

QR Credential Generator

for C•CURE9000

Revision A5 - March 2020

QR Credential Generator

for C•CURE9000

Document Number: IM-008

Revision: A5

Release Date: March 2020

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.

© 2018-2020 Encode Labs

All rights reserved.

Contents

| | |
|---|-----------|
| INTRODUCTION | 4 |
| CONVENTIONS | 5 |
| OBTAINING A LICENSE | 5 |
| SPECIFICATIONS AND COMPATIBILITY | 6 |
| CCURE9000 REQUIREMENTS | 6 |
| SERVER REQUIREMENTS | 6 |
| KNOWN LIMITATIONS | 6 |
| ARCHITECTURE | 7 |
| COMPONENT DETAILS | 7 |
| INSTALLATION | 8 |
| PRE-REQUISITES | 8 |
| SOFTWARE PACKAGE | 8 |
| INSTALLATION | 8 |
| INSTALLATION OF YOUR LICENSE FILE | 11 |
| CONFIGURATION | 12 |
| CONFIGURATION OF THE SERVICE | 12 |
| <i>Configuring the appSettings</i> | 12 |
| <i>Configure the database connection</i> | 13 |
| <i>Changing the account running the service</i> | 14 |
| <i>Setting up the correct database rights</i> | 15 |
| <i>Configuration of the Logging framework</i> | 16 |
| CONFIGURATION OF THE CCURE9000 AUTOMATED IMPORT | 17 |
| SAMPLE DEPLOYMENT CONFIGURATION | 19 |
| <i>Create Visitor Clearances</i> | 19 |
| <i>Create a Visitor Template</i> | 19 |
| <i>Create Visit Site (pre-configuration)</i> | 20 |
| <i>Create a Visit Template</i> | 21 |
| <i>Configure the Visit Site</i> | 22 |
| <i>Testing: Creating a visit</i> | 23 |
| <i>Remarks: Number of cards per person:</i> | 25 |
| APPENDIX A | 26 |
| CONSIDERATIONS FOR SQL EXPRESS | 26 |
| AVOIDING UAC ISSUES | 27 |
| DATETIME ISSUES | 28 |

Introduction

With the release of CCURE9000 V2.60 SP1, Software House released the Visitor Management Phase III which supports the following:

- QR code identification for visitors registering for a visit
- QR codes are now included in emails sent to visitors for visitor identification during visitor registration

The **QR Credential Generator for CCURE9000 (QRCG)** by Encode Labs is a service that will auto generate credentials for visitors that receive a QR code by email. This allows visitors to use their QR code as a credential on designated locations.

This means you can close down your site with Access Control while allowing access to pre-registered visitors through the use of their QR code. This creates a more secured and better controlled site perimeter.

The QRCG service solves the problem of providing a credential to your visitor before he is on site.



Example use case

All your visitors are required to sign in at the front security desk in order to obtain a temporary credential such as an access badge.

You want to close down public access to your visitor parking with a vehicle barrier that is equipped with a QR reader. This way **only pre-registered visitors** can make use of the visitor parking.

Alternatively, you may want to leave a standard parking available, but provide access for VIP visitors on a reserved VIP parking. With the same QR reader you can now provide access functionality to your VIP visitor.

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

Obtaining a license

A license can be purchased through your certified CCURE9000 Integrator.

You will need to provide the following information with your purchase:

| Field | Example |
|------------------------|-------------------------|
| System Serial Number | 9-12345 |
| CCURE9000 Version | 2.80 |
| End User Name | Encode Labs |
| End User Site Location | Gent* |
| Integrator Name | ABC Integrated Security |

Alternatively, you can navigate to the Encode Labs website for registering your copy. Your license file will be sent to you by email once your purchase has been confirmed:

<https://www.encode labs.be/support/software-registration/>



Specifications and Compatibility

CCURE9000 Requirements

- Supported CCURE9000 version
- Visitor Management license option
- CCURE9000 Web Portal installed

Server requirements

This is a CCURE9000 Addon Service. Supported Versions:

- CCURE9000 V2.60 SP1 -> CCURE9000 V2.80

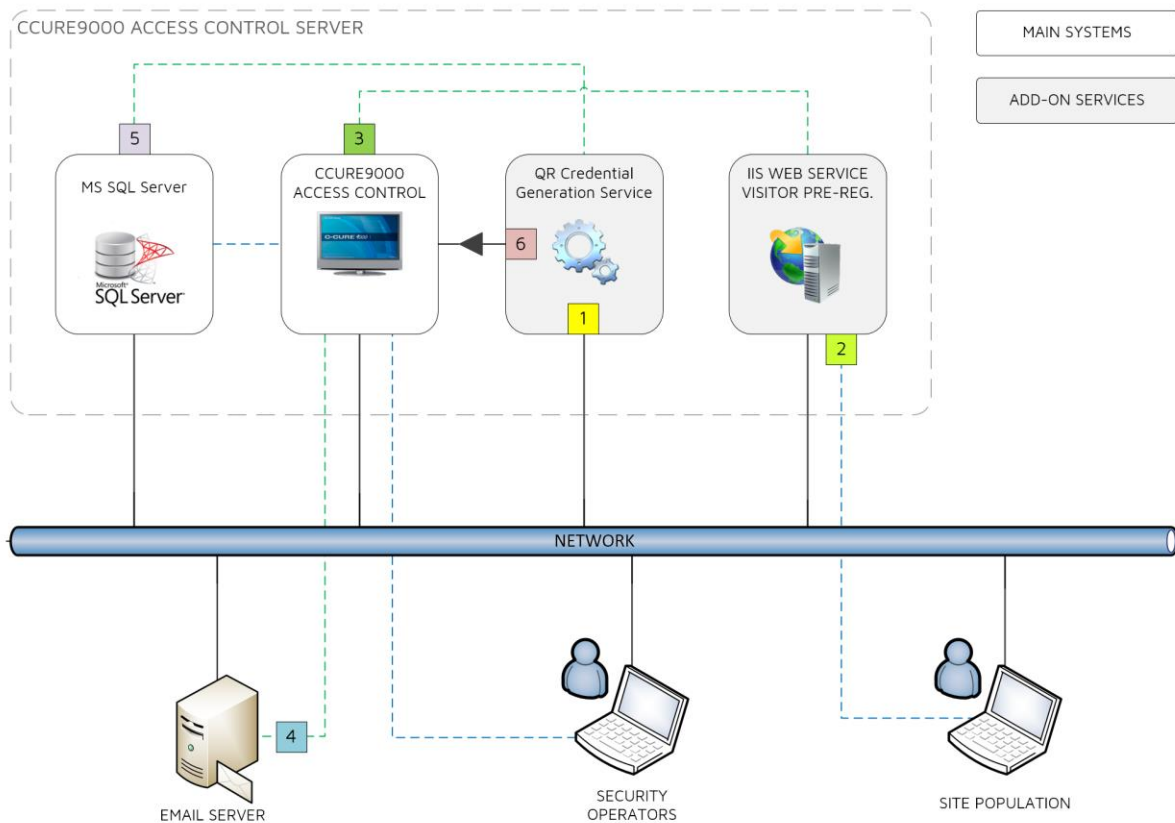
The requirements are those of the CCURE9000 system that is installed:

| OS - Server Series L/M/N/SAS | Version | V2.60 | V2.70 | V2.80 |
|--|---------|-------|-------|-------|
| Windows 7 Professional & Enterprise SP1 or later | 64-bit | ✓ | ✓ | ✓ |
| Windows 8.1 Professional & Enterprise SP1 or later | 64-bit | ✓ | ✓ | ✓ |
| Windows 10 Professional & Enterprise | 64-bit | ✓ | ✓ | ✓ |
| Windows Server 2008 R2 Standard & Enterprise SP1 or later | 64-bit | ✓ | ✗ | ✗ |
| Windows Server 2012 R2 Standard SP1 or later | 64-bit | ✓ | ✓ | ✓ |
| Windows Server 2016 Standard & Enterprise | 64-bit | ✗ | ✓ | ✓ |
| Windows Server 2019 Standard & Enterprise | 64-bit | ✗ | ✗ | ✓ |
| OS - Server Series P/Q/R/R+/S/S+/T/SAS | Version | V2.60 | V2.70 | V2.80 |
| Windows 10 Professional & Enterprise | 64-bit | ✗ | ✓ | ✓ |
| Windows Server 2008 R2 Standard & Enterprise SP1 or later | 64-bit | ✓ | ✗ | ✗ |
| Windows Server 2012 R2 Standard | 64-bit | ✓ | ✓ | ✓ |
| Windows Server 2016 Standard & Enterprise | 64-bit | ✗ | ✓ | ✓ |
| Windows Server 2019 Standard & Enterprise | 64-bit | ✗ | ✗ | ✓ |
| DBMS - Server Series L/M/N/SAS | Version | V2.60 | V2.70 | V2.80 |
| SQL Server 2008 R2 Standard Enterprise SP2 or later | 64-bit | ✓ | ✗ | ✗ |
| SQL Server 2012 Express Standard Enterprise SP2 or later | 64-bit | ✓ | ✓ | ✓ |
| SQL Server 2014 Express Standard Enterprise SP1 or later | 64-bit | ✓ | ✓ | ✓ |
| SQL Server 2016 Express Standard Enterprise All SP's | 64-bit | ✓ | ✓ | ✓ |
| SQL Server 2017 Express Standard Enterprise All SP's | 64-bit | ✗ | ✗ | ✓ |
| DBMS - Server Series Standalone P/Q/R/R+/S/S+/T/SAS | Version | V2.60 | V2.70 | V2.80 |
| SQL Server 2008R2 Standard & Enterprise SP2 or later | 64-bit | ✓ | ✗ | ✗ |
| SQL Server 2012 Standard & Enterprise SP2 or later | 64-bit | ✓ | ✓ | ✓ |
| SQL Server 2014 Standard | 64-bit | ✓ | ✓ | ✓ |
| SQL Server 2014 Standard All Service Packs | 64-bit | ✗ | ✓ | ✓ |
| SQL Server 2014 Enterprise SP1 or later | 64-bit | ✓ | ✓ | ✓ |
| SQL Server 2016 Standard & Enterprise SP1 or later | 64-bit | ✓ | ✓ | ✓ |
| SQL Server 2016 Standard & Enterprise All Service Packs | 64-bit | ✗ | ✓ | ✓ |
| SQL Server 2017 Standard & Enterprise | 64-bit | ✗ | ✗ | ✓ |

Known limitations

No known limitations

Architecture



Component Details

| | |
|---|---|
| 1 | The QR Credential Generation service is usually installed on the CCURE9000 Server. But this is not a requirement. It can actually reside anywhere on the network with access to the database server. |
| 2 | A host will pre-register a visitor on the CCURE9000 Web Portal . |
| 3 | The CCURE server will receive the visit registration and create a new visit. |
| 4 | If the visitors' email address was provided and the configuration was done for sending QR codes, an invitation containing a QR code will be e-mailed to the visitor. |
| 5 | The QR Credential Generation Service will pick up the visit configuration and all visitor data from the database. |
| 6 | The QR Credential Generation Service will push out an XML import file to the CCURE9000 Server to add the credentials to the visitor record. |

Installation

Pre-requisites

The following items are required for installation

- A valid license file for running the QR Credential Generation Service
- Local Administrative account for the installation of the service
- A functional account if required, to run the service
- Read Access to the CCURE9000 ACVScore database

Software Package

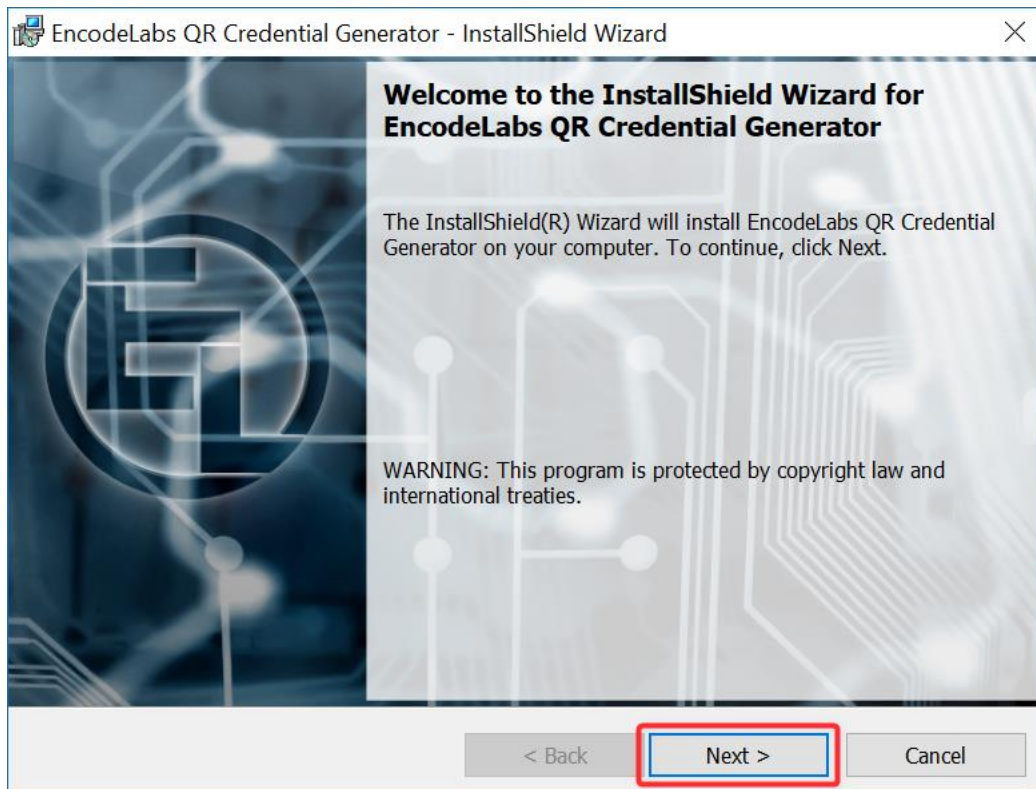
The software package contains the following files:

| Name | Type |
|--|---------------------------|
| Documentation | File folder |
| EncodeLabs QR Credential Generator.msi | Windows Installer Package |
| setup.exe | Application |

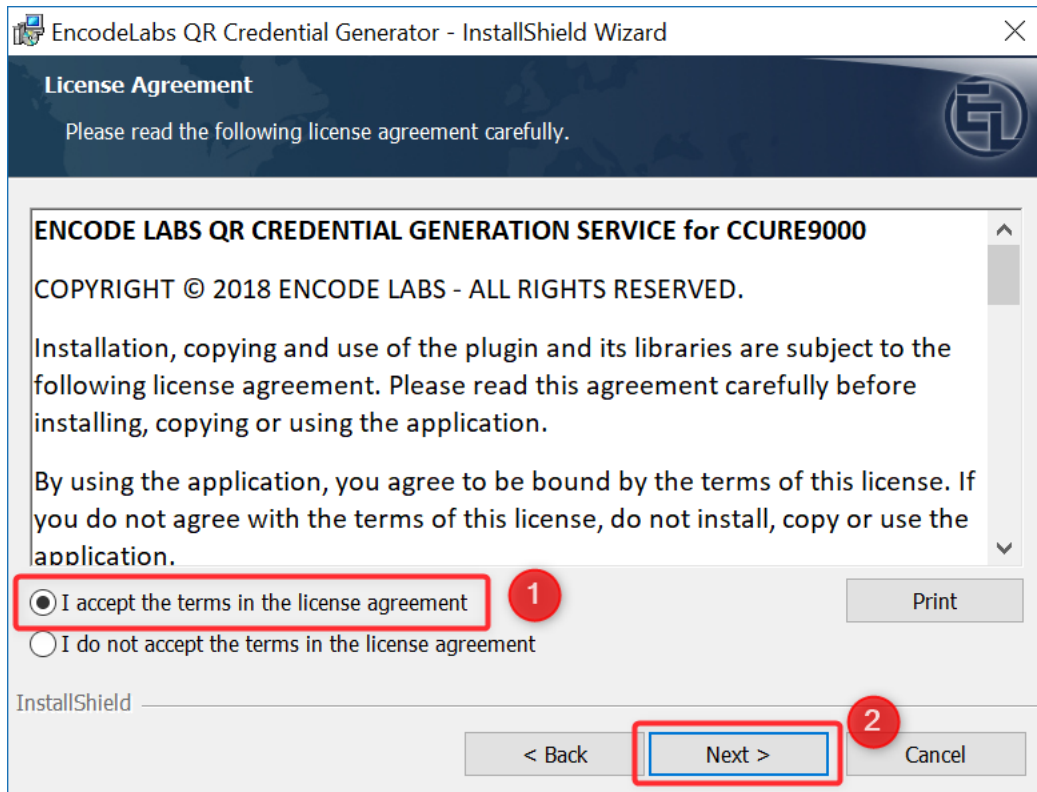
Installation

Run setup.exe

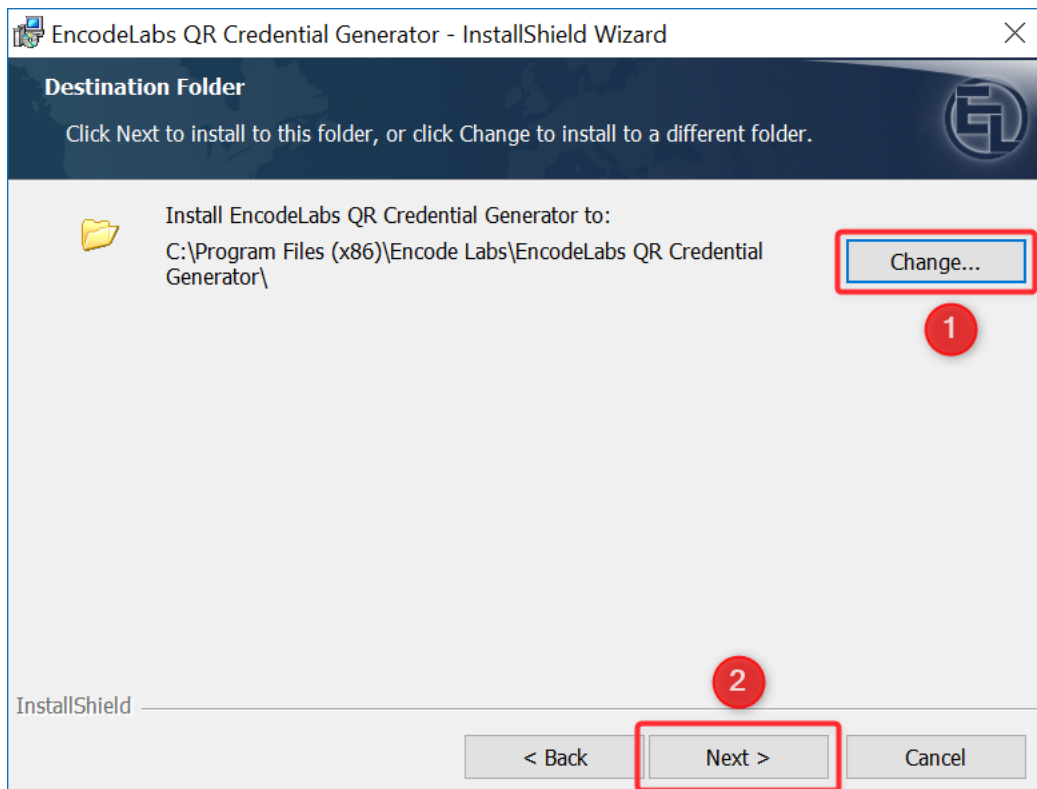
Select "Next"



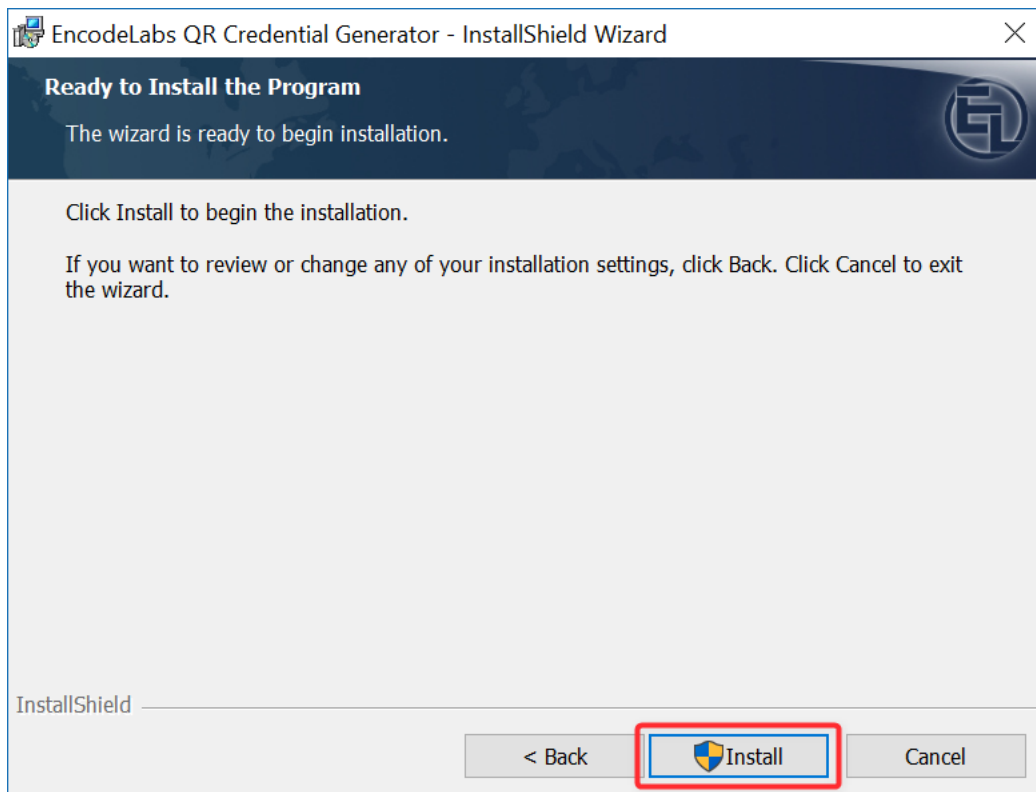
1. Select the required license agreement option
2. Click "Next"



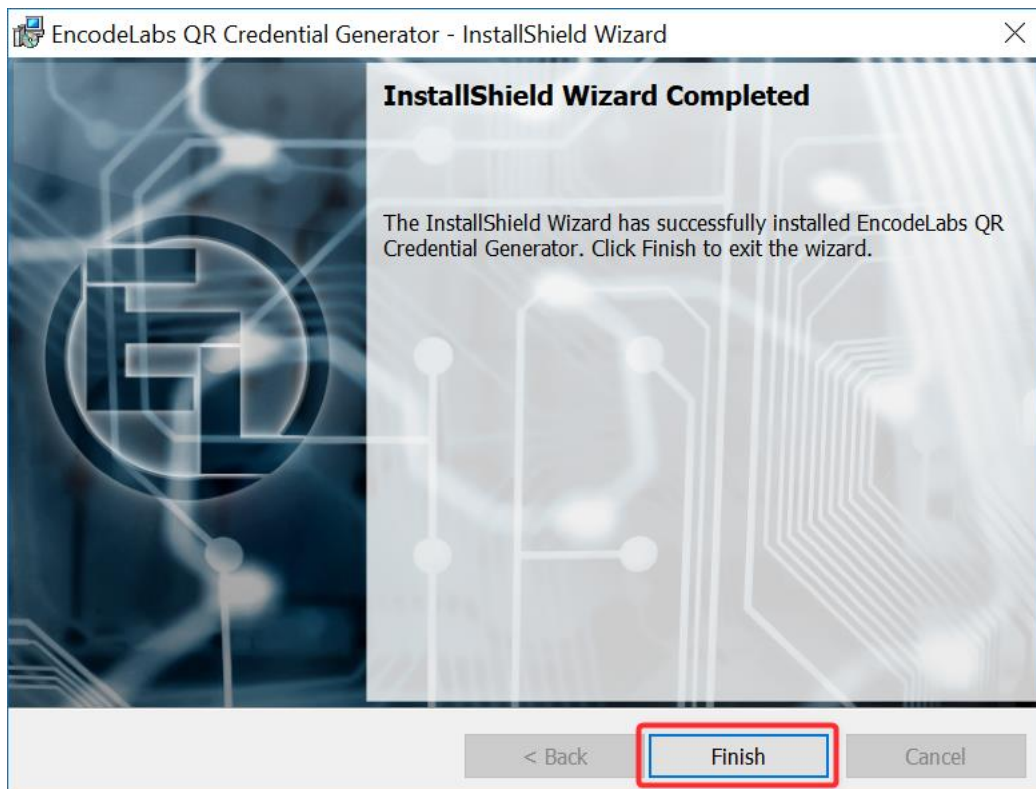
1. Change the location of the installation if required
2. When done, click "Next"



Click "Install"



Click "Finish"



The service should have been installed:

| Name | Description | Status | Startup Type | Log On As |
|--|---|--------|--------------|--------------|
| Encode Labs QR Credential Generation Service | Service for generating credentials from QR codes on CCURE9000 | | Automatic | Local System |

The installation should contain the following files:

This PC > Local Disk (C:) > Program Files (x86) > Encode Labs > EncodeLabs QR Credential Generator

| Name | Type |
|---|------------------------|
| CcureImports | File folder |
| Logging | File folder |
| CCURE9000_ImportDefinition.xml | XML Document |
| Dapper.dll | Application extension |
| Dapper.xml | XML Document |
| EncodeLabs.Ccure.QrCardGenerator.DataAccess.dll | Application extension |
| EncodeLabs.Ccure.QrCardGenerator.lic | LIC File |
| EncodeLabs.Ccure.QrCardGenerator.Objects.dll | Application extension |
| EncodeLabs.Ccure.QrCardGenerator.Service.exe | Application |
| EncodeLabs.Ccure.QrCardGenerator.Service.exe.config | XML Configuration File |
| EncodeLabs.Xtras.Data.Verification.dll | Application extension |
| Newtonsoft.Json.dll | Application extension |
| Newtonsoft.Json.xml | XML Document |
| NLog.config | XML Configuration File |
| NLog.dll | Application extension |
| NLog.xml | XML Document |

Installation of your license file

Just copy the license file into the directory of the installation. The service will pick it up and run normally.


Configuration

Configuration tasks:

- [Configuration of the service on page 12](#)
- [Configure the database connection on page 13](#)
- [Changing the account running the service on page 14](#)
- [Setting up the correct database rights on page 15](#)
- [Configuration of the Logging framework on page 16](#)

Configuration of the service

The configuration of the service is done by editing the config file:

 EncodeLabs.Ccure.QrCardGenerator.Service.exe.config XML Configuration File

Configuring the appSettings

```
<appSettings>
  <add key="PollIntervalSeconds" value="30"/>
  <add key="ExportFileName" value="QrCardGenerator.ImportFile.xml"/>
  <add key="CredentialActivationBuffer" value="120"/>
  <add key="CredentialExpirationBuffer" value="120"/>
  <add key="DateTimeFormat" value="yyyy-MM-dd HH:mm:ss"/>
</appSettings>
```

| Setting Key | Description |
|-----------------------------------|---|
| PollIntervalSeconds | The time in seconds between polling the database for new visits to be processed. |
| ExportFileName | The name of the file to write the QR credentials to. |
| CredentialActivationBuffer | The number of minutes to activate the credential before the official visit start. For example, a visit starting at 9am, with an activation buffer of 60 minutes, will allow the QR credential to have an activation time of 8am. |
| CredentialExpirationBuffer | The number of minutes to add to the visit end date for the expiration of the QR credential. For example, a visit ending at 10am, with an activation buffer of 120 minutes, will allow the QR credential to have an expiration time of 12pm. |
| DateTimeFormat | The DateTime Format to use by the application for querying the database. |

Credential Activation and Expiration times have been limited to the time window of the visit to ensure no credentials remain active within the system in case of no-shows.

Configure the database connection

As show in the [Architecture](#) on page 7, the service requires a connection to the database. The connection string needs to be configured for this.

These settings can be found under connectionStrings.

Sample configuration:

```
<connectionStrings>
  <add name="CcureConnectionString"
        providerName="System.Data.SqlClient"
        connectionString="
          Data Source=localhost\SQLEXPRESS;
          Initial Catalog=ACVSCore;
          Integrated Security=false;
          User Id=ccure_qr_read;
          Password=aZuc5é314;" />
</connectionStrings>
```

| Setting Key | Description |
|---------------------|--|
| name | The connection name. Do not change this value. |
| ProviderName | Driver value. Do not change this value. |
| Data Source | The database server address. In case you are not using the default named instance ([ServerName]\Default) then you MUST add the instance name of the server. This is the case for example for SQLEXPRESS. This value can either be the server name or IP address. |
| Initial Catalog | The name of the database to use. Do not change this value. |
| Integrated Security | Whether or not to use the credentials of the account running the service for logging onto the database. In case your service is being run by the <i>Local System</i> account, maure to give the correct access rights to that account on the ACVSCore database. Refer to Setting up the correct database rights on page 15 for more information. |
| User Id | When the SQL server is configured for SQL authentication, you can specify the user account name through this tag. |
| Password | When the SQL server is configured for SQL authentication, you can specify the user account password through this tag. |



For more information on how to configure a connection string, navigate to the following resources:

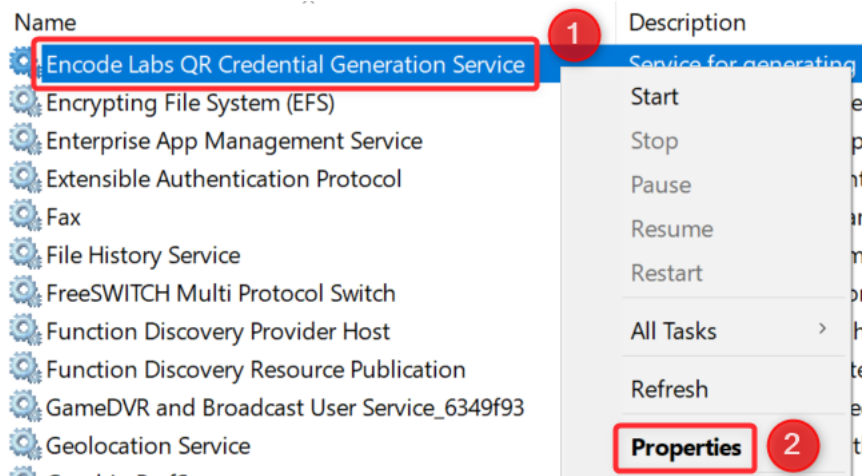
<https://docs.microsoft.com/en-us/dotnet/framework/data/adonet/connection-string-syntax>

<https://www.connectionstrings.com/sql-server/>

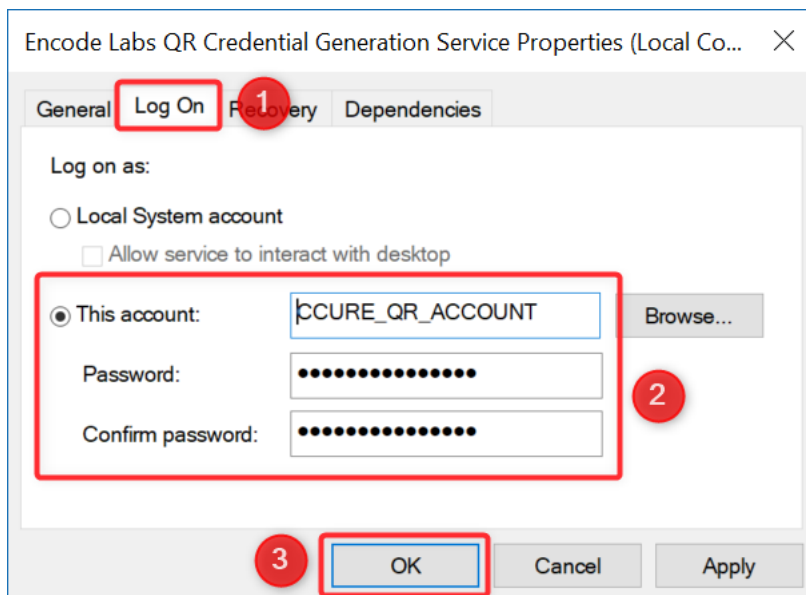
Changing the account running the service

Open the services (services.msc from the command line)

1. Right-click the service
2. Select "Properties"



1. Select the "Log On" tab
2. Enter the account details for running the service
3. Click "OK"

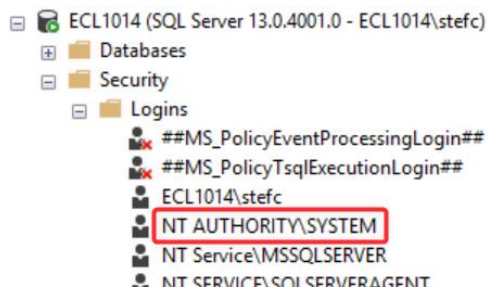


Setting up the correct database rights

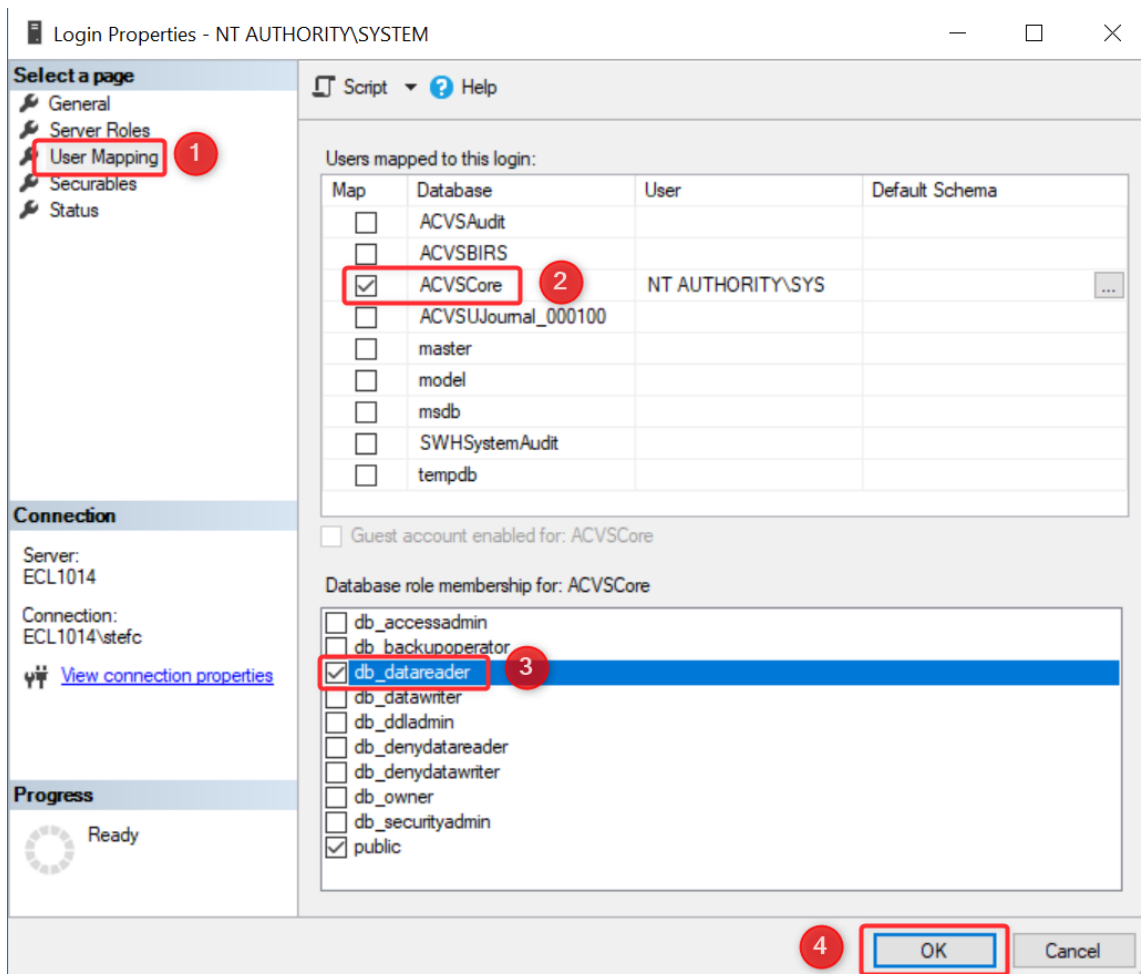
In case you use integrated authentication, you need to make sure the account running the service has got Read access to the ACVSCore database. In our example, the service is being run under the [Local System](#) account.

In MSSQL, this is the [NT AUTHORITY\SYSTEM](#) account. We will need to provide this account with read access:

- From SQL Server Administrator, navigate to [Security -> Logins](#)
- Right-click the [NT AUTHORITY\SYSTEM](#) account and select [properties](#)



1. Select "User Mapping"
2. Check "ACVSCore"
3. Check "db_datareader"
4. Click "OK"

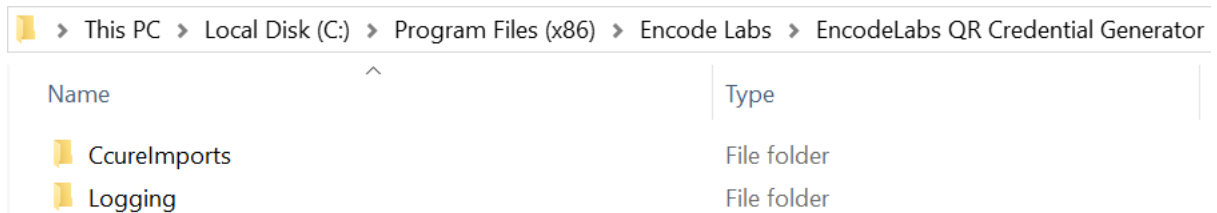


Configuration of the Logging framework

The service makes use of the NLog framework for logging its activity. Configuring the logging is done by editing the NLog.config file:


 NLog.config XML Configuration File

By default, when starting the service for the first time, a Logging folder will be created in the installation directory:



| Name | Type |
|--------------|-------------|
| CcureImports | File folder |
| Logging | File folder |

By default, the logfile is written to the Logging directory under the name:

 EncodeLabs.Ccure.QrCardGenerator.Log Text Document

The file will be archived when it reaches 4Mb in size. A maximum of 10 files will be archived per day.

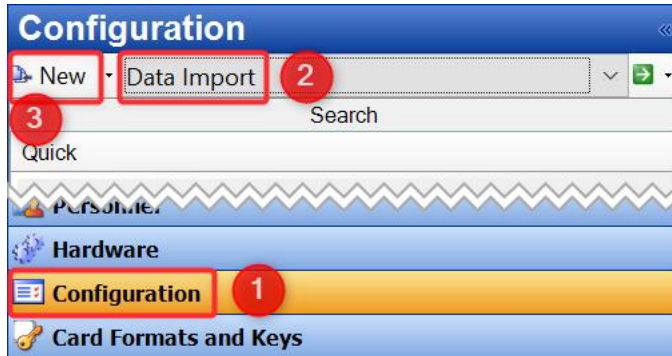
For changing the logging options, please refer to the NLog documentation:

<https://github.com/NLog/NLog/wiki>

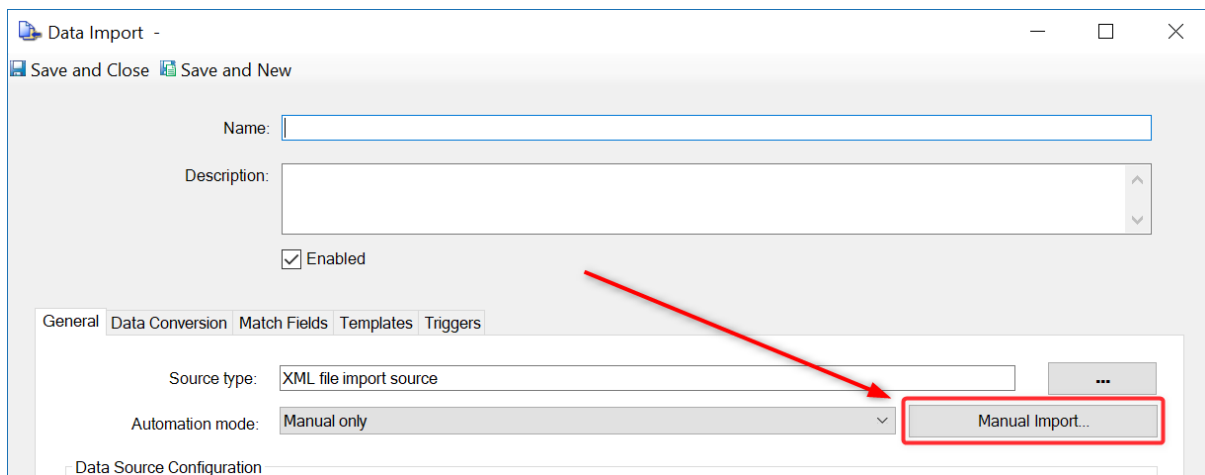
Configuration of the CCURE9000 Automated Import

In order to import the QR credentials, an automated import must be configured.

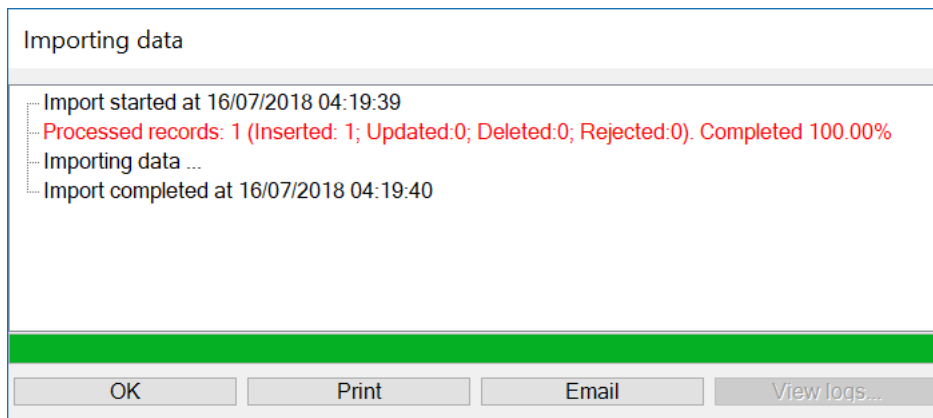
1. Select Configuration
2. Select Data Import
3. Click "New"



Click "Manual Import"



Select the import file that was provided with the installation. The import definition will automatically be imported, no mapping should be required.



The service will generate the files to be imported by the CCURE in the path where the service is installed, under a folder called **CcureImports**. By default this is:

`C:\Program Files (x86)\Encode Labs\EncodeLabs QR Credential Generator\CcureImports.`

Should you encounter any issues importing the definition file, make sure the path in the import definition file exists. You can edit the default path of the file:

```
1 <?xml version="1.0" encoding="utf-8" standalone="yes"?><CR LF
2 <CrossFire culture-info="en-GB" platform-version="2.70.0" product-version="2.70.0"><CR LF
3 <SoftwareHouse.CrossFire.Common.Objects.Import ImportMode="Default"><CR LF
4 <<Name>Encode Labs QR Credentials Generation Import</Name><CR LF
5 <<AutomationMode>ListeningOnData</AutomationMode><CR LF
6 <<DefaultImportMode>Set</DefaultImportMode><CR LF
7 <<DefaultImportPartitionID>0</DefaultImportPartitionID><CR LF
8 <<Enabled>True</Enabled><CR LF
9 <<XmlEncodedDataSchema>&lt;ArrayOfDataSelector xmlns:xsi="http://www.w3.org/2001/XMLSchema=instanc
10 <<SoftwareHouse.CrossFire.Common.Objects.ImportXmlFileSource ImportMode="Default"><CR LF
11 <<EnableListening>True</EnableListening><CR LF
12 <<MainConfig>&lt;?xml version="1.0" encoding="utf-16"?&gt;&lt;ImportXmlFileSource.ConfigInfo xml
13 C:\Program Files (x86)\Encode Labs\EncodeLabs QR Credential Generator\CcureImports
14 &lt;/ServerFolder&gt;&lt;/ImportXmlFileSource.ConfigInfo&gt;</MainConfig><CR LF
15 <<OwnerID>5000</OwnerID><CR LF
16 <<OwnerType>SoftwareHouse.CrossFire.Common.Objects.Import</OwnerType><CR LF
17 </SoftwareHouse.CrossFire.Common.Objects.ImportXmlFileSource><CR LF
18 </SoftwareHouse.CrossFire.Common.Objects.Import><CR LF
19 </CrossFire>
```

It is possible to configure the import manually by letting the system generate a sample file from the service and then mapping the data manually.

From the import view you should be able to see the QR import listening on data:

| Name | Enabled | Automation Mode | Status |
|--|-------------------------------------|-------------------|-----------|
| Encode Labs QR Credentials Generation Import | <input checked="" type="checkbox"/> | Listening on data | Listening |

In case your import status is showing "Disconnected", make sure you have the Import Watcher running:

Open the Server Configurator and activate the Import Watcher

Server Configuration Application

Services: Server Components Database Settings Backup/Restore

Framework Services

- Stop** Name: CrossFire Framework Service
Status: **Running**
Description: Provides support for applications using the CrossFire Framework technology.
Location: C:\Program Files (x86)\Tyco\CrossFire
Version: 3.70.539.289
- Stop** Name: CrossFire Server Component Framework Service
Status: **Running**
Description: Provides Management of Server Components in the CrossFire Framework.
Location: C:\Program Files (x86)\Tyco\CrossFire
Version: 3.70.539.289

Extension Services

- Stop** Name: SoftwareHouse CrossFire Import Watcher
Status: **Running**
Enabled:
Description: Windows Service for CrossFire Import Watcher
Location: C:\Program Files (x86)\Tyco\CrossFire\ServerComponents
Version: 2.70.539.289
- Start** Name: CrossFire GPI Service
Status: **Not Licensed**
Enabled:
Description: Windows Service for CrossFire GPI
Location: C:\Program Files (x86)\Tyco\CrossFire\ServerComponents
Version: 3.70.539.289



Sample deployment configuration

By default, visitors don't have any clearances. They are assigned manually upon check-in, or automatically if the visit itself had any clearances associated with it.

In most cases when deploying the QR Credential Service, you will want your visitors to have a clearance that will allow them to enter the first site perimeter, or any other location such as a dedicated visitor parking before they check in. The QR Credential Service is specifically designed for these use cases.

Working Method

The following method will describe a situation where the visitor receives an initial clearance to access the site perimeter.

When they are checked in, they will receive an additional clearance providing access inside the site as well.

The advantage of this principle is that you do not provide any internal access before the visitor is checked in at the reception desk. They can only use their QR credential at the designated locations for entry.

Tasks

The following tasks need to be performed to set up our example:

- [Create Visitor Clearances](#) on page 19
- [Create a Visitor Template](#) on page 19
- [Create Visit Site \(pre-configuration\)](#) on page 20
- [Create a Visit Template](#) on page 21
- [Configure the Visit Site](#) on page 22
- [Testing: Creating a visit](#) on page 23

Create Visitor Clearances

We need to configure two Clearances: a Perimeter Clearance and an internal Site or Building Clearance.

Perimeter clearance

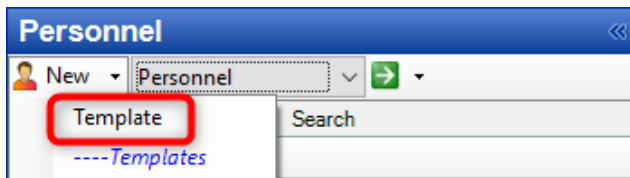
Holds the door of the perimeter only. This will be the entry that has the QR reader on which the visitor will be able to badge.

Site Clearance

Holds the doors that the visitor can access after he is checked in and received a normal credential.

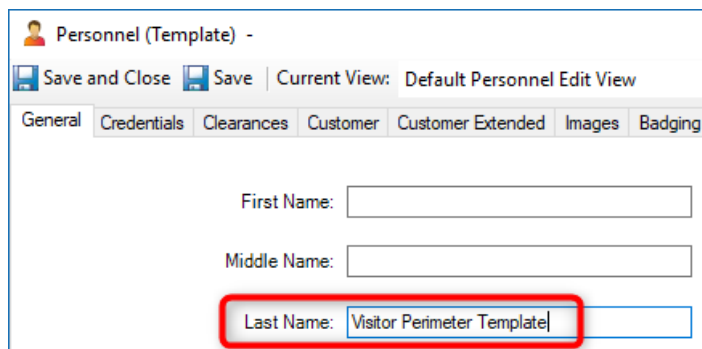
Create a Visitor Template

From the Personnel menu, select the down arrow next to new and create a new Personnel template.

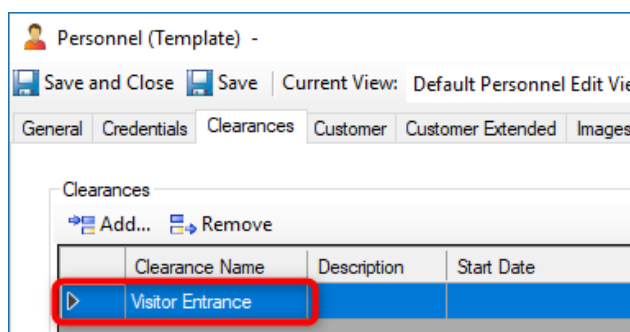


- This template will allow you to specify the default clearance that you will give your visitors, without being checked in: the perimeter clearance.

On the General tab, enter the name of the template



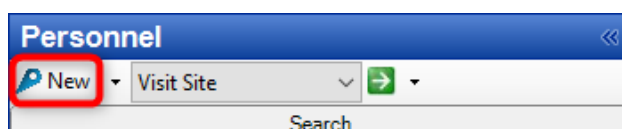
On the Clearance tab, add the Visitor Perimeter Clearance



Save the template.

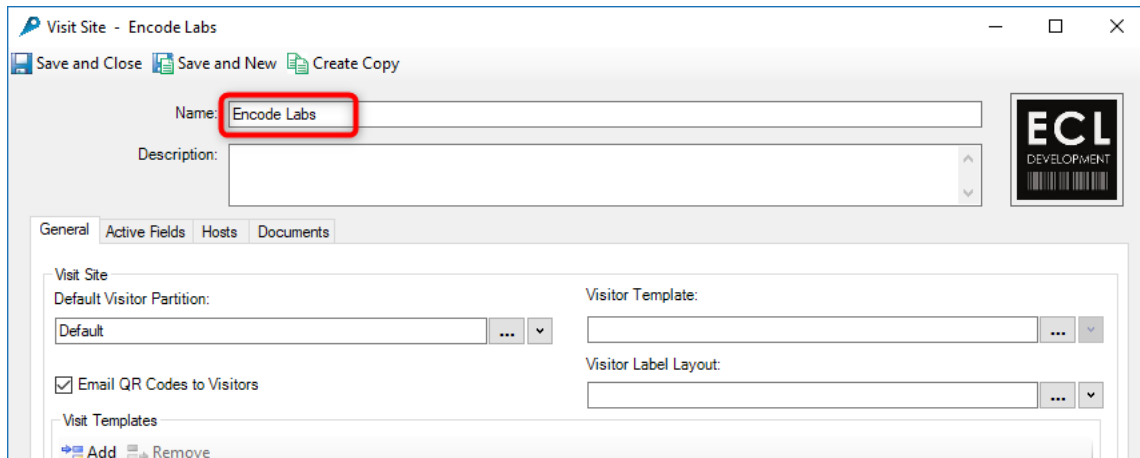
Create Visit Site (pre-configuration)

Create a new Visit Site



At this stage, just enter the name and save it.

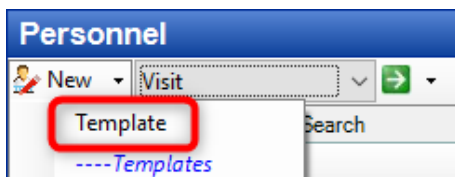
We will get back to this after we created the visit template.



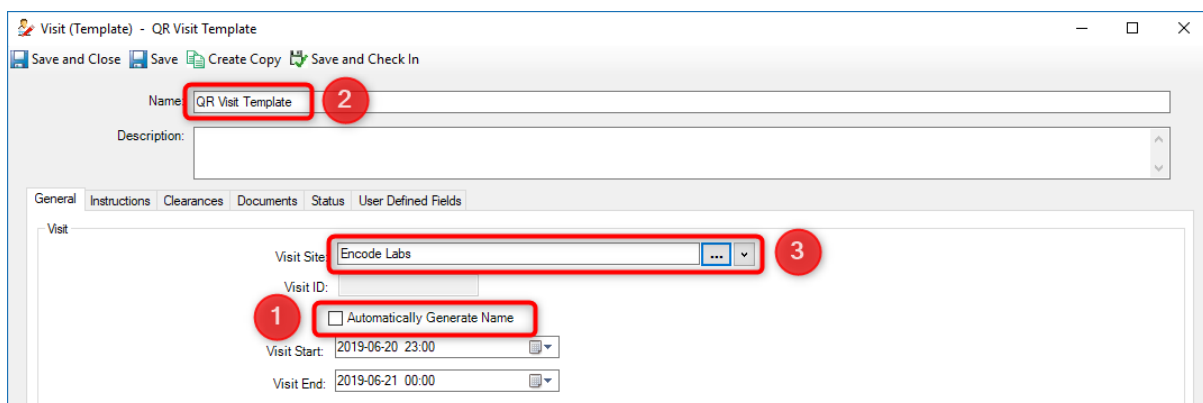
Create a Visit Template

The visit template will hold the clearance the visitor will receive automatically after he is checked in, along with some other configuration you may want to add.

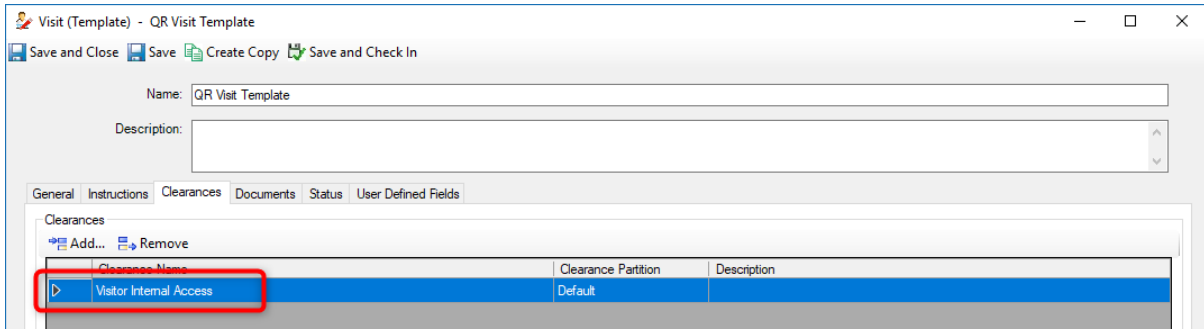
Create a new visit template:



1. Uncheck the auto generated name
2. Enter a name for your visit template
3. Select the site you created earlier



Add the internal visitor clearance (that provides access to the doors on site)

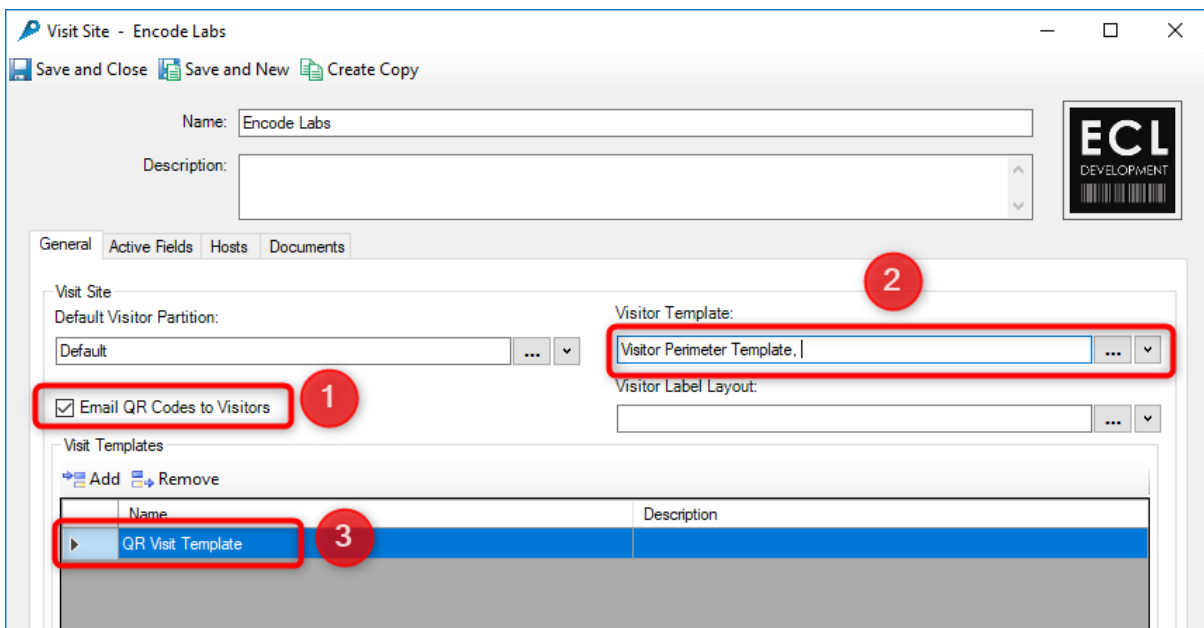


Save the template

Configure the Visit Site

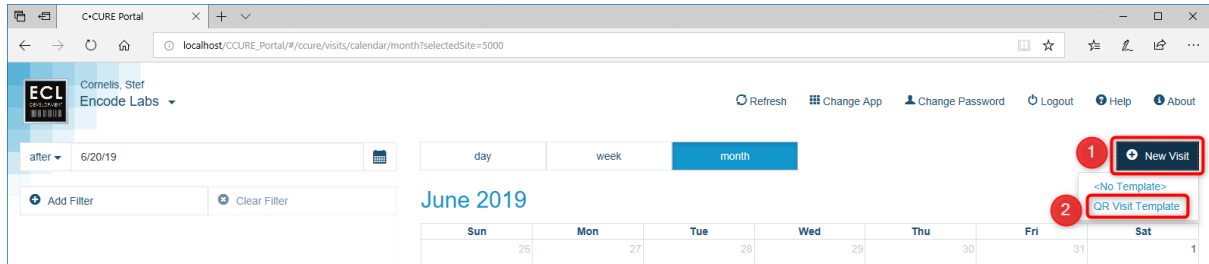
The previously configured objects are now combined into the site configuration:

1. Check the option to email the QR codes to the visitors
2. Select the visitor perimeter template (this provides default perimeter access to the visitors for use with their QR code)
3. Select the visit template (This holds the internal clearance they receive upon checkin)



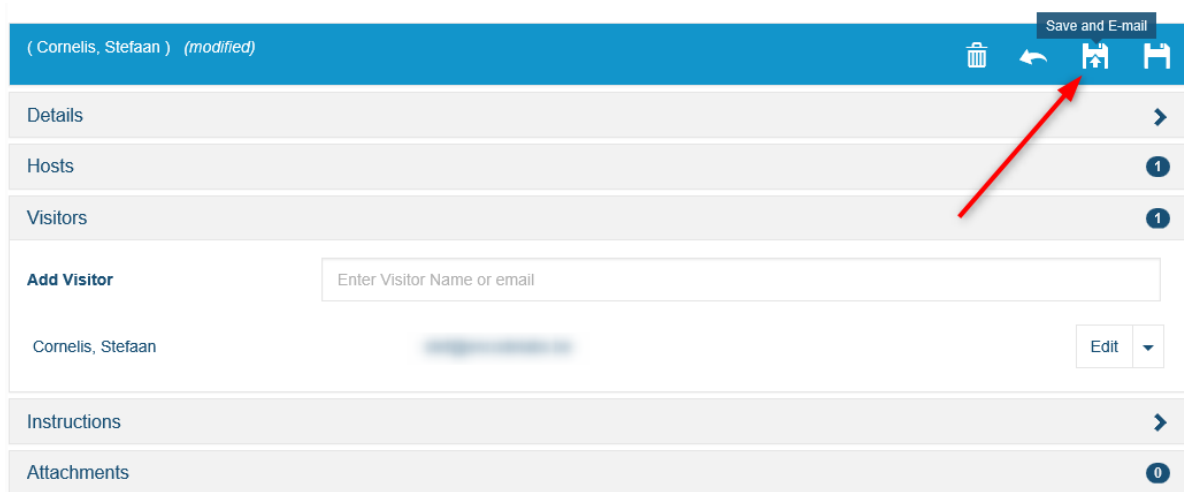
Testing: Creating a visit

1. Click "New Visit"
2. Select the template you created (holding the perimeter clearance)

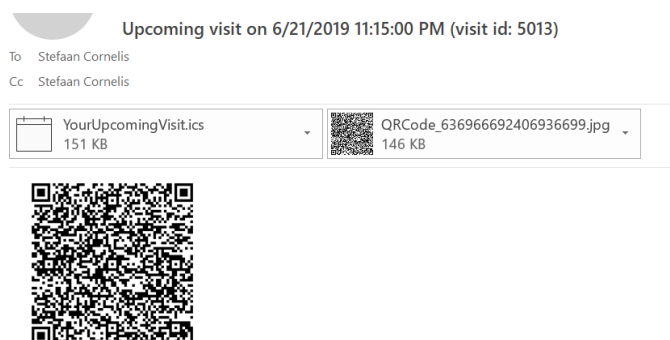


Now you can complete the visit details.

When you completed entering the visitor data, select Save and Email



The visitor will receive the email containing the QR code:

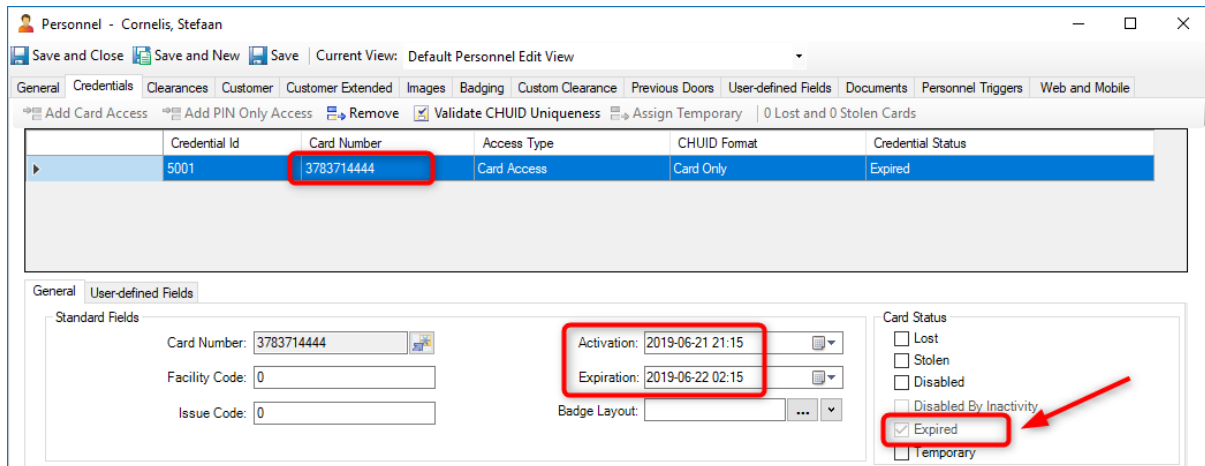


The QR service will generate the credential for that person (log extract from the service log):

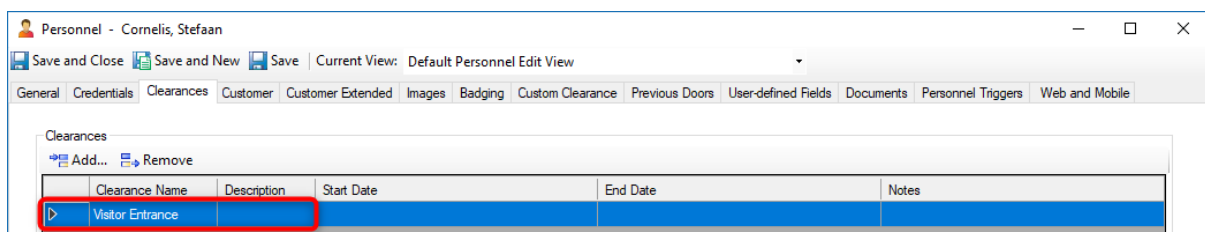
```
Received 1 upcoming visitor records for processing  
Stefaan Cornelis - Adding QR credential with Activation on 2019-06-21 21:15:00Z
```

And the person will have been created inside the CCURE with the QR badge number.

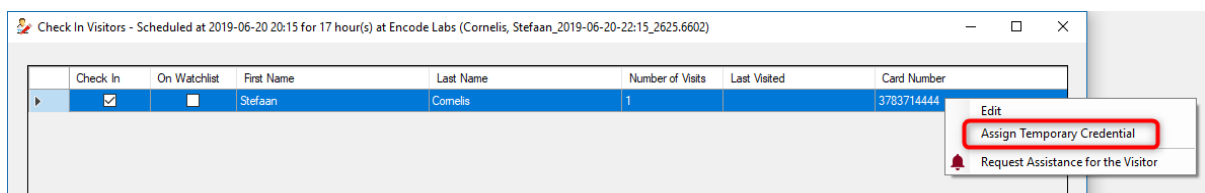
- The badge holds the validity of the visit +/- the configured buffer time
 - This is configured in the configuration file of the service. Refer to [Configuring the appSettings](#) on page 12 for more information)
- Notice how the badge has the status "EXPIRED", because this visit is for the next day, and our test system is configured to activate the badge 2 hours before the official start of the visit, and 2 hours after.



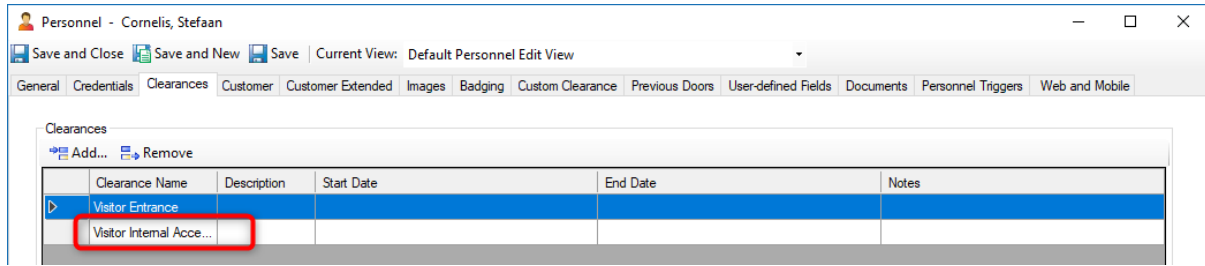
You can also see the visitor has the QR Perimeter Clearance as was configured on the visit template:



When the visitor arrives, you can open the scheduled visit and check in the visitor. You can also assign a temporary credential to the visitor for use during the visit:



When you open the visitor record, you will now see he also received the "Visitor Internal Access" clearance that was assigned to the visit template:



Remarks: Number of cards per person:

If you provide a badge to your visitor for Access Control, you need to make sure the system allows more than one credential from the system variables:

| Name | Description | Value | Minimum | Maximum |
|--------------------------|---|-------|---------|---------|
| Maximum Cards Per Person | The number of cards that users will be able to add to a single person record. | 5 | 1 | 5 |

Appendix A

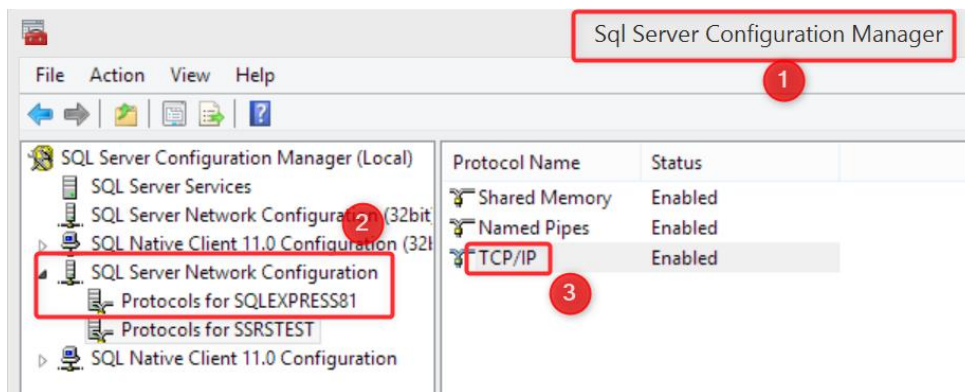
Considerations for SQL Express



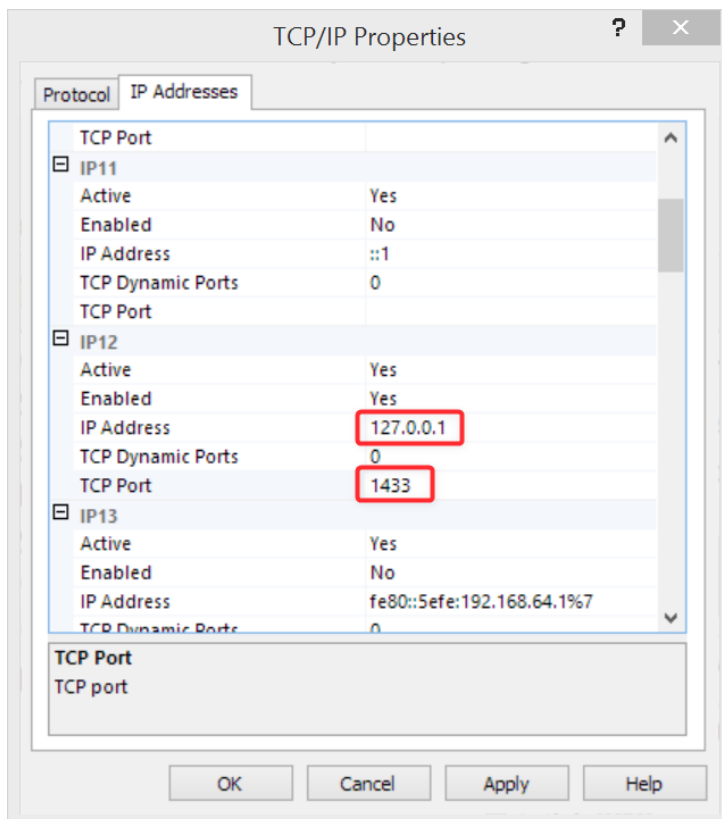
When using SQL Express, you must enter the named instance of the server as well. The default value is `(local)\SQLEXPRESS`

If you can't connect to the SQL server instance, try the following steps:

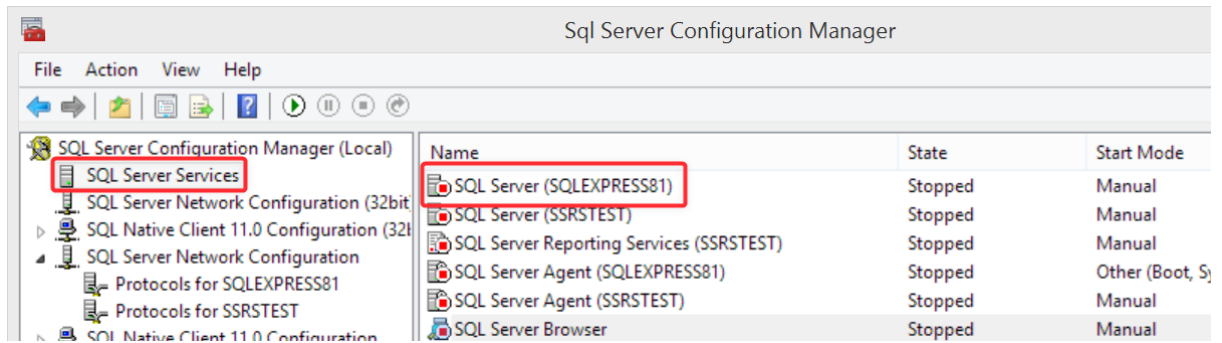
- Open SQL Server Configuration Manager
- Open the TCP/IP properties (also make sure this is enabled)



- Find your local interface (localhost) this is IP12 in the example below
- On the TCP Port add 1433 as the default port for accepting connections



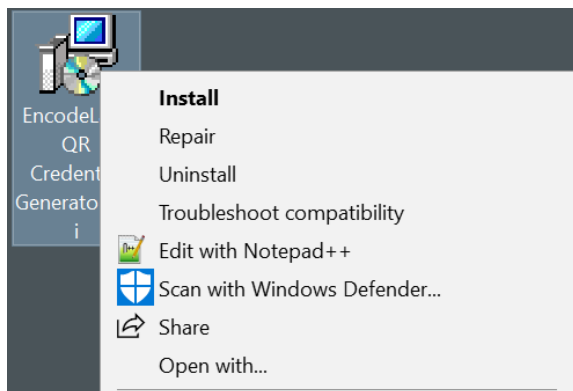
Then restart the SQL service from the configuration manager



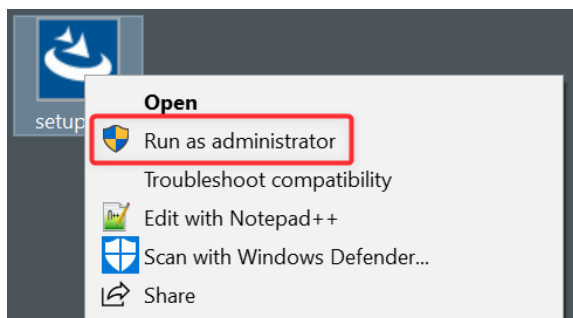
Avoiding UAC issues

When performing the installation on a system that has User Account Control (UAC) activated, you need to run the installer as an administrator.

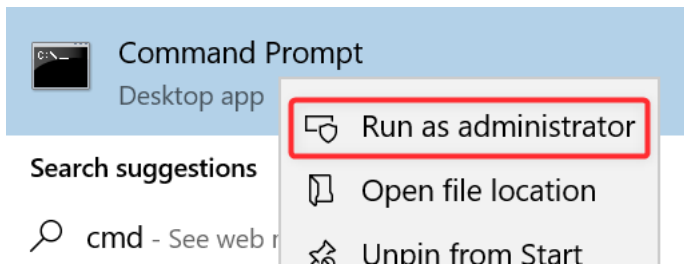
But this is not possible by default from an msi installer package:



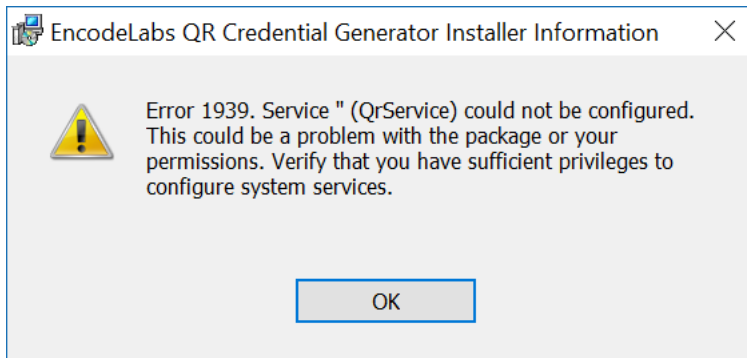
There is a setup.exe containing the same msi installer inside of it, so you can run the installation as admin.



You can also run the msi installer manually from an Administrative command prompt to force it to run with admin privileges:



If not launched as an admin, the installer will fail due to missing access rights:



DateTime issues

Windows 10 and Windows Server 2016 changed the date and time formatting settings for some cultures. Of particular concern are seven cultures for three different regions:

- Finnish
- Norwegian Bokmål ("Norway" and "Svalbard and Jan Mayen" variants)
- Serbian (variants "Cyrillic, Kosovo", "Latin, Montenegro", "Latin, Serbia" and "Latin, Kosovo")

For these cases, it is possible to change the used DateTime format in the settings file under appSettings. You can see this issue generating the following log entry as well in the application:

System.Data.SqlClient.SqlException (0x80131904): The conversion of a nvarchar data type to a datetime data type resulted in an out-of-range value.

In a particular Norwegian support case the time separator ":" (colon) was replaced with "." (period) resulting in a format HH.mm.ss even when specified to be a colon.

You can force a colon by using "\:" as a separator.

Sample ISO DateTime format:

```
<add key="DateTimeFormat" value="yyyy-MM-dd HH:mm:ss"/>
```

Sample DateTime format to bypass the locale issue:

```
<add key="DateTimeFormat" value="yyyy-MM-dd HH\:mm\:ss"/>
```

To help you find formatting issues, you can run the DateTimeCheck application that can be downloaded from our website under the support section.

```
*****  
Default Language Info:  
* Name: en-US  
* Display Name: English (United States)  
* English Name: English (United States)  
* 2-letter ISO Name: en  
* 3-letter ISO Name: eng  
* 3-letter Win32 API Name: ENU  
*****  
Standard format: 2019-06-20 22:11:24  
ISO 8601 Format: 2019-06-20T22:11:24.1260422+02:00  
HH:mm:ss: 22:11:24  
HH\mm\ss: 22:11:24  
ToString FormatProvider en-GB: 20/06/2019 22:11:24  
ToString FormatProvider en-US: 2019-06-20 22:11:24
```

The application will show different conversions on your target system to help provide insights into how to fix the issue.



© 2018-2020 ENCODE LABS BVBA