

# GS2C Security Suite

## Installation Manual

Revision A1 - February 2018

<https://www.encode labs.be>

## GS<sub>2</sub>C Security Suite

### Installation Manual

Document Number: GS2C-IM-001

Revision: A1

Release Date: February 2018

This manual is proprietary information of Encode Labs. Unauthorized reproduction of any portion of this manual is prohibited. The information contained within this manual is for informational purposes only. All information is subject to change without prior notice. Encode Labs assumes no responsibility for incorrect information that may be contained within this manual.

All trademarks, service marks, trade names, trade dress, product names and logos appearing in this manual are the property of their respective owners, including Encode Labs in some instances.

Any rights not expressly granted herein are reserved.

© 2017-2018 Encode Labs

All rights reserved.

# Contents

<b>INTRODUCTION .....</b>	<b>5</b>
OVERVIEW .....	5
CONVENTIONS .....	6
INTRODUCTION .....	6
DESIGN.....	6
COMPONENT OVERVIEW .....	7
<i>Export Service</i> .....	8
<i>Import Service</i> .....	8
<i>Web Server</i> .....	8
<i>File Server</i> .....	8
ARCHITECTURE .....	9
SPECIFICATIONS AND COMPATIBILITY .....	10
<i>Central Server requirements</i> .....	10
<i>Export Server requirements</i> .....	10
<i>Web Server requirements</i> .....	10
<i>Supported Export Server systems</i> .....	10
KNOWN LIMITATIONS .....	10
<b>CERTIFICATES.....</b>	<b>11</b>
OVERVIEW .....	11
CERTIFICATE OVERVIEW .....	12
CERTIFICATE VALIDATION.....	12
CERTIFICATE EXPIRATION .....	13
IMPORTING A CERTIFICATE CONTAINING A PRIVATE KEY.....	14
IMPORTING A CERTIFICATE WITHOUT KEYS .....	17
OBTAINING THE REQUIRED DETAILS FROM YOUR CERTIFICATES .....	18
THE CERTIFICATE STORE NAME.....	19
<b>INSTALLATION .....</b>	<b>20</b>
OVERVIEW .....	20
PRE-REQUISITES .....	21
INSTALLATION OF THE EXPORT SERVICE .....	21
<i>Prerequisite</i> .....	21
<i>Installation</i> .....	21
<i>Configuration of the service user account</i> .....	26
INSTALLATION OF THE IMPORT SERVICE .....	27
<i>Prerequisite</i> .....	27
<i>Creation of the database</i> .....	27
<i>Installation</i> .....	28
<i>Configuration of the service user account</i> .....	34
INSTALLATION OF THE GUARD WEB APPLICATION .....	35
<i>Prerequisite</i> .....	35
<i>Installation of Internet Information Services</i> .....	35
<i>Installation of the .Net Core 2.0 Windows Hosting</i> .....	35
<i>Installation of the main website</i> .....	37
<i>Installation of the image hosting website</i> .....	39
<i>Set the authentication for both sites</i> .....	40
<i>Configure the BackConnectionHostNames key</i> .....	41
<b>CONFIGURATION .....</b>	<b>42</b>

OVERVIEW .....	42
CONFIGURATION TASKS .....	43
CONFIGURING THE EXPORT SERVICE .....	43
CONFIGURING THE IMPORT SERVICE .....	45
CONFIGURING THE WEB APPLICATION .....	48
<i>Configure the database connection</i> .....	48
<i>Set the image hosting address</i> .....	48
<i>Configure the AD group allowed to access the service</i> .....	48
<b>THE IMPORT JOB TOOL .....</b>	<b>49</b>
OVERVIEW .....	49
INTRODUCTION .....	50
IMPORT JOB TASKS .....	50
CREATING IMPORT JOBS .....	50
<i>Sample command line</i> .....	50
MODIFYING IMPORT JOBS .....	51
<i>Site Information</i> .....	51
DELETING IMPORT JOBS .....	51
CRON TRIGGER TUTORIAL .....	51
<i>Format</i> .....	51
<i>Special Characters</i> .....	52
<i>Example CRON specs:</i> .....	53
<b>USING THE WEB APPLICATION .....</b>	<b>54</b>
OVERVIEW .....	54
INTRODUCTION .....	55
OPENING THE WEB APPLICATION .....	55
<i>Personnel Status</i> .....	56
<i>Displaying Personnel Details</i> .....	56
<b>APPENDIX A .....</b>	<b>58</b>
OVERVIEW .....	58
LOCAL MACHINE AND CURRENT USER CERTIFICATE STORES .....	59
LOCATING THE REQUIRED INFORMATION ON A CERTIFICATE .....	59
CERTIFICATE NOT FOUND .....	61
INSTALLATION OF THE MICROSOFT .NET 4.6.2 FRAMEWORK SEEMS TO HAVE FAILED .....	61
THE WEB APP FAILS TO RUN .....	62
<i>Check the dotnet package update</i> .....	62
<i>In internet explorer, you receive a 502.5 error</i> .....	63



# Chapter 1

## Introduction

### Overview

CONVENTIONS .....	6
INTRODUCTION .....	6
DESIGN .....	6
COMPONENT OVERVIEW .....	7
<i>Export Service</i> .....	8
<i>Import Service</i> .....	8
<i>Web Server</i> .....	8
<i>File Server</i> .....	8
ARCHITECTURE .....	9
SPECIFICATIONS AND COMPATIBILITY .....	10
<i>Central Server requirements</i> .....	10
<i>Export Server requirements</i> .....	10
<i>Web Server requirements</i> .....	10
<i>Supported Export Server systems</i> .....	10
KNOWN LIMITATIONS .....	10

## Conventions

The following pictograms are used to indicate important information



Indicates extra information.



Indicates a warning. Pay extra attention to the information that is provided.



Indicates a danger with important consequences. Pay extra attention to the information that is provided and be cautious.

## Introduction

GS<sub>2</sub>C stands for Global Synchronised Security Center.

The GS<sub>2</sub>C suite consists of several software packages that work together as a single security data intelligence entity. Its intention is to provide your Security Department with relevant security information that is aggregated from different systems.

The aggregated information can be consulted and used depending on the modules you choose to deploy such as the Web Service or a File Server.

## Design

Special considerations were made in the design of this solution that are purposefully **security** and **privacy** conscious. Every aspect of the design process, every decision made for the creation of this solution is based on these two critical factors.

Some key points that reflect this:

### Protection

The export services create a separation layer between the end users and the core of your security system: users have no means of accessing your local or global security systems – or their databases – through these services.

### Authentication

The services use Active Directory® integration for the authentication of its users. Unauthorized or inactive accounts cannot make use of the services. People that are removed from your organization automatically lose access to these services.

### Encryption

All data that is transferred is sent over a TLS connection. Added to that, the data itself is also encrypted using private/public key encryption. All encryption algorithms are FIPS 140 compliant.



The Federal Information Processing Standard (FIPS) 140 is a security implementation designed for certifying cryptographic software. FIPS 140 validated software is required by the U.S. Government and requested by other prominent institutions.

### **Integrated Security Components**

The system is designed to offer advanced security options for connecting to different import sources. There is no one single security checkpoint. Every end node features its own set of security rules.

### **Privacy**

We have foreseen the possibility to opt-out certain data synchronization to the global Master Server on a per-person-basis.

### **Modular Architecture**

The modular architecture allows you to install only the components that you want to use. It also allows easy expansion of the system.

### **Distributed Model**

Each site can opt to use the security data for other integrations if needed. You could feed this data into external services such as Workday or HR. The basic idea is that this service offers a data source controlled and verified by your security department.

### **Global Distribution of critical statuses**

When a person no longer has access to a location for any reason, the system can distribute this critical information throughout all connected systems. Allowing security personnel to refuse access to the individual at other locations as well.

### **Email integration**

Allowing for closer monitoring of your system, we integrated email functionality to allow you to receive updates on the status of your system. Be proactively informed of any potential issues that might affect your system.

### **Component overview**

The GS<sub>2</sub>C Suite consists of different components that each have their own specialty service. This offers a robust approach to the stability and modularity of the system.

Each service can be deployed as a Windows Service or executed from a command line.

## Export Service

This service is responsible for consolidating data from a variety of systems and feeding it into the central server. It offers an interface on which the central service will connect for obtaining the data. It is usually installed on the target application server holding the data such as Access Control Software or other.

The export service “Exports” the data from the target application server.

## Import Service

The import service is configured with a number of *import components*. Each import component implements an interface that retrieves data from configured endpoints (Export Services on target systems) and maps it to the internal database.

In short, this means it collects data from several external systems to be stored in a single central database.

The import service will poll its configured endpoints for changes at defined schedules. For instance, it can check your Access Control System for any changes to personnel records every hour, a specific time of day, always or only on certain days.... This is completely configurable per connected endpoint.

Security and extensibility: The security between the import component and its endpoint is a property of the component itself. This means that new import endpoints such as Active Directory, SAP, Workday... any possible data source you can think of, can be added at a later stage without any issues or compromises to the security of your GS<sub>2</sub>C solution.

## Web Server

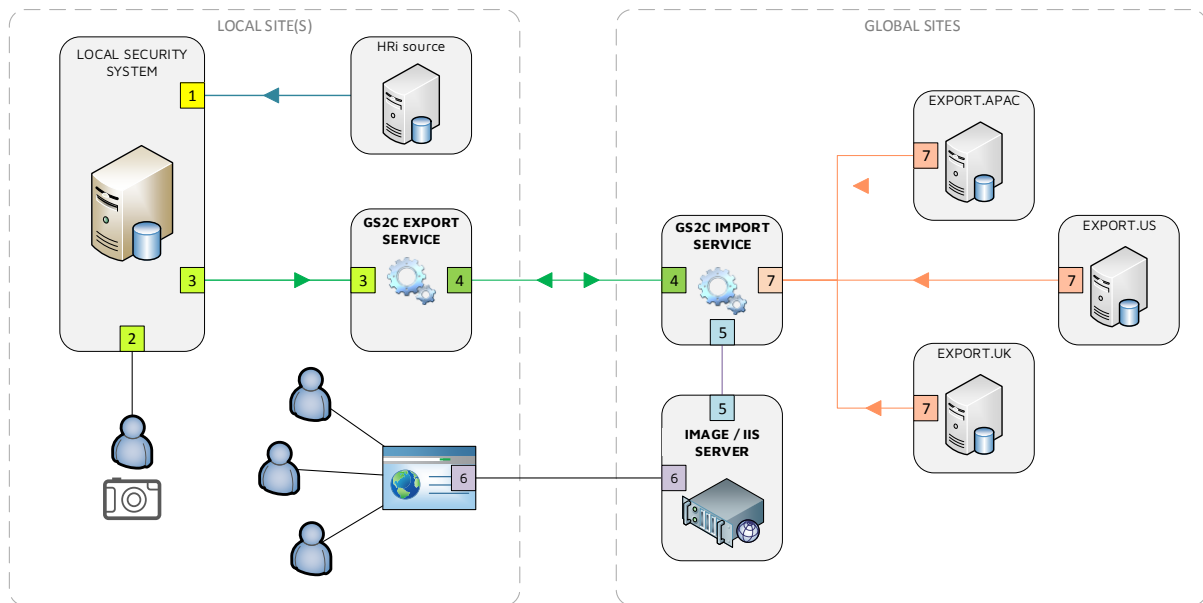
The Web Server offers a website to which Security Operators can connect and consult relevant security data. The operator has to have an account on the domain and must belong to a specific AD group in order to get access to the service.

## File Server

The File Server is used for storing files such as personnel images. These can be stored on the central server itself but could also be loaded to a separate file server to be used for other services such as a corporate phonebook that will be provisioned by a verified image source.



## Architecture



1	<p>Your local server <b>MAY</b> import <b>PERSONNEL RECORDS</b> from an external HRI source (UID between systems must be the same)</p> <ul style="list-style-type: none"> <li>- <b>EXPIRED</b> status is synced globally (Personnel record, Credential records)</li> <li>- Any other personnel statuses <b>ENABLE</b> the Personnel Record</li> </ul>
2	<p>Your photos are taken from <b>YOUR SECURITY SYSTEM</b>. This can be any open non-proprietary system. The GS<sub>2</sub>C Export Service can have different modules for different systems.</p>
3	<p>The <b>EXPORT SERVICE</b> exposes the required data to the IMPORT SERVICE Personnel <b>STATUS</b> can be synced as well for global consistency: people cannot access other locations.</p>
4	<p>The <b>IMPORT SERVICE</b>:</p> <ul style="list-style-type: none"> <li>- All data is synced to the master database</li> <li>- The Import Service usually resides on the <b>CORPORATE NETWORK</b></li> </ul>
5	<p><b>SECURITY INFORMATION</b> including <b>PHOTOS</b> can be stored on a dedicated file server. This provides your organization with <b>VERIFIED</b> and <b>CONTROLLED</b> data.</p>
6	<p><b>SECURITY INFORMATION</b> can be consulted by <b>SECURITY OPERATORS</b> through the <b>GUARD WEB APP</b>.</p>
7	<p><b>MULTIPLE SITES</b> can be connected to the same <b>CENTRALIZED IMPORT SERVICE</b>. All records require a <b>COMMON UNIQUE ID</b> across all system such as an Employee Number.</p>



## Specifications and Compatibility

### Central Server requirements

- .Net 4.6.2
- MSSQL Server 2012R2 or higher

### Export Server requirements

- .Net: Add .Net 4.6.2

### Web Server requirements

- IIS 8.0
- .Net Core 2.0 Windows Hosting

### Supported Export Server systems

C•CURE 9000 2.30R2 or higher

### Known limitations

No known limitations



# Chapter 2

## Certificates

### Overview

CERTIFICATE OVERVIEW .....	12
CERTIFICATE VALIDATION .....	12
CERTIFICATE EXPIRATION .....	13
IMPORTING A CERTIFICATE CONTAINING A PRIVATE KEY .....	14
IMPORTING A CERTIFICATE WITHOUT KEYS .....	17
OBTAINING THE REQUIRED DETAILS FROM YOUR CERTIFICATES .....	18
THE CERTIFICATE STORE NAME .....	19

## Certificate Overview

Certificates serve two functions:

1. They encrypt the actual data that is sent between the different servers.
2. They are used for Mutual TLS authentication to ensure the servers are talking to the correct endpoints.

Below you can find a list of the required certificates per module:

Service	Certificate	Include Private Key	Certificate Store
Any GS <sub>2</sub> C Server	Root CA	No	Machine
Export Server	Export Service	Yes <sup>1</sup>	Personal
Export Server	Import Service	No	Machine/Personal
Import Server	Import Service	Yes <sup>1</sup>	Personal
File Server	N.A.	N.A.	N.A.

## Certificate validation

This section defines the client certificate requirements and has the following properties:

Field	Description
Subject	The <b>subject</b> property of the certificate e.g. CN=uk_export_server
IssuerCN	The <b>issued by</b> property of the certificate e.g. CN=encodelabs.be
Thumbprint	The <b>thumbprint</b> of the certificate. This must be without spaces and in uppercase. e.g. EEA9CB7450D1A5877B5B5C4449623B6C65456D68
VerifyChain	Specifies whether the complete certificate chain must be verified for validity. In a test environment, you can set this to "false", allowing you to use self-signed certificates. In a production environment, it is advised to set this value to "true"

The GS<sub>2</sub>C services ensure that the certificates have not expired and that the Issuer, Subject and Thumbprint properties supplied match those configured.

---

<sup>1</sup> Inclusion of Private Keys is required for supporting data encryption between export and import servers.

## Certificate expiration

Each certificate has an expiration date. The GS<sub>2</sub>C system is designed to warn administrators by email when a given certificate is about to expire. This email will be sent daily until the certificate is renewed again.

The number of days to start warning in advance about this expiration can be configured during setup or changed in the installation config files of the service.



When a certificate is no longer valid, the component to which the certificate applies will no longer work!

It is extremely important that the certificates are managed correctly by the GS<sub>2</sub>C system administrators.

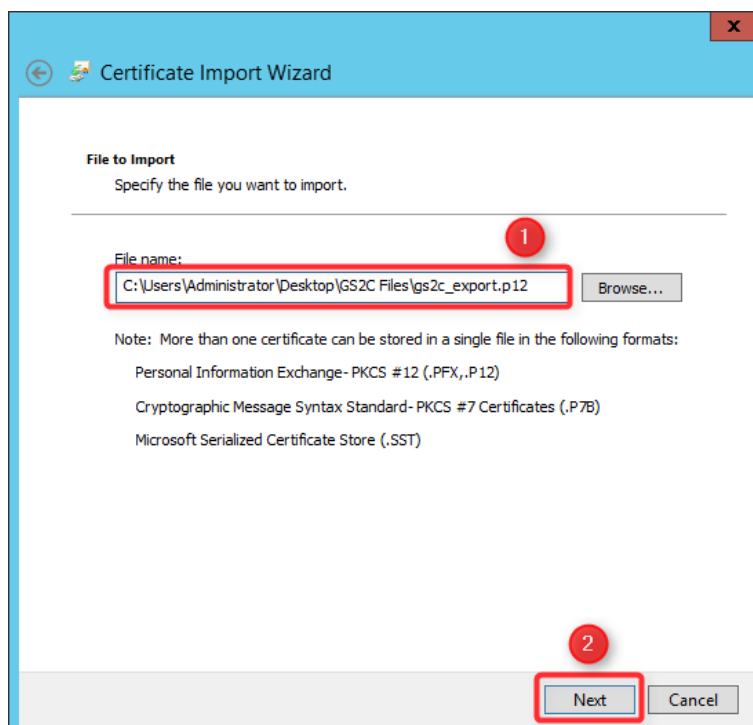
## Importing a certificate containing a private key

Depending on the type of certificate they must be installed in a store. Below is an overview of the certificates required and where they must be installed.

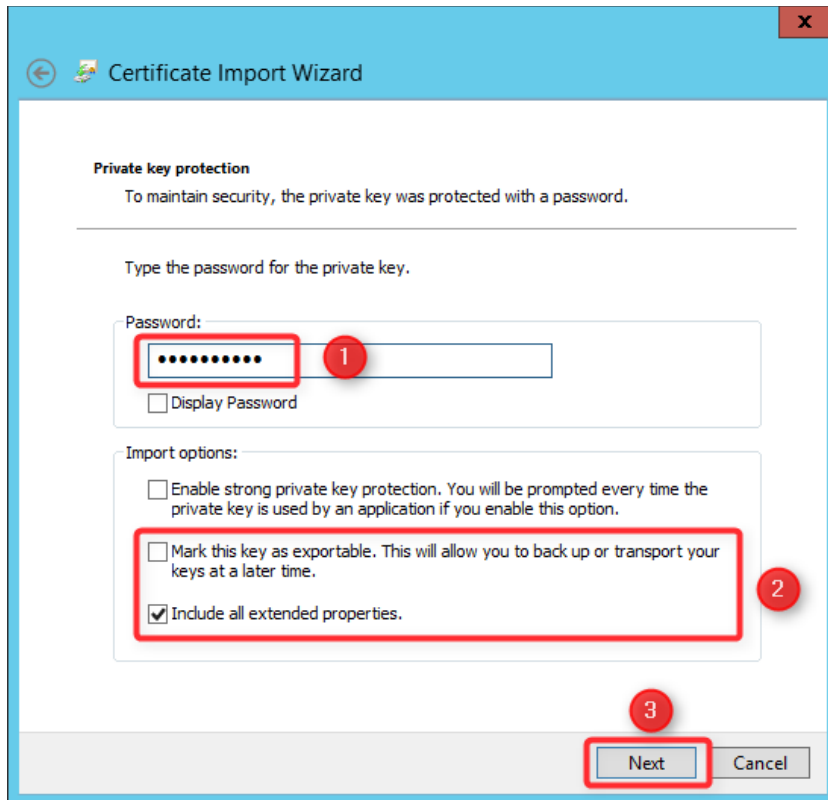
1. Select the certificate store to install to
2. Click "Next"



1. Make sure the correct certificate is selected
2. Click "Next"

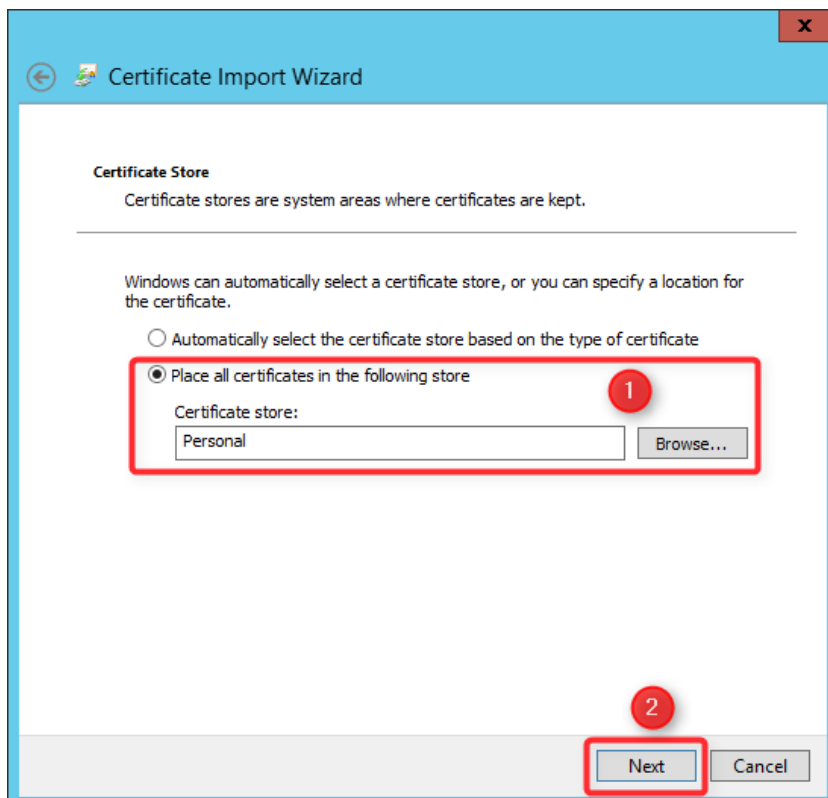


1. Enter the certificate password
2. Make sure the correct options are selected
3. Click "Next"



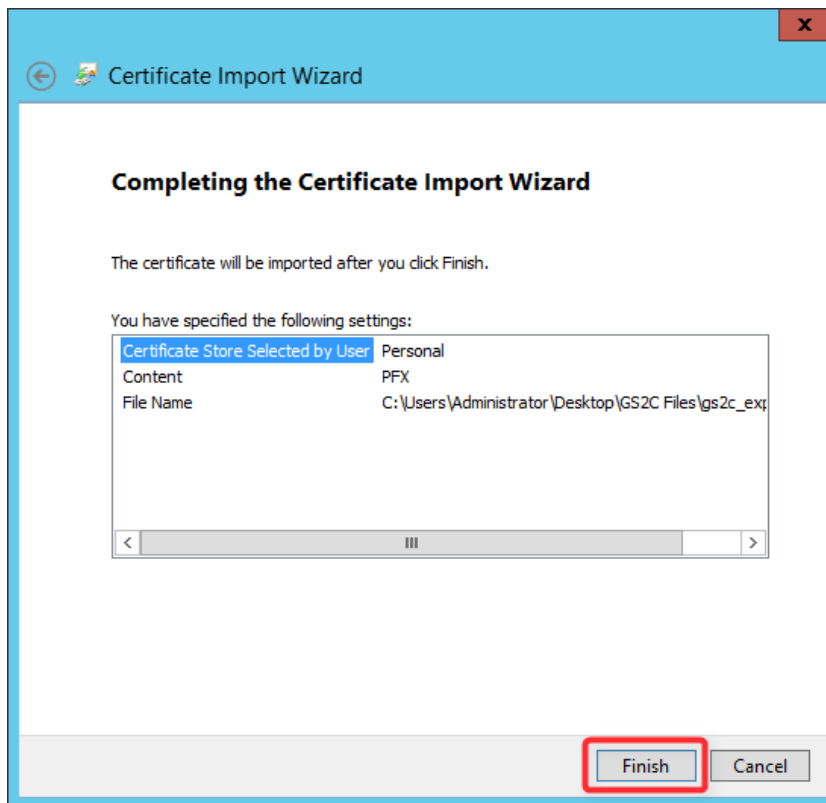
The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Private key protection' step. The window has a blue header bar with a back arrow and the title 'Certificate Import Wizard'. Below the header, the text reads 'Private key protection' and 'To maintain security, the private key was protected with a password.' A section titled 'Type the password for the private key.' contains a 'Password:' label and a text box with masked characters (dots). A red box highlights the text box, and a red circle with the number '1' is next to it. Below the text box is a checkbox labeled 'Display Password'. Another section titled 'Import options:' contains three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.', 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.', and 'Include all extended properties.' A red box highlights the 'Mark this key as exportable' checkbox, and a red circle with the number '2' is next to it. At the bottom right, there are 'Next' and 'Cancel' buttons. A red box highlights the 'Next' button, and a red circle with the number '3' is next to it.

1. Select the certificate store
2. Click "Next"

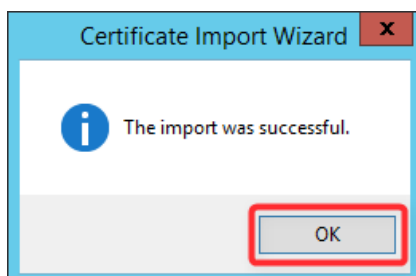


The screenshot shows the 'Certificate Import Wizard' window, specifically the 'Certificate Store' step. The window has a blue header bar with a back arrow and the title 'Certificate Import Wizard'. Below the header, the text reads 'Certificate Store' and 'Certificate stores are system areas where certificates are kept.' A section titled 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' contains two radio buttons: 'Automatically select the certificate store based on the type of certificate' and 'Place all certificates in the following store'. A red box highlights the 'Place all certificates in the following store' radio button, and a red circle with the number '1' is next to it. Below the radio button is a 'Certificate store:' label and a text box containing 'Personal'. A 'Browse...' button is to the right of the text box. At the bottom right, there are 'Next' and 'Cancel' buttons. A red box highlights the 'Next' button, and a red circle with the number '2' is next to it.

Click "Finish"



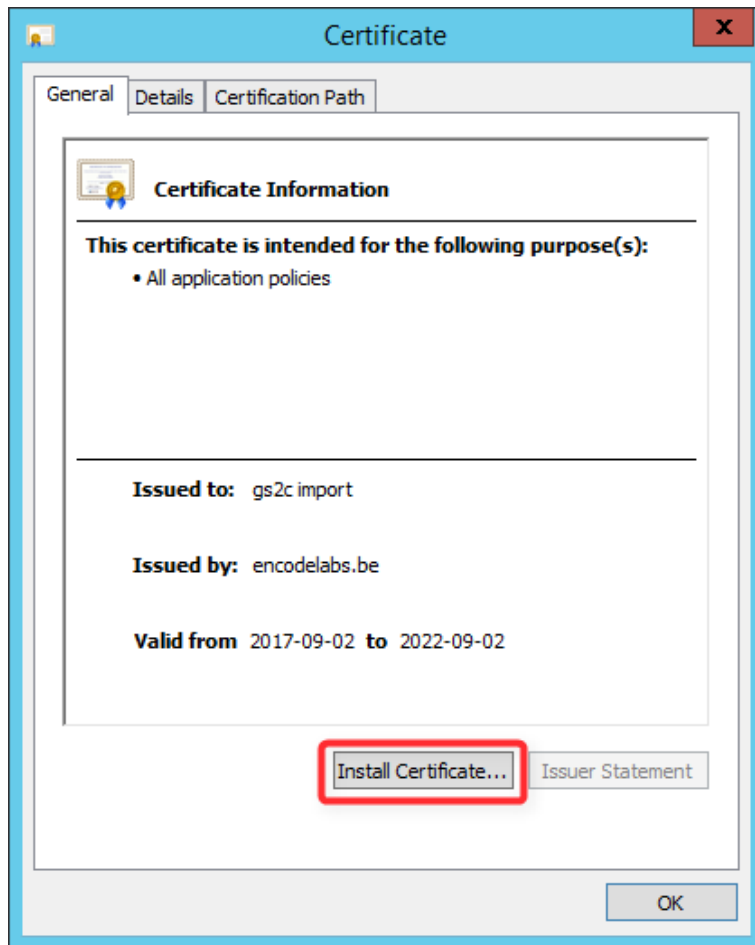
Click "OK"





## Importing a certificate without keys

Open the certificate and Click "Install Certificate"



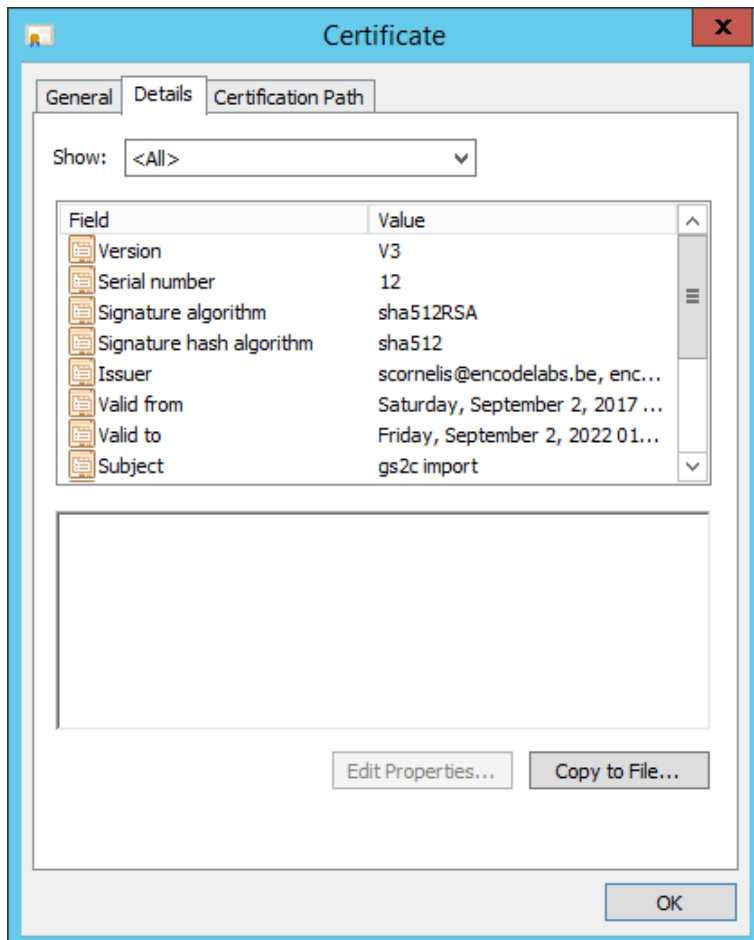
From here on, follow the same procedure as installing a certificate with a key. The only difference will be that you do not have to enter a password for importing the key, nor set the options for it.

## Obtaining the required details from your certificates

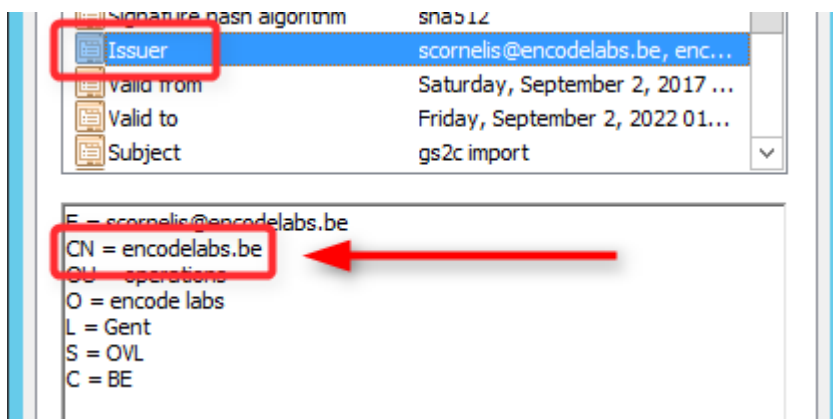
During the installation of the services, you must enter the correct details on which certificates to use. These details can be found in the following location:

Open a certificate from the certificate store (certmgr.msc)

Navigate to the details tab. Here you can find all required information:



Click on an item to show the details. In case multiple tags are present, you need to enter the value for the **CN** (Common Name).



## The certificate store name

The `storeName` values are one of the `StoreNames` enumeration, but it is recommended that it is left as 'My', indicating that the certificate store for the user account under which the service runs is where the certificate is stored.

Specifies the name of the X.509 certificate store to open.

Namespace: `System.Security.Cryptography.X509Certificates`

Assembly: `System` (in `System.dll`)

StoreName	Description
<b>AddressBook</b>	The X.509 certificate store for other users.
<b>AuthRoot</b>	The X.509 certificate store for third-party certificate authorities (CAs).
<b>CertificateAuthority</b>	The X.509 certificate store for intermediate certificate authorities (CAs).
<b>Disallowed</b>	The X.509 certificate store for revoked certificates.
<b>My</b>	The X.509 certificate store for personal certificates.
<b>Root</b>	The X.509 certificate store for trusted root certificate authorities (CAs).
<b>TrustedPeople</b>	The X.509 certificate store for directly trusted people and resources.
<b>TrustedPublisher</b>	The X.509 certificate store for directly trusted publishers.



# Chapter 3

## Installation

### Overview

PRE-REQUISITES .....	21
INSTALLATION OF THE EXPORT SERVICE .....	21
<i>Prerequisite</i> .....	21
<i>Installation</i> .....	21
<i>Configuration of the service user account</i> .....	26
INSTALLATION OF THE IMPORT SERVICE .....	27
<i>Prerequisite</i> .....	27
<i>Creation of the database</i> .....	27
<i>Installation</i> .....	28
<i>Configuration of the service user account</i> .....	34
INSTALLATION OF THE GUARD WEB APPLICATION .....	35
<i>Prerequisite</i> .....	35
<i>Installation of Internet Information Services</i> .....	35
<i>Installation of the .Net Core 2.0 Windows Hosting</i> .....	35
<i>Installation of the main website</i> .....	37
<i>Installation of the image hosting website</i> .....	39
<i>Set the authentication for both sites</i> .....	40

## Pre-requisites

Before beginning the installation, make sure you have the following:

- All required Software Packages
- Functional AD account with the required permissions
- Administrative rights on the target servers
- Certificates for data encryption and TLS
- Export Server Name(s) or IP address(es)
- Port number for hosting the export service

## Installation of the Export Service

The export service is responsible for mining data from the source system and making it available to the import service.

### Prerequisite

The following is required by the Export Service:

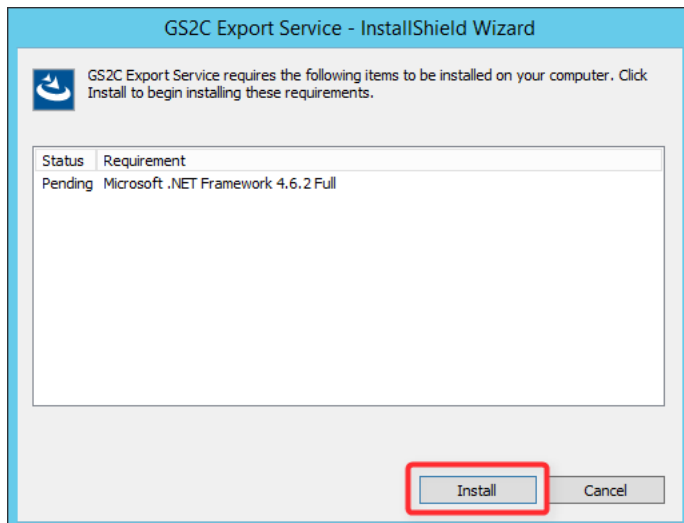
- Microsoft .Net 4.6.2 Full



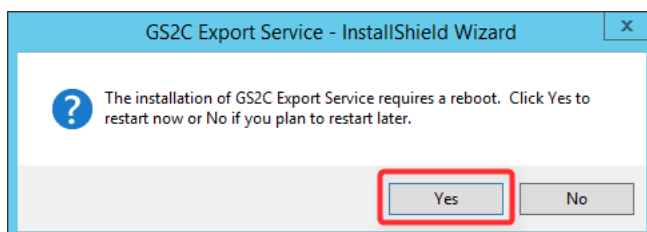
The installation of the framework requires a restart of the server to complete installation.

## Installation

If your server does not have Microsoft .Net 4.6.2 Full installed, click "Install" on the window that will appear:

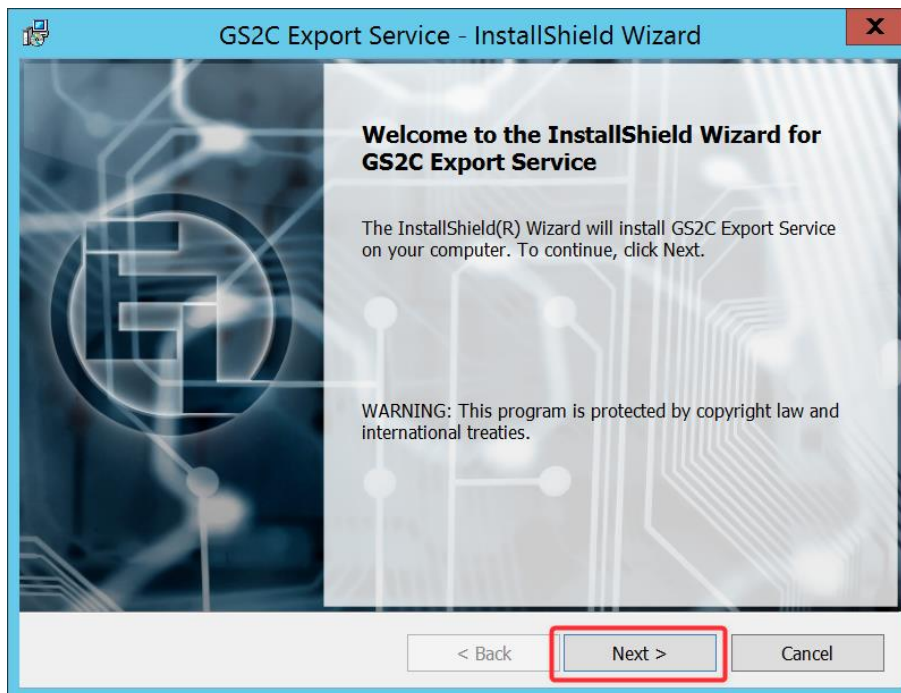


The .Net component will be installed. After the installation, reboot your server:

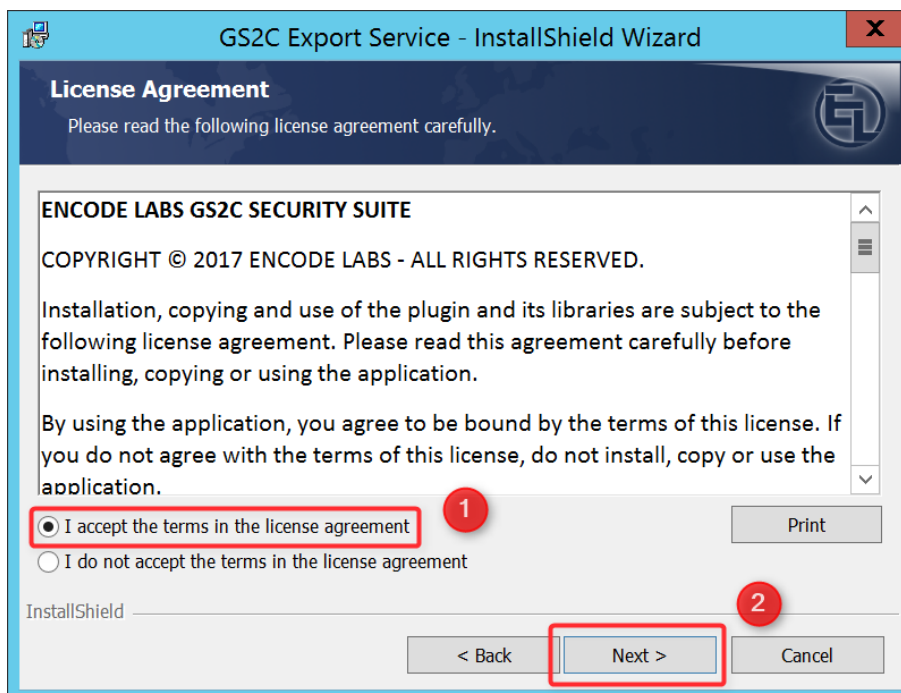


Once the server has rebooted, the installation should continue.

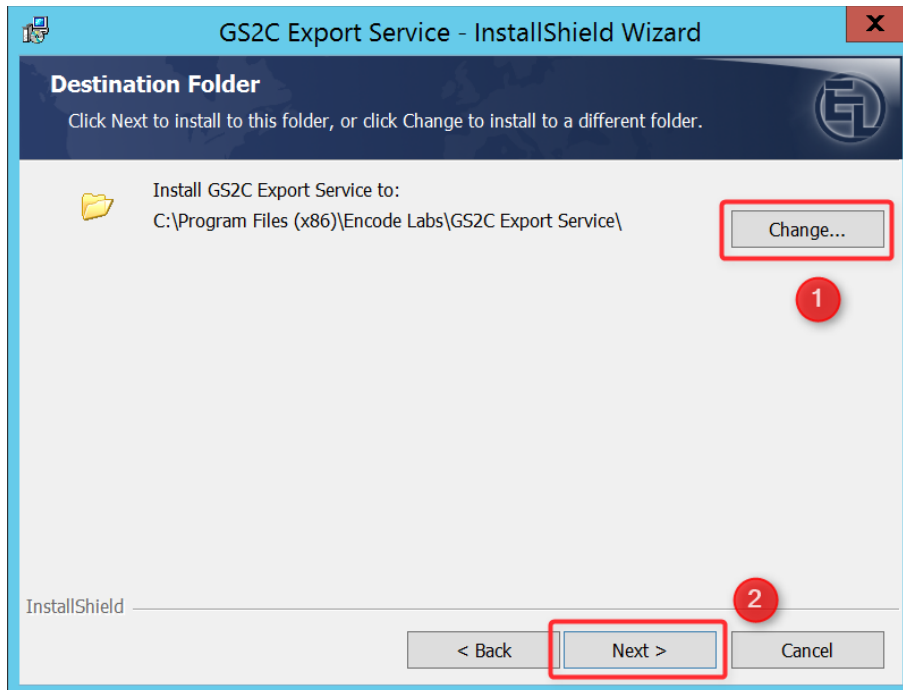
Click "Next"



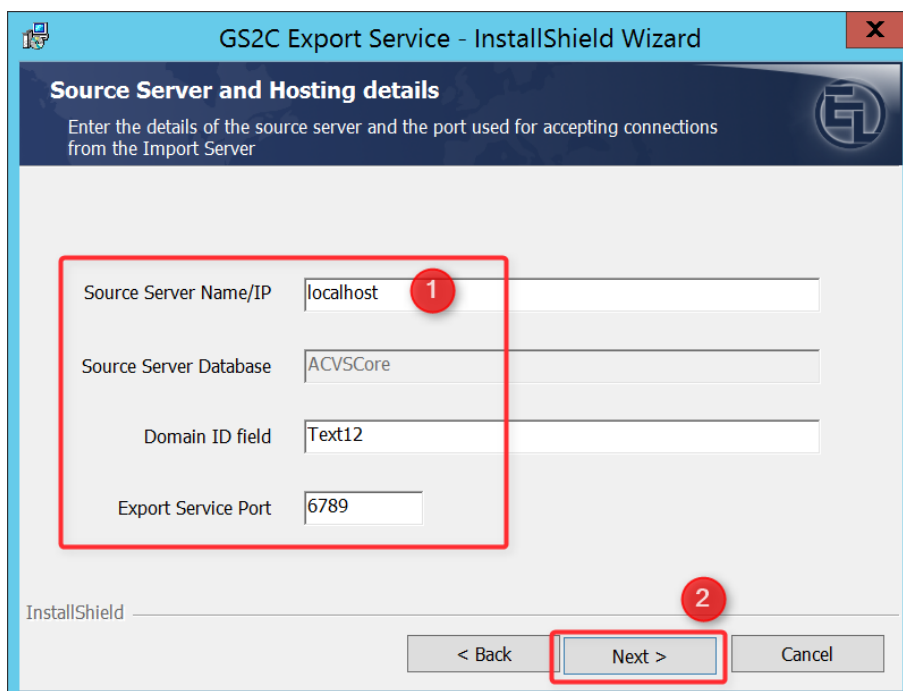
1. Check the appropriate option
2. Click "Next"



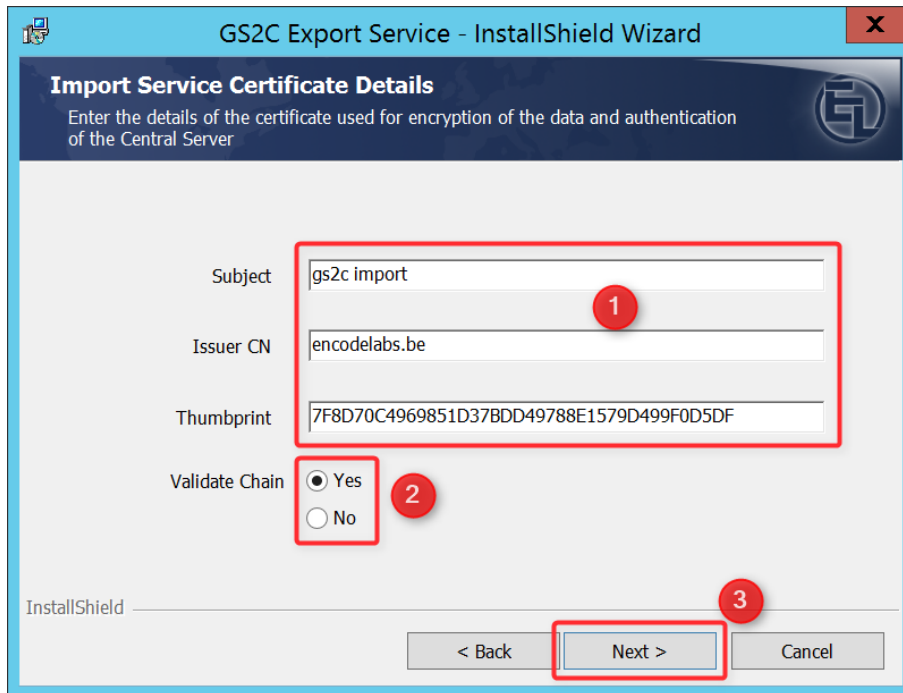
1. Change the location of the installation by clicking "Change..." and selecting the preferred location from the file dialog
2. Click "Next"



1. Enter the required details
  - a. The "Source" server hosts the database of **the system you are adding**
  - b. The DomainId field is the name of the database field that contains the person ID that is unique across all connected systems. This can be a personnel number, a login or any other unique identifier. But it must be unique system-wide.
  - c. The Export Service Port is the port on which the service will listen for connections
2. Click "Next"

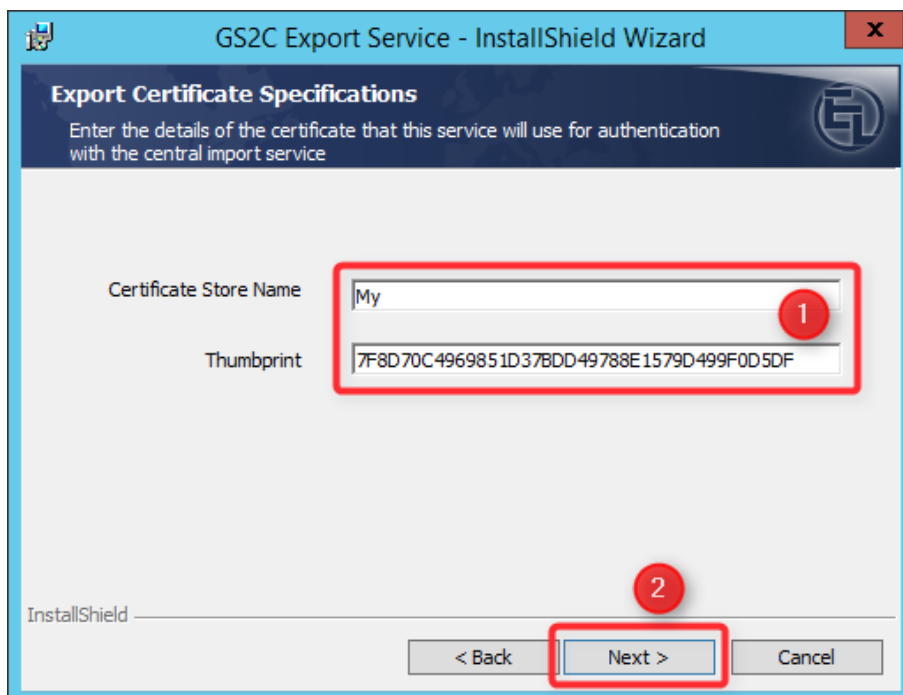


1. Enter the certificate details<sup>2</sup>
2. Select chain validation as required<sup>3</sup>



The screenshot shows the 'Import Service Certificate Details' window of the GS2C Export Service - InstallShield Wizard. The window has a blue header with the title and a close button. Below the header is a dark blue bar with the title 'Import Service Certificate Details' and a subtitle 'Enter the details of the certificate used for encryption of the data and authentication of the Central Server'. The main area contains four fields: 'Subject' with the value 'gs2c import', 'Issuer CN' with the value 'encodelabs.be', 'Thumbprint' with the value '7F8D70C4969851D37BDD49788E1579D499F0D5DF', and 'Validate Chain' with the 'Yes' radio button selected. Red circles with numbers 1, 2, and 3 highlight the 'Subject' field, the 'Validate Chain' section, and the 'Next >' button respectively. The 'Next >' button is highlighted with a red box.

1. Enter the details of the server certificate used for the export service<sup>4</sup>
2. Click "Next"



The screenshot shows the 'Export Certificate Specifications' window of the GS2C Export Service - InstallShield Wizard. The window has a blue header with the title and a close button. Below the header is a dark blue bar with the title 'Export Certificate Specifications' and a subtitle 'Enter the details of the certificate that this service will use for authentication with the central import service'. The main area contains two fields: 'Certificate Store Name' with the value 'My' and 'Thumbprint' with the value '7F8D70C4969851D37BDD49788E1579D499F0D5DF'. Red circles with numbers 1 and 2 highlight the 'Certificate Store Name' field and the 'Next >' button respectively. The 'Next >' button is highlighted with a red box.

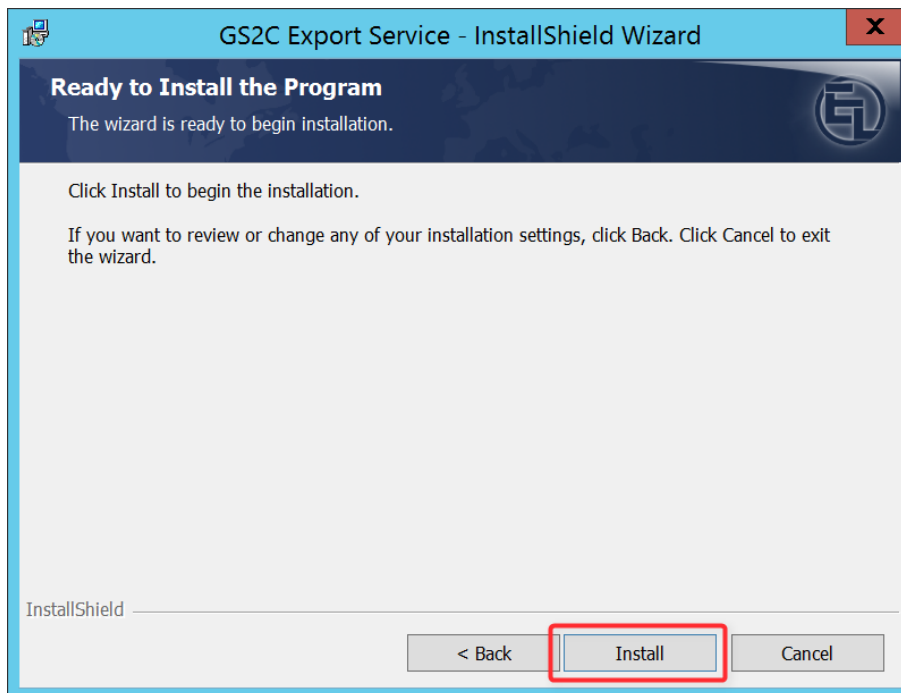
<sup>2</sup> Instructions on locating this information can be found under [Obtaining the required details from your certificates](#) on page 17.

<sup>3</sup> Enable chain validation if your server has access to all the certificates in the certificate chain. If in doubt, consult with a network or certificate administrator.

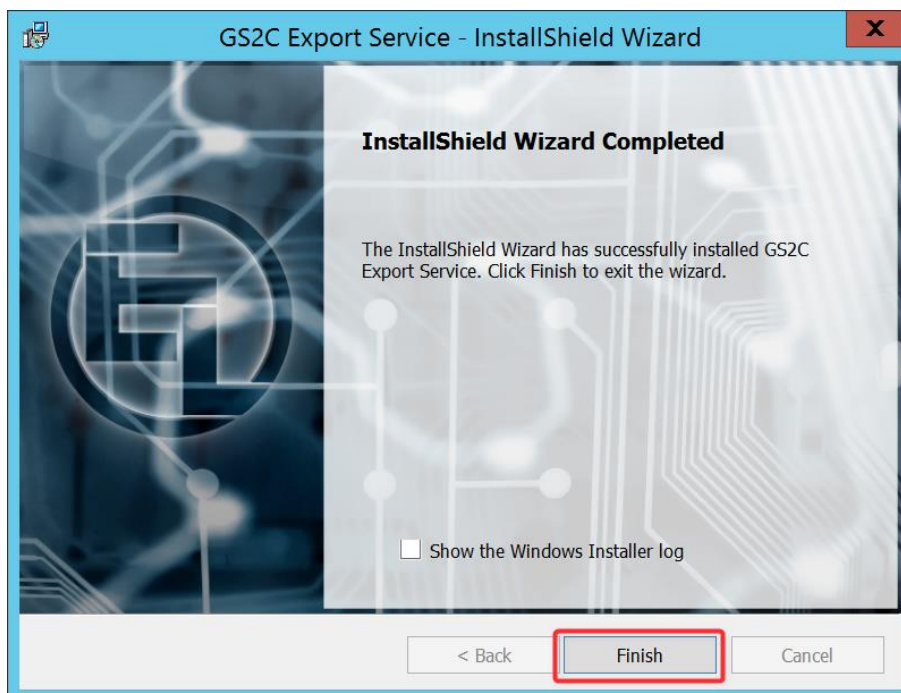
<sup>4</sup> More information on the certificate store can be found in [The certificate store name](#) on page 19.



Click "Install"



Click "Finish"

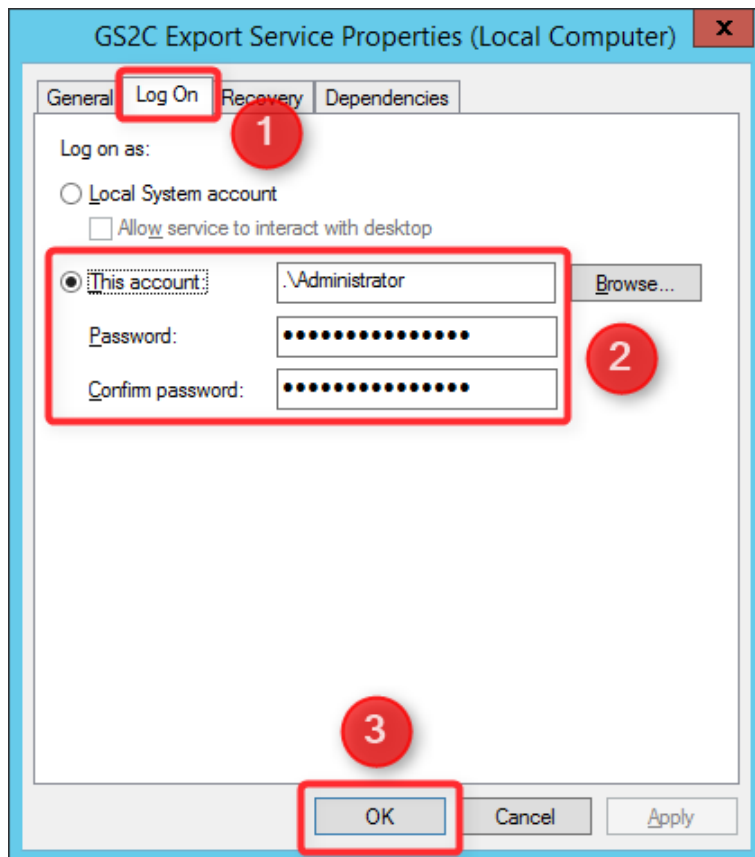


## Configuration of the service user account

Open the services.msc application

Right-click the "GS2C Export Service" and select "Properties"

1. Select the "Log On" tab
2. Enter the credentials of the account that will run the service
3. Click "OK"



## Installation of the Import Service

The import service is responsible for gathering data from all connected export servers as well as offering other services to other modules.

### Prerequisite

The following is required by the Import Service:

- Microsoft .Net 4.6.2 Full
- Microsoft SQL Server 2012R2 minimum
- Domain Functional Account for running the service
- Local administration rights on the server



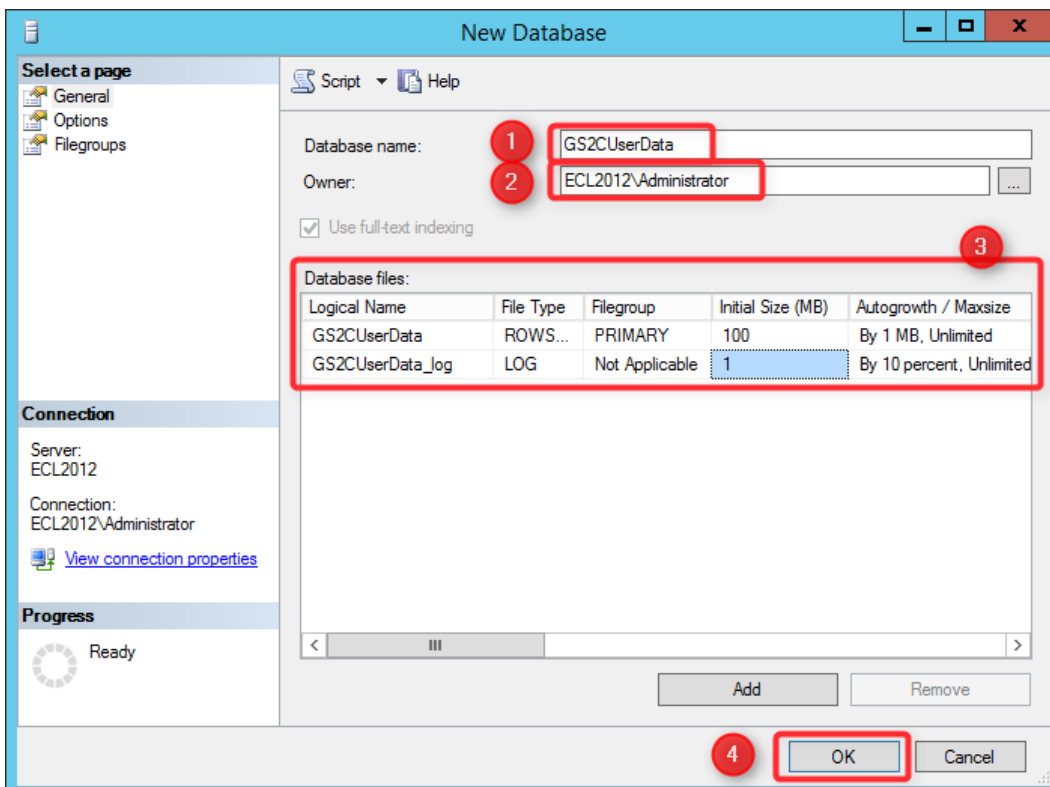
The installation of the framework requires a restart of the server to complete installation.

### Creation of the database

On your database server, create a database called GS2CUserData. Set the owner to the account that will run the import service.

Example in MSSQL:

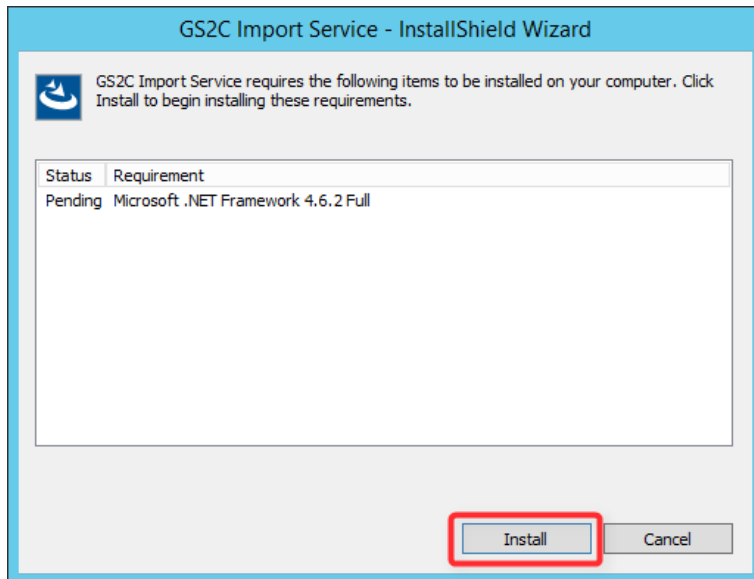
1. Enter the database name
2. Select the user that will be the owner (this is the account running the import service)
3. Set the required options
  - a. You should check with the SQL Administrators if there are any specific requirements
4. Click "OK"



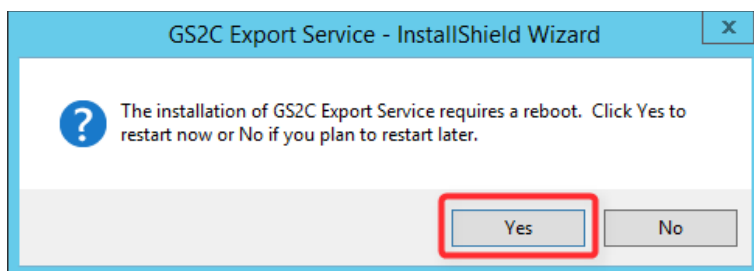
Logical Name	File Type	Filegroup	Initial Size (MB)	Autogrowth / Maxsize
GS2CUserData	ROWS...	PRIMARY	100	By 1 MB, Unlimited
GS2CUserData_log	LOG	Not Applicable	1	By 10 percent, Unlimited

## Installation

If your server does not have Microsoft .Net 4.6.2 Full installed, click "Install" on the window that will appear:

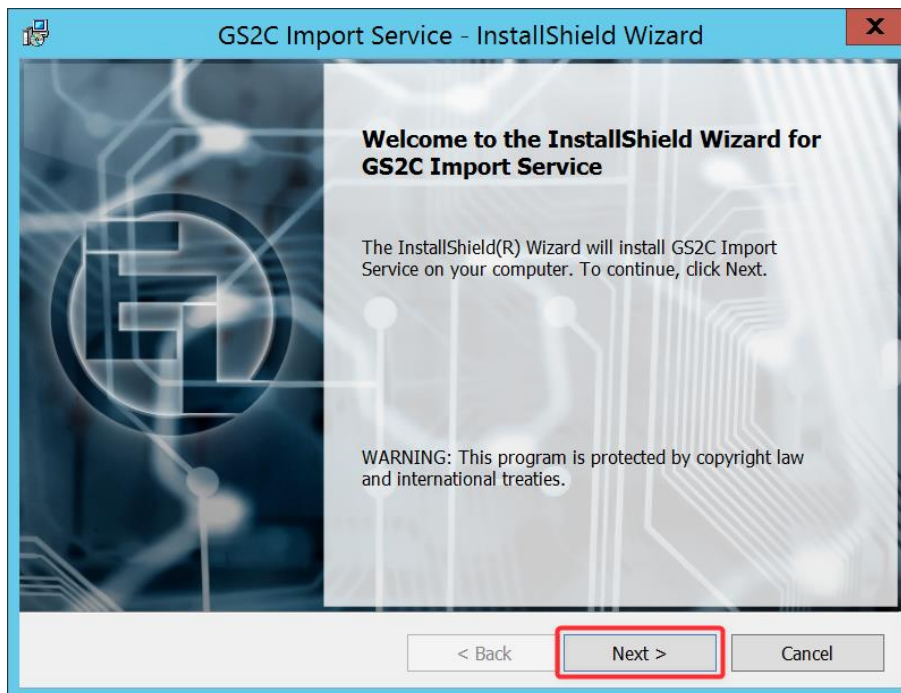


The .Net component will be installed. After the installation, reboot your server:

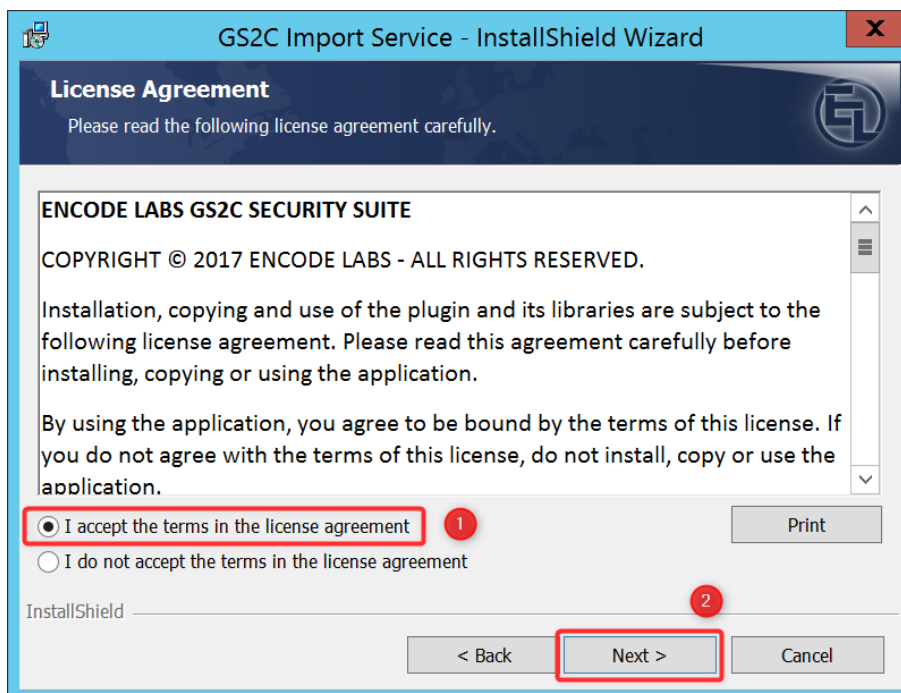


Once the server has rebooted, the installation should continue.

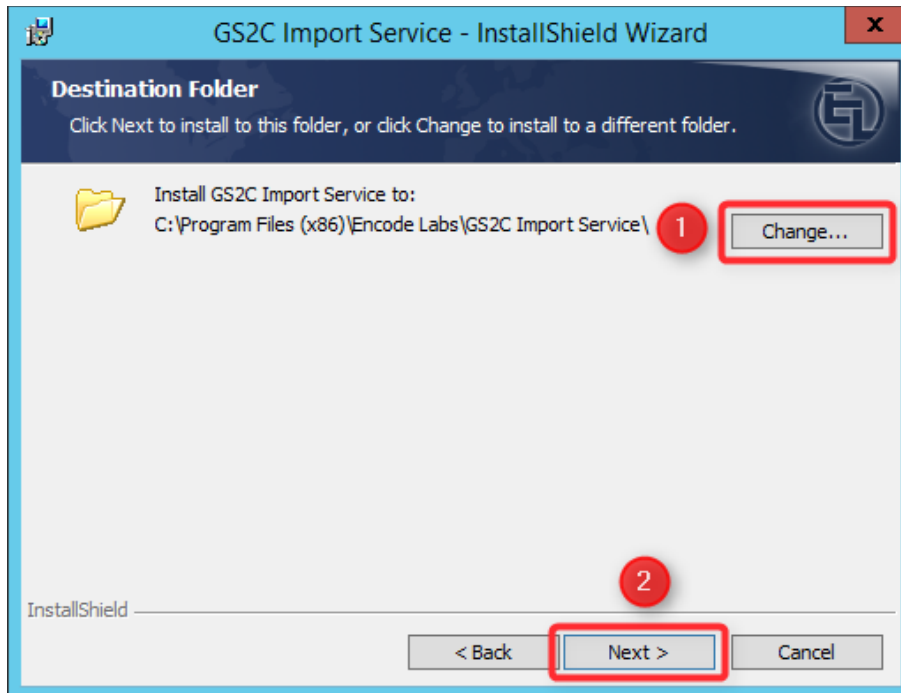
Click "Next"



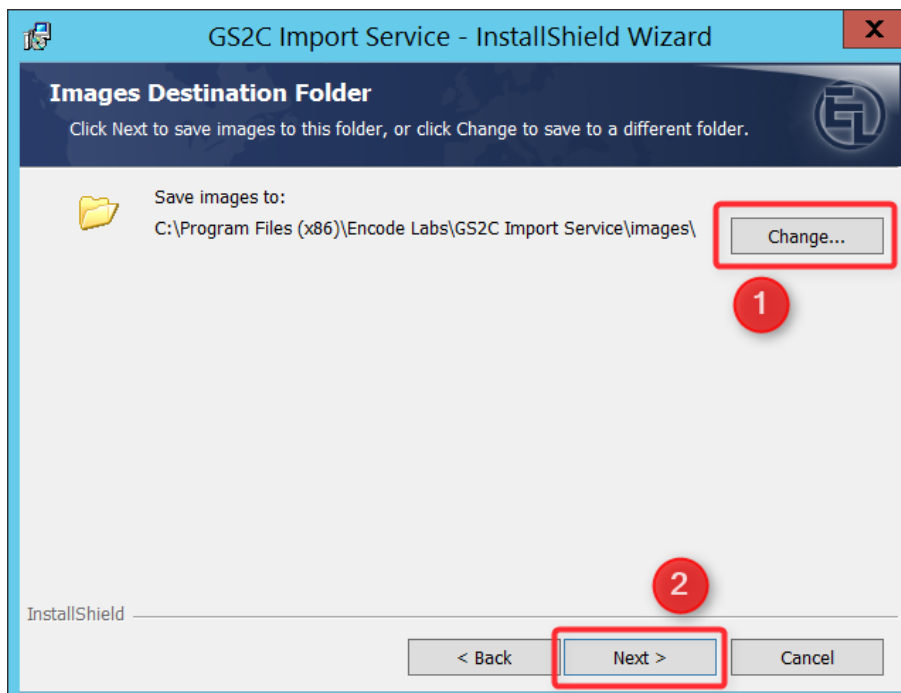
1. Check the appropriate option
2. Click "Next"



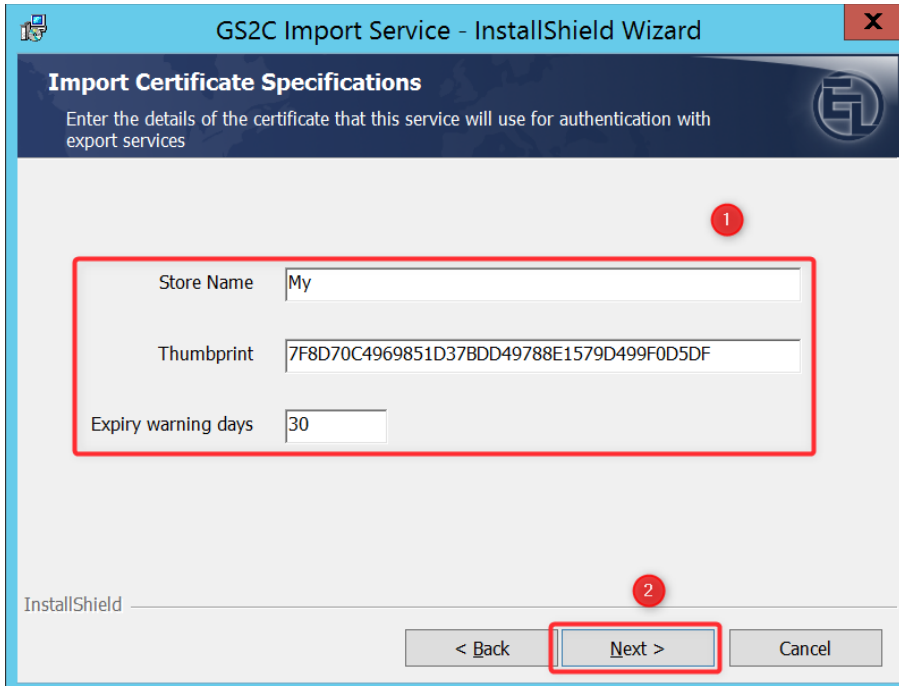
1. Change the location of the installation by clicking "Change..." and selecting the preferred location from the file dialog
2. Click "Next"



1. Change the location where the image files will be saved by clicking "Change..." and selecting the preferred location from the file dialog
2. Click "Next"

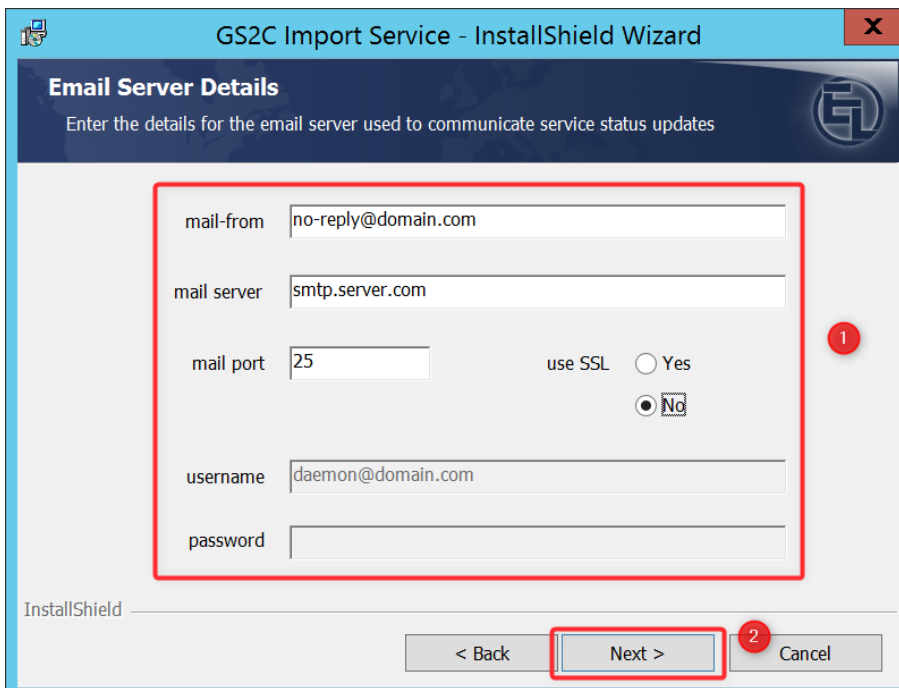


1. Enter the required details
  - a. For information on the expiry warning days, refer to [Certificate](#) on page 13
2. Click "Next"



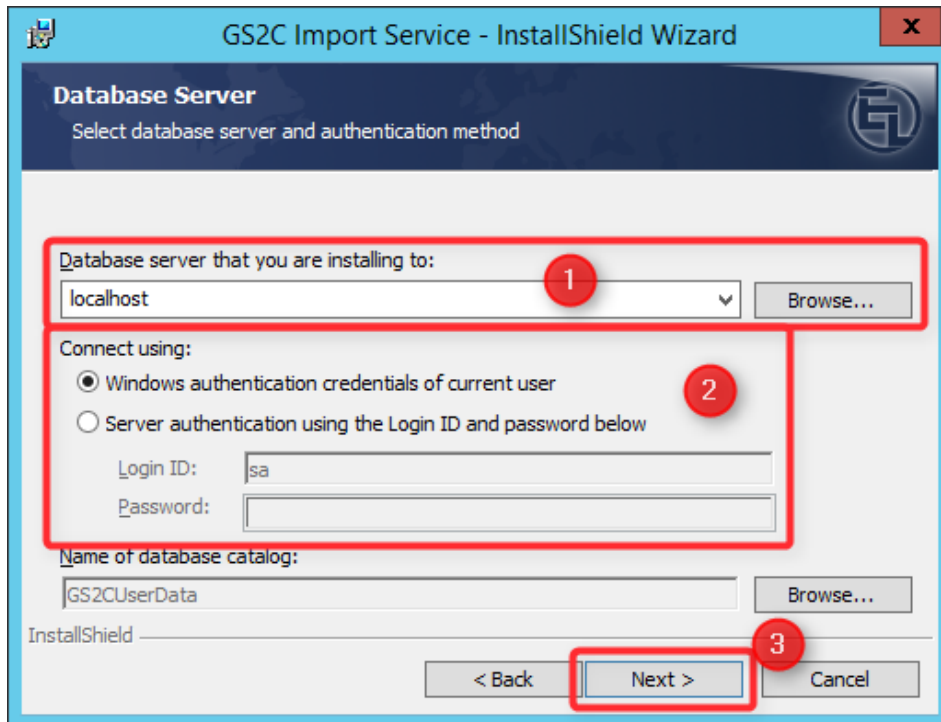
The screenshot shows the 'Import Certificate Specifications' window of the GS2C Import Service - InstallShield Wizard. The window has a blue header bar with the title and a close button. Below the header, there's a dark blue bar with the title 'Import Certificate Specifications' and a sub-header 'Enter the details of the certificate that this service will use for authentication with export services'. The main area contains three input fields: 'Store Name' with the value 'My', 'Thumbprint' with the value '7F8D70C4969851D37BDD49788E1579D499F0D5DF', and 'Expiry warning days' with the value '30'. A red box highlights these three fields, with a red circle containing the number '1' next to it. At the bottom, there's a 'Next >' button highlighted with a red box and a red circle containing the number '2'. There are also '< Back' and 'Cancel' buttons.

1. Enter the required details for your email server
2. Click



The screenshot shows the 'Email Server Details' window of the GS2C Import Service - InstallShield Wizard. The window has a blue header bar with the title and a close button. Below the header, there's a dark blue bar with the title 'Email Server Details' and a sub-header 'Enter the details for the email server used to communicate service status updates'. The main area contains several input fields and a checkbox: 'mail-from' with the value 'no-reply@domain.com', 'mail server' with the value 'smtp.server.com', 'mail port' with the value '25', 'username' with the value 'daemon@domain.com', and a 'password' field. There's also a 'use SSL' checkbox with 'Yes' and 'No' radio buttons, where 'No' is selected. A red box highlights the 'mail-from', 'mail server', 'mail port', 'username', and 'password' fields, with a red circle containing the number '1' next to it. At the bottom, there's a 'Next >' button highlighted with a red box and a red circle containing the number '2'. There are also '< Back' and 'Cancel' buttons.

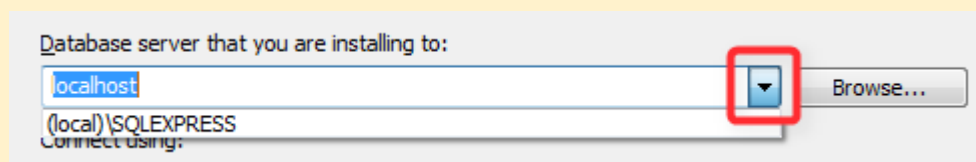
1. Enter the name of the database server
  - a. Alternatively, you can use the drop-down button or click "Browse..." to select the correct server
2. Enter the correct details.
  - a. If using windows authentication, make sure you are logged in with the account that will run the service and is database owner
3. Click "Next"



When using SQL Express, you must enter the named instance of the server as well.

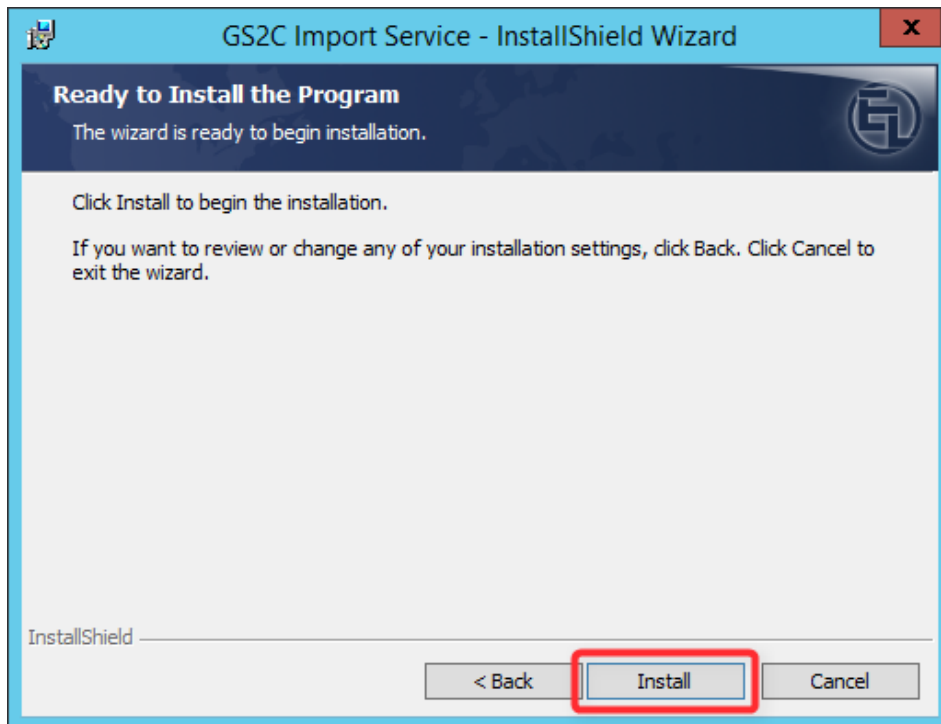
The default value is `(local)\SQLEXPRESS`

You can select the name by selecting the server name from the dropdown box when it is installed on the same server, or by clicking "Browse..." and browsing for the correct named instance.

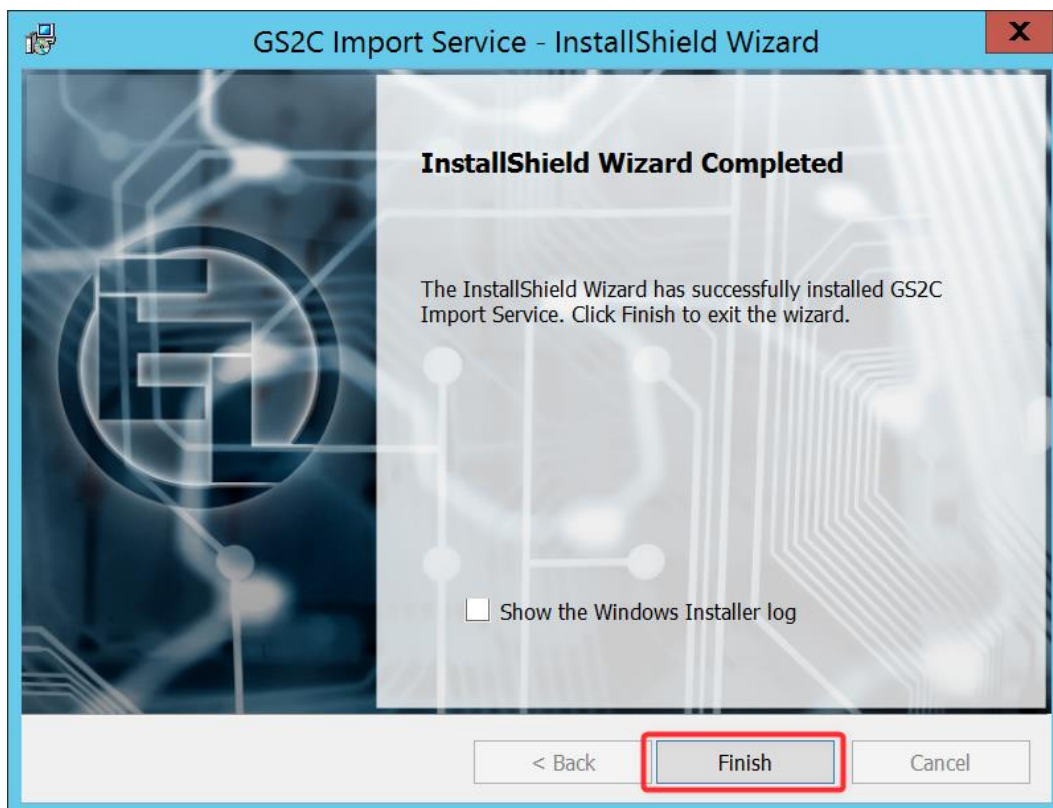




Click "Install"



Click "Finish"

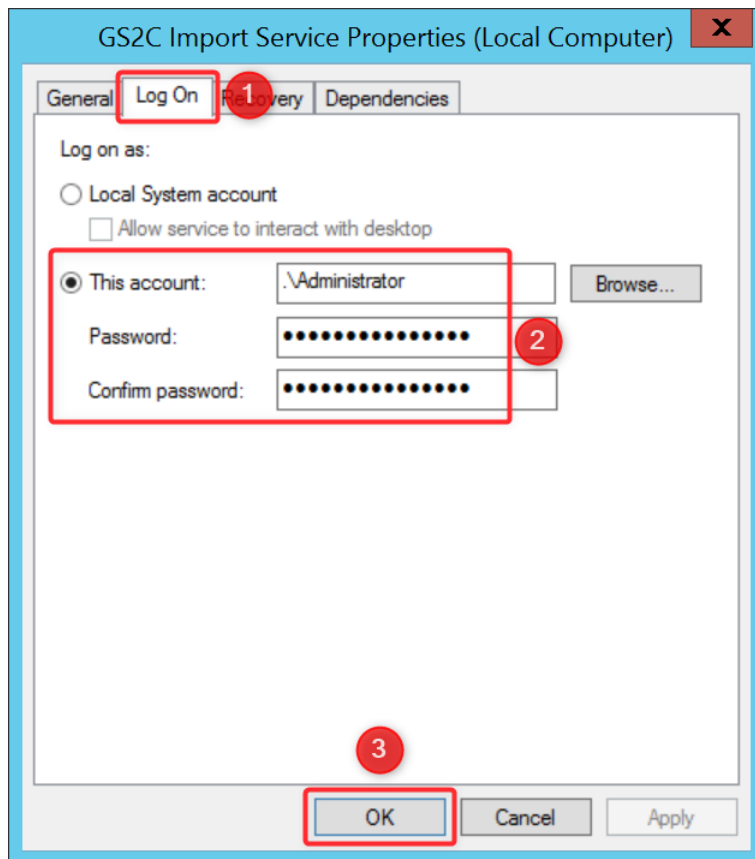


## Configuration of the service user account

Open the services.msc application

Right-click the "GS2C Import Service" and select "Properties"

1. Select the "Log On" tab
2. Enter the credentials of the account that will run the service
3. Click "OK"



## Installation of the Guard Web Application

The Guard Web Application provides a web interface to query the database of known personnel, their activation state and the cards owned as well as the state of the cards.

The server is split into two parts: the main web server and a separate image server. This makes it possible to host the images on a separate file server if preferred.

### Prerequisite

The following is required to host the Guard Web App:

- Microsoft .Net Core 2.0 Windows Server Hosting
- Internet Information Server
- Domain Functional Account for running the service
- Local administration rights on the server
- GS2C Import Service must be installed for populating the database



The installation of the framework requires a restart of the server to complete installation.

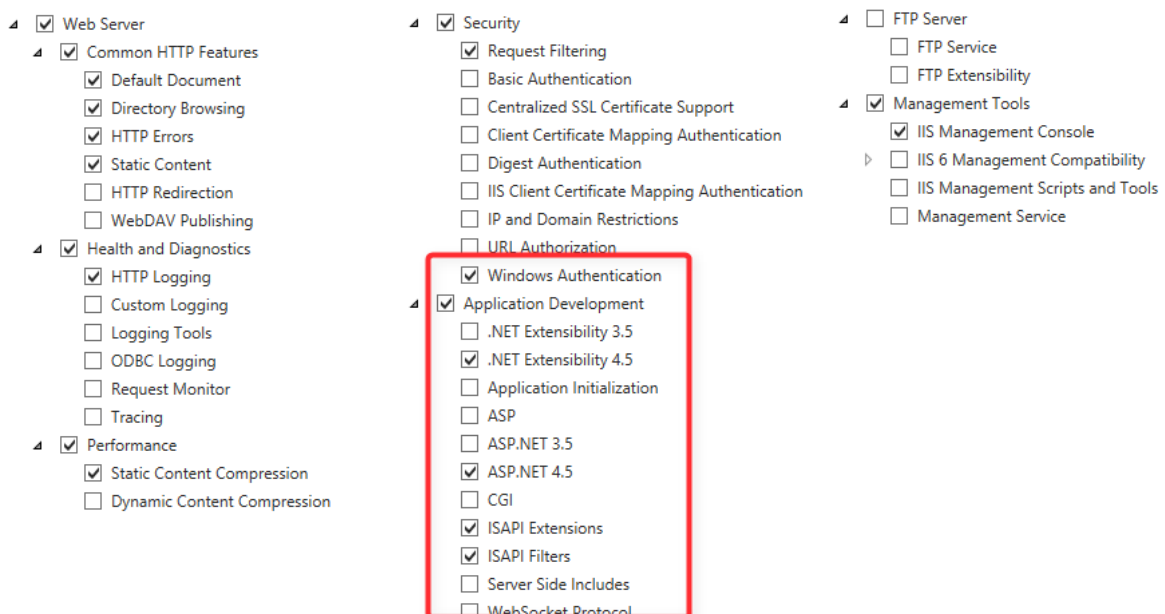
The Guard Web App only functions on a domain as the users must be part of an AD group to be able to use the service.

## Installation of Internet Information Services

Install IIS on your server with the following options:



The screenshots below show the configuration of the validation server. The items marked in the red box are the minimum required options. Depending on your own installation requirements it is possible more options are selected.



## Installation of the .Net Core 2.0 Windows Hosting

Download the .Net Core Web Hosting Runtime installer from Microsoft. It should be located here:

<https://www.microsoft.com/net/download/windows>

## Other Windows Downloads

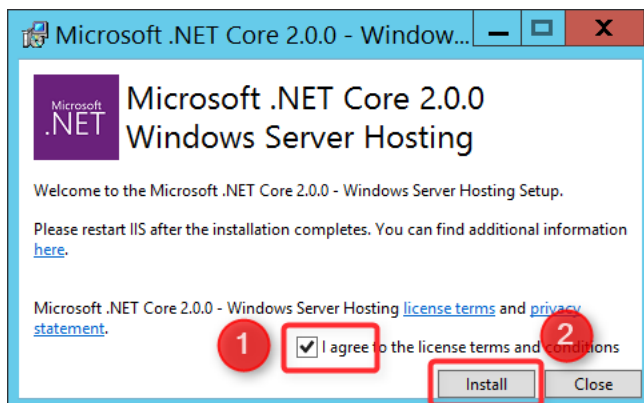
### .NET Core

.NET Core is a cross-platform .NET implementation for websites, services, and console apps that run everywhere.

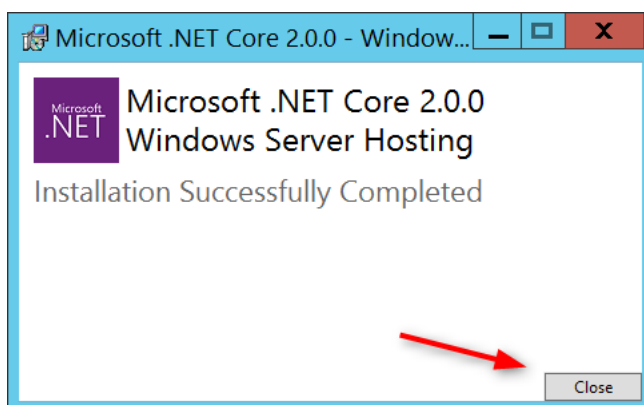
	Current ①	
x64 Installer (.exe)	<a href="#">SDK</a>	<a href="#">Runtime</a>
x86 Installer (.exe)	<a href="#">SDK</a>	<a href="#">Runtime</a>
x64 Binaries (.zip)	<a href="#">SDK</a>	<a href="#">Runtime</a>
x86 Binaries (.zip)	<a href="#">SDK</a>	<a href="#">Runtime</a>
Windows Server Hosting (.exe)	N/A	<a href="#">Runtime</a>
Checksums	<a href="#">SDK</a>	<a href="#">Runtime</a>

Run the installer.

1. Check the license box
2. Click "Install"



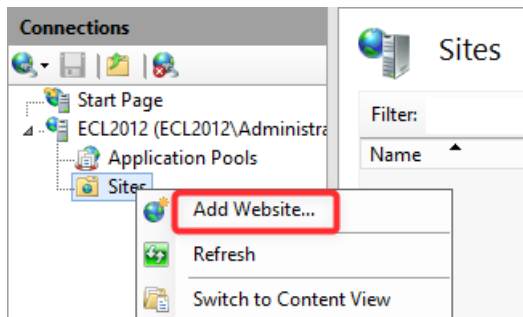
Click "Close"



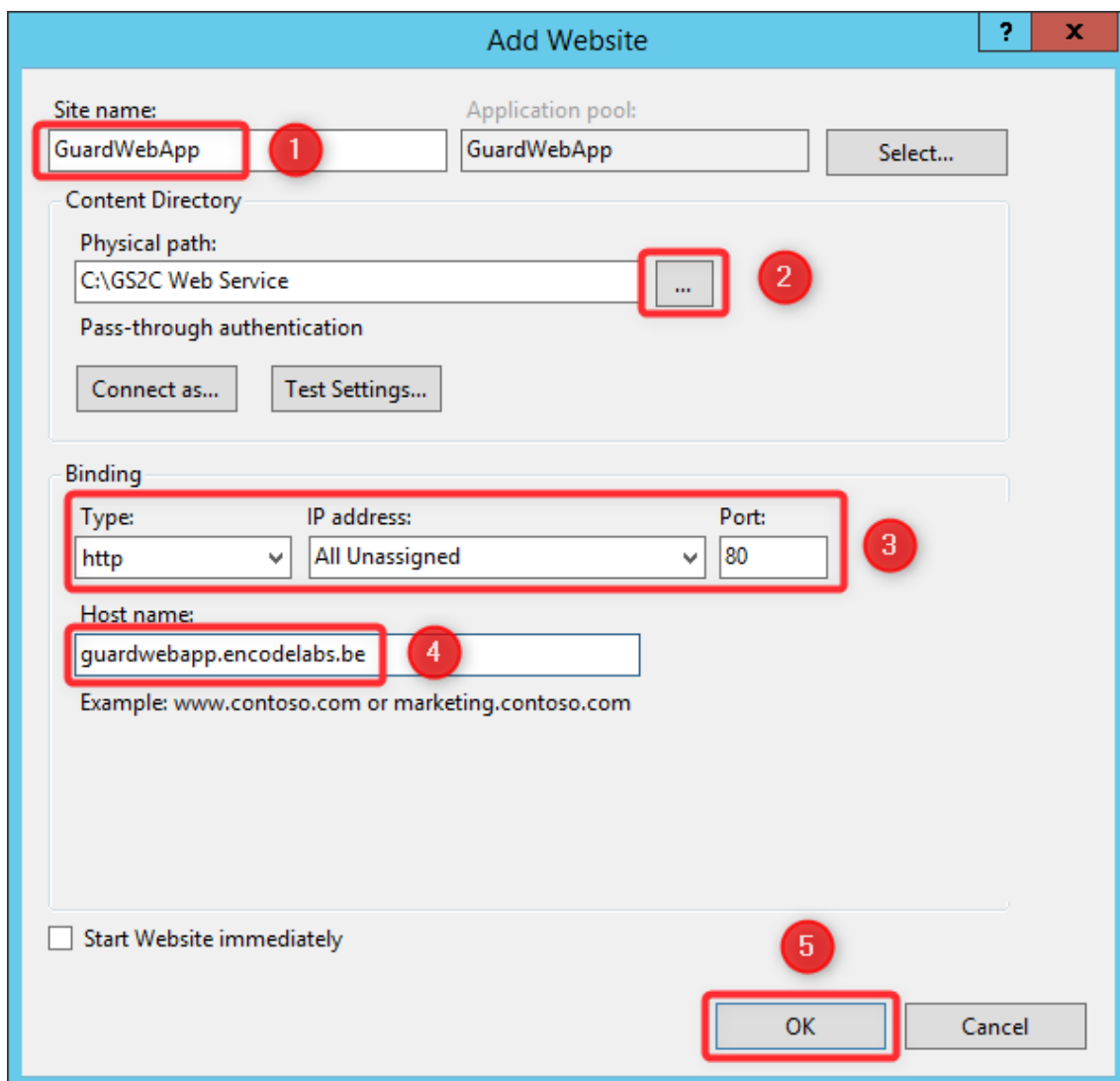
## Installation of the main website

Copy the contents of the GuardWebApp folder to a preferred location on your web server.

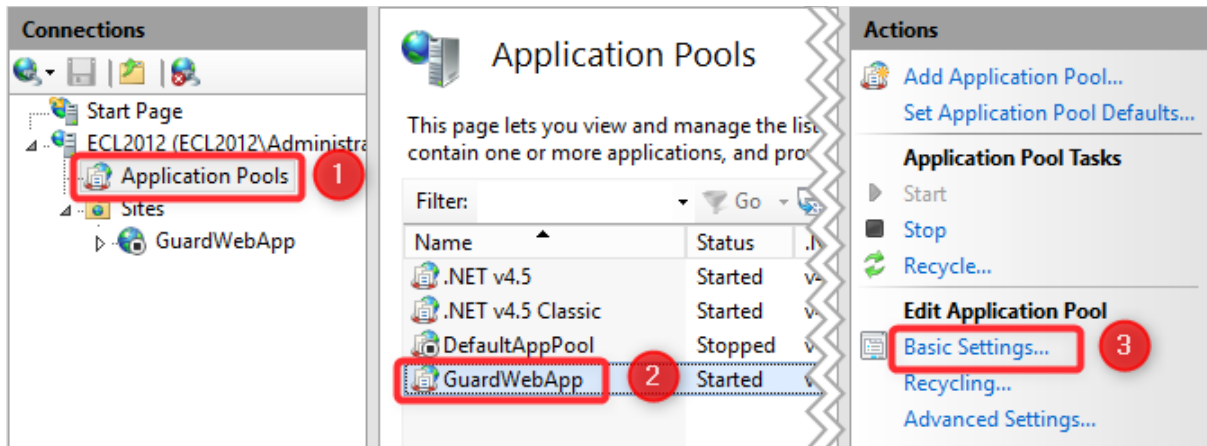
Open IIS Manager and create a new website



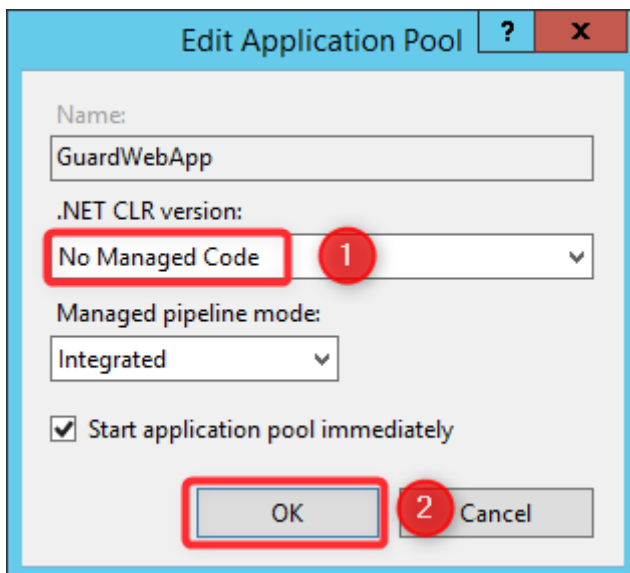
1. Enter the name for the site
2. Browse to the path where you copied the web content
3. Configure the applicable binding
4. Enter the host name/url
5. Click OK



1. Select the Application Pools
2. Select the Application Pool for the website you created
3. Click "Basic Settings"

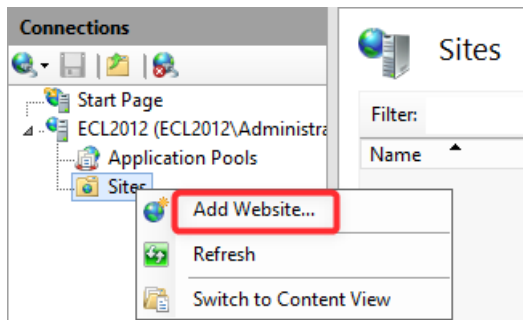


1. Set the .NET CLR Version to "No Managed Code"
2. Click OK



## Installation of the image hosting website

Add a new website



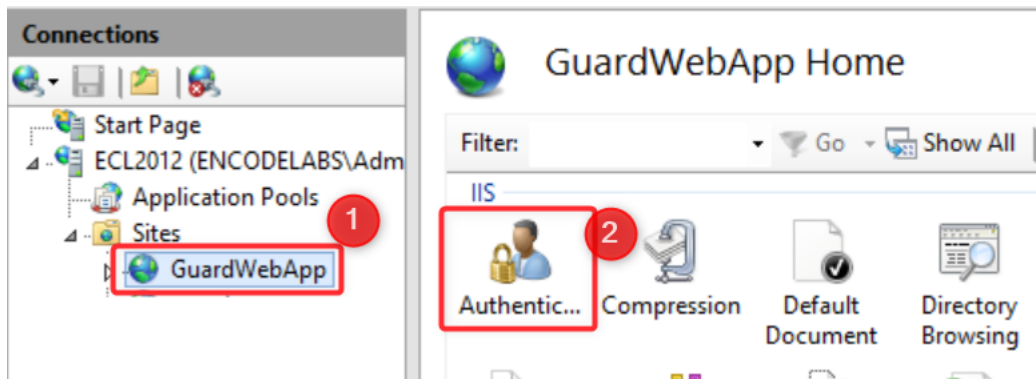
1. Enter the name for the site
2. Browse to the path where you copied the web content
3. Configure the applicable binding
4. Enter the host name/url
5. Click OK

The screenshot shows the 'Add Website' dialog box in IIS Manager. The dialog has a blue title bar with a question mark and a close button. The main content area is divided into several sections:

- Site name:** A text box containing 'gwa\_images' is highlighted with a red box and labeled with a red circle '1'.
- Application pool:** A dropdown menu showing 'gwa\_images' and a 'Select...' button.
- Content Directory:**
  - Physical path:** A text box containing 'C:\Program Files (x86)\Encode Labs\GS2C Import Service' is highlighted with a red box and labeled with a red circle '2'. A browse button ('...') is also highlighted with a red box.
  - Pass-through authentication:** A checkbox that is currently unchecked.
  - Buttons:** 'Connect as...' and 'Test Settings...' buttons.
- Binding:**
  - Type:** A dropdown menu showing 'http' is highlighted with a red box and labeled with a red circle '3'.
  - IP address:** A dropdown menu showing 'All Unassigned' is highlighted with a red box.
  - Port:** A text box containing '8080' is highlighted with a red box.
  - Host name:** A text box containing 'guardwebapp.encodelabs.be' is highlighted with a red box and labeled with a red circle '4'.
  - Example:** 'Example: www.contoso.com or marketing.contoso.com'.
- Start Website immediately:** A checkbox that is checked.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom right. The 'OK' button is highlighted with a red box and labeled with a red circle '5'.

## Set the authentication for both sites

1. Select the website
2. Select "Authentication"



- Disable anonymous authentication
- Enable Windows Authentication

## Authentication

Group by: No Grouping		
Name	Status	Response Type
Anonymous Authentication	Disabled	
Windows Authentication	Enabled	HTTP 401 Challenge

Do the same for the image website.

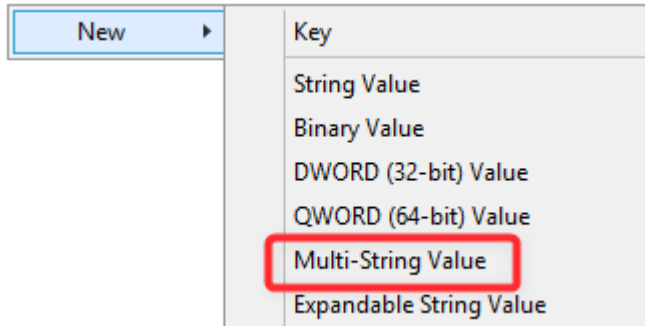


## Configure the BackConnectionHostNames key

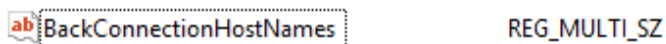
Open the registry editor.

Navigate to HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0

Add a Multi-String value

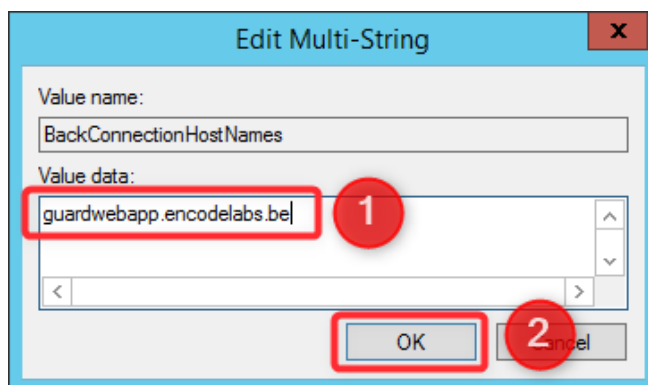


Name the string BackConnectionHostNames

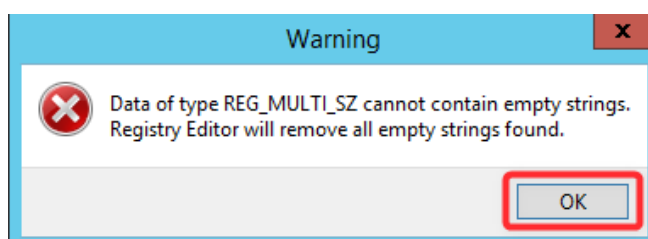


Double Click the key to edit it.

1. enter the Host Name of the website that you will host the application on
2. Click OK



Click OK





# Chapter 4

## Configuration

### Overview

CONFIGURATION TASKS .....	43
CONFIGURING THE EXPORT SERVICE .....	43
ServerSettings .....	43
ImportServiceCertificateValidation .....	43
ExportServiceCertificateSpec .....	43
DataSettings .....	43
MaxImageSizeSettings .....	44
CONFIGURING THE IMPORT SERVICE .....	45
Database Connection .....	45
Certificates .....	45
Email sender details .....	45
Owner emails .....	46
Synchronization .....	47
Logging .....	47
CONFIGURING THE WEB APPLICATION .....	48
<i>Configure the database connection .....</i>	<i>48</i>
<i>Set the image hosting address .....</i>	<i>48</i>
<i>Configure the AD group allowed to access the service .....</i>	<i>48</i>

## Configuration tasks

While some basic aspects of the service are configured during installation, it is possible to change the configuration of the services by editing the configuration files or updating configuration settings in the database.



When changing a service configuration, a restart of the service may be required for the changes to be taken into account.

The following configuration tasks exist:

- [Configuring the Export Service](#) on page 43
- [Configuring the Import Service](#) on page 45
- [Configuring the Web Application](#) on page 48

## Configuring the Export Service

The configuration of the export service is located in the file `appsettings.json`.

It contains the following configuration sections:

### ServerSettings

PortNumber: This is the port on which the Export Service will be hosted.

### ImportServiceCertificateValidation

Contains all data related to the Import Service Certificate. For more details on these fields, refer to the table under [Certificate validation](#) on page 12.

Sample Configuration:

```
"ImportServiceCertificateSpec": {
  "Subject": "CN=gs2c import",
  "IssuerCN": "CN=encodelabs.be",
  "Thumbprint": "7F8D70C4969851D37BDD49788E1579D499F0D5DF",
  "VerifyChain": "true"
}
```

### ExportServiceCertificateSpec

Contains all data related to the Export Service Certificate. For more details on these fields, refer to the table under [Certificate validation](#) on page 12.

Sample Configuration:

```
"ExportServiceCertificateSpec": {
  "Thumbprint": "EEA9CB7450D1A5877B5B5C4449623B6C65456D68",
  "StoreName": "My"
}
```

### DataSettings

Contains the database connection string, maximum batch size and the unique identifier of personnel records.

Field	Description
<b>DbConnectionString</b>	This is the connection string for the source server database.
<b>MaxBatchSize</b>	The number of records that are included in a single upload batch. As the database can be very large, the upload process is split up into several batches to improve record processing.
<b>DomainIdField</b>	The field containing the Unique Id of the personnel record, which is known across all connected systems.

#### Sample Configuration:

```
"DataSettings": {  
  "DbConnectionString": "Data Source=localhost;Integrated Security=True;  
  Persist Security Info=False;Pooling=False;MultipleActiveResultSets=False;  
  Connect Timeout=60;Encrypt=False;TrustServerCertificate=True;  
  Database=ACVSCore",  
  "MaxBatchSize": "100",  
  "DomainIdField": "Text12"  
}
```

#### MaxImageSizeSettings

This setting controls the maximum dimensions of the images returned to the import service. Images will be scaled, preserving aspect ratio but will not exceed either of those dimensions.

#### Sample Configuration:

```
"MaxImageSizeSettings": {  
  "MaxHeight": 800,  
  "MaxWidth": 600  
}
```

## Configuring the Import Service

The configuration of the import service is located in the file [EncodeLabs.GS2C.ExportService.exe.config](#)

There are several configuration sections. The most important ones are:

- Database Connection
- Certificates
- Email
- Synchronization
- Logging

### Database Connection

ConnectionString contains the database connection string for the import service.

Sample configuration:

```
<connectionStrings>
  <add
    name="userDataDb"
    connectionString="Data Source=(localdb)\MSSQLLocalDB;Integrated
Security=True;Persist Security Info=False;Pooling=False;
MultipleActiveResultSets=False;Connect Timeout=60;Encrypt=False;
TrustServerCertificate=True;Database=GS2CUserData"
    providerName="System.Data.SqlClient" />
</connectionStrings>
```

### Certificates

exportCertExpiryWarningDays: specifies the number of days to start warning in advance when a registered export service certificate will expire. The warning is sent by email to the registered system administrators.

thumbprint: contains the thumbprint of the certificate used by the import service for authentication and decryption.

storeName: the certificate store containing the certificate

expiryWarningDays: specifies the number of days to start warning in advance when the import service certificate will expire.

Sample Configuration:

```
<appSettings>
  <add key="exportCertExpiryWarningDays" value="30"/>
</appSettings>

<importServiceCertGroup>
  <importServiceCert
    thumbprint="F05267FEC0CD0B24688A1E0202665D959AF52C45"
    storeName="My"
    expiryWarningDays="30"/>
</importServiceCertGroup>
```

### Email sender details

alias: the alias to use for the mail sender

email: the email address to use for the sender

host: the IP address or url of the email server

port: the network port of the email server

enableSsl: whether to use SSL for the email connection or not

userName: the user name used for authentication

password: the password used for authentication

#### Sample Configuration:

```
<mailSenderGroup>
  <mailSender
    alias="EncodeLabs Import Service"
    email="donotreply@encodelabs.be"/>
  </mailSender>
</mailSenderGroup>

<system.net>
  <mailSettings>
    <smtp
      deliveryMethod="Network">
        <network
          host="smtp.upcmail.ie"
          port="25"
          enableSsl="false"
          userName="user@domain.com"
          password="unhackablepassword" />
        </network>
      </smtp>
    </mailSettings>
  </system.net>
```

#### Owner emails

In case of a synchronization issue or a certificate that is about to expire, the import service will send an email to the registered owner of the application. Adding owners is done in the database.

The information is contained in [GS2CUserData.dbo.EmailRecipients](#)

The following query shows all configured recipients:

```
SELECT [Id]
      ,[Alias]
      ,[Email]
      ,[Culture]
FROM [GS2CUserData].[dbo].[EmailRecipients]
```

Adding an owner is done as follows:

```
INSERT INTO GS2CUserData.dbo.EmailRecipients (Id, Alias, Email, Culture)
VALUES (NEWID(), 'Steven Cornell', 'steven.cornell@encodelabs.be', 'en')
```

Where you change the values of the name and email address accordingly for each owner to add.

### Synchronization

This section contains the configuration of the synchronisation framework used for synchronising the different export servers.

Only change these settings on the request of Encode Labs support engineers.

### Logging

This section allows you to configure the logging options for the import service.

The import service uses NLog as its logging framework. For more information on the configuration of the logging options, refer to the NLog manual.

Sample Configuration:

```
<common>
  <logging>
    <factoryAdapter type="Common.Logging.NLog.NLogLoggerFactoryAdapter,
      Common.Logging.NLog41">
      <arg key="configType" value="FILE" />
      <arg key="configFile" value="~/NLog.config" />
    </factoryAdapter>
  </logging>
</common>
```

## Configuring the Web Application

The configuration of the web portal is located in the file `appsettings.json`

### Configure the database connection

DataSettings -> DbConnectionString

Sample configuration:

```
"DbConnectionString": "Server=.;Database=GS2CUserData;User  
ID=gs2cUser;Password=gs2c;MultipleActiveResultSets=True;Connect Timeout=5"
```

For more information on how to configure a connection string, navigate to

<https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax>

### Set the image hosting address

ImageSettings -> BaseUrl

```
"ImageSettings": {  
  "BaseUrl": "http://guardwebapp.encode labs.be:8080/",  
  "Extension": ".jpg"  
},
```

Set the address where the images are served. You can use a separate website hosted in IIS or get them from another location on your network.

### Configure the AD group allowed to access the service

Fill in the name of the AD group of which the users must be a member to be allowed to use the application.

```
"RequiredGroup": "Administrators"
```





# Chapter 5

## The Import Job Tool

### Overview

INTRODUCTION .....	50
IMPORT JOB TASKS .....	50
CREATING IMPORT JOBS.....	50
<i>Sample command line</i> .....	50
MODIFYING IMPORT JOBS.....	51
<i>Site Information</i> .....	51
DELETING IMPORT JOBS .....	51
CRON TRIGGER TUTORIAL.....	51
<i>Format</i> .....	51
<i>Special Characters</i> .....	52
<i>Example CRON specs:</i> .....	53

## Introduction

### Import Job Tasks

- [Creating Import Jobs](#) on page 50
- [Modifying import jobs](#) on page 51
- [Deleting import jobs](#) on page 51

### Creating Import Jobs

Creating import jobs is done through the import job tool. This tool is located in the installation folder of the GS2C Import Service, under [GS2C Import Service/ImportJobCreator](#)

An Import Job can be created from the command line as follows:

```
ImportJobCreator.exe [file -i <InputFile> ] | [site -n <siteName> -u <url> -t  
<thumbprint> [-v] [-b <size>] -c <cron string>]
```

parameter	Description
<b>-i &lt;InputFile&gt;</b>	The path to a CSV file defining the jobs to create.
<b>-n &lt;siteName&gt;</b>	The name of the site. Choose whatever helps identifying the site easily.
<b>-u &lt;url&gt;</b>	The URL for the site. Should include the protocol and optionally the port. Should not include the trailing '/'.
<b>-t &lt;thumbprint&gt;</b>	The thumbprint for the site's certificate expressed as an uppercase hex string.
<b>-v</b>	Whether to validate the certificate chain or not. Optional and defaults to false.
<b>-b &lt;batch size&gt;</b>	The number of users to retrieve in each batch from the site. Optional. Defaults to 50.
<b>-c &lt;cron spec&gt;</b>	The cron job format specification for the job, e.g. 0 0/5 * ? * *

### Sample command line

Sample to create an import job that syncs every minute with a locally installed export service:

```
ImportJobCreator.exe site -n "Main Site" -u "https://localhost:6789" -t  
"EEA9CB7450D1A5877B5B5C4449623B6C65456D68" -c "0 * * ? * *"
```

When the file verb is specified, only the -i parameter is allowed and the file specified must be a CSV file of the form

siteName, url, thumbprint, validate chain, batch size, cron spec

ImportJobCreator.exe

## Modifying import jobs

At this moment, modifying import jobs is done directly in the database.

### Site Information

Located in `GS2CUserData.dbo.ExportServiceSites`

```
SELECT [Id]
      ,[Name]
      ,[Url]
      ,[Thumbprint]
      ,[ValidateChain]
      ,[BatchSize]
FROM [GS2CUserData].[dbo].[ExportServiceSites]
```

Here you can modify the certificate thumbprints when they change, the URL of the export service etc.

## Deleting import jobs



Stop the Import Service before changing any import tasks



Only a certified engineer should make these changes. Performing these tasks wrongly can result in a non-functioning service. When in doubt, contact Encode Labs support to

Deleting import jobs is done by deleting the associated entries of a job in the following database tables:

- `dbo.QRTZ_CRON_TRIGGERS`
- `dbo.QRTZ_FIRED_TRIGGERS`
- `dbo.QRTZ_JOB_DETAILS`

You can identify the appropriate entry by their Trigger Name.

## CRON trigger tutorial

CRON is a UNIX tool that has been around for a long time, so its scheduling capabilities are powerful and proven. The CronTrigger class is based on the scheduling capabilities of cron.

CronTrigger uses "cron expressions", which are able to create firing schedules such as: "At 8:00am every Monday through Friday" or "At 1:30am every last Friday of the month".

### Format

A cron expression is a string comprised of 6 or 7 fields separated by white space. Fields can contain any of the allowed values, along with various combinations of the allowed special characters for that field. The fields are as follows:

Field Name	Mandatory	Allowed Values	Allowed Special Characters
------------	-----------	----------------	----------------------------

Seconds	YES	0-59	, - * /
Minutes	YES	0-59	, - * /
Hours	YES	0-23	, - * /
Day of month	YES	1-31	, - * ? / L W
Month	YES	1-12 or JAN-DEC	, - * /
Day of week	YES	1-7 or SUN-SAT	, - * ? / L #
Year	NO	empty, 1970-2099	, - * /

So cron expressions can be as simple as this: \* \* \* \* ? \*

or more complex, like this: 0/5 14,18,3-39,52 \* ? JAN,MAR,SEP MON-FRI 2002-2010

## Special Characters

- \* ("all values") - used to select all values within a field. For example, "\*" in the minute field means "every minute".
- ? ("no specific value") - useful when you need to specify something in one of the two fields in which the character is allowed, but not the other. For example, if I want my trigger to fire on a particular day of the month (say, the 10th), but don't care what day of the week that happens to be, I would put "10" in the day-of-month field, and "?" in the day-of-week field. See the examples below for clarification.
  - - used to specify ranges. For example, "10-12" in the hour field means "the hours 10, 11 and 12".
- , - used to specify additional values. For example, "MON,WED,FRI" in the day-of-week field means "the days Monday, Wednesday, and Friday".
- / - used to specify increments. For example, "0/15" in the seconds field means "the seconds 0, 15, 30, and 45". And "5/15" in the seconds field means "the seconds 5, 20, 35, and 50". You can also specify '/' after the ' character - in this case ' is equivalent to having '0' before the '/'. '1/3' in the day-of-month field means "fire every 3 days starting on the first day of the month".
- L ("last") - has different meaning in each of the two fields in which it is allowed. For example, the value "L" in the day-of-month field means "the last day of the month" - day 31 for January, day 28 for February on non-leap years. If used in the day-of-week field by itself, it simply means "7" or "SAT". But if used in the day-of-week field after another value, it means "the last xxx day of the month" - for example "6L" means "the last Friday of the month". You can also specify an offset from the last day of the month, such as "L-3" which would mean the third-to-last day of the calendar month. When using the 'L' option, it is important not to specify lists, or ranges of values, as you'll get confusing/unexpected results.
- W ("weekday") - used to specify the weekday (Monday-Friday) nearest the given day. As an example, if you were to specify "15W" as the value for the day-of-month field, the meaning is: "the nearest weekday to the 15th of the month". So, if the 15th is a Saturday, the trigger will fire on Friday the 14th. If the 15th is a Sunday, the trigger will fire on Monday the 16th. If the 15th is a Tuesday, then it will fire on Tuesday the 15th. However, if you specify "1W" as the value for day-of-month, and the 1st is a Saturday, the trigger will fire on Monday the 3rd, as it will not 'jump' over the boundary of a month's days. The 'W' character can only be specified when the day-of-month is a single day, not a range or list of days. \*\* The 'L' and 'W' characters can also be combined in the day-of-month field to yield 'LW', which translates to "last weekday of the month".
- # - used to specify "the nth" XXX day of the month. For example, the value of "6#3" in the day-of-week field means "the third Friday of the month" (day 6 = Friday and "#3" = the 3rd one in the month). Other examples: "2#1" = the first Monday of the month and "4#5" = the fifth Wednesday of the month. Note that if you specify "#5" and there is not 5 of the given



day-of-week in the month, then no firing will occur that month. \*\* The legal characters and the names of months and days of the week are not case sensitive. MON is the same as mon.

#### Example CRON specs:

0 * * * * *	Run every minute
0/10 * * * * *	Run every 10 seconds
0 0/5 * * * *	Run every 5 minutes
0 0 * * * *	Run every hour



# Chapter 6

## Using the Web Application

### Overview

INTRODUCTION .....	55
OPENING THE WEB APPLICATION.....	55
<i>Personnel Status</i> .....	56
<i>Displaying Personnel Details</i> .....	56
State Display .....	57

## Introduction

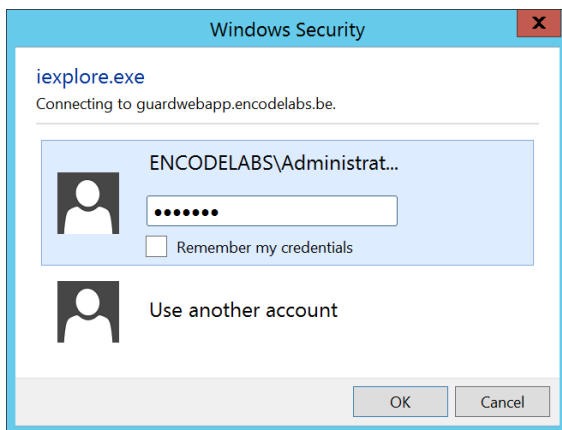
The Guard Web Application is a website to which Security Operators can connect and consult relevant security data.

The operator has to have an account on the domain and must belong to a specific AD group in order to get access to the service.

## Opening the web application

Open your favourite web browser and navigate to the configured web page

Enter your credentials to log in and click "OK":



You should be able to see the default landing page that allows you to perform lookups:

EncodeLabs GS2C

ENCODELABS\Administrator!

### Personnel Search Criteria

*Note:* You may search by an individual's card number or by part of their name. If both are supplied, only the card number will be used.

Card Number:

Enter the person's card number here.

Name:

Enter part of the person's name here

Search

### Search Results

You can look up data by card number or by person name.

### Search Results


⏮

⏪

1

⏩




⏭

Image	Name	Card Number	Site
	Cornelis, Stefaan	101	Main Site

## Personnel Status

In the result list, the results can have different colors:

- RED means the person is not enabled.
- YELLOW means the person has no valid credentials
- WHITE means the person is enabled and has a valid credential

	Langfordjr, Steven	211802	Main Site
	Meister, Ralph		Main Site
	Norton, Christeen	116552	Main Site

## Displaying Personnel Details

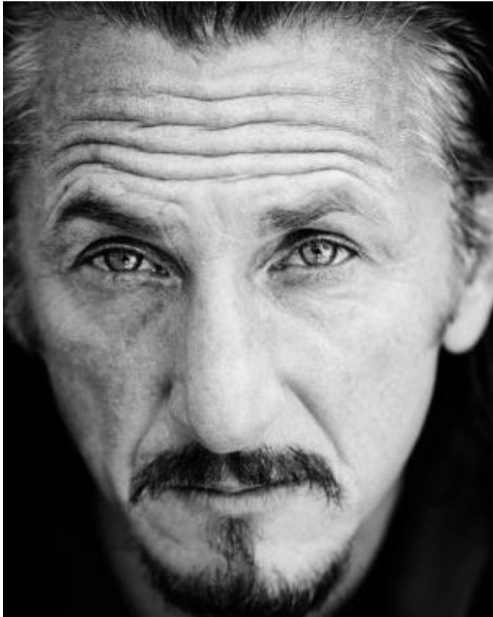
Click on the line of a person to see the details.

The file will show the source site of the data, the personnel (user) status, and credential information.

Encode Labs GS2C

ENCODELABS\Administrato

### Personnel Info



**Name**  
Penn, Sean

**Site**  
Main Site

**User State**  
Enabled

**Date Received**  
Invalid Date

**Card Number**  
456

**Credential State**  
Active

**Activation Date Time**  
2018-02-15 13:39:00

**Expiration Date Time**  
2023-02-15 13:39:00

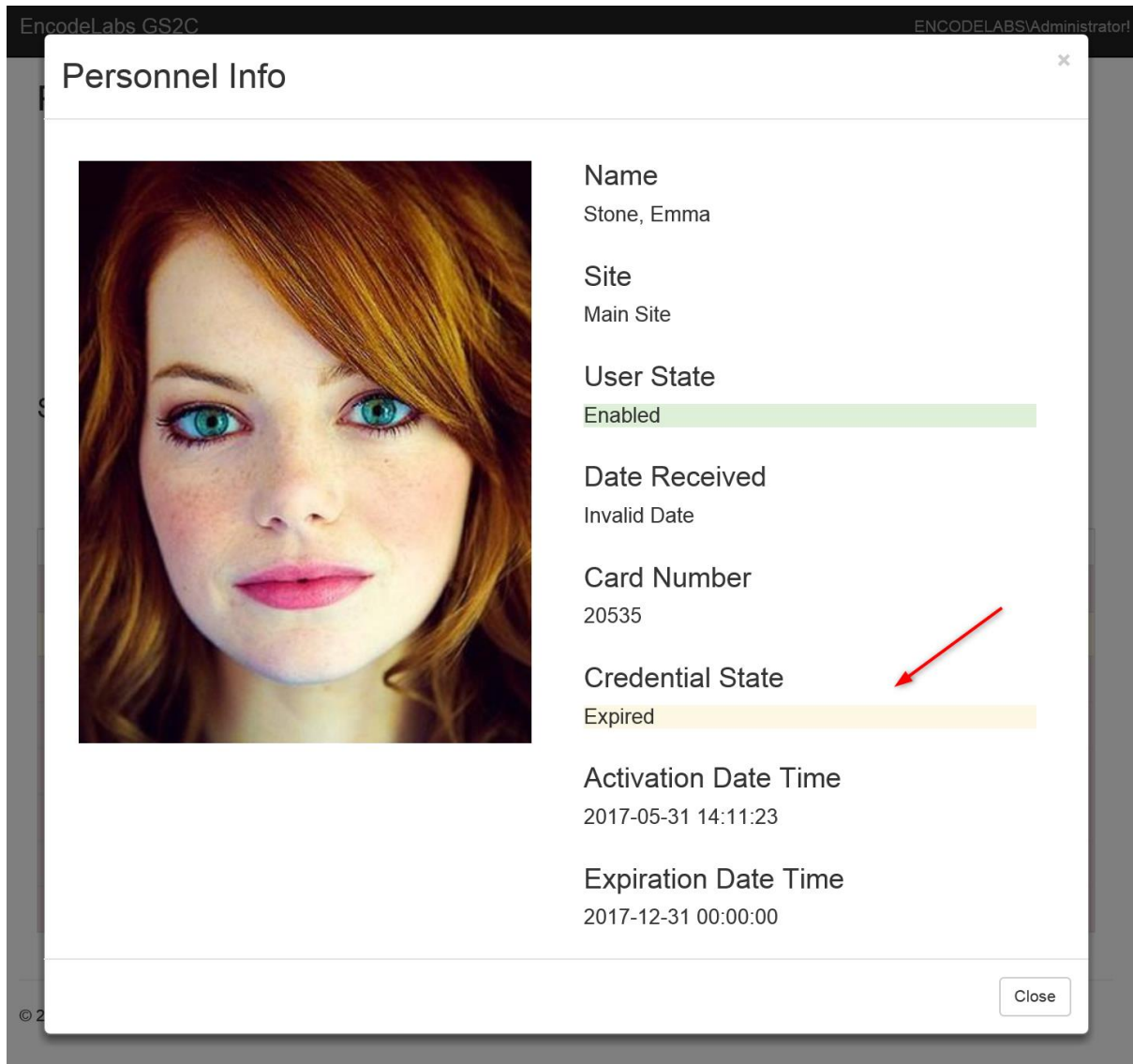
Close



### State Display


The User and Credential states use background colors to quickly identify data validity.

- A GREEN background means the user is ENABLED or the credential is VALID
- An ORANGE background means the User is disabled or the credential is INVALID (Expired, Lost, Stolen etc.)



Encodel abs GS2C ENCODELABS\Administrator

### Personnel Info



**Name**  
Stone, Emma

**Site**  
Main Site

**User State**  
Enabled

**Date Received**  
Invalid Date

**Card Number**  
20535

**Credential State**  
Expired

**Activation Date Time**  
2017-05-31 14:11:23

**Expiration Date Time**  
2017-12-31 00:00:00

Close



# Troubleshooting

## Appendix A

### Overview

LOCAL MACHINE AND CURRENT USER CERTIFICATE STORES .....	59
LOCATING THE REQUIRED INFORMATION ON A CERTIFICATE .....	59
CERTIFICATE NOT FOUND.....	61
INSTALLATION OF THE MICROSOFT .NET 4.6.2 FRAMEWORK SEEMS TO HAVE FAILED .....	61

## Local Machine and Current User Certificate Stores

There are two certificate store types on each system:

### Local Machine certificate store

This certificate store is local to the computer and global to all users on the computer. It is located in the registry under the HKEY\_LOCAL\_MACHINE root.

### Current User certificate store

This certificate store is local to a user account on the computer. It is located in the registry under the HKEY\_CURRENT\_USER root.

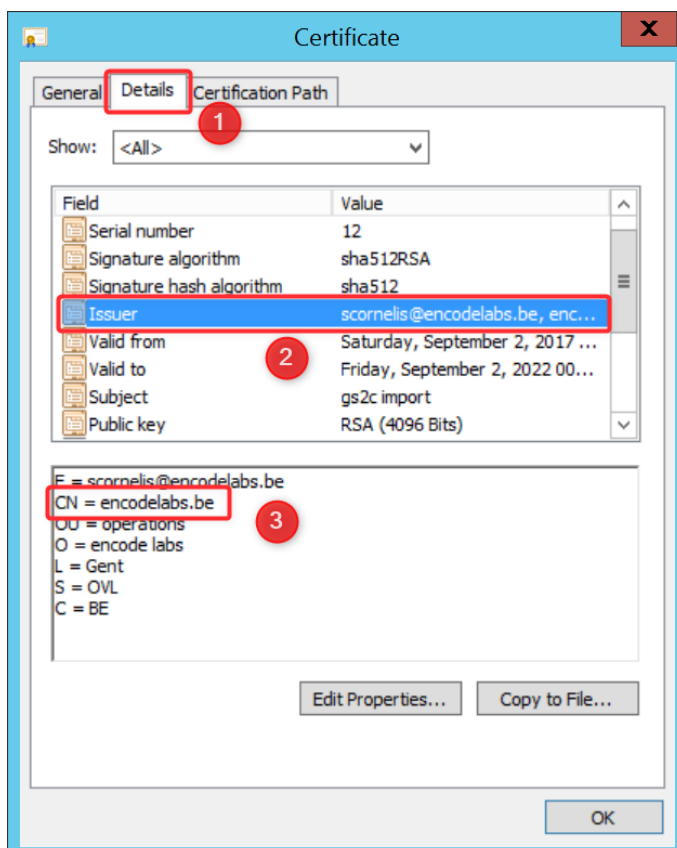
Keep in mind that all Current User certificate stores inherit the contents of the Local Machine certificate stores. For example, if a certificate is added to the local machine Trusted Root Certification Authorities certificate store, all current user Trusted Root Certification Authorities certificate stores also contain the certificate.

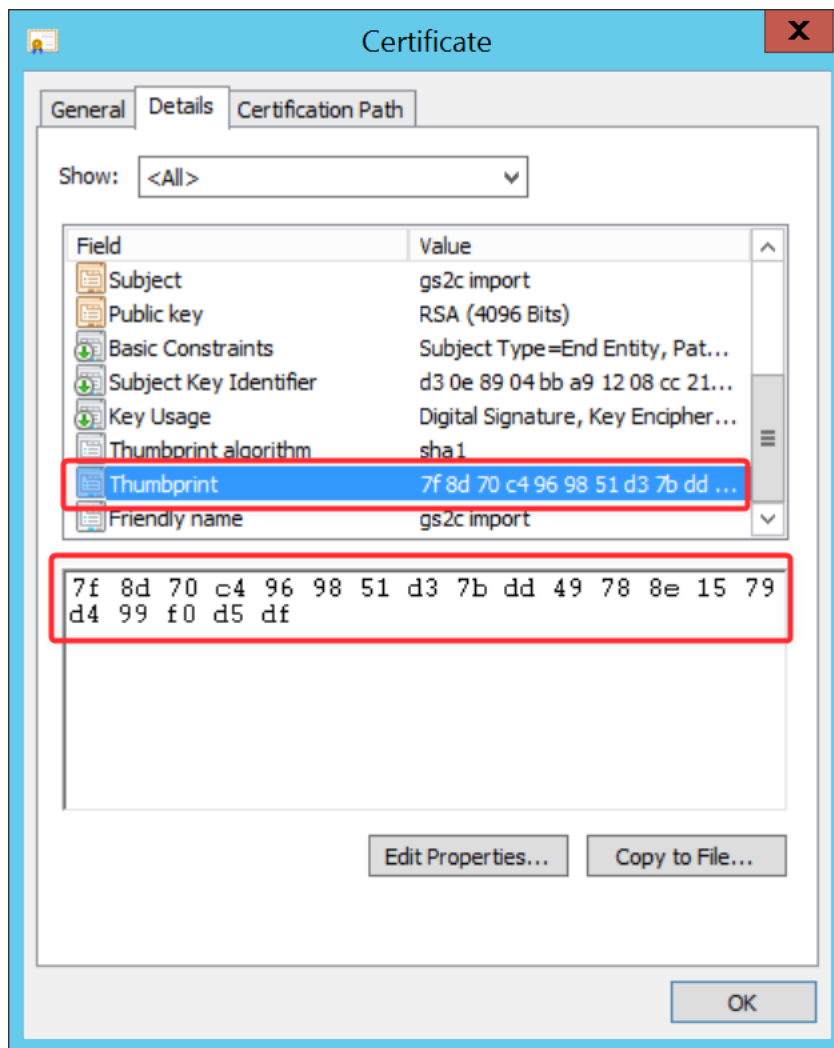
## Locating the required information on a certificate

Open the server certificate store

Select the certificate and open it.

1. Select the Details page
2. Select the field you want information from
3. The required data is found below (in this case the Common Name CN is displayed)





## Certificate not found

Run certmgr.msc to check if the certificate is present in the certificate store.

If the certificate is not present, try reinstalling it. When the certificate is visible in the store, try to start the service again.

### Checking the certificate thumbprint

When your certificate is present in the store and it can still not be found, check the certificate thumbprint.

If you have copy-pasted the thumbprint from another location such as the certificate information dialog box to the config file (or to a string literal in the code, for that matter), it is possible that the first character is an invisible Unicode character.

If you have an editor like Notepad++, you can change the file encoding from UTF-8 to Ansi to verify this. A sample:

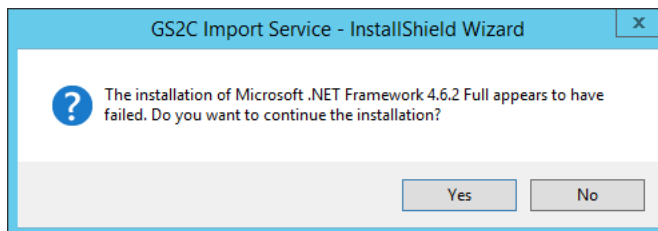
Encoding	Thumbprint
UTF-8	"Thumbprint": "7F8D70C4969851D37BDD49788E1579D499F0D5DF"
ANSI	"Thumbprint": "��7F8D70C4969851D37BDD49788E1579D499F0D5DF"

Delete the ANSI part and save the file again.

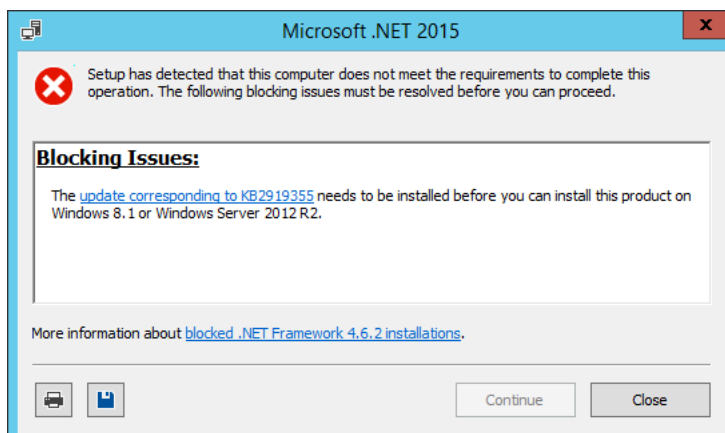
Alternatively, you can type the thumbprint by hand if you can't switch your editor to ANSI coding for verification.

## Installation of the Microsoft .Net 4.6.2 framework seems to have failed

In some cases, during installation, the following dialog can appear:



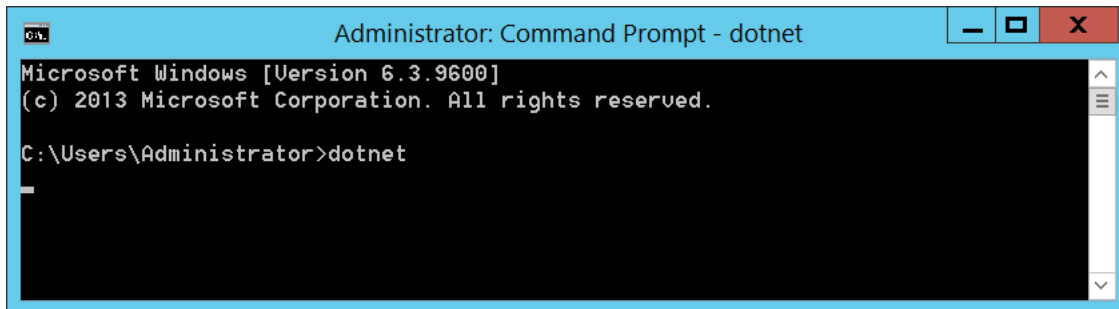
In order to find out what the precise issue is, run the prerequisite manually from the installation folder: It is located in the folder [ISSetupPrerequisites](#). The file is named [NDP462-KB3151800-x86-x64-AllOS-ENU.exe](#). This will bring up a dialog with more information on how to solve the issue. Example:



## The Web App fails to run

### Check the dotnet package update

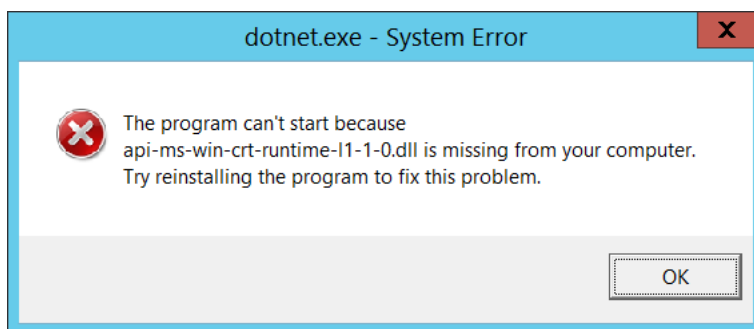
Open a command line and type "dotnet"



```
Administrator: Command Prompt - dotnet
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dotnet
```

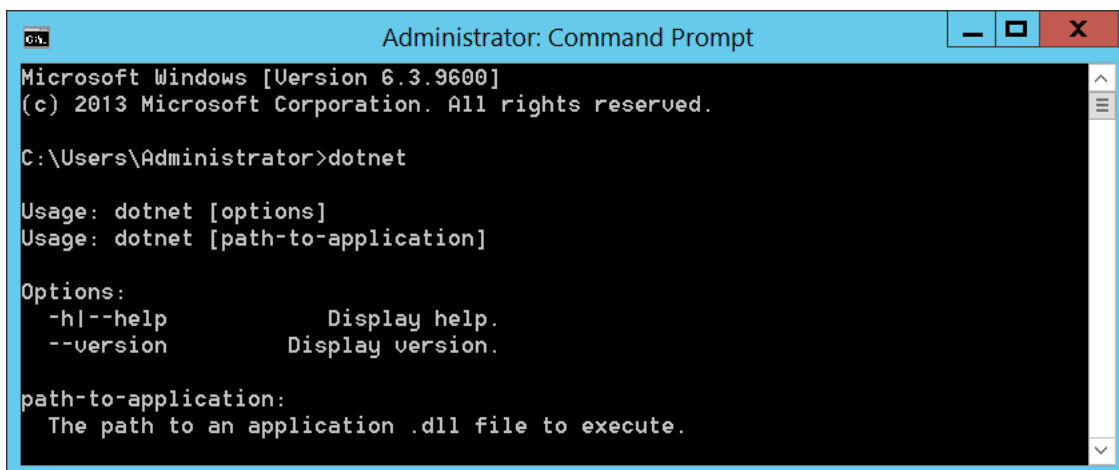
If you receive the following error:



Then you need to install the update package KB2999226. More information can be found here:

<https://support.microsoft.com/en-us/help/2999226/update-for-universal-c-runtime-in-windows>

The correct output should look somewhat like this:



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>dotnet

Usage: dotnet [options]
Usage: dotnet [path-to-application]

Options:
  -h|--help          Display help.
  --version          Display version.

path-to-application:
  The path to an application .dll file to execute.
```

### In internet explorer, you receive a 502.5 error

Check in the Windows Event log for more information on the specific error. In some cases when the path becomes corrupted, it might be the application cannot be found.

#### Dotnet Application not found

Locate the dotnet executable path. This is usually located in the program files folder. Note the full path.

In the web.config file of your web app folder:

For the element Configuration -> System.Web -> aspNetCore

Try replacing the value of processPath with the full path of the dotnet.exe you located.

Restart the IIS server and try to reconnect.



© 2017 ENCODE LABS BVBA