merbon
SCADA

Operating information

domat
control system

Contents

domat
control system

1 Operating information

The **scada** folder, which contains projects to be loaded after SCADA startup, is to be found at the path C:\vision_data. It is advised to make a backup of this folder before every rewriting of the project(s) by a new version exported from RcWare, or basically before every major editing of the project(s).

There is also **events.db** file inside **scada** folder. It is database file which contains data about all user operations in Merbon SCADA client (e.g. datapoints values changes, schemas viewing, alarm acknowledge). Under normal circumstances the file´s size is not very big. Yet if there are a lot of projects uploaded on SCADA server and installation is running more than a few years the file can grow to size that big that it may cause slow loading of events history. In case of some incorrect use of user scripts a file can grow to such a size that SCADA service is unable to be started. The solution of this problem is making a backup copy of **events.db** file and deleting it from its original location in **scada** folder. If we wish to preserve file continuity it is necessary to use some SQLite tool (HeidiSQL) for database browse and files size edit (e.g. deleting records older than 2 years). Maximum file size depends on PC performance, disk size etc. In general files up to 500 MB are mostly trouble-free. From 500 MB to 2 GB the user can observe changes during events history loading. With sizes over 2 GB there can occur problems with history loading or running services.

User settings, configuration of services, and history are stored in folders „**Warehouse**“ in the installation directory, typically C:\Apps\Merbon.

The SCADA pages are edited in RcWare Vision. The RcWare Vision projects are stored in the **DATA** folder where RcWare Vision is installed (e.g. C:\RcWare\DATA).

Every installed component of Merbon SCADA has its own configuration file. The configuration files are named *.config, *.json, or *.js, and are located in the folders where the respective services are installed.

1.1 SCADA services running on the PC

After Merbon SCADA is installed, the running services can be monitored using the installer (in the *Services* panel) or in Windows application *Services*. Some parts of Merbon SCADA use only one Windows service, while others use more services. Some services also use web, which may be checked in the IIS Manager application. If there are problems, a good start to solve it is to check if all services and webs are running properly.

domat
control system

1.1.1 List of services:

Merbon Domain server:

DS2Database

Merbon.NetCoreServiceShell Server # MerbonDomainServer2

Merbon SCADA server:

Merbon SCADA # MerbonSCADAServer

Merbon Alarm server:

Merbon Alarm Server # MerbonAlarmServer

Merbon Domain Server Bridge # AlarmServerBridge

Merbon Messaging Server # MerbonMessaging

Merbon Database:

Merbon DB # MerbonDB

1.1.2 List of webs:

Merbon Domain server:

MerbonDomain_Web

Merbon SCADA server:

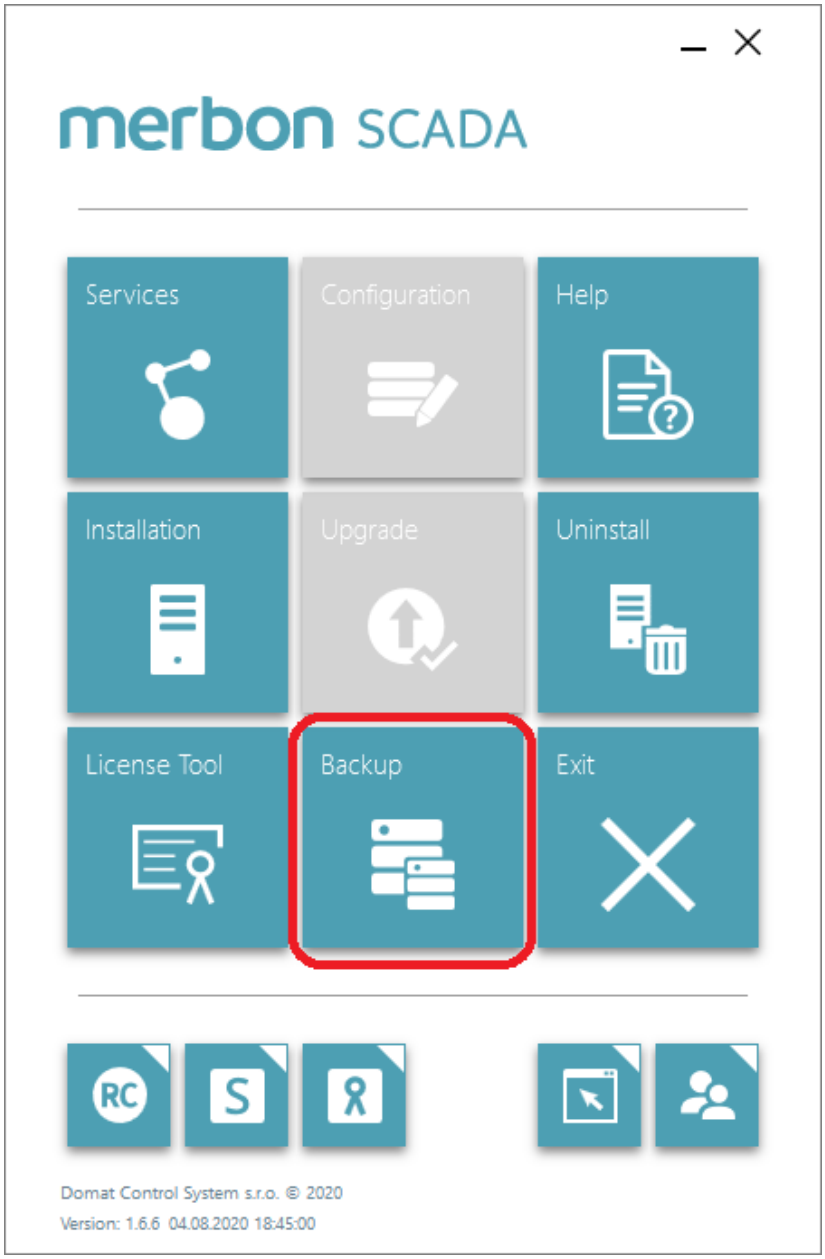
MerbonScada_Web

Merbon Database Adapter:

MerbonDatabaseAdapter

2 Backup

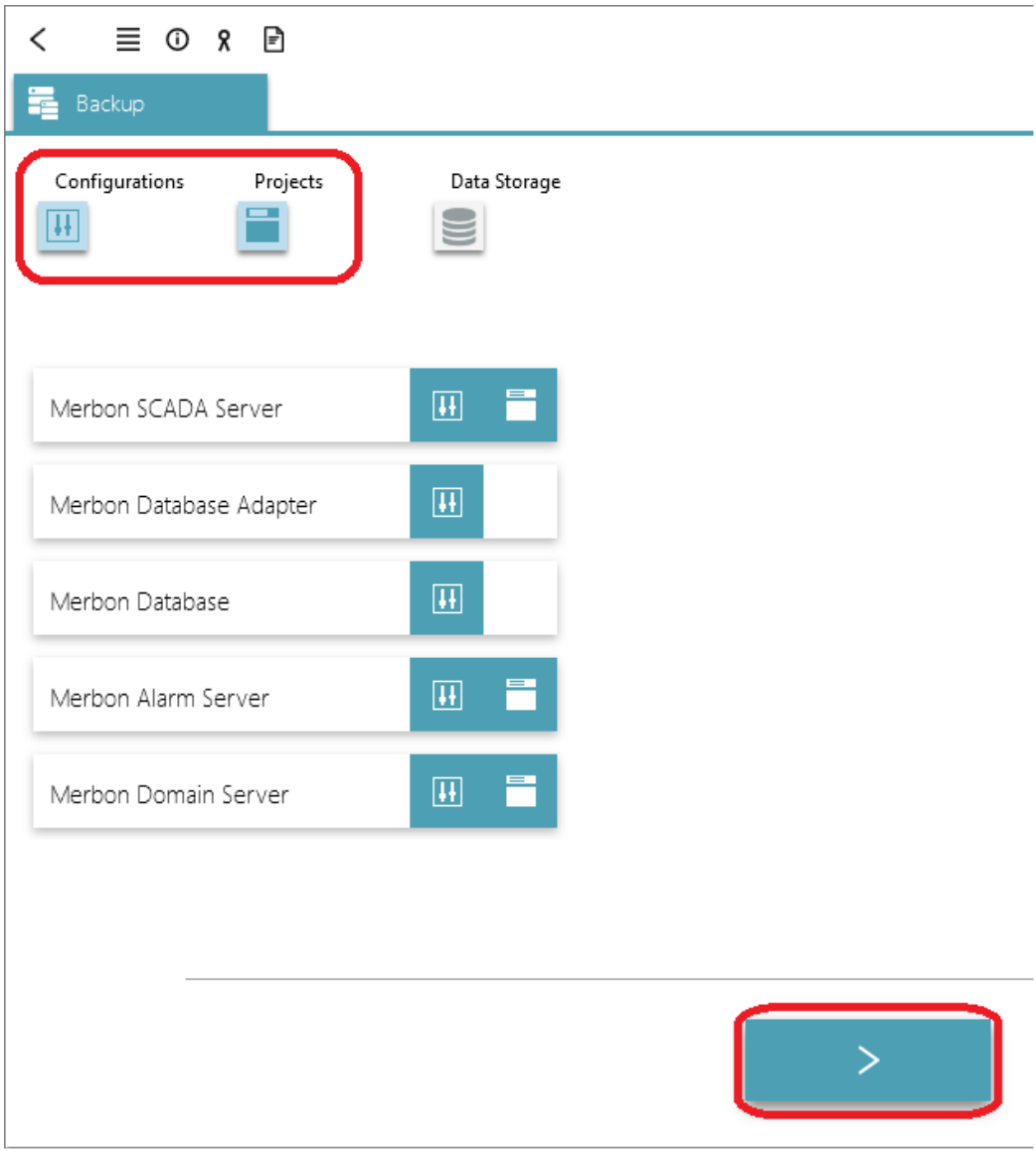
To make a backup of the installation, the Backup function can be used. It is part of the installer and can be launched from the main tile menu of the Merbon Installer program.



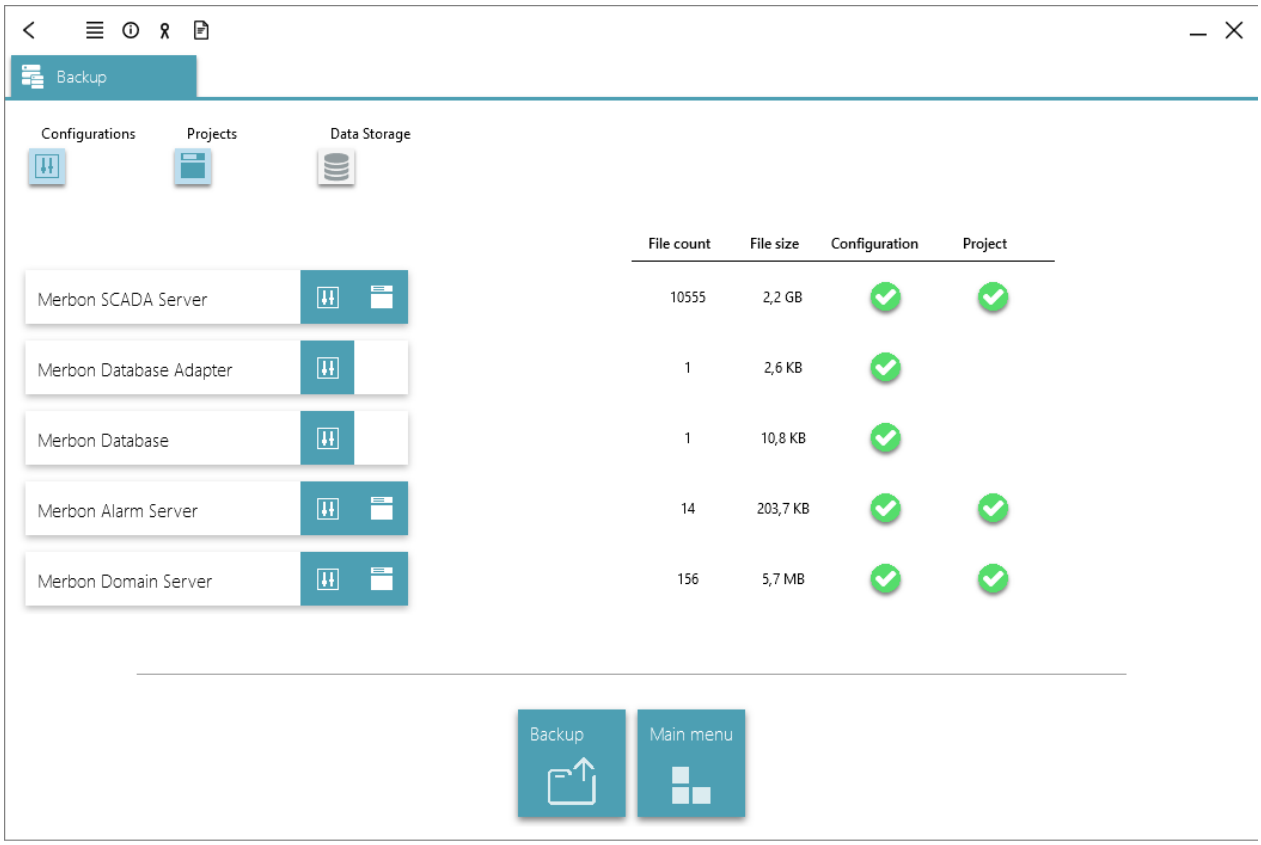
In the Backup bookmark there are all services currently installed. Two buttons on the top of the panel are used to choose whether you want to create backup of configuration files or projects. „Backup“ function still does not make copy of the datapoints history. If we wish to create this backup it is necessary to proceed manually. In case of the file history we make copy of the

folder defined during RcWare Vision export. There is an option to include this folder to “Backup” function, if the path is set somewhere inside C:\vision_data folder. Whole vision_data folder is copied during Merbon SCADA server project backup.

In case of database it is necessary to create a backup of Merbon Database Warehouse folder.



We can run the backup function using button in the bottom of the panel. At the end of the process the result is shown for all components. At the same time file count and file size is listed for every installed service.



By clicking “Backup” button we can check the backup result in the file explorer. Backup folder is set on path C:\Apps\Merbon_BACKUP by default.

To prevent data loss on unexpected hardware or software problems, it is recommended to back up files which can be used for system restore on a new machine together with the complete settings and trend data.

The regular backup period depends on the application type, and on the period of data loss acceptable at particular installation.

Below is the list of all folders which must be copied in order to completely restore the services installed using the Merbon SCADA installer:

Folder C:\Apps\Merbon

Merbon Database Warehouse

Alarm Server Warehouse

Merbon DS2 Database Warehouse

In folder C:\Apps\Merbon\Merbon DS2

file: **appsettings.json**

In folder C:\Apps\Merbon\Web Client\Merbon Scada Web

file: **config.js**

In folder C:\Apps\Merbon\Web Client\Merbon Scada Web\api

file: **web.config**

In folder C:\Apps\Merbon\Alarm Server Bridge

file: **ESG.Domain2.Domain1Bridge.Host.exe.config**

In folder C:

vision_data

In folder RcWare\DATA where the RC Ware editor is installed:

All folders

If file history recording is enabled, the history files should be backuped too. The path where history is saved is set up when the project is exported from RcWare Vision.

3 SSL security certificate for Merbon SCADA servers

3.1 Introduction

The IIS server where a Merbon SCADA server is installed should contain a SSL security certificate. Otherwise most of the browsers will consider the site insecure and show warning messages or refuse to display the web pages completely.

HTTPS/SSL protocol can secure the data travelling between client and server and back. This means that the data flow between the browser and the server cannot be monitored by a third party. Standard TCP port for HTTPS/SSL communication is 443, while HTTP standard port is 80.

The addresses of web pages secured with SSL start with the https:// protocol name. The browsers display a padlock icon in the address row and tinge the address with different colours: green for full compliance, yellow or orange for a secured page with problems (such as containing a valid certificate issued for another domain), and red for a wrong certificate. If the certificate has been created using OpenSSL or IIS (self-signed certificate) the browser may show a message that the web is not trustworthy when accessed over the Internet. This problem can be solved by a certificate issued by an external authority.

Issuing a certificate by an external authority is a paid service (about 10 to 50 € per year). The price depends on the trustworthiness of the issuing authority, validity length of the certificate, degree of security, etc. The certificates must be prolonged as their validity is limited by time. The expiration date is stored directly in the certificate and can be viewed e.g. in a web browser. As soon as the certificate expires, it is automatically considered invalid. Maximum validity length is usually 2 years. This means that even if the server is certified at the installation time, it loses its

validity after maximum two years of operation, and SCADA „stops working“ just by itself. This is long before the warranty time ends (which may be up to 5 years at the turnkey projects).

If the Merbon SCADA server is operated exclusively in an intranet, i.e. without access from the Internet, using SSL is not necessary and browsers tend to accept unencrypted connection too (http://, TCP port 80). Then the standard installation manual for Merbon SCADA server setup is to be followed.

If the Merbon SCADA server shall be accessible from the Internet, the IIS server should have a SSL certificate installed. The certificate is issued by a certification authority. It is bound to the domain name which is used to access the server, for example merbonscada.company.com. This name has to be agreed with the IT manager of the network the server is installed in. The IT must also configure the network so that the server is available from the Internet.

A certificate is a file with .pfx extension. There are also other certificate formats, however, the IIS server requires a .pfx file. The file is imported in the IIS server settings (Server certificates) and then selected in the MerbonScada_Web configuration (Bindings, Add…, Type: https to port 443, and select the certificate file which was imported in the previous step).

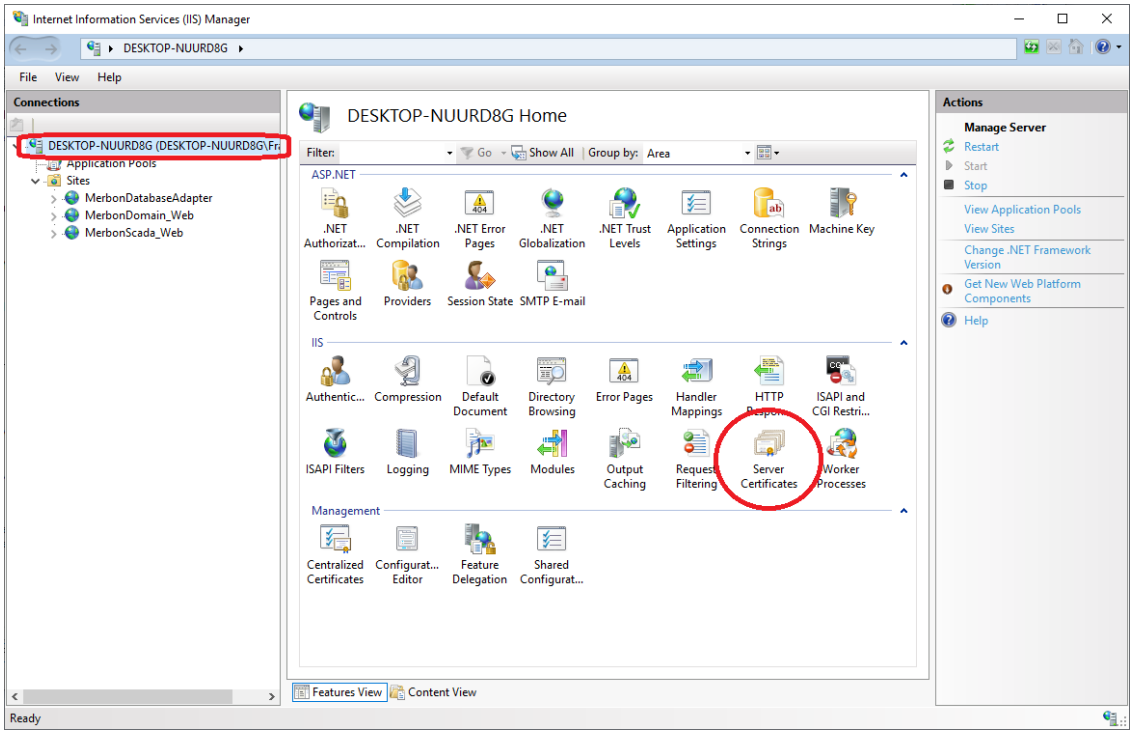
As a certificate is subject to expiration, it must be updated regularly. At system (turnkey) project supplied by Domat, Domat as a supplier guarantees a valid certificate for a period of 2 years or until end of the warranty time according to the contract. Then a new certificate must be either ordered extra as a post-warranty service or got by the site owner or operator.

If the Merbon SCADA licence is supplied as a product, the system integrator or IT department of the IIS server owner are fully responsible for issuing of a certificate, its installation and configuration of the IIS server. All system integrators are asked to get to know the SSL problematics and the Merbon SCADA Server environment thoroughly before the commissioning starts. It is advised to organize the connection to the Internet, domain name and issuing of a certificate in advance. It saves time spent on commissioning. Please note that the IIS server configuration takes about 30 minutes plus time required for communication with the local IT and a certification authority.

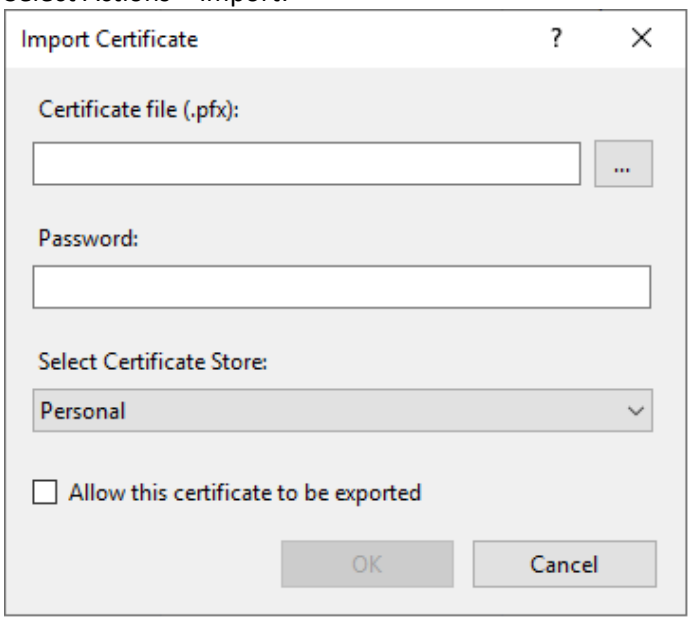
In general, for the issuing of the certificate, its installation and updates, the IIS server operator is responsible rather than the SCADA system supplier.

4 How to install the certificate in the IIS

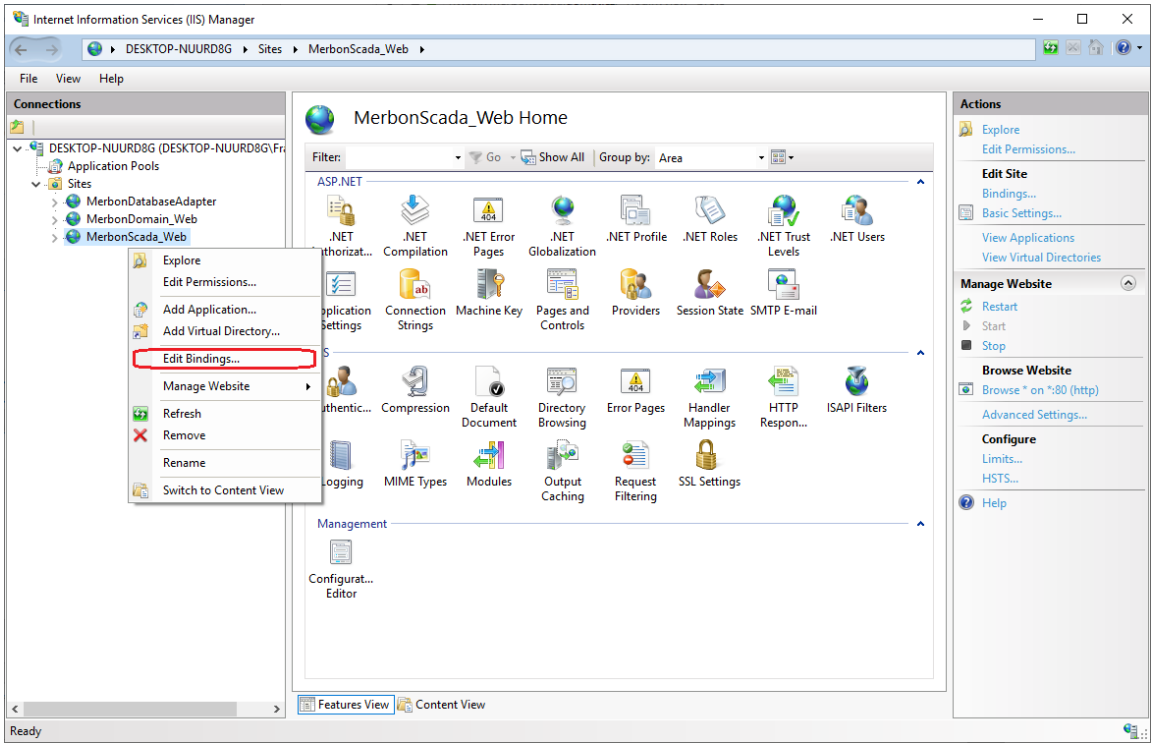
Open the IIS manager (v C:\Windows\System32\inetsrv the InetMgr.exe file)
Select the server and click Server certificates



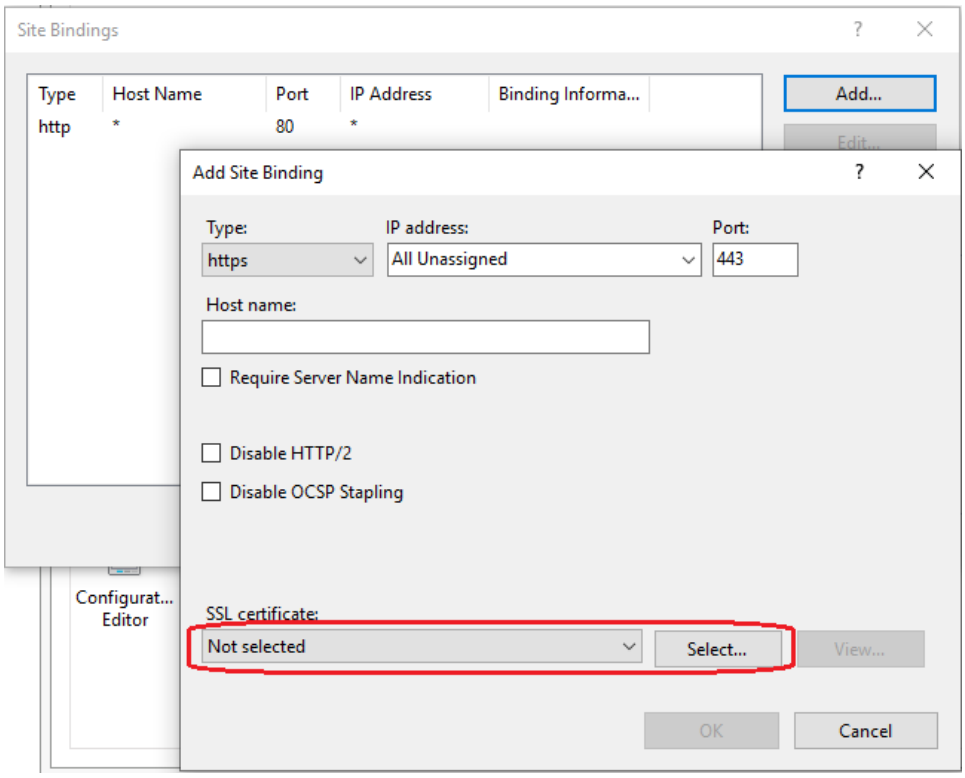
Select Actions – Import:



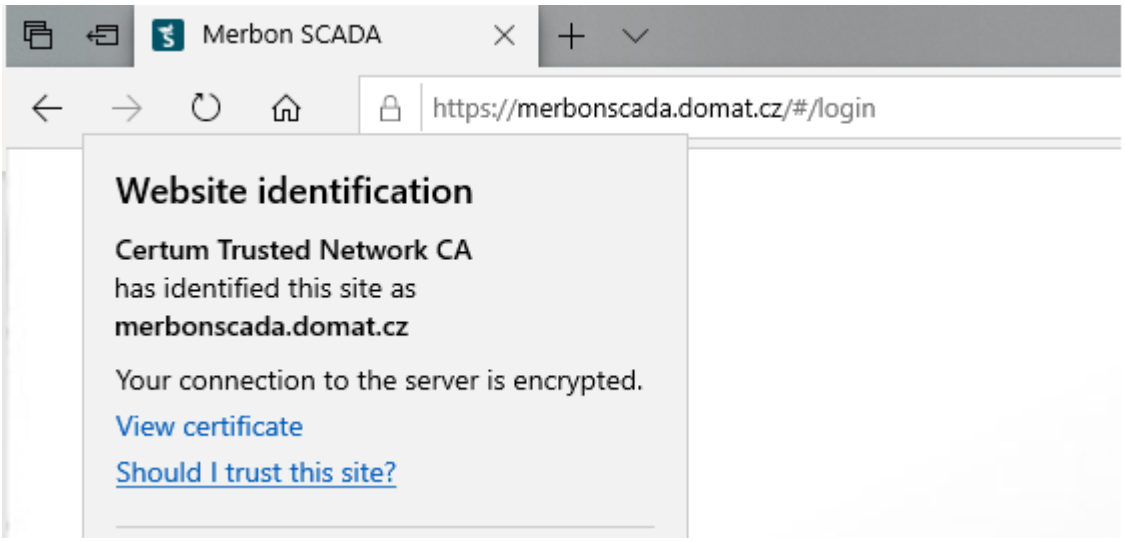
Select the certificate file and enter the import password provided by the issuing authority. Click OK. The certificate is now imported in the server.
In the IIS settings select the Merbon SCADA web and in the properties go to Edit web, Bindings…



Add a https binding and select the imported certificate.



Confirm by OK and restart the web. The web is now certified.


Merbon SCADA
https://merbonscada.domat.cz/#/login
Website identification
Certum Trusted Network CA
has identified this site as
merbonscada.domat.cz
Your connection to the server is encrypted.
View certificate
Should I trust this site?