following screen:



To remove the previous created windows schedules for purging, press ‘Remove redundant tasks’

For more details on logging, please refer to document “Use case-4: Log EUCARIS message”.

5.2.10.5 Set local service URLs

EUCARIS has a number of specific services which should be set to the local server by default. During a regular setup, these services are set up correctly. If for some reasons the services configuration has been corrupted, the “Set local service URLs” can restore this. The following local services are being set:

Service	EUCARIS Site	Endpoint
File transfer service	Public	FileTransferService.asmx
Message service	Public	Messageservice.asmx
Generic service	Public	Genericservice.asmx

The ‘Tasks’ > ‘Set local service URL’s’ will set the local URL’s. This includes the URL’s for the local File Transfer Service and the Notification Service and notifies the user they are set correctly.

5.2.10.6 Configure SSL on IIS using configured certificate

The EUCARIS certificate is used for both signing as for Transport Layer Security (TLS, https) between member states. When the TLS is terminated on the local EUCARIS server, the EUCARIS.External website must have a TLS binding (port 443) with the EUCARIS certificate configured. The ‘Tasks’ > ‘Configure SSL on IIS using configured certificate’ provides the functionality to configure automatically. When configuring the certificate (see 0 or 5.2.6 Certificate configuration), the EUCARIS Configuration tool will ask if the specified certificate must be configured as TLS certificate on the EUCARIS.External website, so this task should normally not have to be used.

5.2.10.7 Configure http namespace ACLs

Namespace reservation assigns the rights for a portion of the HTTP URL namespace to a particular group of users. A reservation gives those users the right to create services that listen on that portion of the namespace. Reservations are URL prefixes, meaning that the reservation covers all sub-paths

of the reservation path. The IIS Management tool automatically creates HTTP URL namespace reservation based on the specific website bindings. The EUCARIS Configuration Tool creates the required HTTP URL namespace reservation for the Broker during the configuration of the Broker. This screen allows the user to check and optionally adapt the HTTP URL namespace reservation in case of analysis of problems.

5.2.10.8 Restart EUCARIS Services

The 'Tasks' > 'Restart EUCARIS Services' restarts the EUCARIS services and applications. All EUCARIS software share the same configuration data. Therefore, it is important that ALL EUCARIS components are shutdown prior to be restarted.

NOTE: In case the user decides to restart the services manually it is important to keep in mind that the new configuration will only be reloaded in case all services are stopped before starting them again. Therefore, it is advised to restart the services using the Configuration Tool.

NOTE: Restarting includes a recycle of all EUCARIS IIS applications, causing a short interruption of service for all EUCARIS related message transfers.

5.2.11 Tools

The EUCARIS Configuration Tool offers a number of specific tools which may be needed to properly configure and/or analyse the EUCARIS System:

5.2.11.1 Event log viewer

EUCARIS logs informational, warning and error events to the Windows Application Event log. Therefore, the Configuration Tool provides a short-cut to the Windows Event log Viewer.

5.2.11.2 IIS manager

Large parts of the EUCARIS application are hosted in Internet Information Service. The Configuration Tool provides an easy access to the Internet Information Service Manager.

5.2.11.3 WebClient

The 'Tools' > 'WebClient' will open the Web Client web application of EUCARIS.

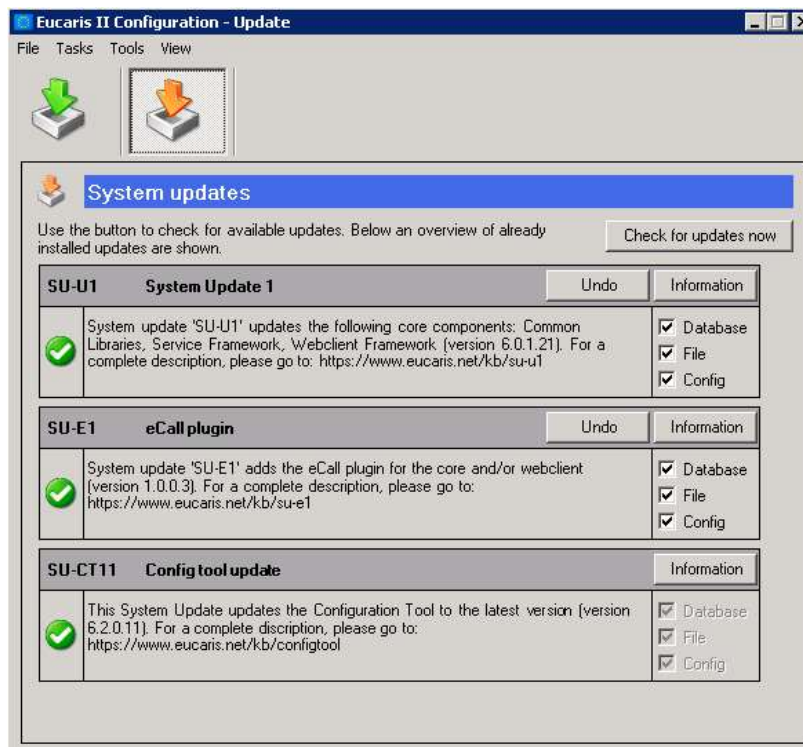
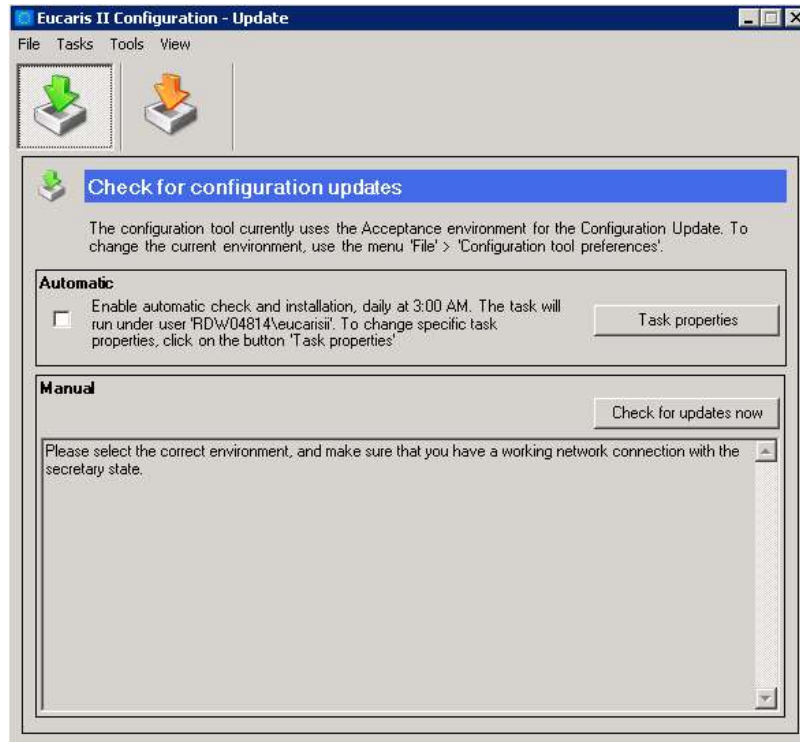
5.2.11.4 Configuration wizard

The 'View' > 'Configuration wizard' will switch the mode of the Configuration Tool to wizard mode. Please refer to paragraph 5.1 for more information.

5.3 Update mode

The Configuration Tool has an update mode, allowing the user to:

- update the configuration of EUCARIS as described in paragraph 5.3.1
- update the EUCARIS system software as described in paragraph 5.3.2



5.3.1 Configuration Update Service

Because of the additional responsibilities of *EUCARIS Operations* the Configuration Update Service has been created allowing *EUCARIS Operations* to issue updated configurations and member states to adopt these changes in their local configuration.

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

NOTE: Using the Configuration Update Service is only possible when a working network connection with *EUCARIS Operations* is available. This means that a fully functional TESTA connection should be available to download updates, but it is also possible to execute an update that is send through mail.

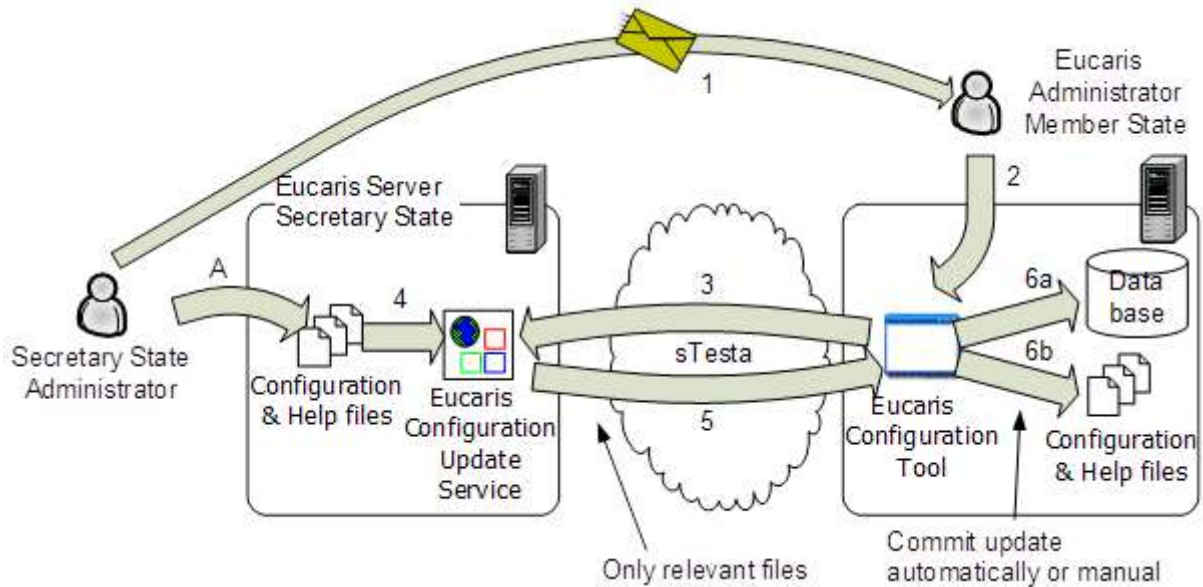
5.3.1.1 Overview

A published configuration update can make a number of common and specific changes to EUCARIS and is environment specific, meaning a configuration update can be published separately for both the 'Acceptance' and 'Production' EUCARIS installations.

Changes that are possible are the following:

- **IP addresses or URLs of other member states**
This defines which IP addresses and URLs are used by the other member states
- **IP addresses of certificate revocation lists**
This defines the address the member states have to use to allow verification of the certificate revocation list. EUCARIS will not work in case these checks cannot be performed
- **Authorisations for services**
This defines which member states can access which services of the other participating member state. Not all member states are participating in all communications
- **Connected countries definitions**
Definitions of the member states that are connected to EUCARIS
- **Specific local configuration changes**
Defines changes that are made to the local configuration as defined by *EUCARIS Operations*
- **Default logging configuration changes**
For each EUCARIS agreement a minimum logging configuration has been defined for both auditing and logging purposes. This minimum logging configuration is checked by the Configuration Tool and updates are created and distributed by *EUCARIS Operations*
- **Endpoints**
Defines changes that are made to the endpoint configuration as defined by *EUCARIS Operations*. Endpoints are managed with a second update file, which applies after installing EUCARIS Core SU-U52 or higher.

Schematically the creation of configuration updates by *EUCARIS Operations* and the usage of these configuration updates by the member states is shown below:



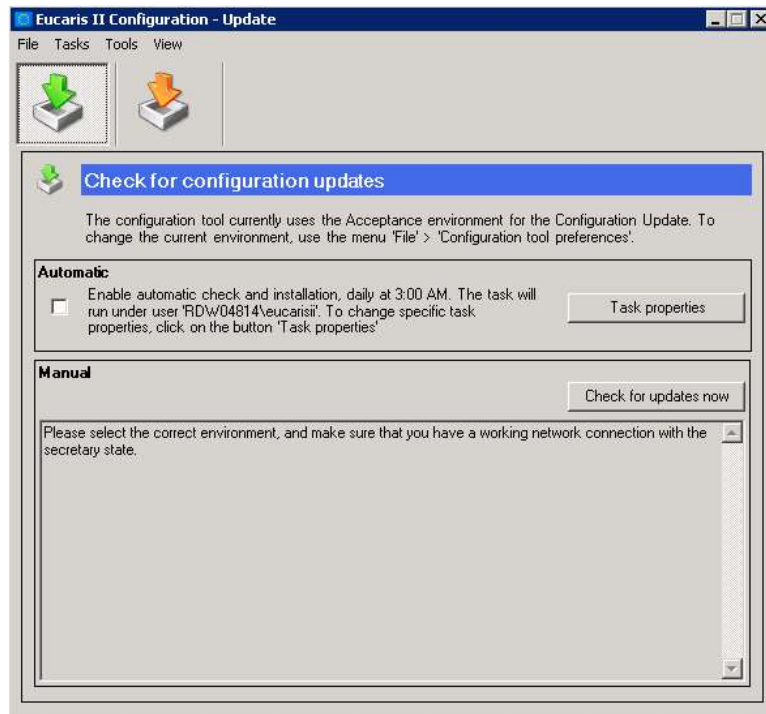
A configuration update is created and tested by *EUCARIS Operations* administrator after which it is uploaded (A) to the server where the Configuration Update Service is located. Next all the member states are notified (1) via e-mail that a configuration update is available, after which the administrators of the member states start (2) the Configuration Tool to retrieve the update from the Configuration Update Service (3). The Configuration Update Service retrieves the update (4) and returns it to the Configuration Tool (5) of the member state. The Configuration Tool then makes the required changes (6a and 6b) to the EUCARIS server of the member state.

5.3.1.2 Download and install a new Configuration Update

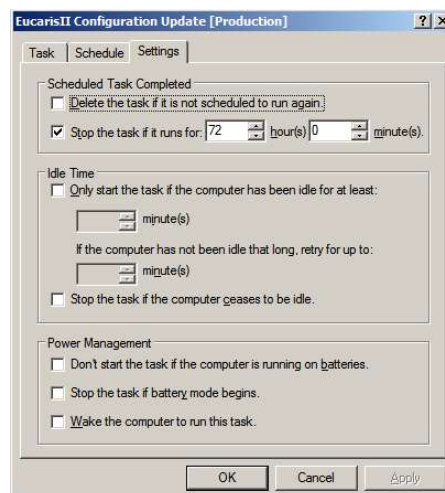
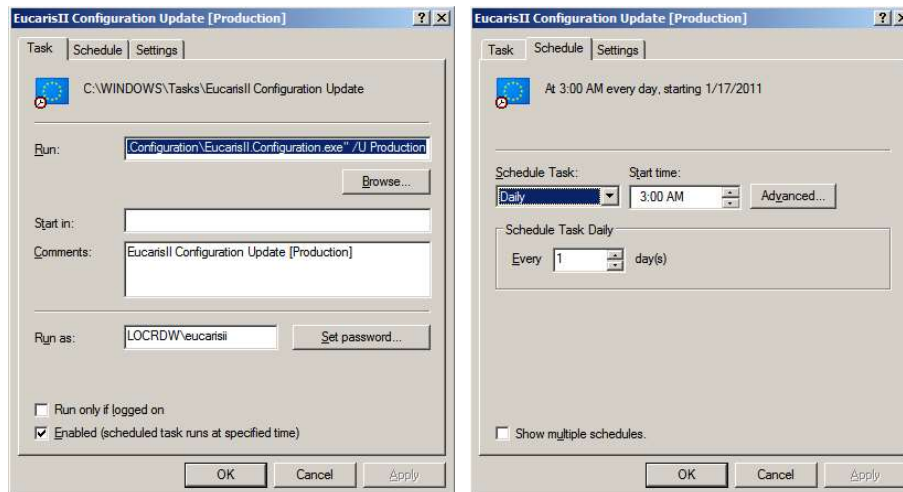
Start the Configuration Tool in Update mode and select the 'Check for configuration updates' page. On this page the user can choose between 'Automatic' and 'Manual' and in case of 'Automatic' the schedule can be set.

NOTE: 'Automatic' mode downloads AND installs configuration updates fully automatically

If 'Manual' is chosen there is a distinct separation between downloading the configuration update and installing the configuration update.



In case of 'Automatic' the 'Task properties' is used to specify the details of this automated process:



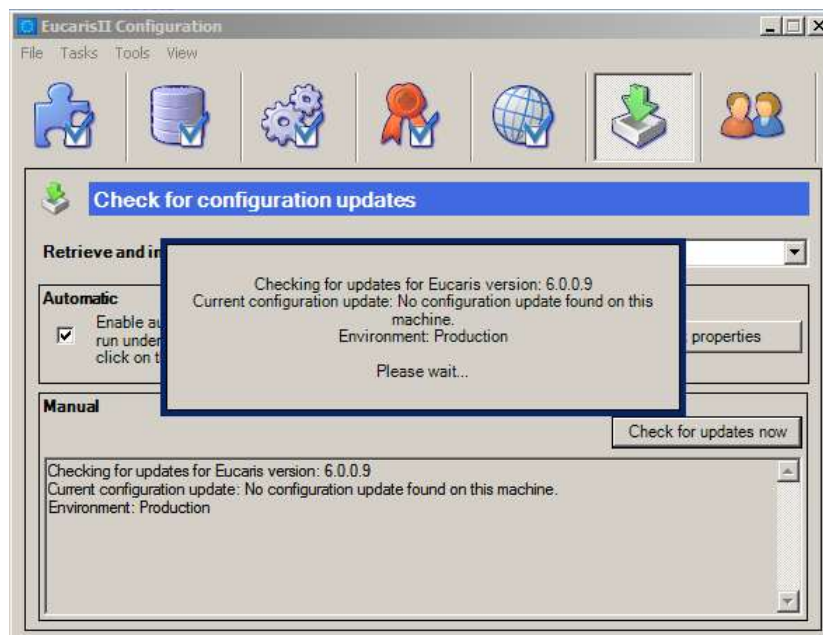
After setting up these details, the EUCARIS server, will check for updates automatically according the specified schedule, but if the user chooses 'Manual' or wants to check now 'Check for updates now' can be used, which triggers the following steps to be done, matching the overview in 5.3.1.1:

3. The Configuration Tool sends an update request to the Configuration Update Service, which is located on a server at *EUCARIS Operations*. In this request the Configuration Update Service is supplied with the environment, the EUCARIS version and the configuration version.
4. The Configuration Update Service uses this information to check for available updates.
5. The Configuration Update Service either delivers the most recent configuration definition files to the Configuration Tool or notifies the Configuration Tool there is no update available.
6. The user uses the Configuration Tool to carry out the database and configuration changes.

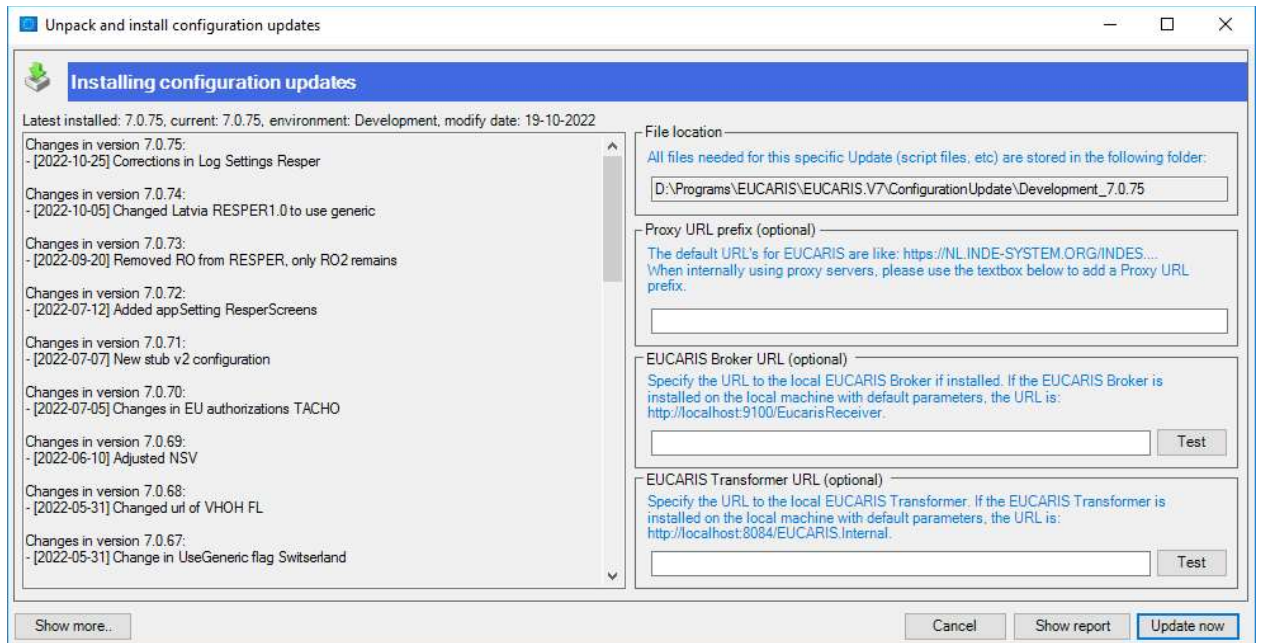
Steps 3 to 6 are repeated for the endpoints Configuration Update, which is another request to the Configuration Update Service.

Since a configuration update might contain sensitive data the communication between the Configuration Tool and the Configuration Update Service is signed and encrypted, therefore the logged in user is required to access the private key of the EUCARIS certificate. Please refer to 5.2.6 on how to grant a user access to the certificates private key.

The Configuration Tool continues to check for updates and downloads them if there are any updates:



When updates are downloaded the 'Unpack and install configuration updates' screen is shown:

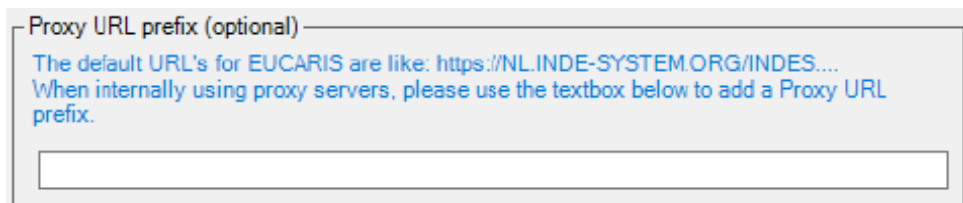


If the user decides not to install at this time the user can choose for a 'Manual update' to make sure it does not have to be downloaded again. The moment the installation has to be done this can be triggered from the Configuration Tool via 'File' – 'Load previously downloaded update', which will open the above screen.

In this dialog the user has the following options:

Configure a proxy URL prefix

All EUCARIS URLs are stored as '*https://XXX.YYY.Eucaris.Testa.Eu/eucaris...*' (where XXX is the organisation code and YYY the ISO2 country code) that are correct as long the EUCARIS server is directly connected to the TESTA network. If a proxy server is used it is possible to configure the Proxy URL prefix:

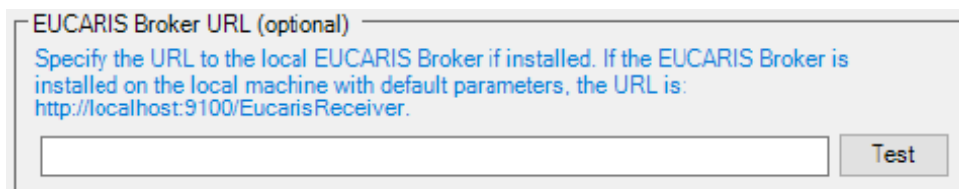


This example will configure the URLs as:

'http://internal.proxy/proxy.asp?url=https://XXX.YYY.Eucaris.Testa.Eu /eucaris...'

Configure the EUCARIS Broker URL

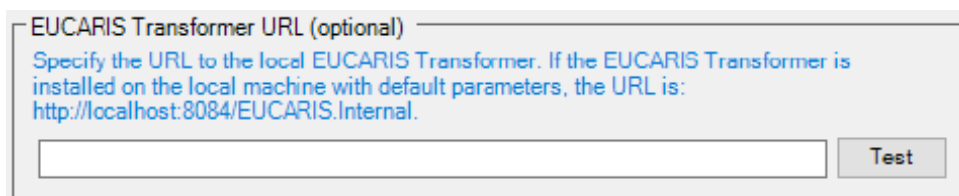
This field is mandatory when using the EUCARIS Broker to communicate with a central hub. The Configuration Tool will substitute this address for all countries communicating via the central hub regarding specific treaties or services. If the EUCARIS Broker is installed using its default configuration, this URL should be: <http://localhost:9100/EUCARISReceiver>. Use the 'Test' button to check whether there is an EUCARIS Broker listening to this address and port.



The screenshot shows a configuration dialog box titled "EUCARIS Broker URL (optional)". It contains a text input field and a "Test" button. The text inside the dialog reads: "Specify the URL to the local EUCARIS Broker if installed. If the EUCARIS Broker is installed on the local machine with default parameters, the URL is: <http://localhost:9100/EucarisReceiver>."

Configure the EUCARIS Transformer URL

This field is mandatory when using the EUCARIS Transformer to transform messages from the generic interface to the messageservice interface and vice versa. The Configuration Tool will substitute this address for all transformer related configuration in the Configuration Update. If the EUCARIS Transformer is installed using its default configuration, this URL should be: <http://localhost:8084/EUCARIS.Internal>. Use the 'Test' button to check whether there is an EUCARIS Transformer listening to this address and port.



The screenshot shows a configuration dialog box titled "EUCARIS Transformer URL (optional)". It contains a text input field and a "Test" button. The text inside the dialog reads: "Specify the URL to the local EUCARIS Transformer. If the EUCARIS Transformer is installed on the local machine with default parameters, the URL is: <http://localhost:8084/EUCARIS.Internal>."

Perform a complete or partly automatic update

If the user decides to perform the update automatically, the user can still decide parts to be done manually. The required scripts for performing the updates are always generated regardless of the selections made. These scripts are stored in the EUCARIS application folder in the subfolder ConfigurationUpdates and each update is stored in a separate subfolder. For the following items it can be decided to install them automatically or manual:

Hosts File

- **Automatic**
Modifies the current hosts file to contain the IP addresses of other member. Changing this file is only useful when not using an internal proxy server.
- **Manual**
Generates the modified hosts file in the script directory, which can be installed manually.

EUCARIS configuration files

- **Automatic**
Modifies the current configuration according to the update definition. If there are significant changes, they will be described in the release notes of this update.
- **Manual**
Generates the configuration files in the scripts directory, which can be installed manually.

Countries

- **Automatic**
Modifies the country descriptions and certificate authorisations in the database.

- **Manual**
Creates the 'CountryUpdate.sql' script, which can be run manually on the database.

Service URL's

- **Automatic**
Modifies the URLs of the services of other member states in the database.
- **Manual**
Creates the 'ServiceCountryinfo.sql' script, which can be run manually on the database.

Default service descriptions

- **Automatic**
Modifies the service descriptions in the default language (df) in the database.
- **Manual**
Creates the 'ServiceUpdate.sql' script, which can be run manually on the database.

Authorisation

- **Automatic**
Updates the member states authorization based on the signed treaties.
- **Manual**
Creates the 'RegistrationOfRightsInRecipientCountries.sql' and 'AuthorizationOfOtherCountries.sql' script, which can be run manually on the database.

Default logging settings

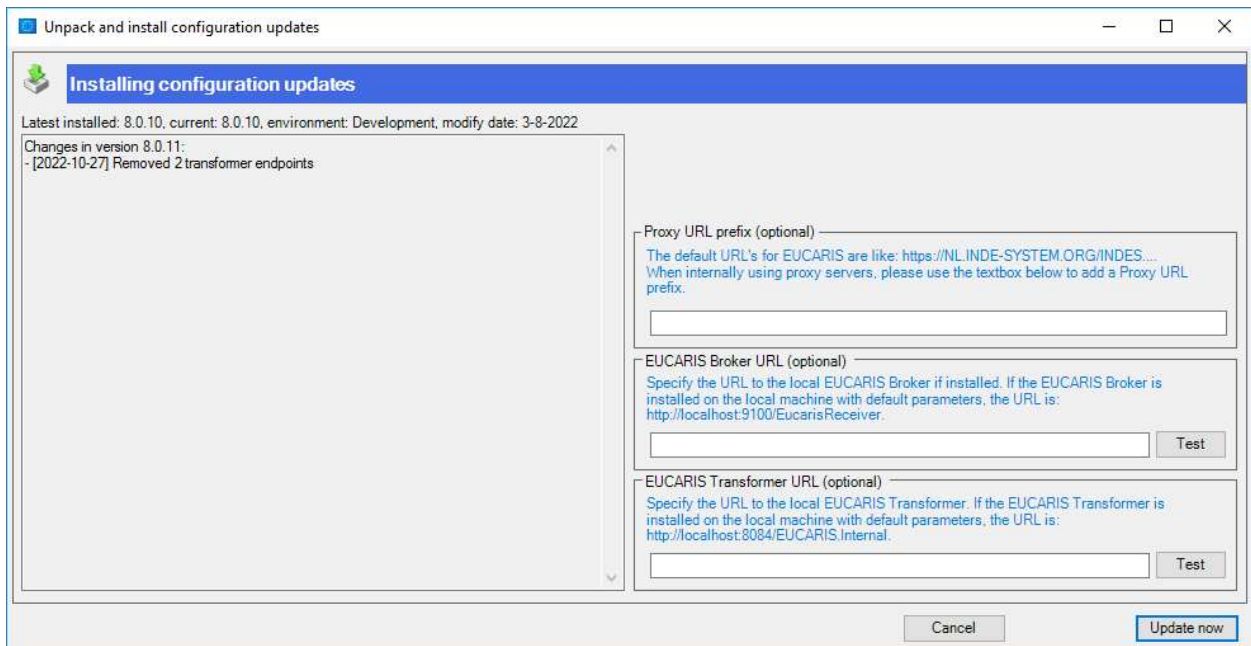
- **Automatic**
Modifies the default logging settings in the database according to the treaties the member state is participating in.
- **Manual**
Creates the 'DefaultLogging.sql' script, which can be run manually on the database.

Perform a manual update

If an automated update is not desirable, the user can opt for a manual update. All scripts and files are created in the 'Update files folder' location and they have to be executed manually.

5.3.1.3 Install an Endpoints Configuration Update

Once the previous Configuration Update is executed, the EUCARIS Configuration Tool will also check if an Endpoints Configuration Update is available:

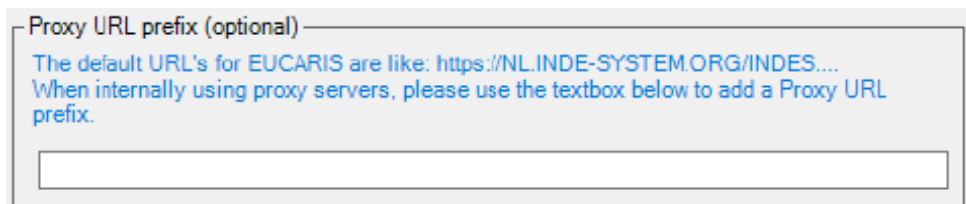


If the user decides not to install at this time the user can choose for a 'Manual update' to make sure it does not have to be downloaded again. The moment the installation has to be done this can be triggered using the 'File' – 'Load previously downloaded update', which will open the above screen.

In this dialog the user has the following options:

Configure a proxy URL prefix

All EUCARIS URLs are stored as '*https://XXX.YYY.Eucaris.Testa.Eu/eucaris...*' (where XXX is the organisation code and YYY the ISO2 country code) that are correct as long the EUCARIS server is directly connected to the TESTA network. If a proxy server is used it is possible to configure the Proxy URL prefix:

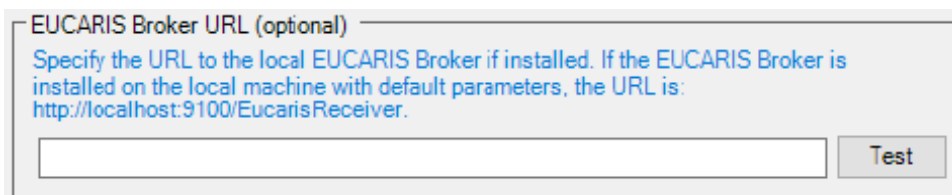


This example will configure the URLs as:

'http://internal.proxy/proxy.asp?url=https://XXX.YYY.Eucaris.Testa.Eu /eucaris...'

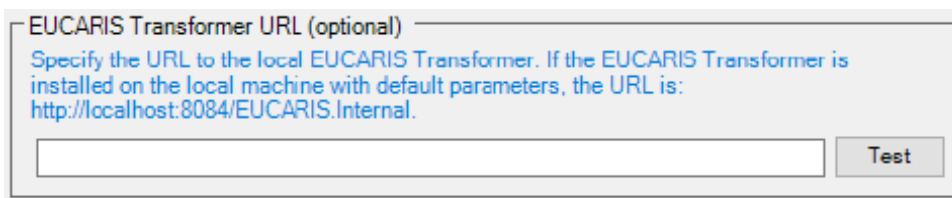
Configure the EUCARIS Broker URL

This field is mandatory when using the EUCARIS Broker to communicate with a central hub. The Configuration Tool will substitute this address for all countries communicating via the central hub regarding specific treaties or services. If the EUCARIS Broker is installed using its default configuration, this URL should be: <http://localhost:9100/EUCARISReceiver>. Use the 'Test' button to check whether there is an EUCARIS Broker listening to this address and port.



Configure the EUCARIS Transformer URL

This field is mandatory when using the EUCARIS Transformer to transform messages from the generic interface to the messageservice interface and vice versa. The Configuration Tool will substitute this address for all transformer related configuration in the Configuration Update. If the EUCARIS Transformer is installed using its default configuration, this URL should be: <http://localhost:8084/EUCARIS.Internal>. Use the 'Test' button to check whether there is an EUCARIS Transformer listening to this address and port.



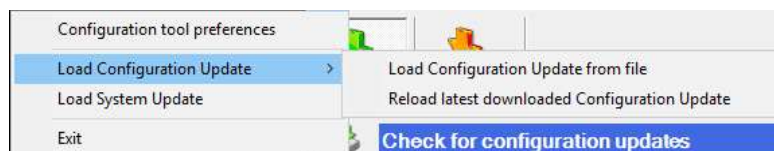
The Endpoints Configuration Update cannot be installed partly.

5.3.1.4 Install a previously downloaded Configuration Update

A previously downloaded update should be installed in the following scenarios:

- A new extension is installed using System Updates and no new Configuration update is available. In this scenario the newly installed extension must be configured using the latest downloaded Configuration Update,
- The user decides not to run the update directly after it is downloaded.

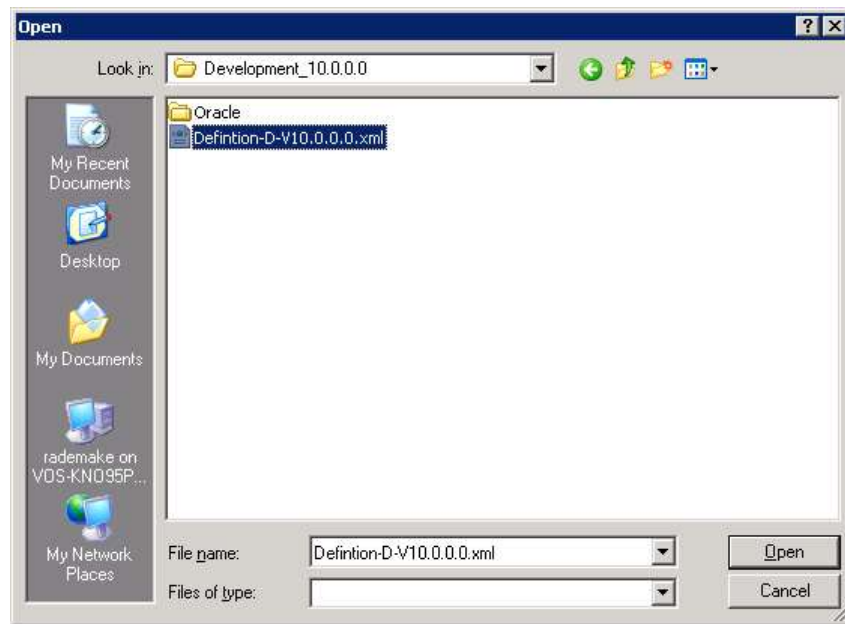
In Update mode, select Menu 'File' > 'Load Configuration Update':



The user can choose whether to Reload the latest downloaded Configuration Update, in which case the latest downloaded Configuration Update is applied again. This applies for both the Configuration Update as well as the Endpoints Configuration Update.

When the option 'Load Configuration Update from file' is chosen, the user can browse for a previously downloaded update in the Configuration Update folder or the location where the otherwise received update has been stored. The default locations are:

- Configuration Update:
[EUCARIS Rootfolder]\EUCARIS\EUCARIS.V7\ConfigurationUpdate
- Endpoints Configuration Update:
[EUCARIS Rootfolder]\EUCARIS\EUCARIS.V7\ConfigurationUpdateV8



For downloaded updates the update is stored in a subfolder with the following convention:

[Environment: Development, Test, Acceptance, Production]_[Version number].

For the names of the updates the following convention is used:

Definition-[Environment: D, T, A, P]-V[Version number].xml

After selecting the required update the Installing Configuration Update dialog is loaded and the in paragraph 5.3.1.2 or 5.3.1.3 described process can be followed.

5.3.2 System Update

EUCARIS release 6 is based on a 'pluggable framework architecture'. This means that the functionality of EUCARIS can be easily extended or adapted. The system updates supports this feature by adding functionality or additions which have been issued by *EUCARIS Operations* on demand. More information about System Updates can be obtained via <https://www.EUCARIS.net/kb/system-updates>.

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 Configuration Tool.

NOTE: Currently the automated distribution of System Updates requires TESTA, but for test and development systems it is possible to download a System Update manually. Please contact EUCARIS2help@rdw.nl for more information.

5.3.2.1 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

5.3.2.1.1 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 core components. 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 all EUCARIS core components.

5.3.2.1.2 Extension

An Extension consists of a web client- and/or service 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).

5.3.2.2 Details

A System Update can be downloaded by using the Configuration Tool. The software components are received via the secure TESTA channel and all software is checked for viruses and signed by *EUCARIS Operations*. The 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 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 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:

- database scripts (both for Oracle and MSSQL)
- EUCARIS related Microsoft .Net libraries (assemblies), scripts, web applications
- EUCARIS XML configuration files
- XSDs

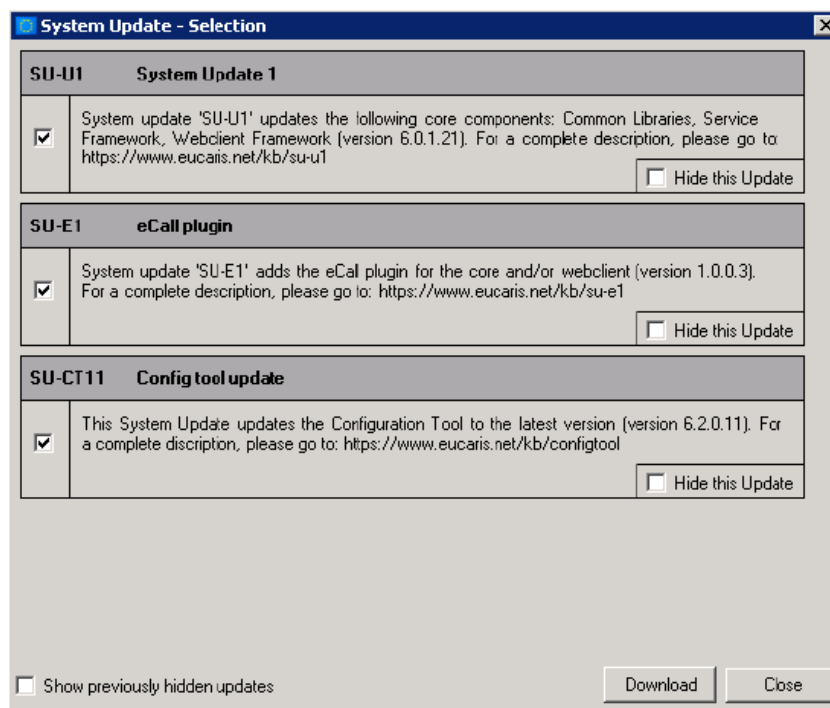
The system administrator is able to fully automatically execute the complete System Update. In case of separate roles for System-, Application- and Database administration it is possible to manually install some or all parts of the update. The actions a System Update performs are divided into the following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

- Database actions; all scripts which influence the structure or contents of the EUCARIS database
- 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.

5.3.2.3 Downloading System Updates

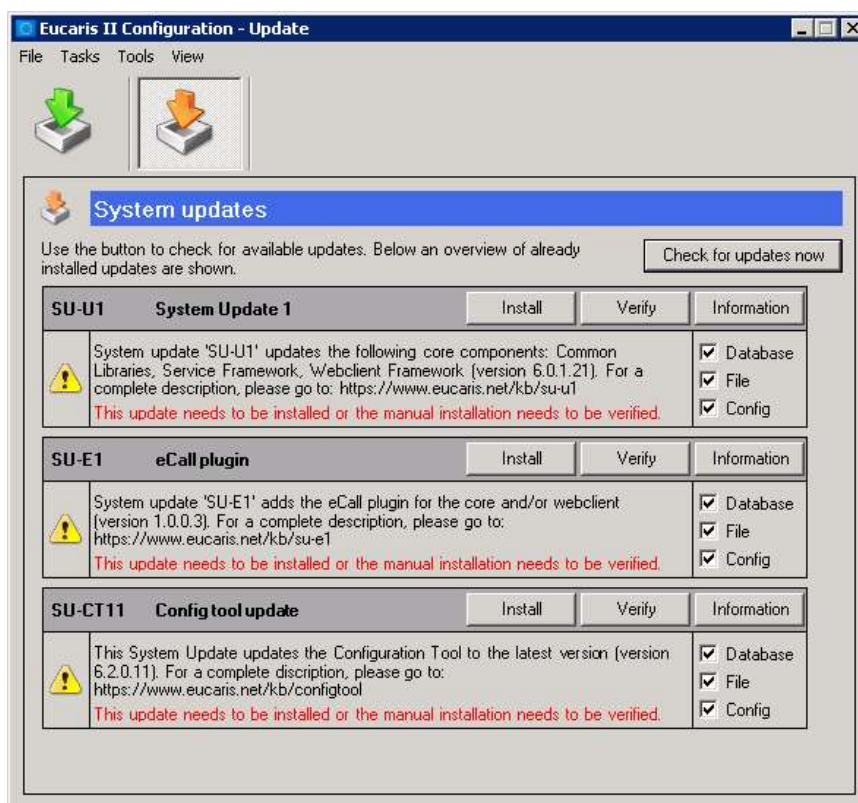
The availability of System Updates is announced via an e-mail from *EUCARIS Operations*, after which the administrators of the member states start the Configuration Tool in the Update mode, selects the System Update screen and press the button “Check for updates now”:



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”). Any available update of the core components (denoted with SU-Uxx, where xx is a sequence number) are considered to be mandatory and are required for any available extension (denoted with SU-Exx, where xx is a sequence number). 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 (Database, 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. When running a database script, the connection string configured in EUCARIS is being used to connect to the database. Note that when using MSSQL and the connection string uses integrated security, the logged in System Administrator’s account is used to connect to the database. Please make sure that this account has the correct privileges since the database script may also contain Data Definition Language (DDL) instructions, which adds, deletes or modifies the structure of the table(s).

Partly automatic:

Consider to manually run the database scripts if the configured database account does not have privileges to execute DDL instructions or 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.

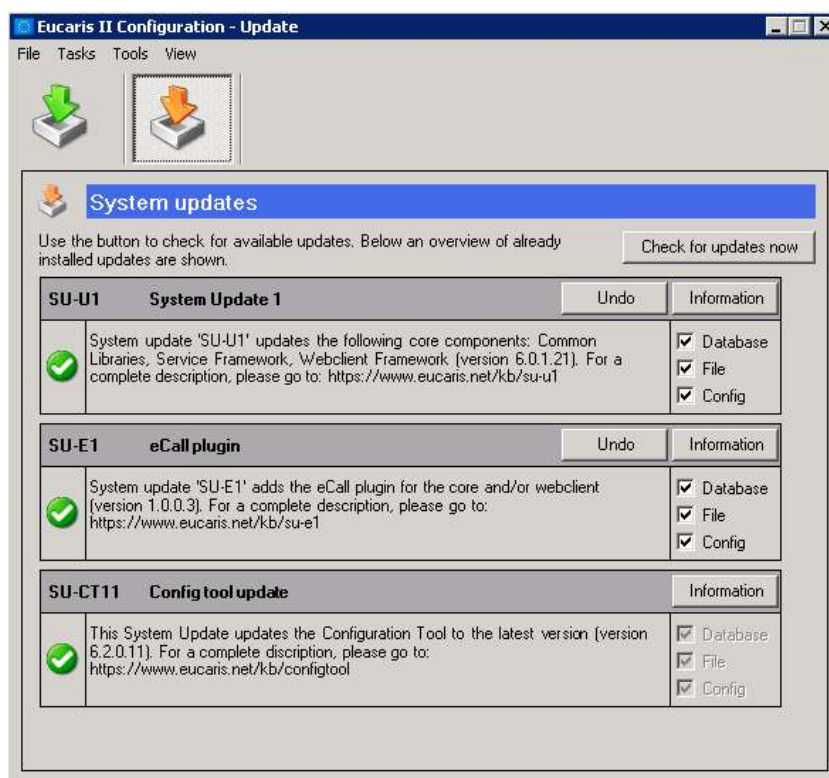
NOTE: When performing steps manually, the System Update can only successfully finish after all manual actions have been completed.

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. After clicking “Verify” the status of the Update will be set to either Installed (green tick) or Failed (red cross).

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.



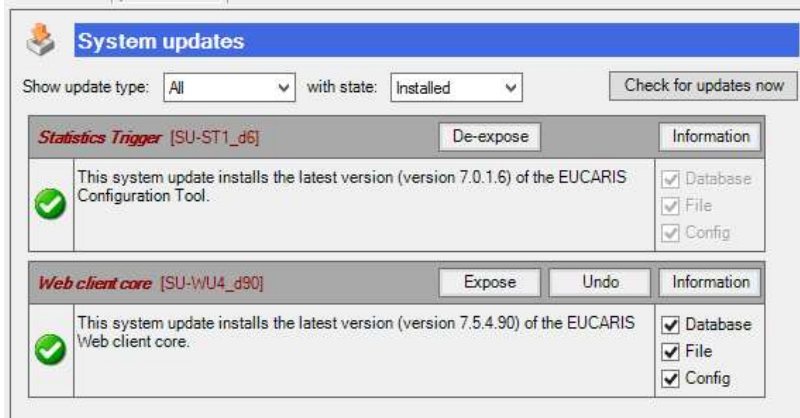
NOTE: It is not possible to undo a System Update that updates the Configuration Tool.

Expose and De-expose:

In case the machine that runs the configuration tool also runs an EUCARIS Update Service, the configuration tool can be used to make Updates available to clients connecting to this Update Service. An Update can only be exposed after it has been installed; the “Expose” button will appear.

The expose action uploads the Update to the Update Service, so that it can provide the update to its clients. Note that an exposed Update cannot be uninstalled.

De-exposing is the opposite; once an update is exposed, it can be made unavailable again for clients of the Update Service by clicking “De-expose”. Once it is de-exposed, the Update can be uninstalled again.



NOTE: The Expose and De-expose buttons are only available if Update.Url.Local is set in Eucaris.Configuration.exe.config.

5.4 Broker configuration mode

EUCARIS is used by a large number of European countries for the cross-border exchange of transport related information. EUCARIS contains a pluggable extension framework which can be used to extend the EUCARIS system with ERRU, RESPER and TACHO functionality. Member states within the EU can use these extensions to implement the electronic data exchange required by the ERRU, RESPER and TACHO regulations and rules. EUCARIS offers an interface to the European Commission’s central hub infrastructure which is implemented in the EUCARIS Broker. For more information regarding the functionality and configuration refer to document: **EUCARIS-ERRU-TACHO-RESPER-ODOCAR-and-ProDriveNet-integration.pdf**

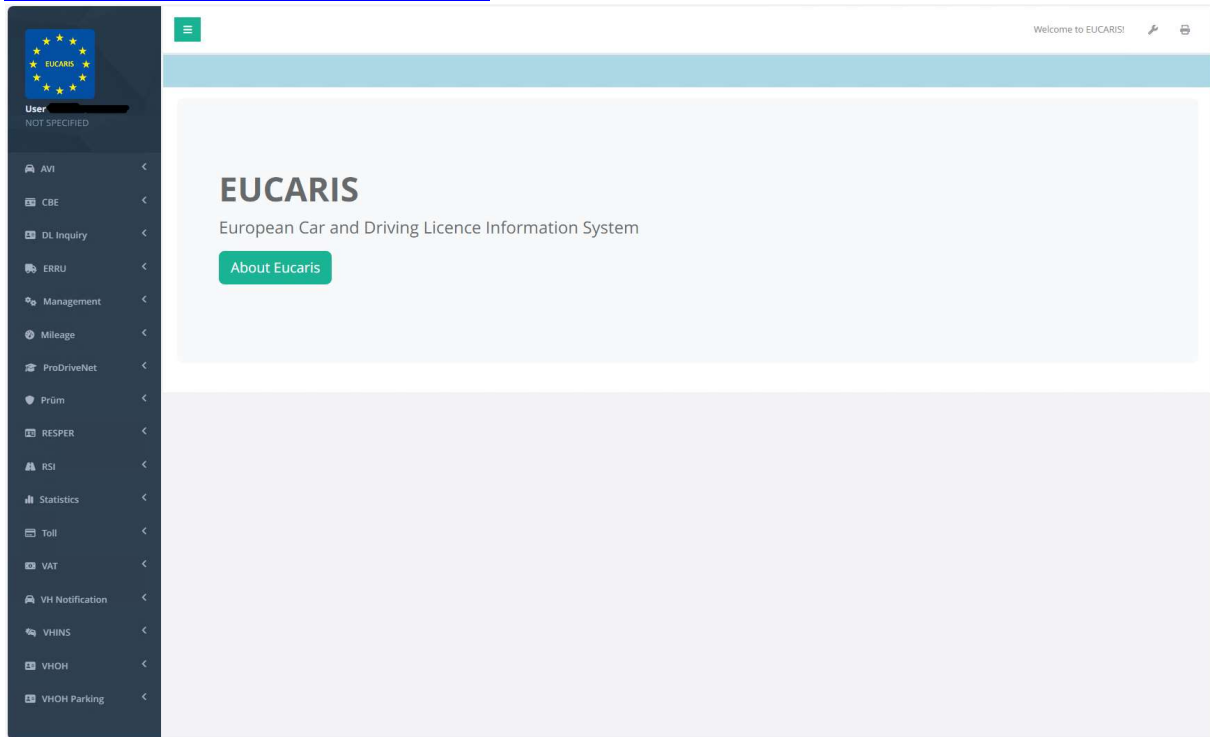
5.5 Installation test

After all configuration settings are done and **all the available System Updates are installed**, the member state is ready to use EUCARIS outbound to request information from other countries. To use EUCARIS inbound to provide information to other countries, it is necessary to develop custom software to retrieve information from the local register. Please refer to the ‘EUCARIS – Custom Development’ document for details on this subject.

5.5.1 Test EUCARIS Web Clients

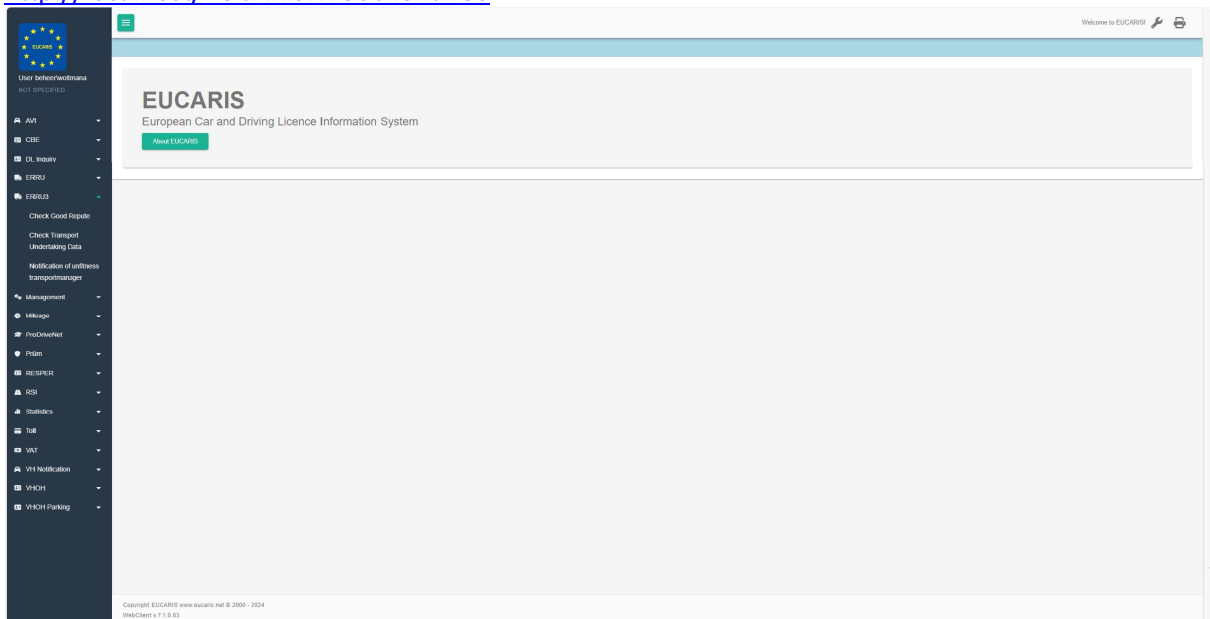
To verify correct installation of the Web Client v75 browse to the following URL:

<http://localhost/EUCARIS.WebClient.v75>



To verify correct installation of the Web Client v80 browse to the following URL:

<http://localhost/EUCARIS.WebClient.v80>



Note: The check on the Web Client V80 can only be done when the Web Client v80 is available for download in your Member State.

5.5.2 EUCARIS Test Tools

EUCARIS Operations has created two test tools to ease the development of the custom software and to verify correct configuration of EUCARIS. These tools are a stub, which mimics EUCARIS responses and the other tool is a test client, which allows sending requests to the stub. Please contact the EUCARIS support team by email on EUCARIS2help@rdw.nl for more information about these tools.

6. Security

One of the main added values of the EUCARIS application is the ability to securely transport messages to other member states. This chapter describes the security features used by EUCARIS and the security features available to local clients (the EUCARIS API), including how to configure and maintain these features. EUCARIS exposes 3 types of interfaces; the External-, the Public- and Internal interface. The available security features on each of the interfaces are described below.

6.1 Securing External Services

The communication between member states is handled using the External Services Interface. To ensure secure transfer of messages the following security measures are taken:

Dedicated channel

Connection can only be established via TESTA (Secured Trans European Services for Telematics between Administrations). TESTA is a private, highly-secured closed network for public administrations in Europe.

Encryption

EUCARIS uses Transport Layer Security (TLS) between member states so the data is encrypted between the EUCARIS instances of the Member States.

Signing

EUCARIS messages are signed using an X509 certificate. Each participating member state receives a unique certificate issued by *EUCARIS Operations*.

The External Services interface is (by default) terminating the TSL connection, though a member state might decide to terminate the TLS connection on an appliance within their network infrastructure.

The External Services interface is hosted by an IIS website which must accept anonymous requests. The External Services interface only accepts EUCARIS messages which are signed using a x509 certificate. The used x509 certificate is also used to identify the sender country and to check the authorisation. The link between certificate and member state is accomplished by configuration. Please refer to chapter **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** for more information. Authorisation is set on a country & service base. Authorisation can be set using configuration. Please refer to **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.** and **Fout! Verwijzingsbron niet gevonden. Fout! Verwijzingsbron niet gevonden.**

NOTE: Certificates and authorisation is centrally configured by EUCARIS Operations and updated through Configuration Updates. Please do not make manual changes unless absolutely required.

6.2 Securing Public Services

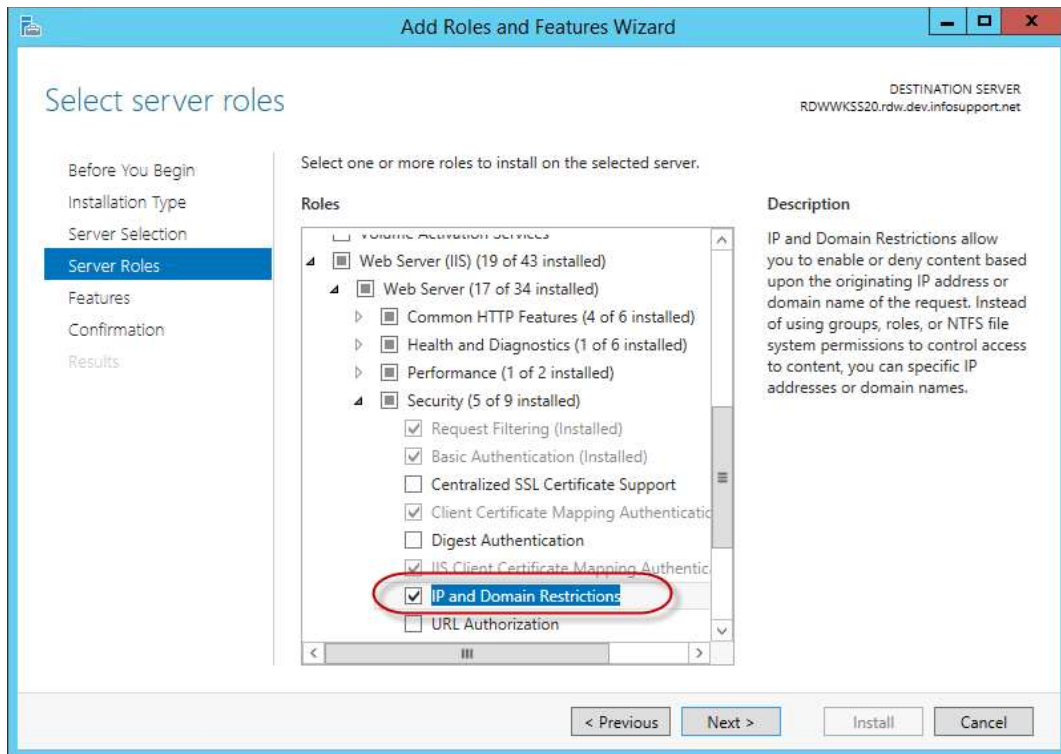
The EUCARIS Public Services is the interface available for clients (EUCARIS web client, custom client, legacy) to request other member states for both synchronous and asynchronous services. The Public Services interface is hosted by an IIS website which accept anonymous requests, and unsigned EUCARIS messages by default. The EUCARIS NPO must implement the appropriate security measures in order to prevent unauthorised access to the EUCARIS Public Services interface.

NOTE: It is the responsibility of the EUCARIS NPO to apply the appropriate and available security measures to prevent unauthorised access to the EUCARIS public services interface.

Below are some examples of possible and supported security measures.

6.2.1 IP and Domain Restrictions

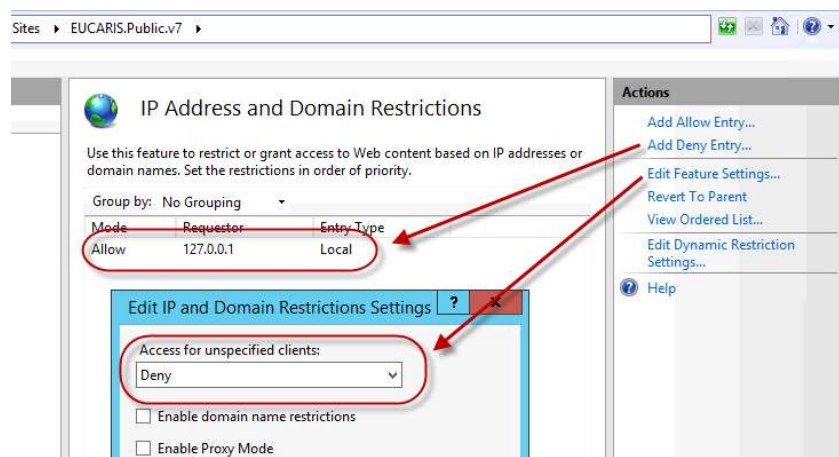
The Public Services can be secured by restricting access on originating IP (range) or domain. Add the Web Server feature “IP and Domain Restrictions” using the server’s Add Roles and Features Wizard:



After installation of the feature, select the “IP Address and Domain Restrictions” feature on the EUCARIS.Public website in the IIS Manager. Consult the documentation on [https://technet.microsoft.com/en-us/library/hh831785\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/hh831785(v=ws.11).aspx) or <https://www.iis.net/configreference/system.webserver/security/ipsecurity> for more information regarding this feature.

6.2.1.1 Configure the EUCARIS Web Client

For IP and Domain restrictions, no specific configuration is required for the EUCARIS Web Client. Assuming a default installation of EUCARIS and the EUCARIS Web Client, the Public Services can be restricted to the IP address of the localhost. Add to the restriction the IP addresses of the application server hosting your custom client:



6.2.2 Client Certificate Mapping

The Public Services can be secured by restricting access on supplied client certificate. Client Certificate Mapping Authentication uses client certificates to authenticate a user. A client certificate is a digital ID from a trusted source. IIS offers two types of authentication using client certificate mapping:

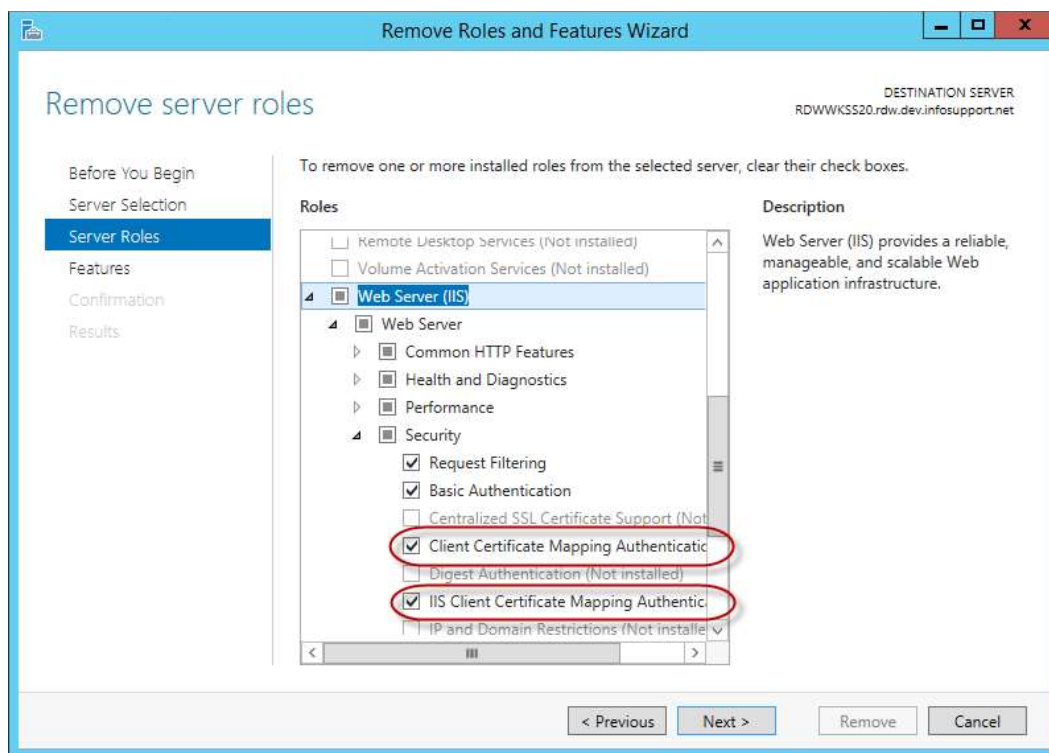
Client Certificate Mapping based on Active Directory

This type uses Active Directory to offer one-to-one certificate mappings across multiple web servers.

Client Certificate Mapping based on IIS Configuration

This type uses IIS to offer one-to-one or many-to-one certificate mappings. Native IIS mapping of certificates offers better performance.

Add the Web Server feature “Client Certificate Mapping Authentication” or “IIS Client Certificate Mapping Authentication” using the server’s Add Roles and Features Wizard:



After installation of the feature, follow the instructions in the following link. Please note that the Client Certificate Mapping configuration must be performed on site level (and not on application level!).

Client Certificate Mapping based on Active Directory:

<https://www.iis.net/configreference/system.webserver/security/authentication/clientcertificatemappingauthentication>

Client Certificate Mapping based on IIS Configuration:

<https://www.iis.net/configreference/system.webserver/security/authentication/iisclientcertificatemappingauthentication>.

6.3 Securing Internal Services

The EUCARIS Internal Services is the interface available for clients (EUCARIS web client, custom client, legacy) and the EUCARIS core application to request EUCARIS metadata. The Internal Services interface is hosted by an IIS website which accept anonymous requests, and unsigned EUCARIS messages by default. The EUCARIS NPO must implement the appropriate security measures in order to prevent unauthorised access to the EUCARIS Internal Services interface

NOTE: It is the responsibility of the EUCARIS NPO to apply the appropriate and available security measures to prevent unauthorised access to the EUCARIS internal services interface.

The security measures available are identical to the measures enlisted in the previous paragraph (Securing Public Services).

6.4 Support for Malware detection

EUCARIS Release SU-U22 (core version 7.0.22.x) supports the detection of malware by scanning of messages that can contain (file) attachments. The EUCARIS application does not contain any logic for scanning and detecting malware, but delegates these tasks to the operating system and the installed anti-malware application. This delegation is a two-stage procedure, consisting of:

- Temporarily write the attachment to a specified quarantine location, and reading one byte of the file to memory. This should trigger the On Access Scanner of the installed anti-malware application. If malware is detected, the outcome may differ per detected malware and/or product, but should be:
 - the file is moved to a quarantine location, or
 - access to the file is denied, or
 - the file is deleted.
- If the file is still available on the temporary location, EUCARIS will ask the *Microsoft Windows Attachment Manager*¹ if the file is trusted.

NOTE: Make sure to install an anti-malware application able to perform disk 'On Access Scan'. The first step will yield no result when no anti-malware application is installed, or the application is not able to perform On Access Scans.

NOTE: Make sure to configure the anti-malware application to remove infected files, and not try to clean them. For more details refer to paragraph 7.3.

NOTE: A Member State is responsible for the purchase, installation and regular maintenance of an anti-malware application and/or security policies. EUCARIS will not include an anti-malware application in its installation package.

If the result of one of these steps is that the file cannot be trusted, EUCARIS will not accept nor store the file. The specific process and response after rejecting a message due to detected malware is depending per installed extension. Currently the following extensions support malware detection:

- RESPER extension (release SU-E89, version 7.0.89.x and higher)
- Salzburg extension (release SU-E88, version 7.0.88.x and higher)

EUCARIS Supports malware detection for both inbound and outbound messages. Inbound messages (messages received from other member states) are scanned after the message-signing and authorisation has been checked, and the message is valid. Outbound messages (messages received from local clients) are scanned after the authorisation has been checked and the message is valid.

NOTE: It is advised to enable both inbound and outbound scanning of attachments.

Malware scanning can be switched on or off, per extension that supports the functionality, independently. If virus scanning is switched on for 1 or more extensions, then it is required to also set general configuration. Note that the malware detection functionality is not available for the generic File Transfer functionality of EUCARIS. The following paragraphs describes the configuration options for the malware detection functionality.

¹ The Microsoft Windows Attachment Manager integral part of the operating system. More info: <https://support.microsoft.com/en-us/kb/883260>

6.4.1 General configuration

The general configuration is set in the EUCARIS configuration file: "indes.properties.config", stored in the [EUCARIS Application Root folder]\Configuration folder.

6.4.1.1 Malware scan directory

It is required to configure a location where EUCARIS can temporary store the received attachments, in order to read a single byte and in order to trigger an On Access Scanner. EUCARIS will create a random directory on this location per received message, since each message might contain multiple attachments. EUCARIS automatically deletes the files and directories once it is done processing.

Key: Indes.Core.MalwareScanDirectory

Value: The folder which will be used to temporary store attachments. The defined folder must exist, and will be created by the Core System Update.

Default value: C:\ProgramData\EUCARIS\Temporary files\MalwareScan\

Opmerking: Default = C:\Temp\EUCARIS\MalwareScan volgens config. Folder bestaat niet op die locatie, maar wel op C:\ProgramData\EUCARIS\Temporary files\MalwareScan\

Example: `<add key="Indes.Core.MalwareScanDirectory" value="C:\ProgramData\EUCARIS\Temporary files\MalwareScan\" />`

6.4.1.2 Malware scan delay

In order to give the On Access Scanner enough time to be triggered it is possible to incorporate a small delay. Usually a delay of 600 milliseconds (0,6 second) will be sufficient, but that might differ per anti-malware application.

Key: Indes.Core.MalwareScanDelayInMilliseconds

Value: any value in milliseconds.

Default value: 600

Example: `<add key="Indes.Core.MalwareScanDelayInMilliseconds" value="600" />`

6.4.2 Configuration per extension

The configuration file of an extension can be found at the following location: [EUCARIS Application Root folder]\Configuration folder\Plugins\EUCARIS.Services.Plugin.[ServiceName].config.

6.4.2.1 Configure outbound malware detection

Enable this feature to be able to scan outbound requests containing attachments (messages from a local client to another member state)

Key: MalwareScanSendEnabled

Value: true or false

Default value: depending on extension.

Example: `<add key="MalwareScanSendEnabled" value="true" />`

6.4.2.2 Configure inbound malware detection

Enable this feature to be able to scan inbound requests containing attachments (messages from another member state)

Key: MalwareScanReceiveEnabled

Value: true or false

Default value: depending on extension.

Example: `<add key="MalwareScanReceiveEnabled" value="true" />`

6.4.3 Malware application specific configuration

The EUCARIS malware detection functionality depends on the installed anti-malware application and its On Access Scanning (OAS) abilities. If AOS is disabled by design, then configure the application to perform OAS on the Malware scan directory configured in paragraph 7.1.1. Also make sure that the default action is set to “remove file”², or “deny access”² and not “clean file”². **EUCARIS will not detect if a file gets cleaned, and it will not use the cleaned file for the transfer. This might possible result in a transfer of an infected file.**

EUCARIS uses a small external application to read one single byte from the application. This application is started as a new process, and if possible, should be configured as “High Risk”² process within your anti-malware application. This application is located at the following location:

```
[EUCARIS Application root]\Web\Services\PublicAndExternal\bin\EUCARIS.Core.Utils.FileRead.exe
```

NOTE: Most anti-malware applications will try to clean the file first by default. Make sure to check and reconfigure this behaviour!

6.4.4 Malware detected

EUCARIS will report the detection of malware in the Windows Application Eventlog as a warning. The following errors and/or warnings will occur:

6.4.4.1 Inbound

If inbound malware detection is enabled, and malware is detected, the following warning will be logged:

```
Windows or the installed Malware scanner have detected malware which was sent using EUCARIS from country D.  
Service: RSPSecureMessage.  
Business case ID: 'DD88-454-1'.  
The message is not stored and a NACK/NOK is sent to the sender country.
```

```
Additional info:  
D:\Temp\MalwareScan\tonb4byj.3fy\Final_Decision.pdf: Unauthorized access. Probably OAS. Remove.
```

The sent message is not accepted, and no messages are stored. The sender will be notified by a ‘not acknowledge’ sent by the recipient country, containing the specified code for ‘malware detected’. No further action is required on the EUCARIS server.

6.4.4.2 Outbound

If the recipient country has inbound malware detection enabled, and detects malware in the sent attachments, the following warning will be logged:

```
File 38541' (file name:'AC_document', case id:'DD88-454-1') for service 'RSPSecureMessage' to country 'D' is deleted (virus or malware detected by member state).
```

² Terms might differ per anti-malware application. Please refer to the manual of your anti-malware application.

EUCARIS has deleted the possible infected message from the upload queue in order to maintain the integrity of the system. The client will be notified by a 'not acknowledge' sent by the recipient country, containing the specified code for 'malware detected'. No further action is required on the EUCARIS server.

If the sender country has outbound malware detection enabled, and detects malware in the sent attachments when a client uploads a message, the following error will be logged:

virus or malware detected in one or more attachments from a client upload for service RSPSecureMessage
Additional info:
D:\Temp\MalwareScan\zzkzxdd1.sns\Final_Decision.PDF: Unauthorized access. Probably OAS. Remove.

The client is directly notified by a SOAP-exception raised by the EUCARIS service. No further action is required on the EUCARIS server.

6.5 Setting up SSL for web client

The web client connects to EUCARIS instance through three different endpoints:

- ExtendedClientLogic
- GenericService
- GenericAsyncService

The following instructions explain how to setup the usage of SSL for the webclient. This involves some actions on both the EUCARIS and the web client installation. In short the steps are:

EUCARIS

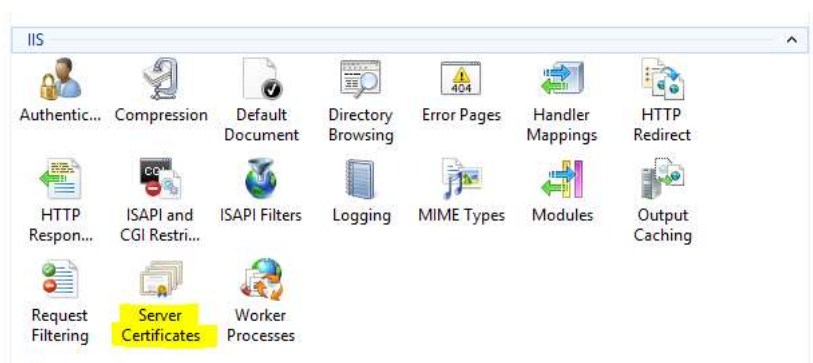
- Make sure there is a certificate (with private key) available that is hostname of the server
- Configure IIS:
 - Add certificate to IIS server certificates
 - Add binding for HTTPS and associate a certificate with it
- Update web.config of web services

Web client

- Update web.config of the web client

6.5.1 IIS configuration - Certificate

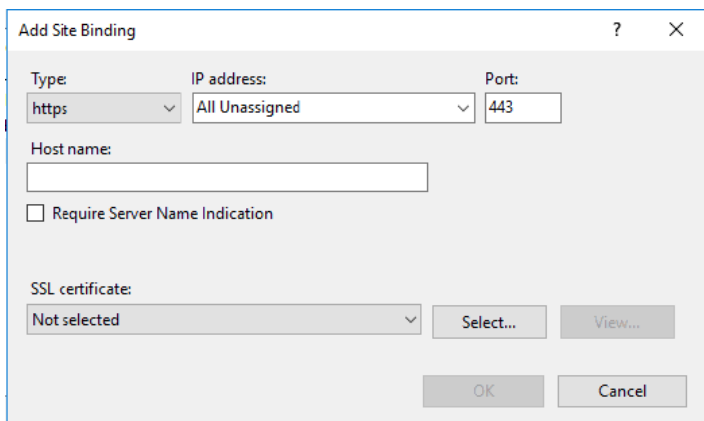
The creation of the certificate is out of scope for this manual; we simply assume it to be available. To install it, in IIS navigate to the server in the left pane and go the item Server Certificates:



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.

6.5.2 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 6.5.1

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

6.5.3 Web.config – EUCARIS 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.

6.5.4 Web.config – web 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 6.5.2.

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 6.5.2.

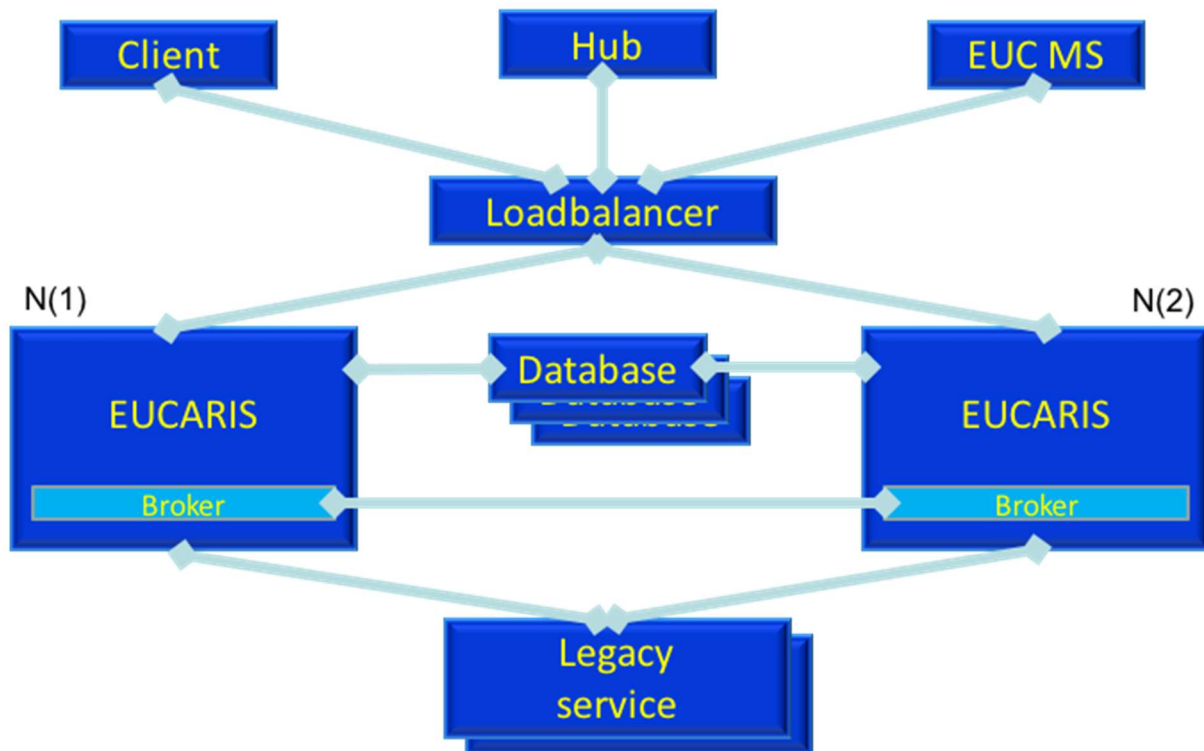
Repeat the last two replacements for the other two bindings.

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

7. Performance and scaling

EUCARIS is designed to be scaled horizontally in order to increase reliability, performance and availability using load-balancing. The following requirements apply:

1. All EUCARIS installations (also known as EUCARIS instances) must be identical;
 - All instances share the same configuration and certificate,
2. The database must be logically one entity;
 - All instances must use the same database, or must be able to connect to the same logical database using an identical connection string,
3. The legacy services must be accessible from all instances using the same URL;
 - Since the configuration and database is shared, the Legacy Services endpoints are the same for all instances.
4. The EUCARIS Broker must be able to contact all other instances of EUCARIS using a TCP connection;
 - The EUCARIS Broker must be able to exchange received messages between all instances of EUCARIS in order to make a correct correlation between asynchronous messages received from the hub.



NOTE: For reliable functionality, maintainability and creating statistics it is of great importance to have all EUCARIS instances connected to the same database in the production environment. Having multiple (not synchronized or clustered) databases in a production environment may lead to unexpected results or even loss of service.

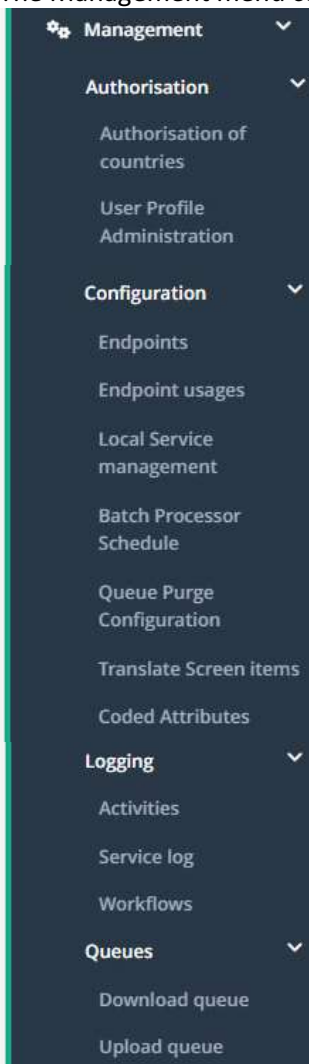
8. Operation

This chapter will discuss operational details while using EUCARIS, it is divided into a description about how to administer the EUCARIS installation, how to maintain the EUCARIS installation and how to outscale the EUCARIS installation.

8.1 Management

If a user is either a local functional administrator or a local system administrator, the Management menu is available in the EUCARIS Web Client. The Management menu can contain the following items depending on the role of the logged on user and the core version of EUCARIS.

The Management menu contains the following items:



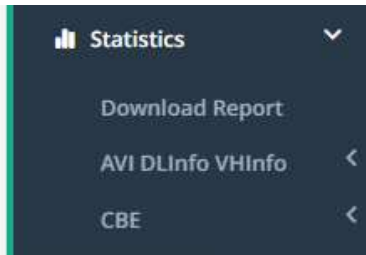
For each of the items in this menu there are manuals available on www.eucaris.net.

8.2 Statistics

EUCARIS supports the possibility to generate custom statistical reports, for services where statistical reporting is required. Currently there are 3 types of statistics processes:

- Toll-EETS Statistics (to be found via “Download Report”)
- AVI, VHInfo and DLInfo Statistics
- CBE Statistics

The Statistics menu in the Web Client contains the following items:



For each of the items in this menu there are manuals available on www.eucaris.net.

8.3 Maintenance

In regards to maintaining the EUCARIS installation some final remarks are given regarding the database, backups and the configuration & system updates.

8.3.1 Database

The EUCARIS database is mainly used for storing configuration data for EUCARIS. The only tables each member state has to maintain actively is the *Service Log*, the *File Transfer Upload Queue* and the *File Transfer Download Queue* table. These tables will automatically grow when using EUCARIS and needs to be purged on a regular basis. This purging can be done by using the Configuration Tool (please refer to paragraph 5.2.10.4) for Service Log data and the Queue Purge (please refer to paragraph **Fout! Verwijzingsbron niet gevonden.**) for File Transfer Queue data. Depending on data protection and retention agreements made per treaty, the Service Log must be purged regularly.

More information on database management can be found at the EUCARIS.net knowledgebase at <https://www.EUCARIS.net/kb/database-management>

8.3.2 Backup

We advise to make backups of your server and database on a regular basis. Please refer to the documentation of your database and operating system on how to create proper backups.

8.3.3 Configuration updates

Whenever a new member state is added or a member state changes their services or its address all member states will be notified there is a new configuration update available. It is advised to download and install this update as soon as possible to guarantee trouble free functioning. Please refer to paragraph 5.3 for more detailed information.



9. 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>

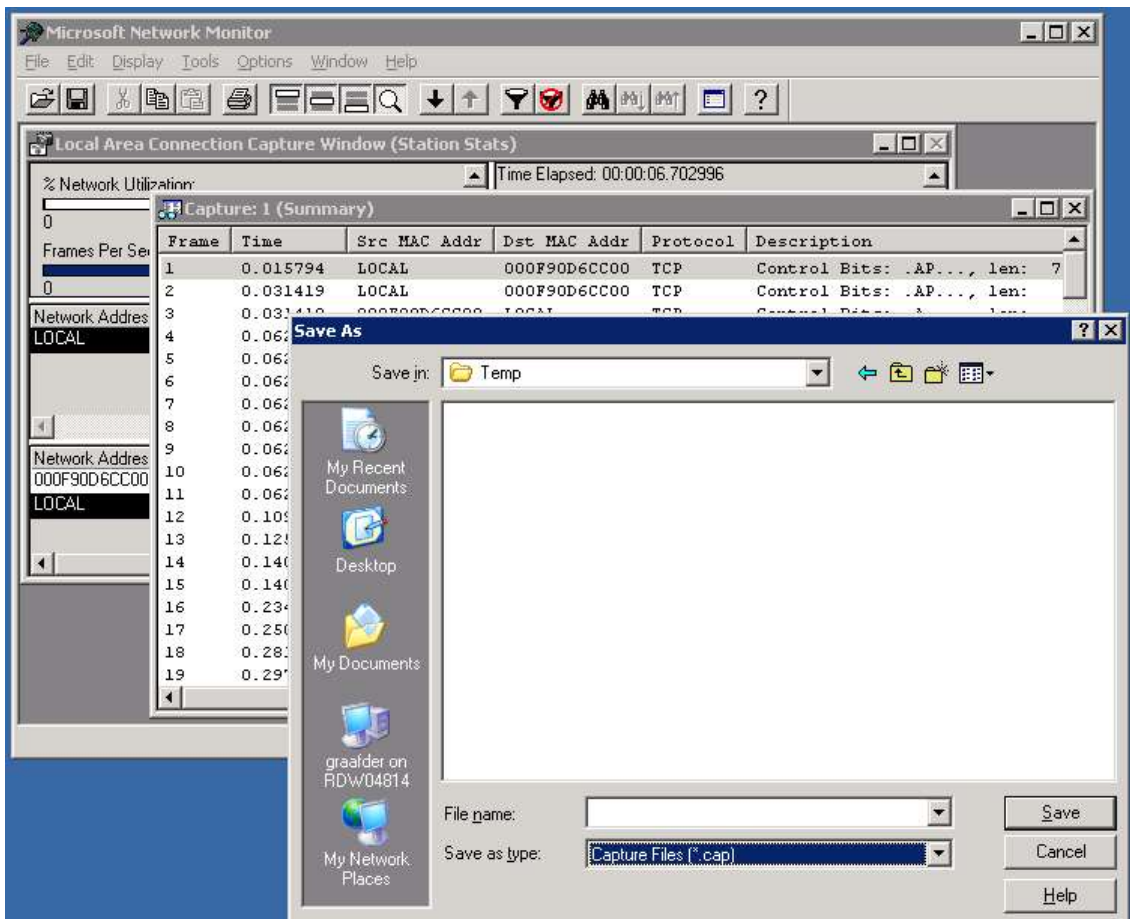
This chapter will further describe tips on troubleshooting network problems, certificate issues, problems related to the database, problems with the EUCARIS application and issues with IIS.

9.1 Network

Network problems can be analysed in multiple ways. The first one is doing a network analysis using the Configuration Tool, as described in chapter 5. Another method of troubleshooting network problems is by starting a telnet session using the command line tool. After starting the telnet session, you can try the following command and use the output for further troubleshooting:

```
>> telnet eucop.nl.eucaris.testa.eu 443 for the production environment or  
>> telnet eucop.nl.eucaris-acc.testa.eu 443 for the test and acceptance environment.
```

Another troubleshooting method is to make a network trace, while trying to connect to other member states, to see where the problem occurs. Some of the tools that can be used to create a network trace are the Microsoft Network Monitor or WireShark. The trace has to be saved in *.cap format, which can be send to EUCARIS2help@rdw.nl when help is needed to solve the problem.



9.2 Certificates

Although the Configuration Tool is able to handle most of the problems that can occur using the EUCARIS certificates, there might still be situations where the Configuration Tool is not able to fix the issues. The Configuration Tool is able to analyse the required certificates for their validity and verify access to the Certificate Revocation List. If problems occur due to the Certificate Revocation List not being accessible, the EUCARIS installation is not able to run correctly. Another method to check or install certificates is using the Microsoft Management Console as described in detail in the appendix.

9.3 Database

When the script that creates the database or the script that creates the user rights on the database is operated wrongly, sometimes a situation may occur in which the problem is hard to resolve. The easiest solution in this case is to completely uninstall the database and reinstall it according to the steps provided in chapter 4.1.1 and the installation manual of the chosen database.

9.4 Application

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

9.4.1 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. These groups and their rights are documented in paragraph **Fout! Verwijzingsbron niet gevonden..** Local users can be setup with the Configuration Tool and domain users have to be added manually to the groups.

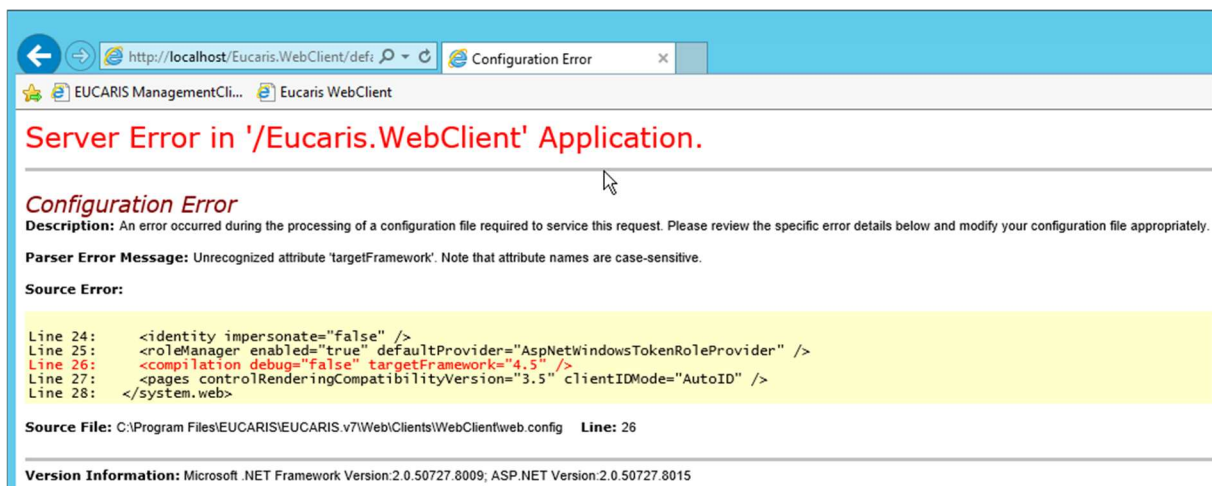
The user does not have a user profile in the database.

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.

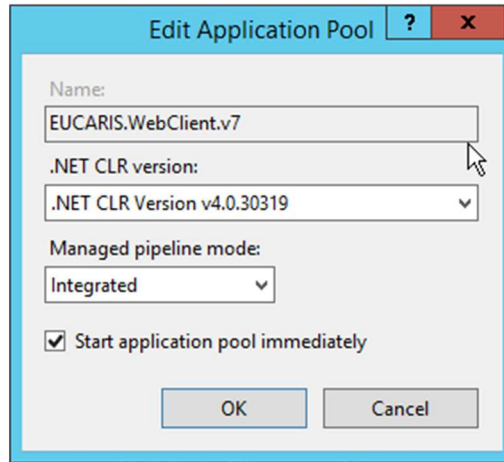
If all configuration settings described above are correct, the problem is probably caused by the database. Please refer to chapter 9.3 on how to solve that problem.

9.4.2 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 ? X

Name:
EUCARIS.WebClient.v7

.NET CLR version:
.NET CLR Version v4.0.30319

Managed pipeline mode:
Integrated

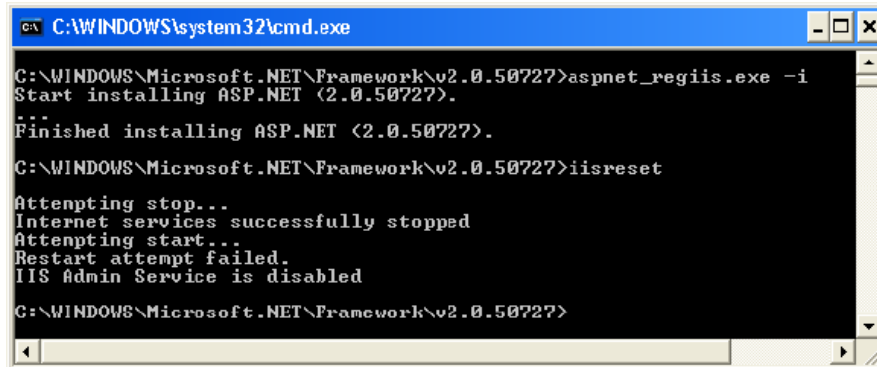
Start application pool immediately

OK Cancel

9.5 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:

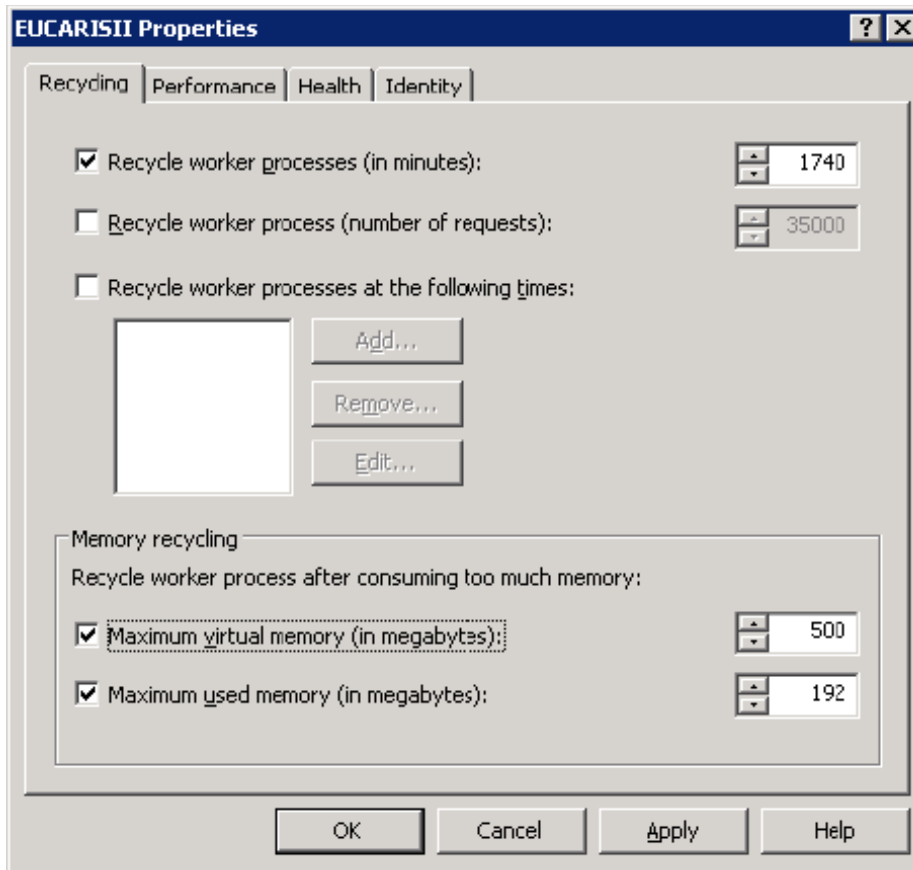
'drive:\WINDOWS\Microsoft.NET\Framework64\v4.0.30319\aspnet_regiis.exe -i



```
C:\WINDOWS\system32\cmd.exe
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>aspnet_regiis.exe -i
Start installing ASP.NET (2.0.50727).
...
Finished installing ASP.NET (2.0.50727).
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>iisreset
Attempting stop...
Internet services successfully stopped
Attempting start...
Restart attempt failed.
IIS Admin Service is disabled
C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727>
```

9.5.1 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

10. 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.

10.1 How To: Adding Root and Intermediate certificates via MMC

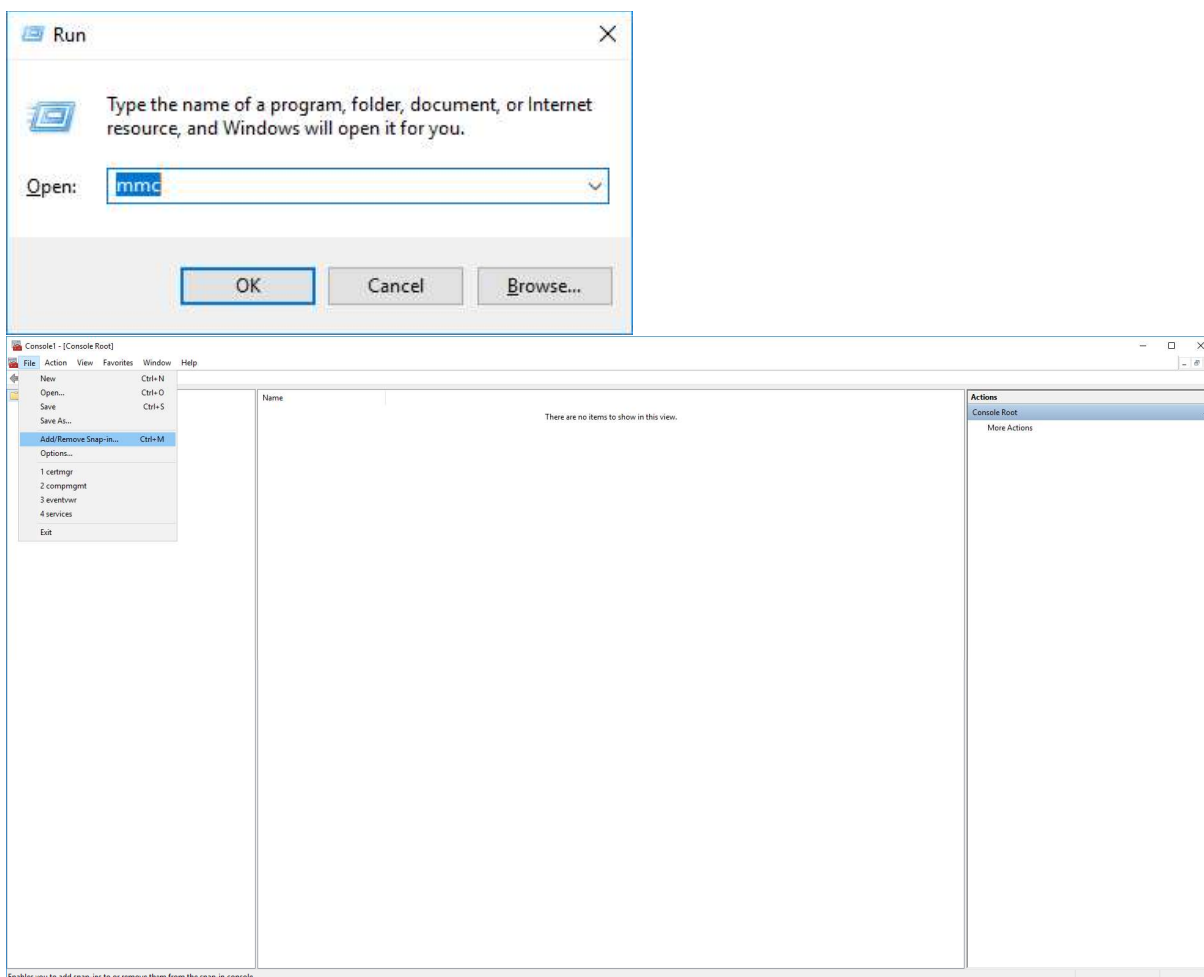
Files to have on hand: Root and/or Intermediate certificate files. If you're unsure which to get or which is which, please contact us at EUCARIS2help@rdw.nl

Root and Intermediate Certificate installation via MMC

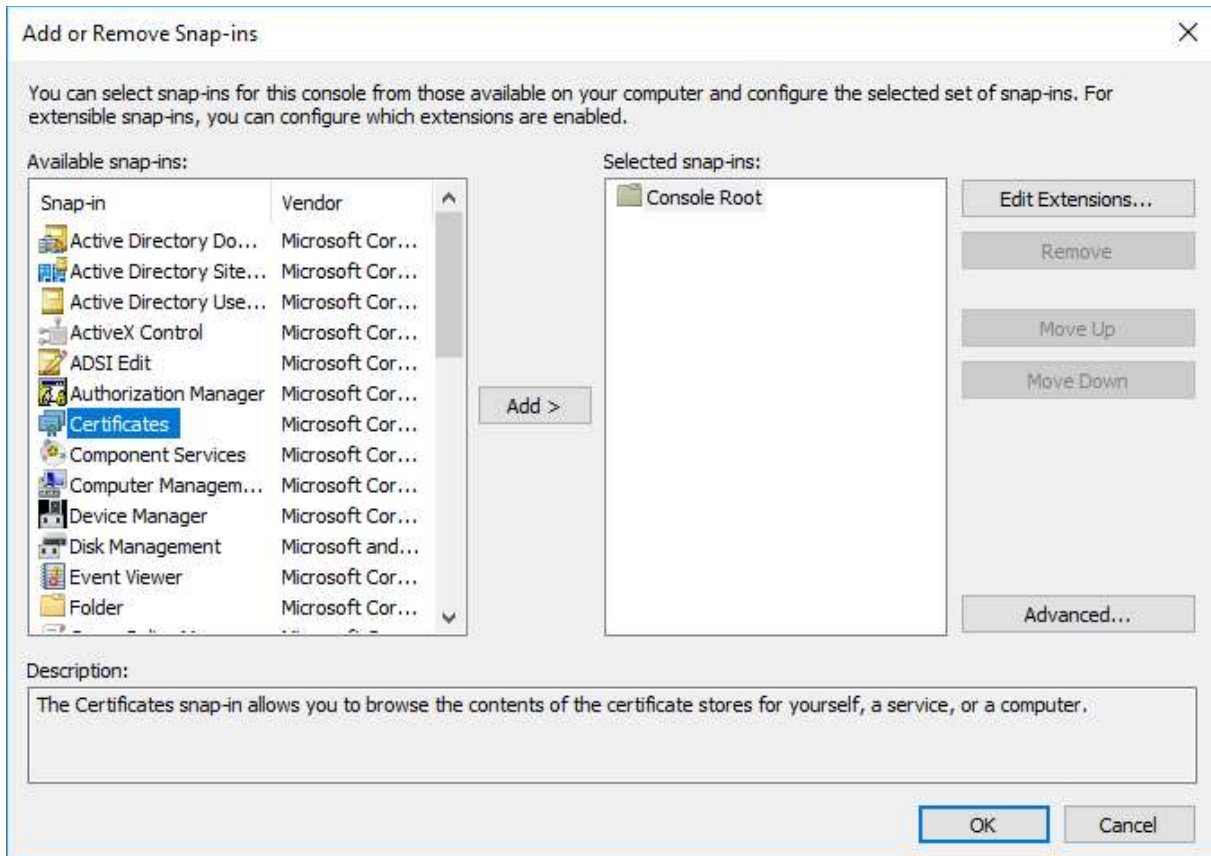
1. Open up the Microsoft Management Console (MMC)

Start -> Run -> Type "mmc" (without quotes) and Click 'OK' or hit Enter on your keyboard.

2. Open 'Add/Remove Snap-in' Window

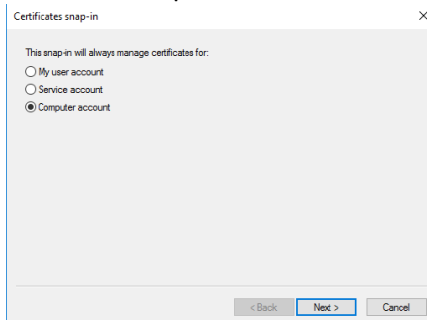


File -> Add/Remove Snap-in 3. Add the Certificates Snap-in



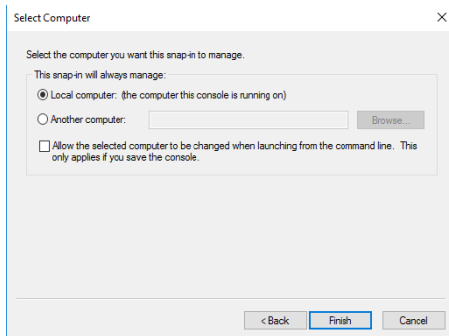
Click 'Add'.

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



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

5. 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.

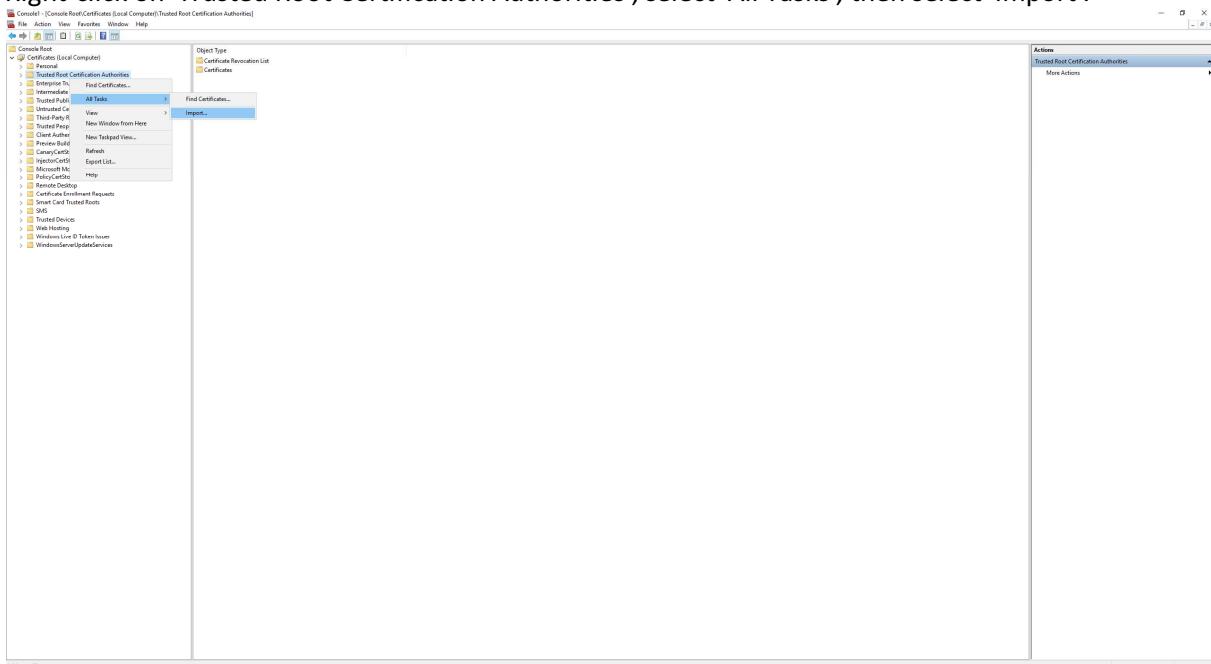
Install/Import the Root and Intermediates Certificate

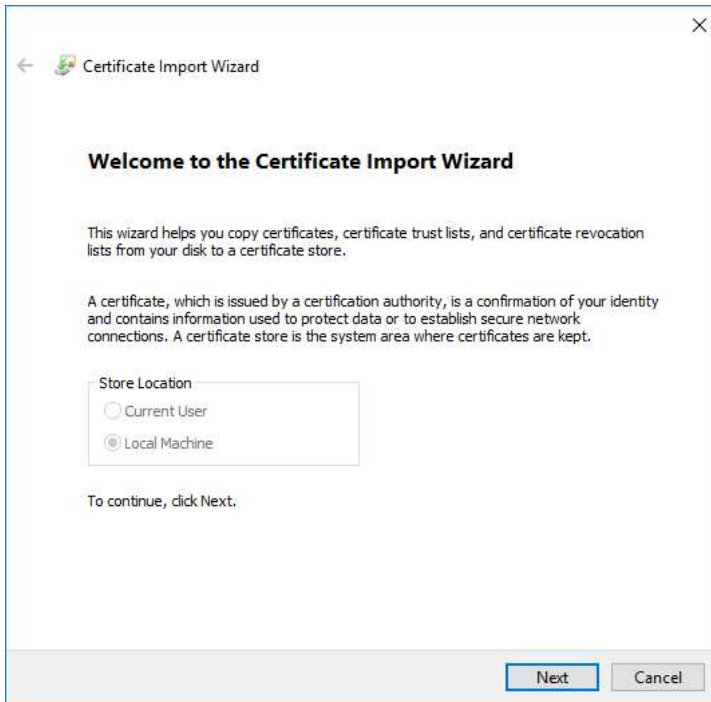
* Procedure for ROOT certificates:

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

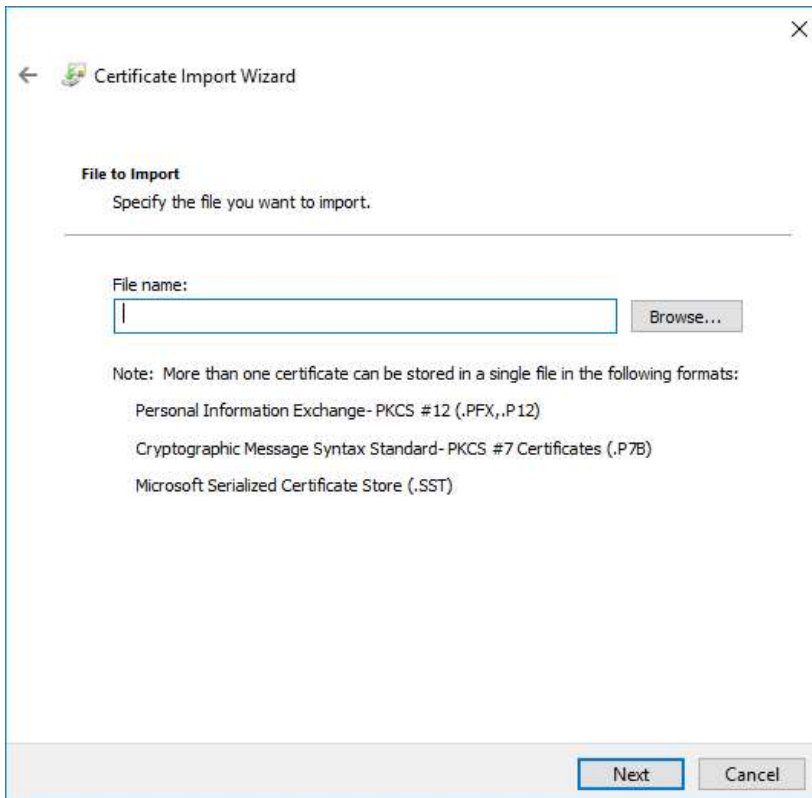
2. Import the Root Certificate

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





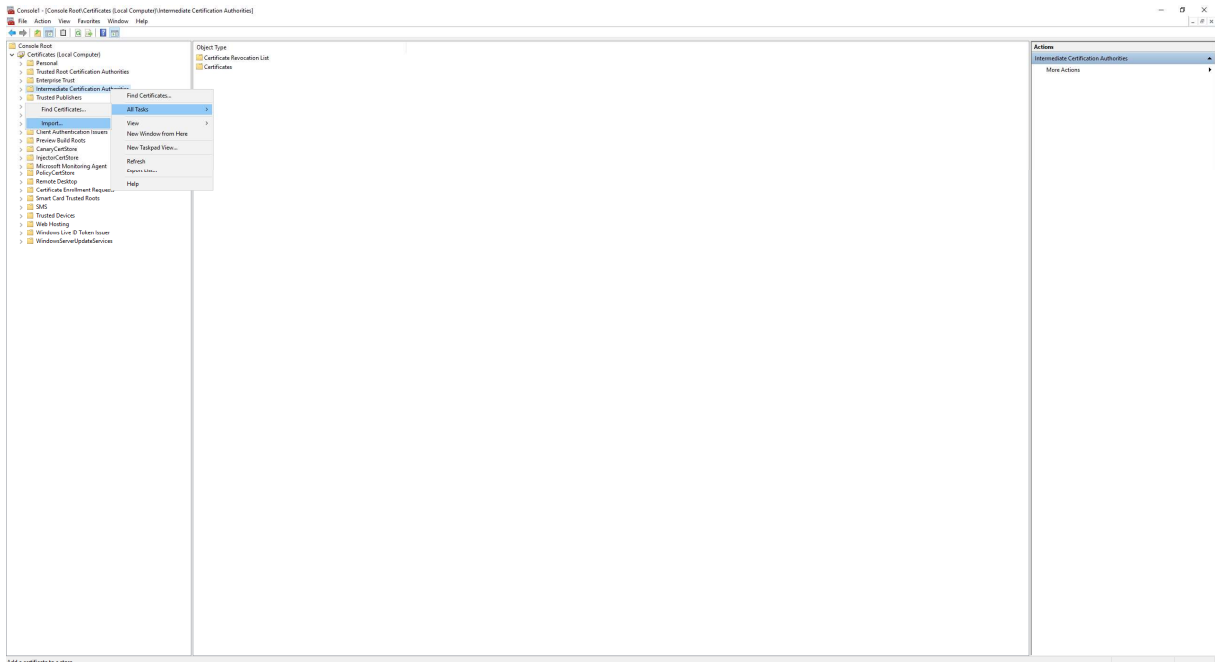
Click 'Next'.



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

*** Procedure for Intermediate certificates:**

2. 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 through the EUCARIS Configuration Tool.

10.2 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.

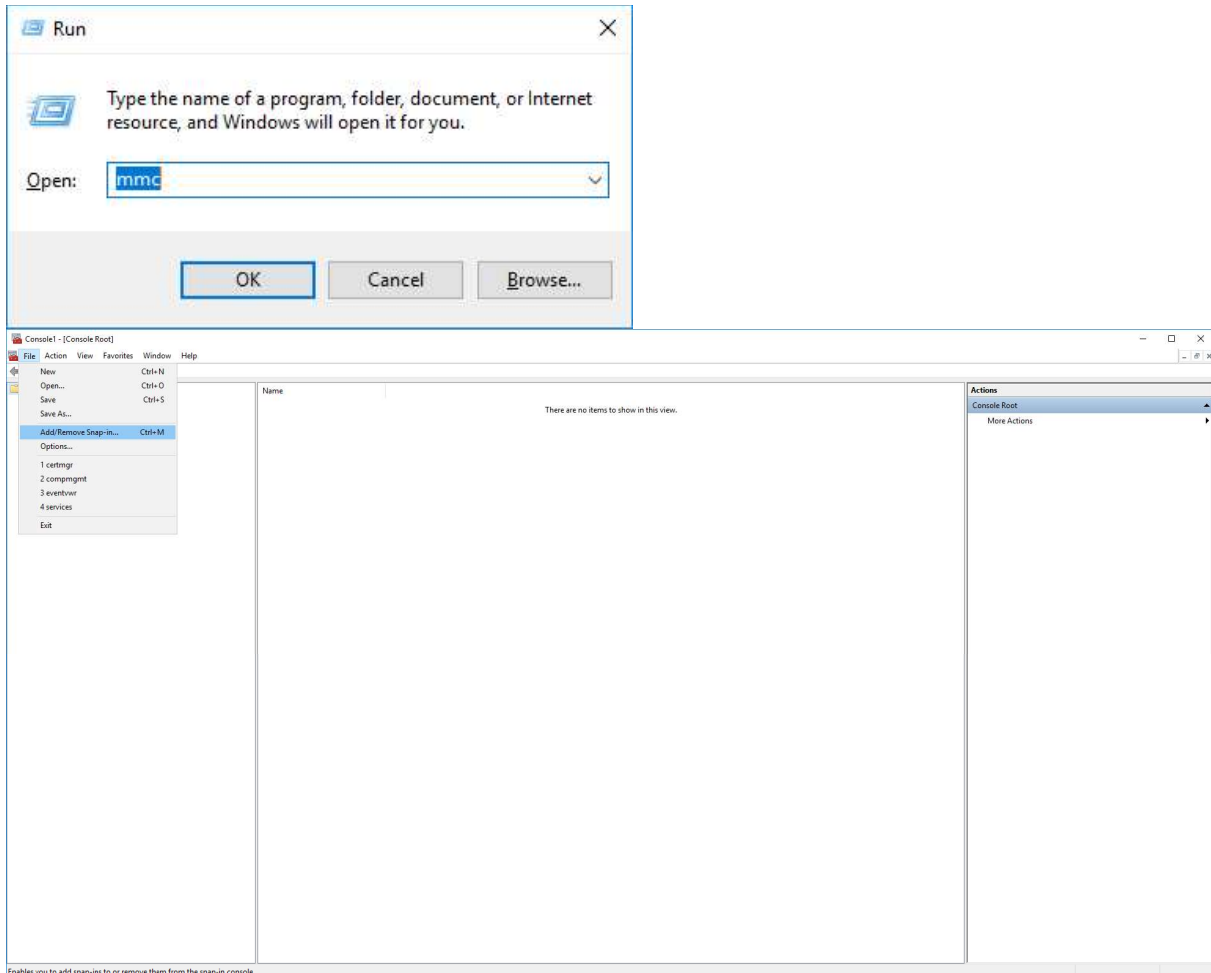
10.3 How To: Manually delete a certificate from the EUCARIS server

Certificates expires after time. To prevent that all expired certificates are still on the EUCARIS server, the certificates can be deleted by following these steps:

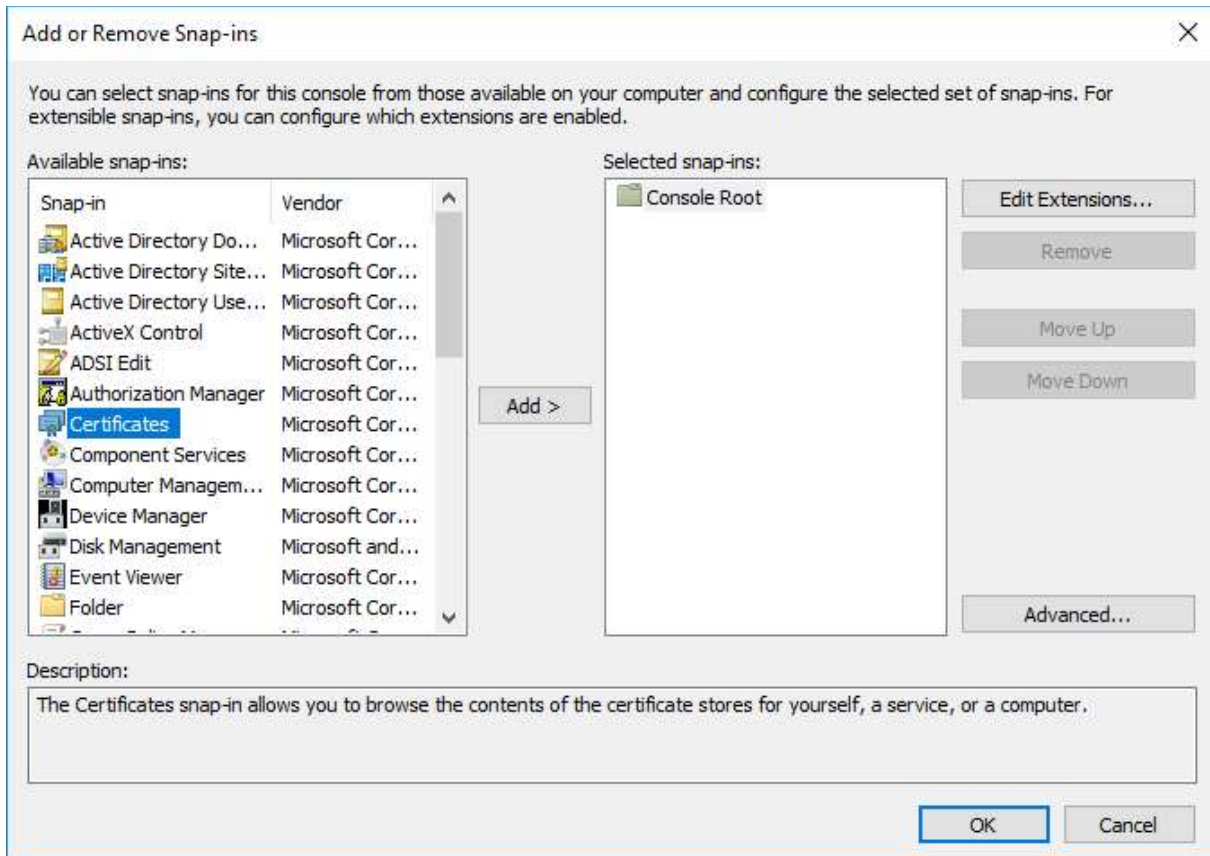
Open up the Microsoft Management Console (MMC)

Start -> Run -> Type "mmc" (without quotes) and Click 'OK' or hit Enter on your keyboard.

2. Open 'Add/Remove Snap-in' Window

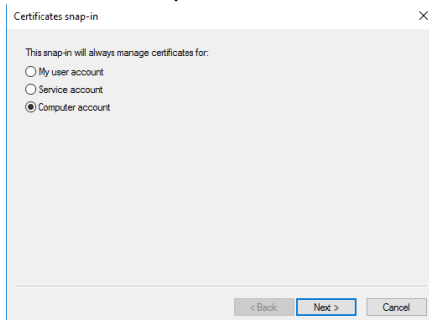


File -> Add/Remove Snap-in 3. Add the Certificates Snap-in



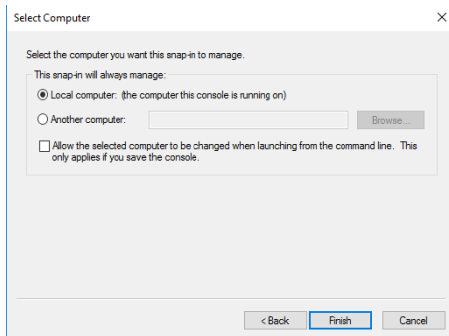
Click 'Add'.

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'

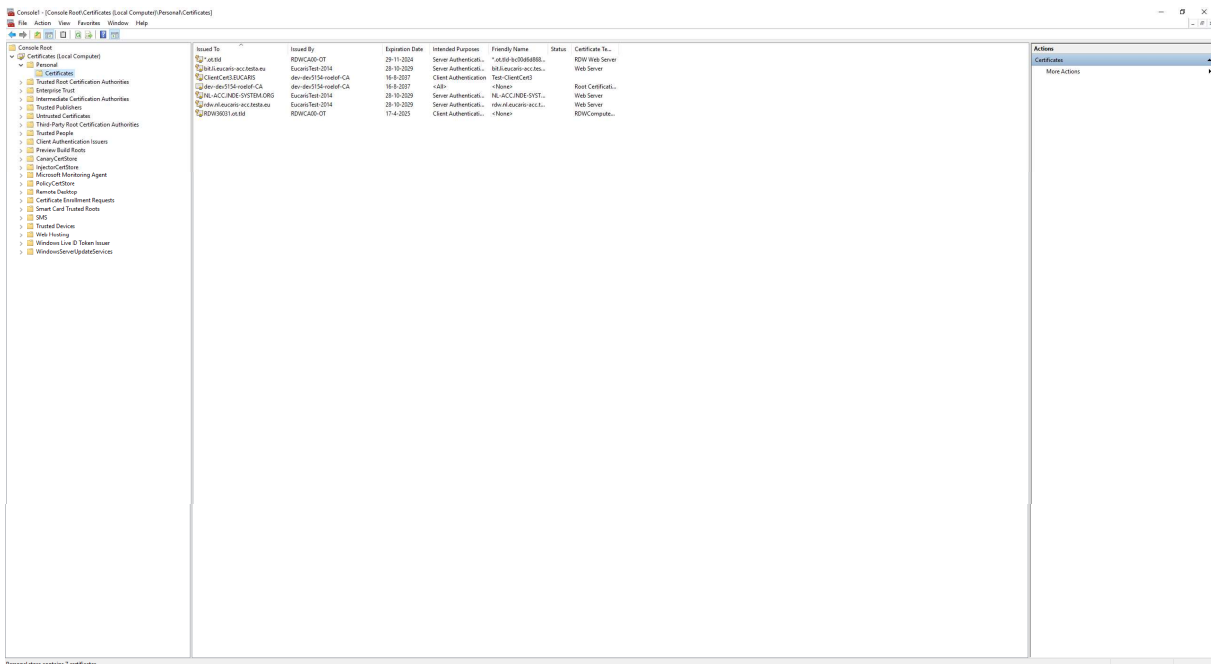


6. Close the 'Add Standalone Snap-in' window and click 'OK' in the 'Add/Remove Snap-in' Window.
7. Will now be returned to the MMC.

Delete a Certificate

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

2. Select 'Personal' and then 'Certificates'



3. Select the certificate that needs to be deleted, press the right mouse button and select 'Delete' from the menu.



EUCARIS - Installation and Operation Manual

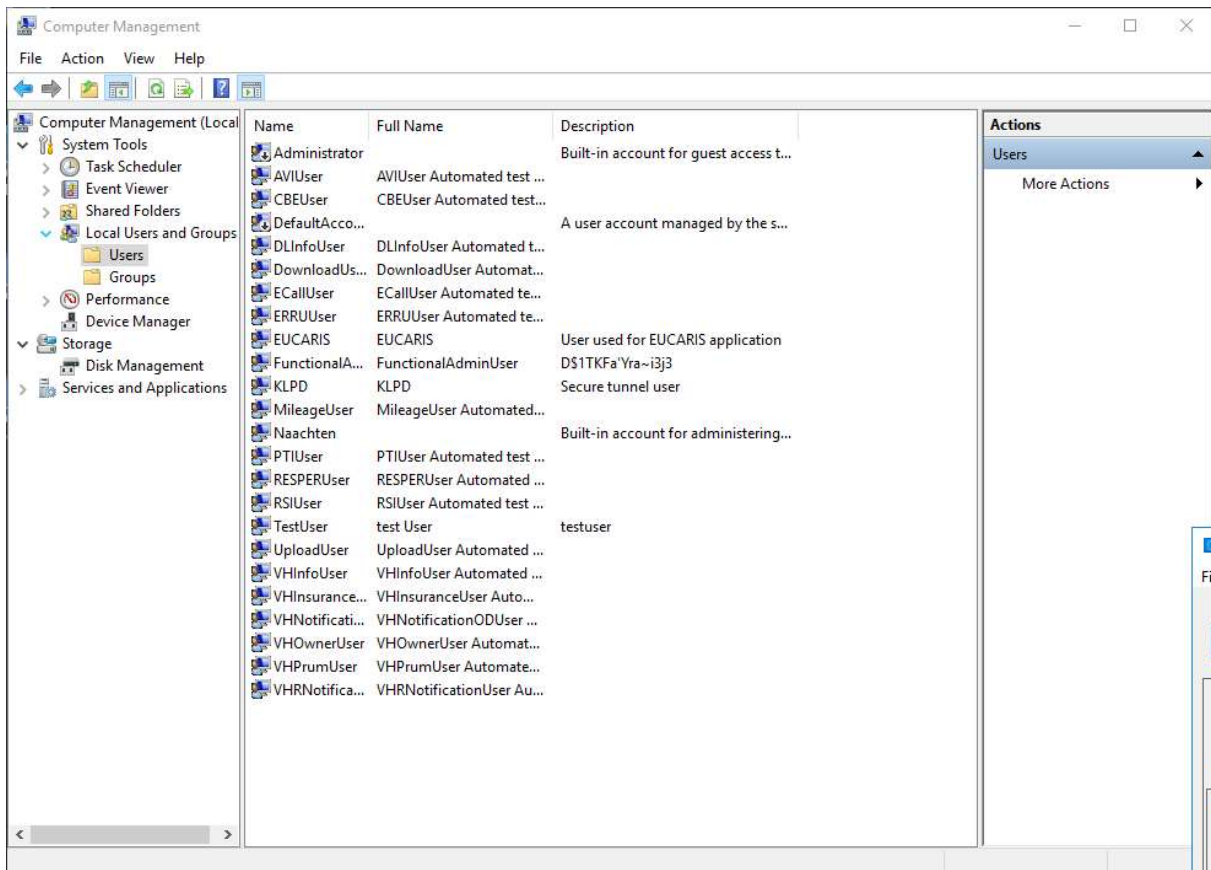
The screenshot shows the Windows Certificate console window. The title bar reads "Certificate - [Console Root\Certificates (Local Computer)\Personal\Certificates]". The interface includes a menu bar (File, Action, View, Favorites, Window, Help), a toolbar, and a tree view on the left. The tree view is expanded to "Personal" under "Certificates". The main pane displays a table of certificates with columns: Issued To, Issued By, Expiration Date, Intended Purposes, Friendly Name, Status, and Certificate Te... (truncated). A context menu is open over the selected certificate, showing options: Open, All Tasks, Cut, Copy, Paste, Properties, and Help.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te...
RDW\jared	RDW\CAD-07	26-11-2024	Server Authentication	*c:*\\$b3058988...	RDW Web Server	
RDW\jared@accidnet.eu	European-2014	26-10-2026	Server Authentication	RDW\jared@accidnet.eu	Web Server	
ClientCert13-EUCARIS	RDW-acc134-roulet-CA	16-8-2027	Client Authentication	Test-ClientCert13	Root Certificate...	
ClientCert15-EUCARIS	RDW-acc154-roulet-CA	16-8-2027	Client Authentication	<None>	Root Certificate...	
ClientCert16-EUCARIS	RDW-acc164-roulet-CA	16-8-2027	Client Authentication	RDW-acc164-roulet-CA	Web Server	
ClientCert17-EUCARIS	RDW-acc174-roulet-CA	16-8-2027	Client Authentication	<None>	RDW Computer...	
ClientCert18-EUCARIS	RDW-acc184-roulet-CA	16-8-2027	Client Authentication	<None>	RDW Computer...	
ClientCert19-EUCARIS	RDW-acc194-roulet-CA	16-8-2027	Client Authentication	<None>	RDW Computer...	
ClientCert20-EUCARIS	RDW-acc204-roulet-CA	16-8-2027	Client Authentication	<None>	RDW Computer...	

2.

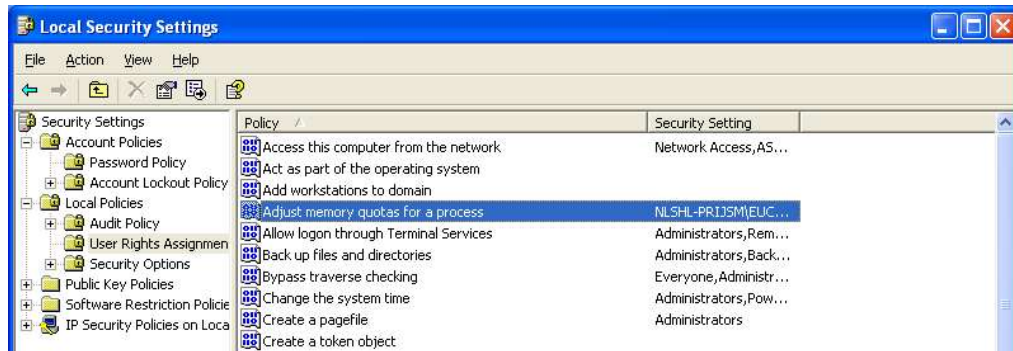
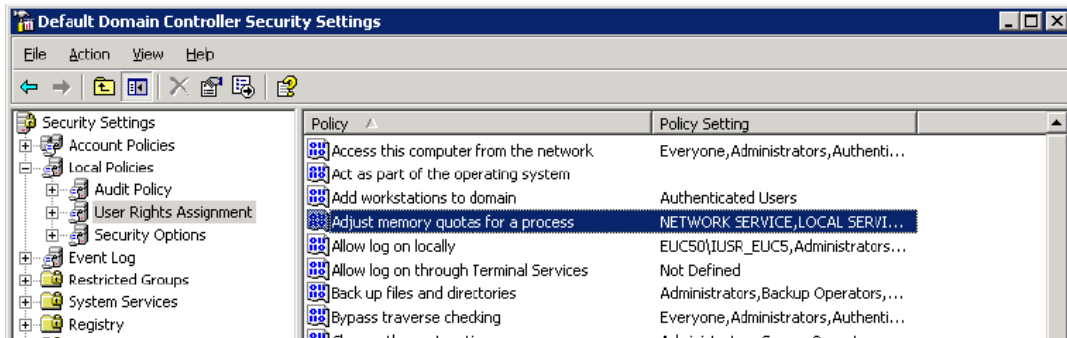
10.4 How To: Manually create an EUCARIS service account

On Windows Server 2008 this is done by opening the 'Computer Management' console and locating 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:'.



10.5 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:



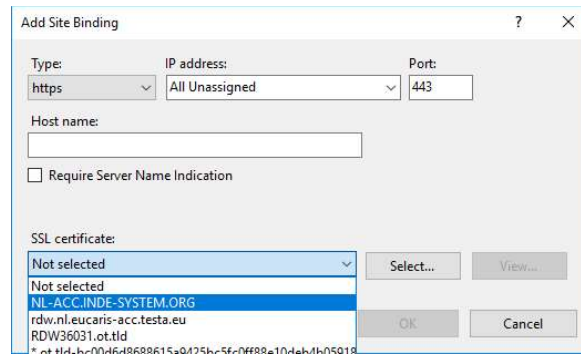
Locate the following policies and add the EUCARIS service account to these policies, by opening the properties and use the 'Add User or Group' button to add the account:

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

10.6 How To: Manually set SSL authentication for External application on IIS

The 'EUCARIS.External' site should be available through HTTPS, which means SSL has to be setup for this site. To configure this open 'Internet Information Services (IIS) Manager' through 'Administrative Tools' in the Windows start menu and select the 'EUCARIS.External.v7' site.

Right-click the site and select 'Edit Bindings' and in the 'Site Bindings' window click 'Add'



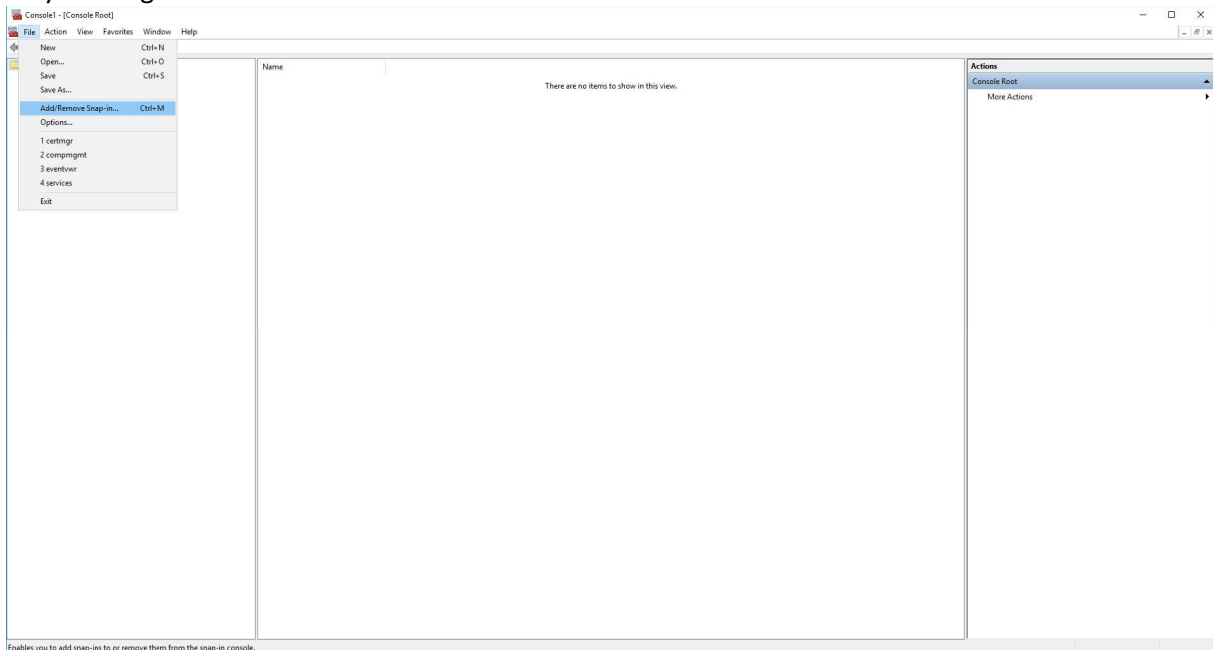
Select 'https' as the type and 443 or if in use 444 for the port and select the member state certificate and press 'OK' to save the settings. Verify the https entry is now available in the 'Site Bindings' dialog.

10.7 How To: Manually add a client certificate to legacy service connections

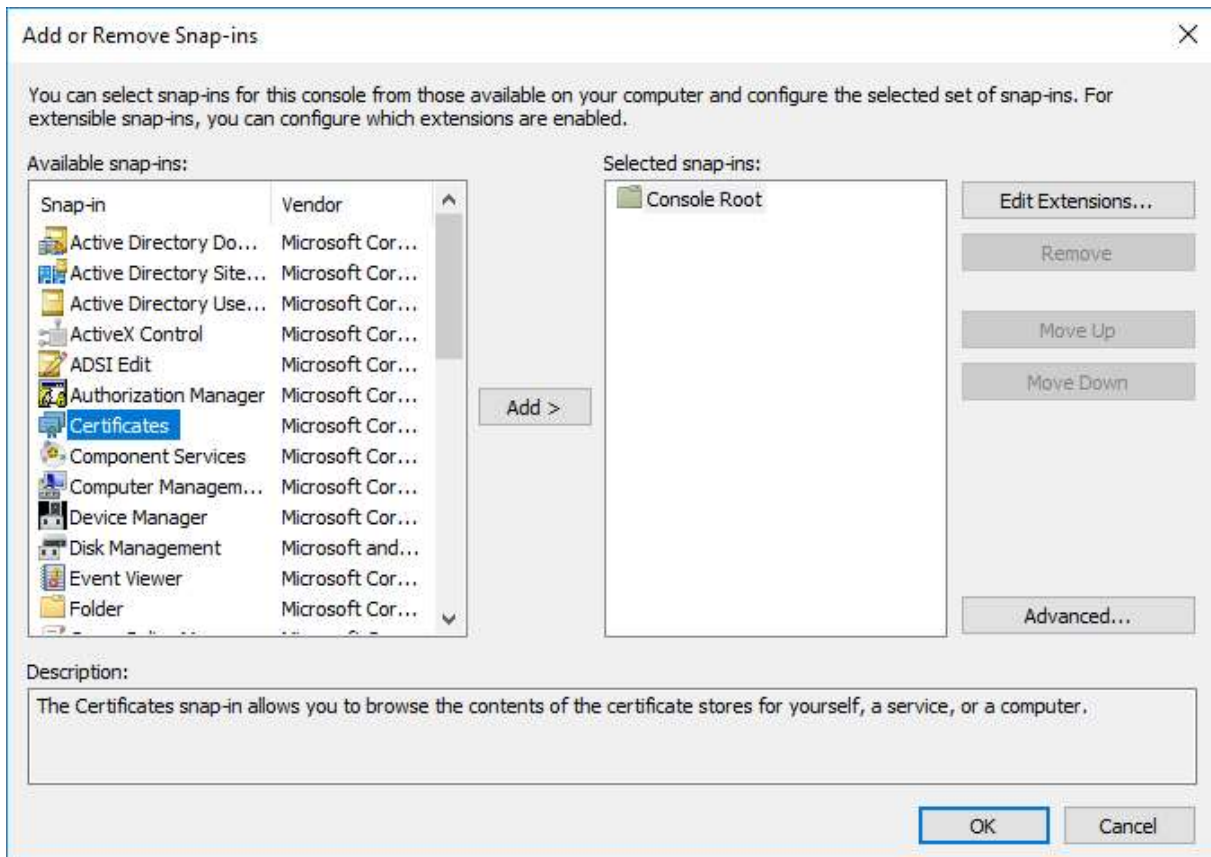
The EUCARIS core can add a client certificate with the https connection to your legacy services. The configuration of this option is added to the EUCARIS management client, and we will show you how to configure this. This chapter shows the steps to configure it on Windows 2008:

Install the certificate to use in the LocalComputer store

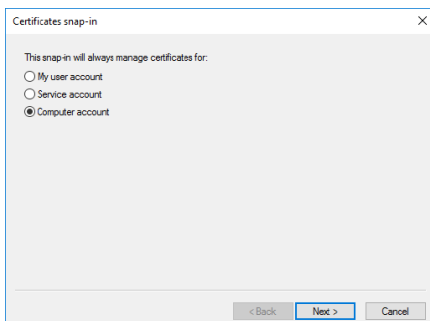
Before configuring EUCARIS you have to install the client certificate you will use in the LocalComputer store of your EUCARIS server(s). You have to supply this certificate yourselves. Install it by starting the MMC from Start->Run.



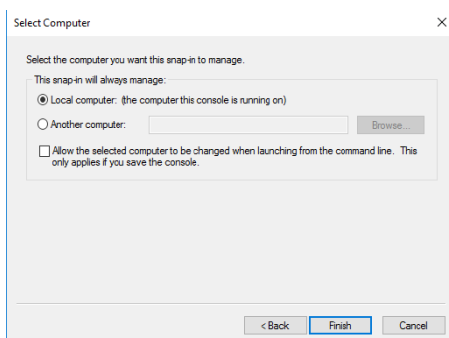
From the File menu select “Add/Remove Snap-in...”



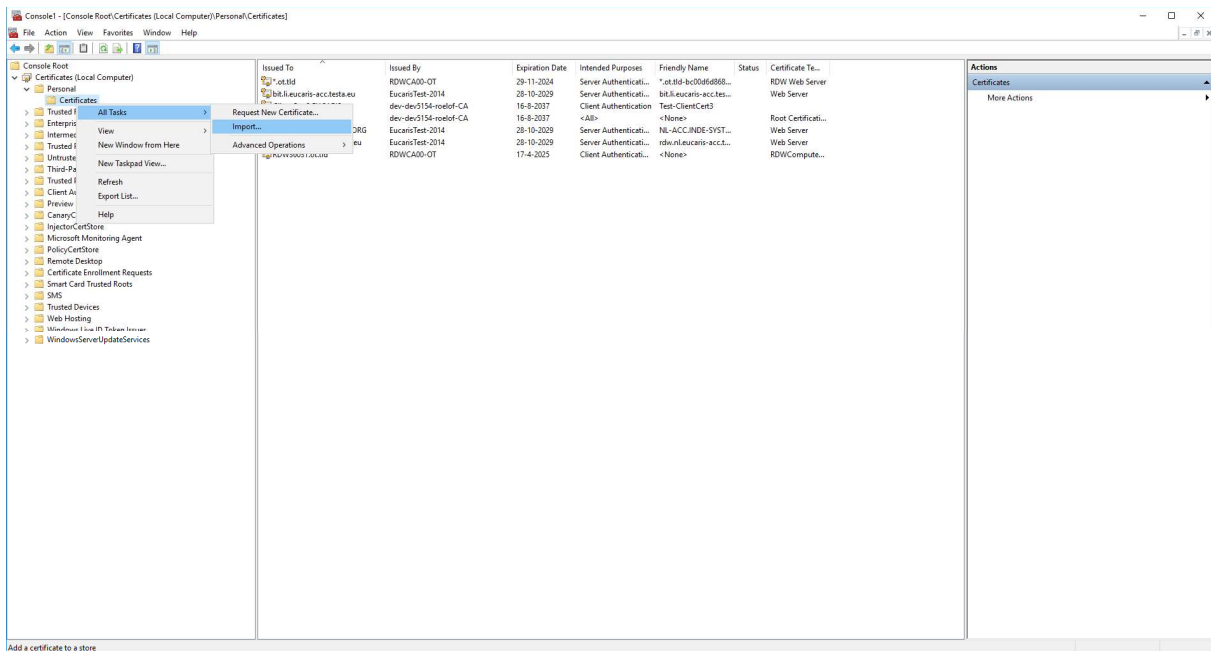
Select "Certificates" and click "Add"



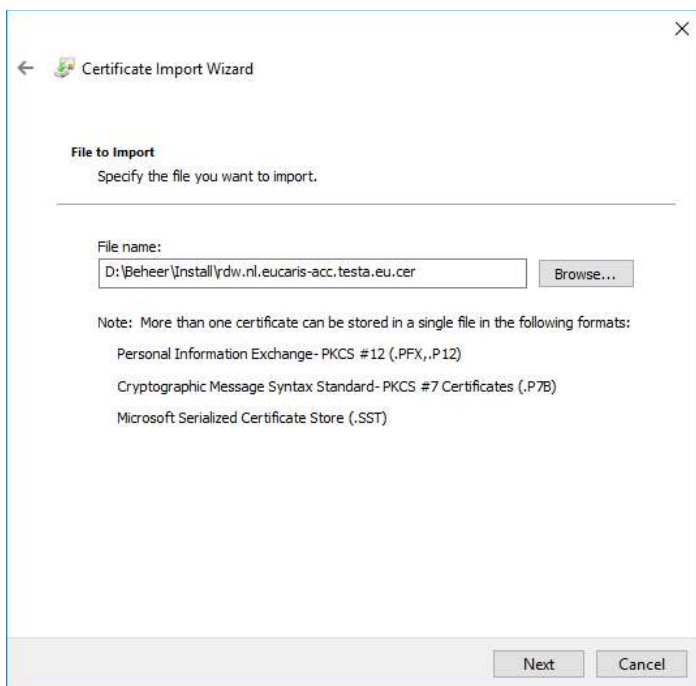
Select "Computer account" and click "Next"



Select "Local computer", click "Finish" and "OK" to leave the add/remove plugin window.



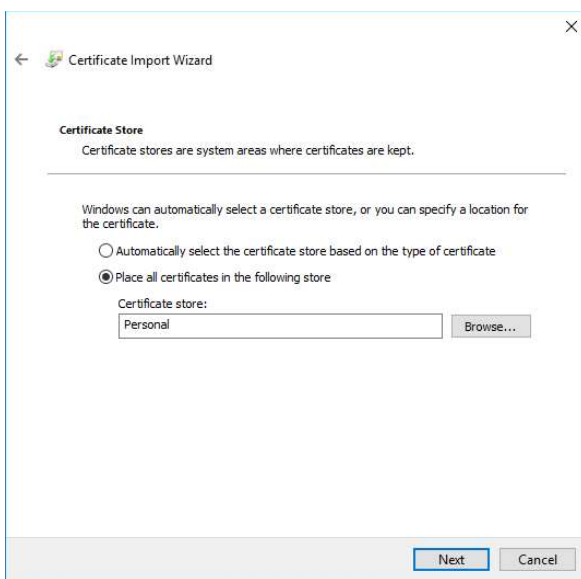
Browse to the Personal->Certificates hive, right click and select All Tasks->Import



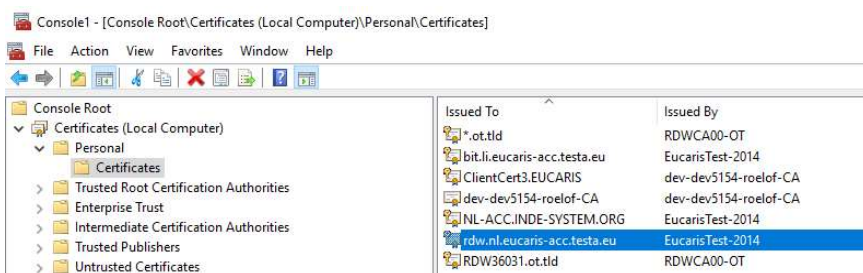
In the Certificate Import Wizard enter our select your certificate file. Remember that it should include a private key. Click "Next"



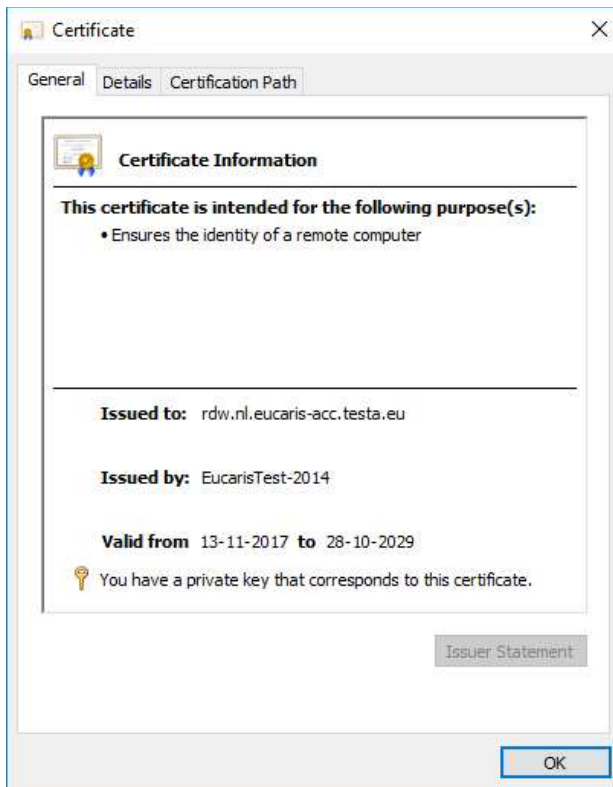
Enter the password for the certificates private key and click “Next”



Place the certificate in the “Personal” store and click “Finish”

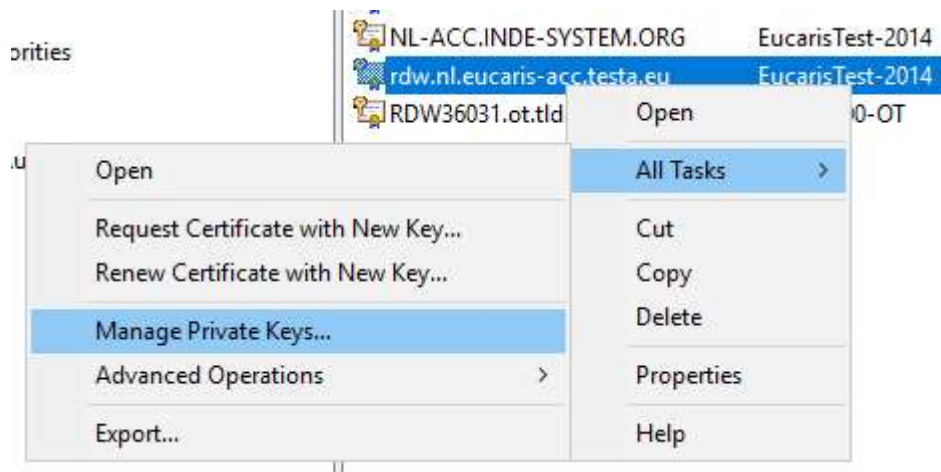


The certificate should show up in the list. Double click it to see the details



Setup access for application pool user

After importing the certificate you should give access to the user that is running the EUCARIS application pools. To check or set this select the certificate and click “More Actions->All Tasks->Manage Private Keys”



Check if the application pool user is in the list of users having access

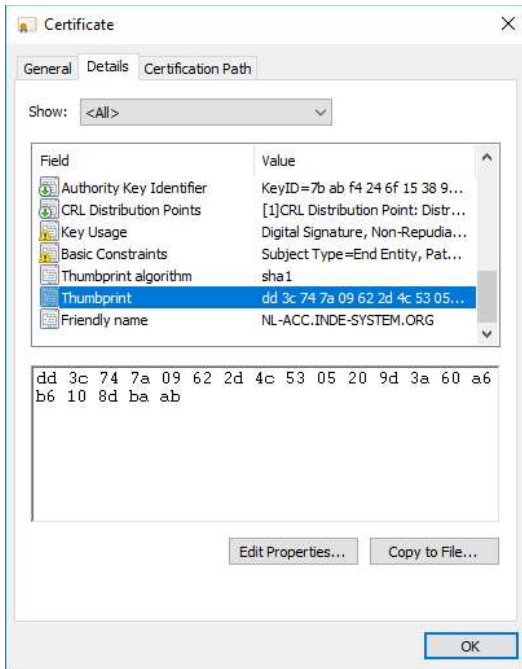


In the example we add the user RDW04618\EUCARISII



Configure EUCARIS to use the certificate

The certificate is available now to use as client certificate in EUCARIS. Open the certificate from the MMC again, goto the "Details" tab and find the Thumbprint.



Copy the Thumbprint and paste it for the correct legacy service in the Management Client:



10.8 How To: Install a Certificate using System Updates

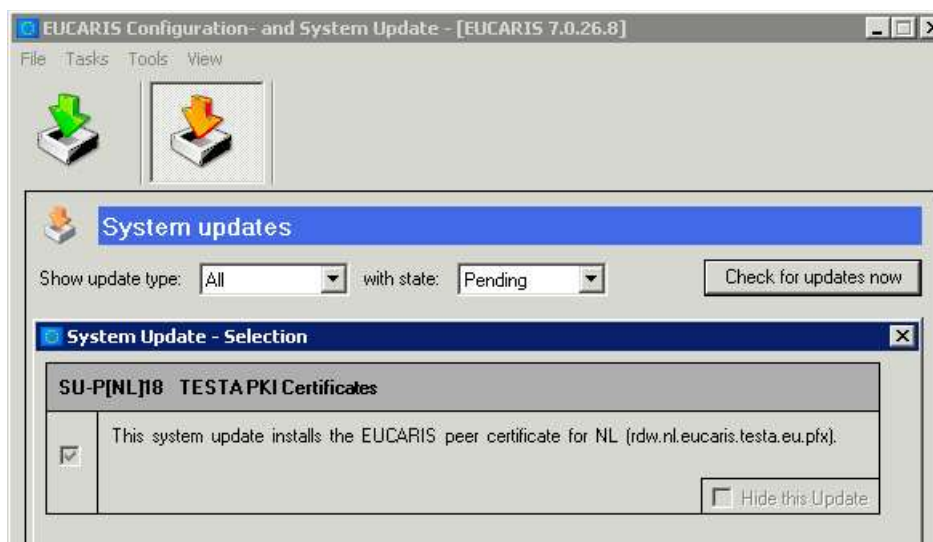
EUCARIS Certificates are distributed via System Update Packages. There are 2 options to obtain this package:

- Online via the EUCARIS Update Service. This requires a working connection via the TESTA network, including an existing and valid installed and configured EUCARIS certificate. This option is usually used during renewal of EUCARIS Certificates.
- Offline on request via EUCARIS Operations. The package is delivered as file and can be placed and imported on the server.

Both options are described below.

10.8.1 Online

Your (new) certificate is available for download once you receive a mail notification from EUCARIS Operations. Use the EUCARIS Configuration Tool in Update mode to download the certificate package. The update package will be selected automatically:



The package name contains the following items: SU-P[xx]yy, where xx denotes the EUCARIS Country Code and yy the last two digits of the year of issuing of the certificate. Press "Install after download of the certificate package:



NOTE: The certificate password is required during installation of the certificate package. EUCARIS Operations sends this password to one known person in the organisation in front.

After installation, the EUCARIS Certificate is imported in the Local Machine store including the private key and.

NOTE: This only installs the certificate. This procedure will not (re)configure EUCARIS in order to use the new certificate. This process is described in paragraph 5.2.6 Certificate configuration.

10.8.2 Offline

When the server is not connected to the TESTA network, or the server is an initial installation, the certificate must be installed using an offline System Update package. Please contact EUCARIS Operations in order to receive the offline System Update package.

Open the EUCARIS Configuration Tool in Update mode, and select Menu > File > Load System Update. Select the received offline System Update package (with file extension .upd). The procedure to install the certificate or updates are now identical with respect to the online System Updates.

10.9 How To: configure a satellite country in EUCARIS

EUCARIS is able to support satellite countries for both outbound and inbound requests. Satellite countries are countries hosted on another (existing) EUCARIS instance so that they are able to send and receive requests without the need to have a separate installation and/or instance of EUCARIS. An existing EUCARIS installation of a member state is re-used.

NOTE: this is a very specific scenario and must only be considered in close cooperation with EUCARIS Operations.

10.9.1 Outbound configuration

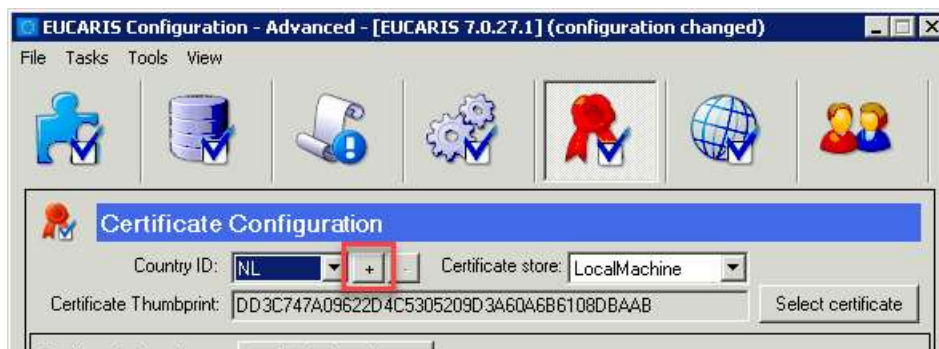
A country specific certificate is required in order to send requests on behalf of the satellite country and will be supplied by EUCARIS Operations. To be able to configure this certificate, locate and edit the following file:

```
[EUCARIS Configuration Tool application folder]\EUCARIS.Configuration.exe.config
```

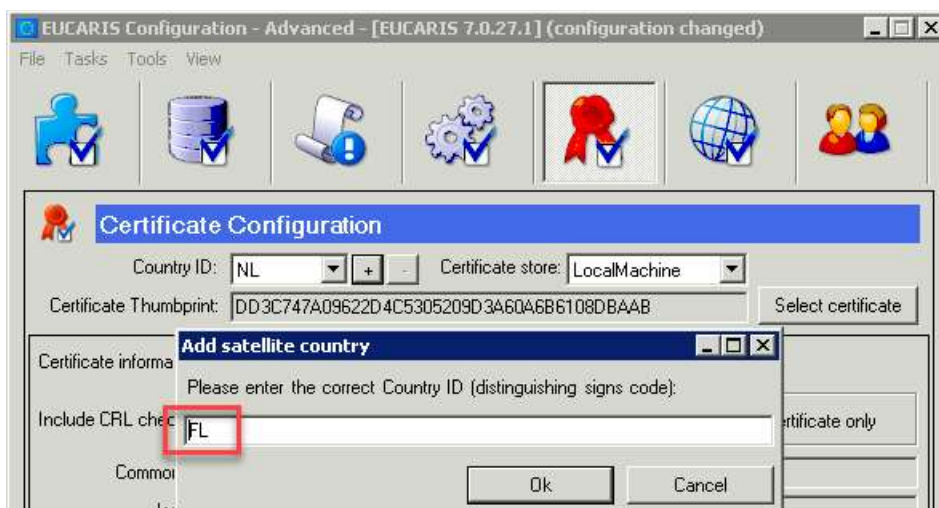
And change the value for `SatelliteCountries` to `true`:

```
<!-- SatelliteCountries: manage countries hosted by this member state. Possible values: true or false. Default is: false; -->  
<add key="SatelliteCountries" value="true" />
```

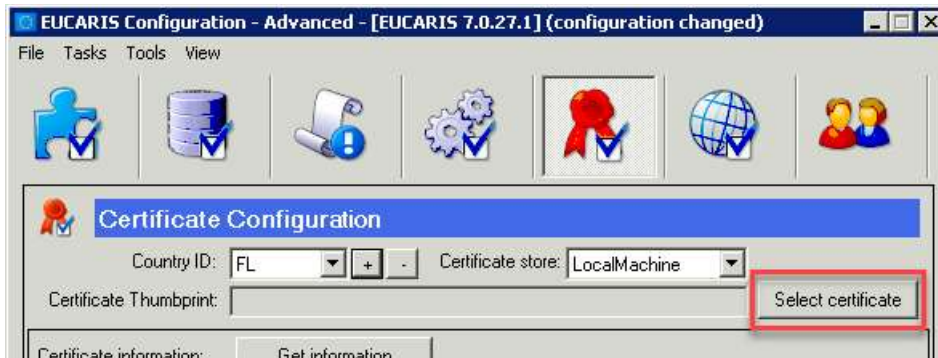
Now (re) open the Configuration Tool in Advance Mode and proceed to the certificate configuration screen. Click on the "+" button next to the country ID:



Enter the country code which is supplied by EUCARIS Operations (FL is used in this example):

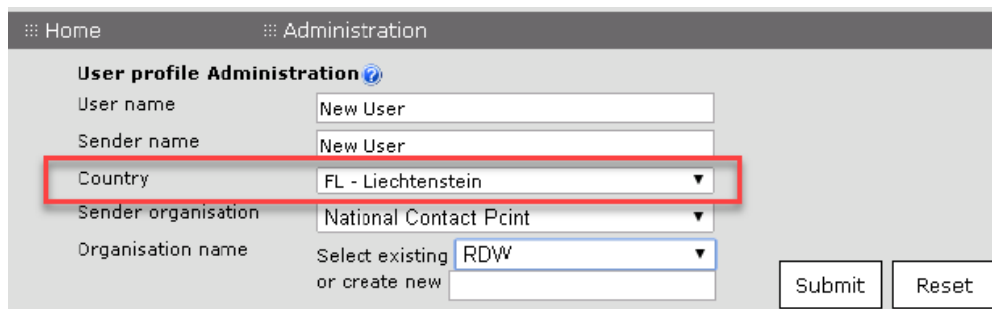


Now select the newly added country ID in the drop-down list, and click *Select Certificate* in order to configure a certificate for this new satellite country:



Now import and/or select the correct certificate for this member state as described in section 5.2.6, Certificate configuration.

Additional configuration is required in order to send request on behalf of the satellite country using the EUCARIS web client. Open the EUCARIS Management Client and navigate to menu Administration > User Profiles and create a new user which is allowed to send request on behalf of the satellite country:



Or change an existing user to allow to send a request of the satellite country:



NOTE: Requests sent to the public services of EUCARIS have to contain the correct SenderCountryId element in order to be able to send on behalf of the satellite country (in this example FL):

```
<VHOwnerHolderByChassisAndDate xmlns:xsd="http://www.w3.org/2001/XMLSchema-instance"
  - <Header>
    <MessageID>6c44e3b6-8e48-4d52-a86b-e6d81aaa1ebf</MessageID>
    <MessageVersion>1.0</MessageVersion>
  - <ServiceExecutionReason>
    <ServiceExecutionReasonCode>5</ServiceExecutionReasonCode>
    <ServiceExecutionReasonDesc>TEST</ServiceExecutionReasonDesc>
  </ServiceExecutionReason>
  <RecipientCountry>D</RecipientCountry>
  <SenderCountry>FL</SenderCountry>
  <SenderOrganisation>
```

EUCARIS automatically uses the correct certificate for signing the request, if correctly configured.

10.9.2 Inbound configuration

A country specific Legacy Service is required in able to respond to requests on behalf of the satellite country. This Legacy Service can re-use the same Legacy Service of the hosting member state, but it is possible to define a specific and new endpoint per service for this purpose. To configure EUCARIS satellite countries for inbound traffic, locate and edit the following file:

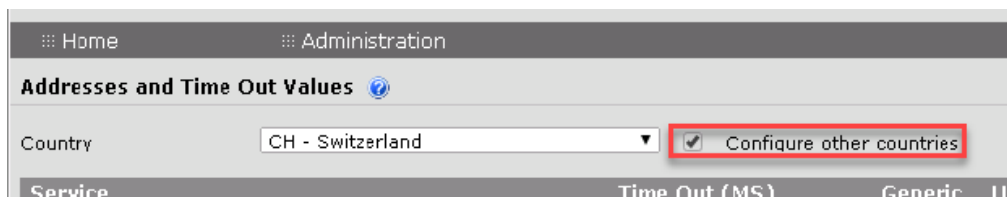
[EUCARIS root application folder]\Configuration\Indes.Properties.config

And change (or add) the value Indes.Core.SatelliteCountries. Add the Country code(s) for the satellite countries received from EUCARIS Operations:

```
<?xml version="1.0" encoding="utf-8"?>
<appSettings>
  <add key="Indes.Core.LocalCountry" value="CH" />
  <add key="Indes.Core.SatelliteCountries" value = "FL" />
  <add key="Indes.Core.Validation.YedLocation" value="C:\Pr
```

NOTE: After changing and saving the configuration file, a restart of the EUCARIS services is required before the changes will take effect.

In order to configure the Legacy Services endpoints, proceed with the EUCARIS Management Client, menu Administration > Service configuration, and check the “Configure other countries” check box:



Now select the satellite country (in this example FL), and configure the local services accordingly, eventually using asynchronous forwarding if required:

Service	Time Out (MS)	Generic	Async Forward	URL	Message version	Client Certificate Thumbprint
VHOH						
Asynchronous multiple owner holder request	100000	✓	<input type="checkbox"/>	http://	1.0	
Asynchronous multiple owner holder response	100000	✓	<input checked="" type="checkbox"/>	http://eucop-tools.ot.tld/eucaris.legacy.stub/genericsyncservice.asmx	1.0	
Vehicle owner by chassis number and date	20000	✓	<input type="checkbox"/>	http://eucop-tools.ot.tld/eucaris.legacy.stub/genericservice.asmx	1.0	
Vehicle owner by registration number and date	20000	✓	<input type="checkbox"/>	http://eucop-tools.ot.tld/eucaris.legacy.stub/genericservice.asmx	1.0	
VHOH Parking: multiple owner holder request	10000	✓	<input type="checkbox"/>	http://	1.0	
VHOH Parking: multiple owner holder response	10000	✓	<input type="checkbox"/>	http://	1.0	
VHOH Parking: Vehicle owner by registration number and date	10000	✓	<input type="checkbox"/>	http://	1.0	

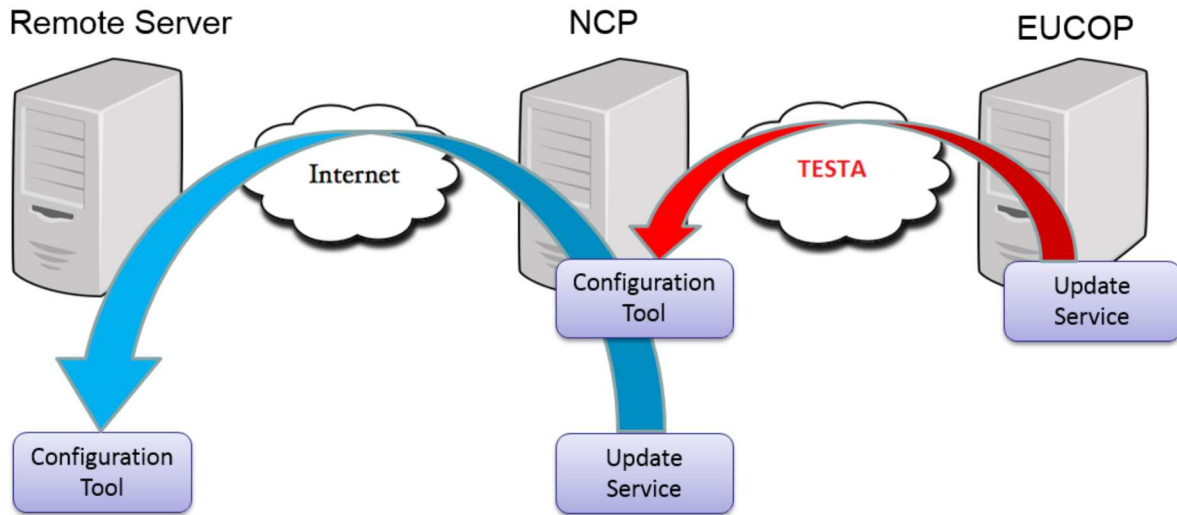
NOTE: The EUCARIS Batch Processor can be configured to handle inbound asynchronous request messages on behalf of the EUCARIS satellite country. No other additional configuration is required other than the default configuration required to properly enable the batch processor. Please review section Fout! Verwijzingsbron niet gevonden., Fout! Verwijzingsbron niet gevonden. for more details.

NOTE: Please review section Fout! Verwijzingsbron niet gevonden., Fout! Verwijzingsbron niet gevonden. for more information on service configuration.

10.10 How To: Install the EUCARIS Update Service

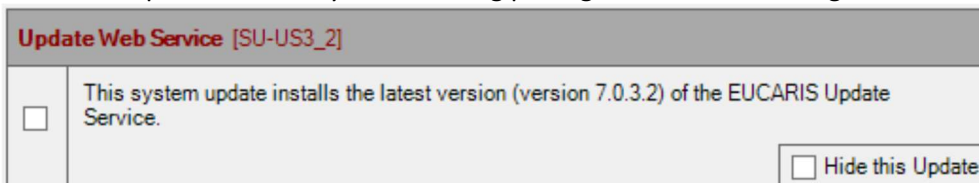
It is possible for a NCP to install an own Update Service. Normally a NCP connects by use of the configuration tool to the Update Service of Eucop to get and download update packages. But by installing an Update Service themselves the NCP can choose which update packages to provide to third parties. The NCP will be considered to be a hub for the third party in this case.

This will look like this



10.10.1 Installing the update service

Install the Update Service by downloading package SU-US in the configuration tool

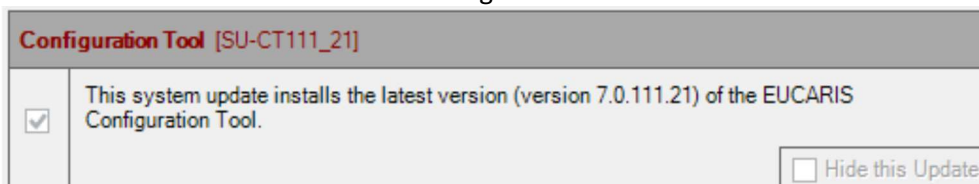


The minimum required version is SU-US3

After the installation the update web service will be exposed in IIS

10.10.2 Exposing updates

Download the latest version of the configuration tool:



The minimum required version is SU-CT111.

Expose/De-expose is explained in 5.3.2.3 and possible after configuration as explained in 10.10.3

10.10.3 Configuration

After installing both the update web service and the new configuration tool, we have to let the configuration tool know where it can find the local update web service

Open Eucaris.Configuration.exe.local

Default located in 'C:\Program Files\EUCARIS\Tools\EUCARIS.Configuration'

Find the key "Update.Url.Local" and set the value to the local update service url, normally:

<http://localhost:8090/EUCARIS.Update/SystemUpdate.asmx>

10.10.4 Certificate configuration

For the third party to correctly connect to the update service it is important that the third party trusts the root of the certificate used in the update service and that the update service recognises the certificate used by the third party itself to make the call to the update service.

Installing a certificate is explained in 10.7

After that the configuration of the update service has to be set to only allow that certificate. This also overwrites the default Eucaris certificates checks for this update service.

Open web.config of the update service

Default located in 'C:\Program Files\EUCARIS\Tools\EUCARIS.Update'

Find the key "OverwriteCertificateSubjectMustContainList" and set the value as a ';' seperated or single value of the certificate(s) used by the third party to sign the communication to the update service. E.g. "communication.certificate.ncp.com;alternativecommunication.certificate.ncp.com"

Find the key "SigningCertificateFindValue". This certificate is used by the update service to sign the responses to the third party. So the third party must trust the root of this certificate.

The installation of the certificate used by the third party is explained in "EUCARIS - Standalone Web client Installation Manual"

10.11 How To: get remote support on the EUCARIS server

Analysing issues can take a lot of time for both member states as for EUCARIS Operations. In some occasions it will be a lot more efficient and effective if EUCARIS Operations can 'take a look' on the EUCARIS Server. If such an option is allowed by local (security) policies then EUCARIS offers a custom solution (**EUCARIS Remote Desktop**) which reuses the for EUCARIS available infrastructure:

- TESTA Network
- Port 443 (https)
- EUCARIS External website endpoint

The main advantage of reusing the available infrastructure is:

- It is already available and (if infrastructure is not the issue to begin with) functional
- The network layer is secure and not using open and public networks
- There is no additional infrastructure configuration required

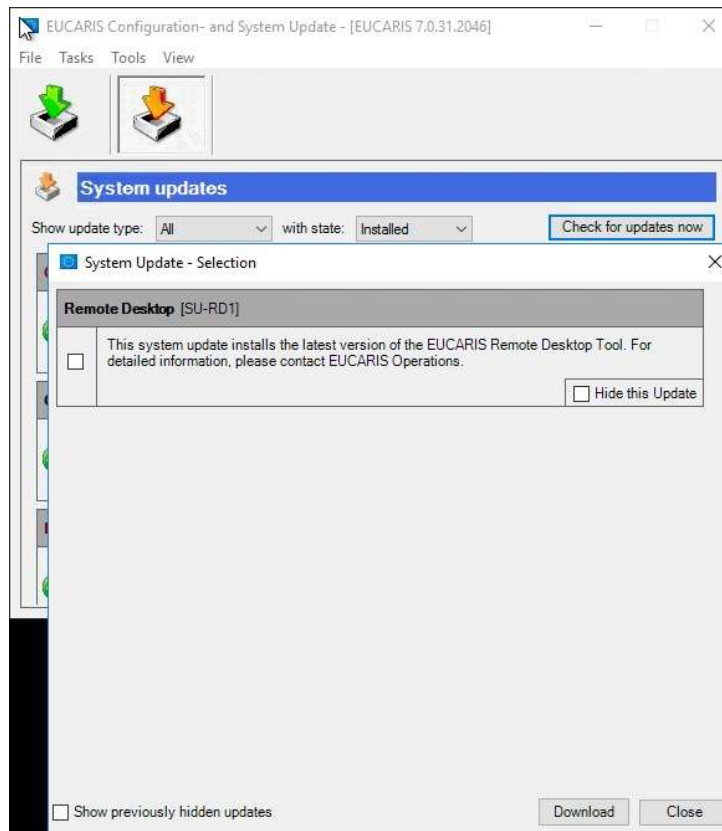
The EUCARIS Remote Desktop consists of a Web Application (open source: <https://cedrozor.github.io/myrtile/>) which offers Remote Desktop Access. The application is distributed and installed using EUCARIS System Updates. The System Update will create the following:

- Virtual directory hosting the application on the EUCARIS External website *EUCARIS.External/EUCARIS.RemoteDesktop*. The application will be available from TESTA on this endpoint. The application is disabled (offline) by default.
- Application folder [*program files*]\EUCARIS\Tools\EUCARIS.RemoteDesktop,
- Windows Service *EUCARIS.v7 Remote Desktop* which acts as a bridge between the web application and the RDP protocol. The Windows Service is disabled by default.
- A local user called *EUCOP*. During installation the administrator is required to enter a new password for this user. This user is by default disabled and no member of any Windows Group.

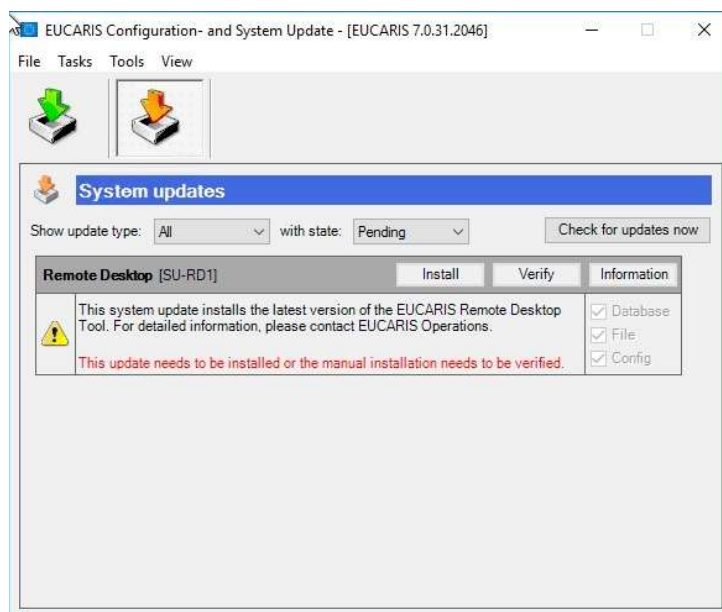
The EUCARIS Remote Desktop application is available on request. The installation procedure and methods to enable and disable are described in the next paragraphs.

10.11.1 Installation procedure

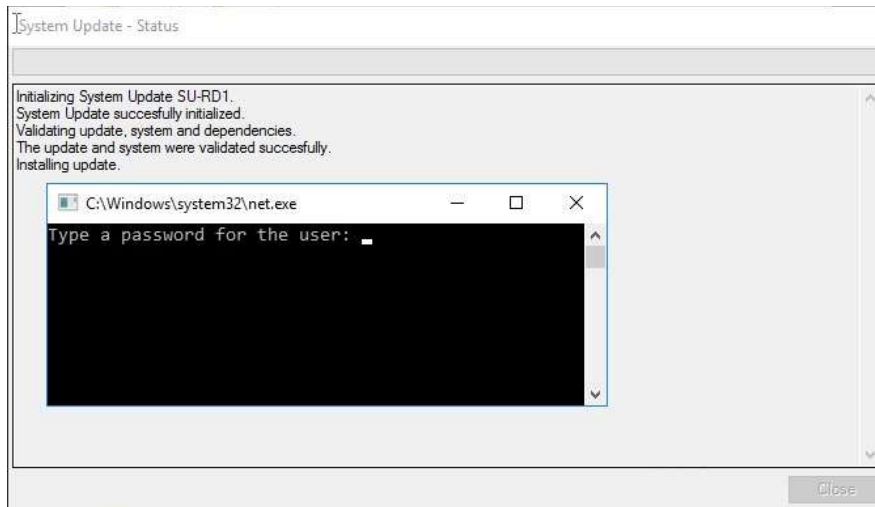
1. Download the System Update containing the EUCARIS Remote Desktop application.



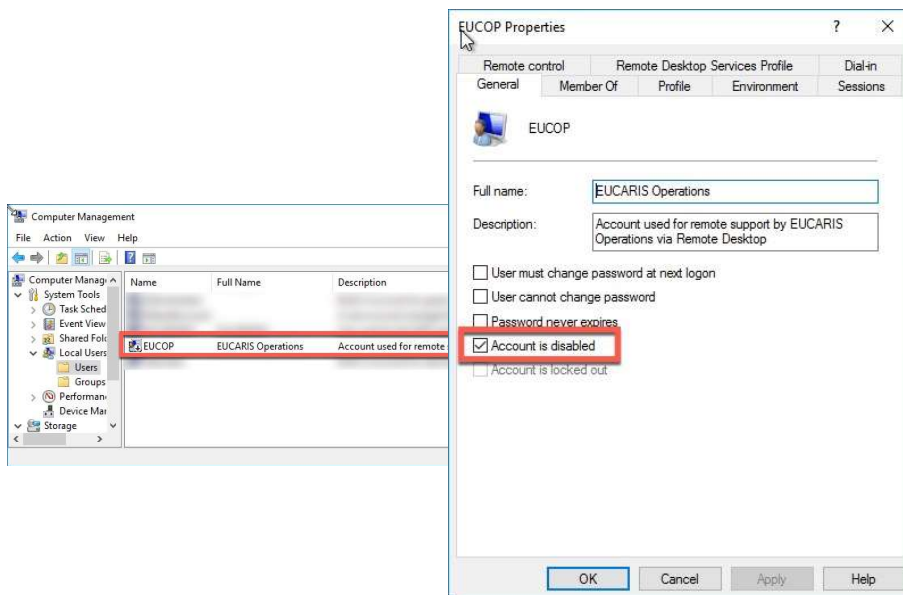
2. Install the update just as any other EUCARIS System Update by clicking **Install**.



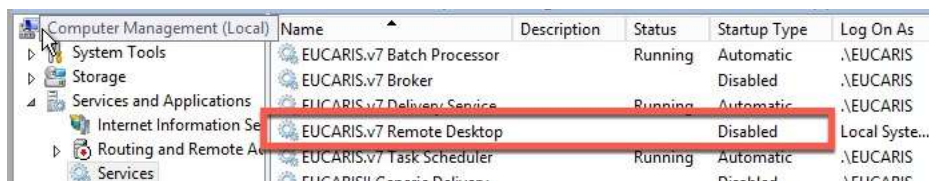
3. During the installation, fill in the password for the newly created local EUCOP user. Please make sure to adhere to local password complexity policies.



After this step, the installation is finalized and the Local user is created, but disabled:



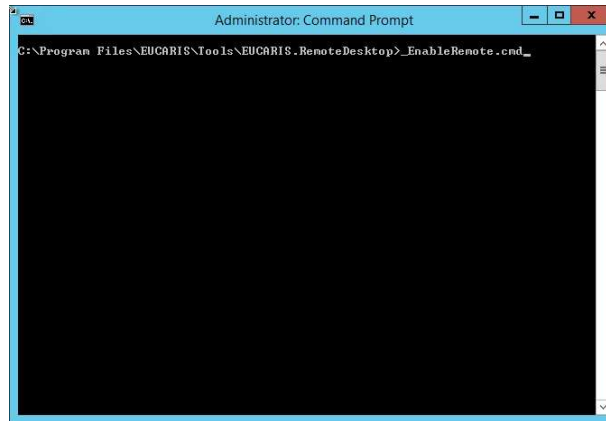
Also, the required Windows Service is disabled:



10.11.2 Enable EUCARIS Remote Desktop

In order to enable the EUCARIS Remote Desktop, open a command prompt with elevated privileges (run as administrator), and change directory to [programs folder]\EUCARIS\Tools\EUCARIS.RemoteDesktop and execute the following script:

_EnableRemote.cmd



This script will:

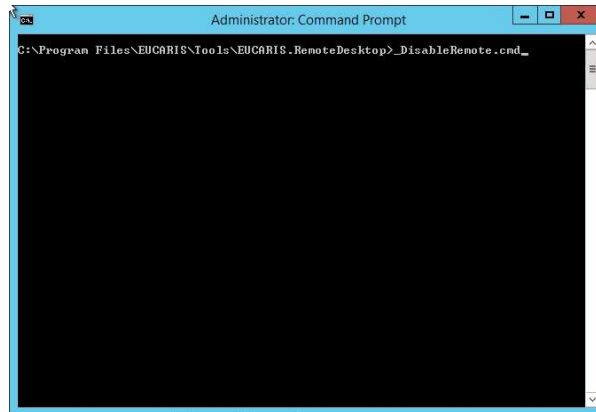
- Enable the local EUCOP user
- Add the EUCOP user to the administrators group
- Enable the EUCARIS.Remote Desktop Windows service
- Enable the EUCARIS.Remote Desktop web application

Now share the local EUCOP users' password with EUCARIS Operations in order for the support to log on to the server.

10.11.3 Disable EUCARIS Remote Desktop

In order to disable the EUCARIS Remote Desktop, open a command prompt with elevated privileges (run as administrator), and change directory to [programs folder]\EUCARIS\Tools\EUCARIS.RemoteDesktop and execute the following script:

_DisableRemote.cmd



This script will:

- Disable the local EUCOP user
- Removes the EUCOP user from the administrators group
- Disables the EUCARIS.Remote Desktop Windows service
- Disables the EUCARIS.Remote Desktop web application

Now you may leave the application on the server, but for extra security it is advisable to remove the application by clicking Undo in the configuration tool:

