Net2WebServer

Installation guide
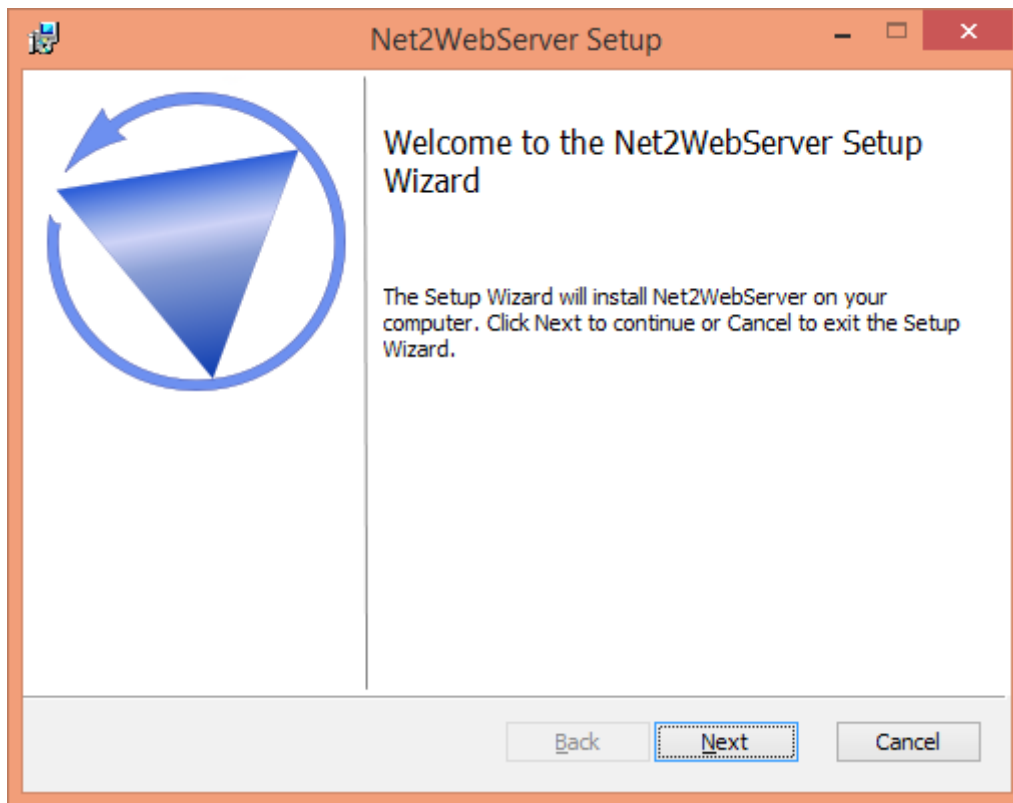
Version: 2.0
Date: 12-07-2016
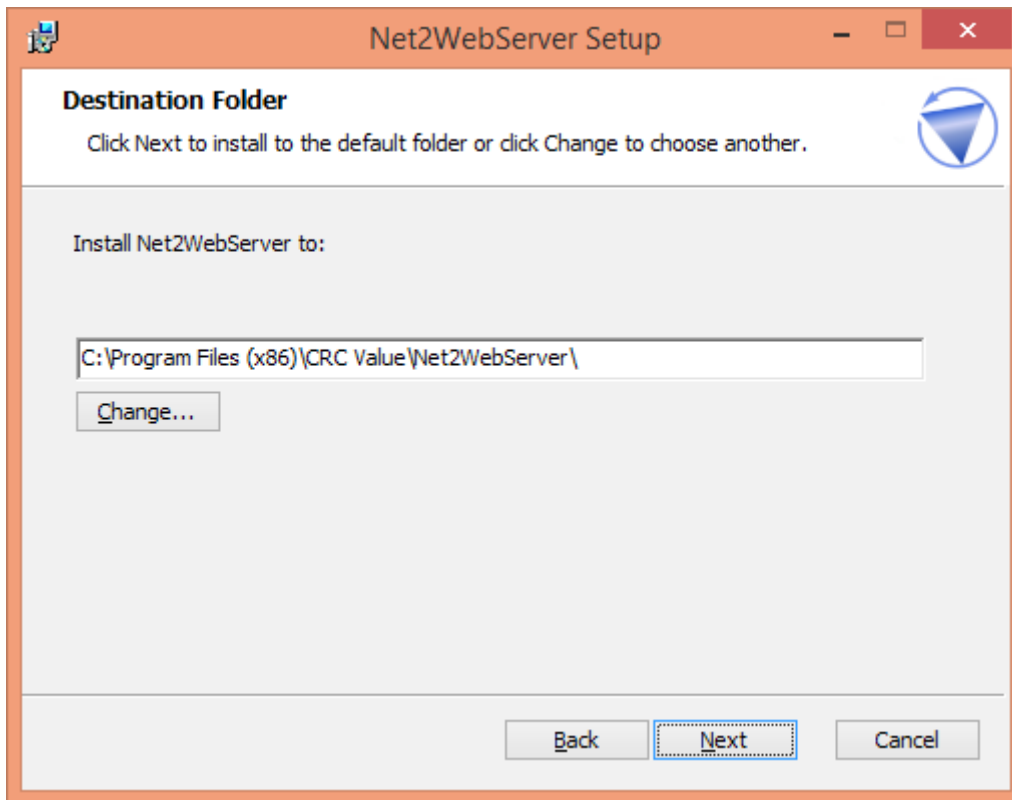Copyright: CRC Value B.V.

Index

Installation

Make sure you have downloaded the latest version from http://www.net2-solutions.com. Place the file 'Net2WebServerSetup.msi' on any machine in your network. The only restriction is that this machine has network access to the machine running the Net2 Server.

☑ Click 'Next'.

☑ Change, if desired, the installation folder.

☑ Click 'next>'.
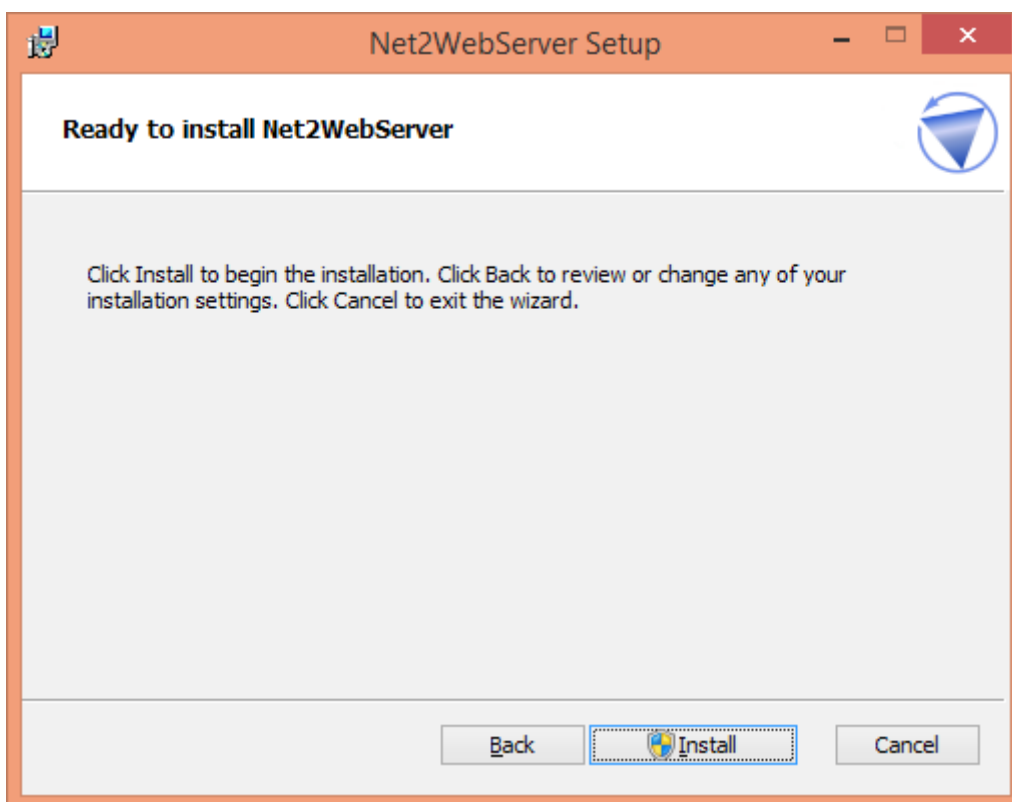
☑ Confirm all settings by clicking 'Install'.
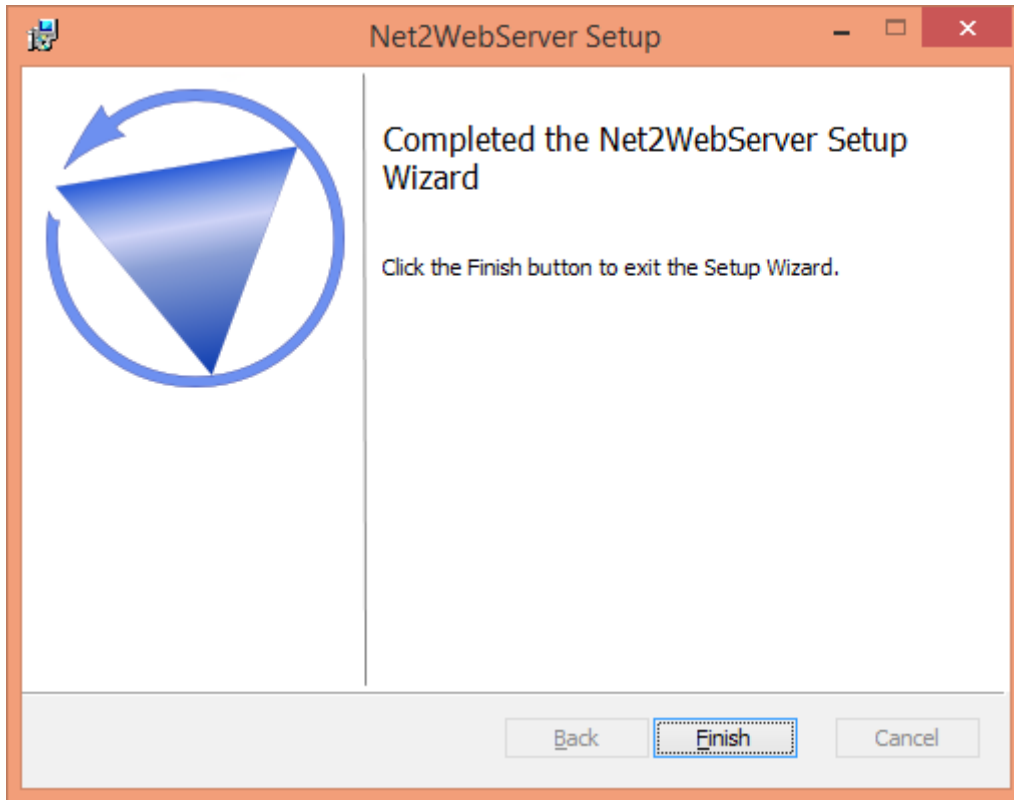
☑ Click 'Finish' to shut down the Net2WebServer installer.

Configuration

After the installation the Net2WebServer is installed as a 'service' but not yet started. The Net2WebServer needs to be configured first.

Go through the following steps to configure the Net2WebServer:
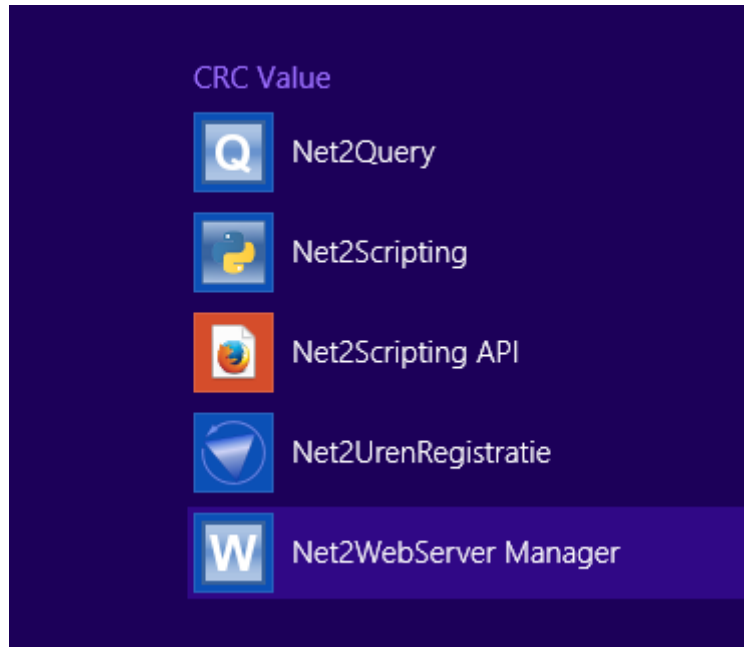
☑ Start the Net2Server Manager.

A 'splash screen' will be shown for a short period.
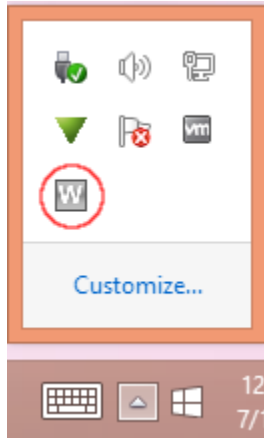
You can access the Net2WebServer Manager by 'right-clicking' on the light-gray (W) icon, located on the right side of the task bar.

At the first start you'll be asked to perform an initial configuration.

☑ Select 'Configure first!'.

As soon as the initial configuration is completed, the other menu items will become available also.

Configuration

A configuration window with 5 separate tab-pages will now be opened. On every tab you can define a certain aspect of the configuration.

Configuration-tab: 'Web'.

On the first tab-page you can state at what port and according to what protocol the Net2WebServer will listen for incoming requests.
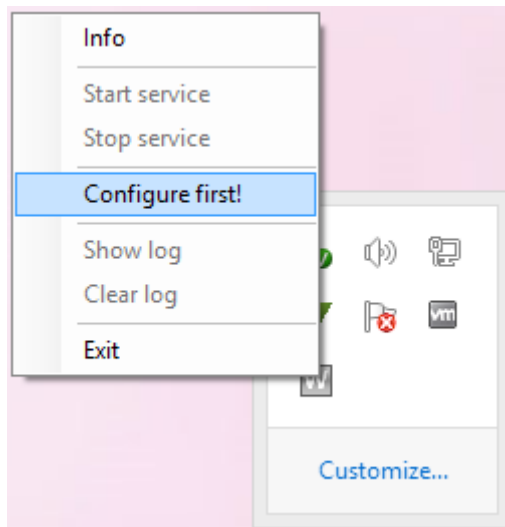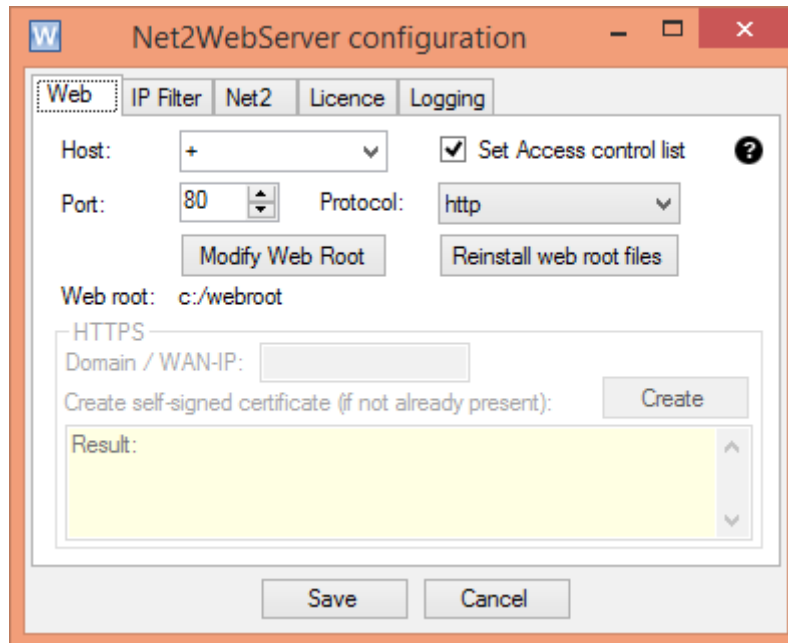
The option 'host' is only relevant when IIS is running on the same machine as the Net2WebServer. Leave it as it is otherwise.

Under normal circumstances HTTP traffic uses port 80. Leave this port unchanged unless you have a good reason for changing it. A good reason could be an other service already listening to port 80.

The 'protocol' option gives you the opportunity to use the more secure HTTPS protocol.

See section: "Net2WebServer Security" for a more elaborate discussion of the usage this protocol.

We suggest to keep all settings unchanged, at least for a first test. When this first test succeeds it is probably a good idea to switch to the HTTPS protocol.

Make sure the check-box 'Set Access control list' is ticked whenever you select a different port and/or protocol.

The 'webroot' is the location the Net2WebServer application will store its webpages.

Configuration-tab: 'IP Filter'
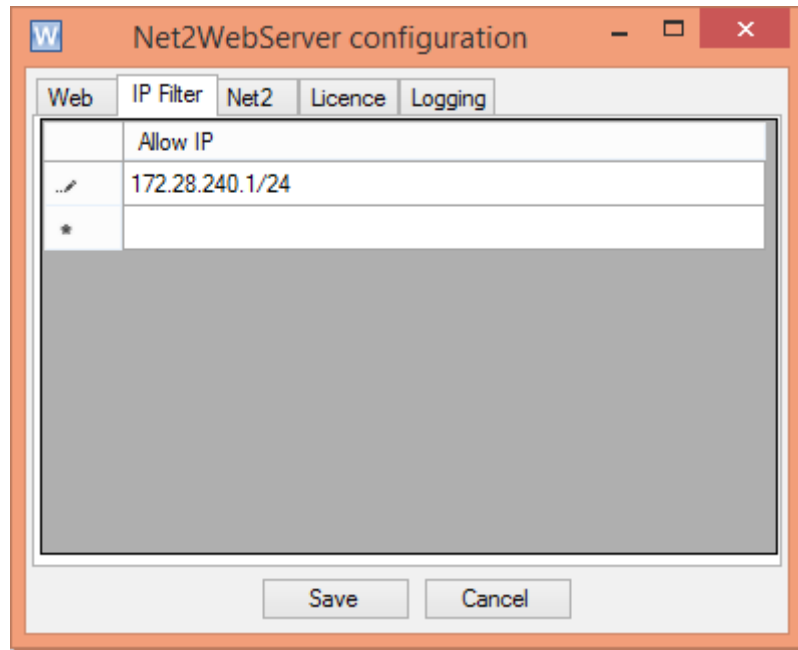
On this page you can define the IP address, or range of IP Addresses from which a client is allowed to access the webserver. If this page is left blank there will be no restriction.

Configuration-tab: 'Net2'
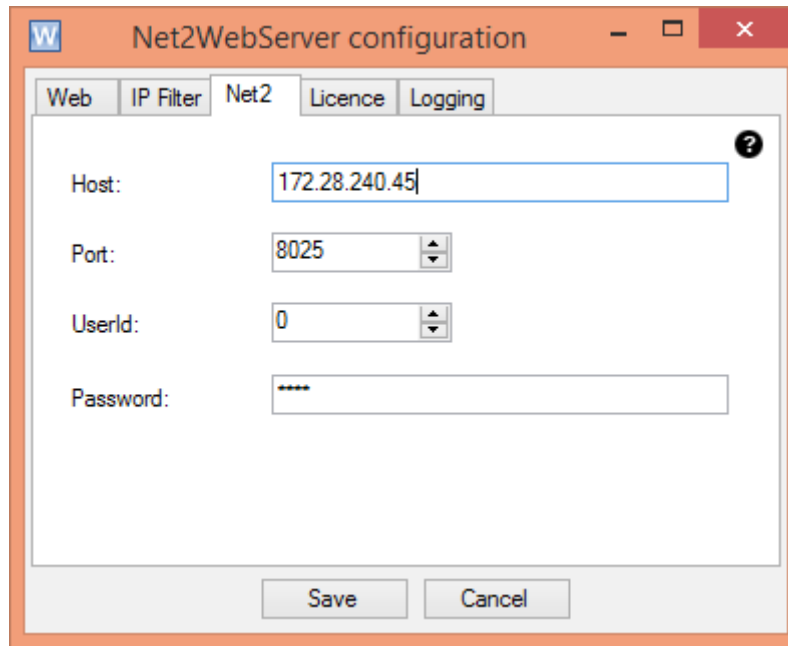

This third tab is about the connection between the Paxton Net2 Server and the Net2WebServer.

The option 'host' refers to the location the Paxton Net2 Server is running. Leave it at 'localhost' when both application are running on the same machine. Add the IP-address of the machine on which the Net2 Server is running otherwise.

The 'port' option refers to the port number on which the Net2Server is listening for remote connections. Unless you have deliberately altered this port number on the Net2 Server, 8025 should be OK.

The option 'UserId' refers to a Net2 user with administrator rights. Normally '0' will do.

The 'Password' fields can be used to enter the Net2 password you are using to log in to any of the Net2 applications. The default password is 'net2'.

Configuration-tab: 'Licence'
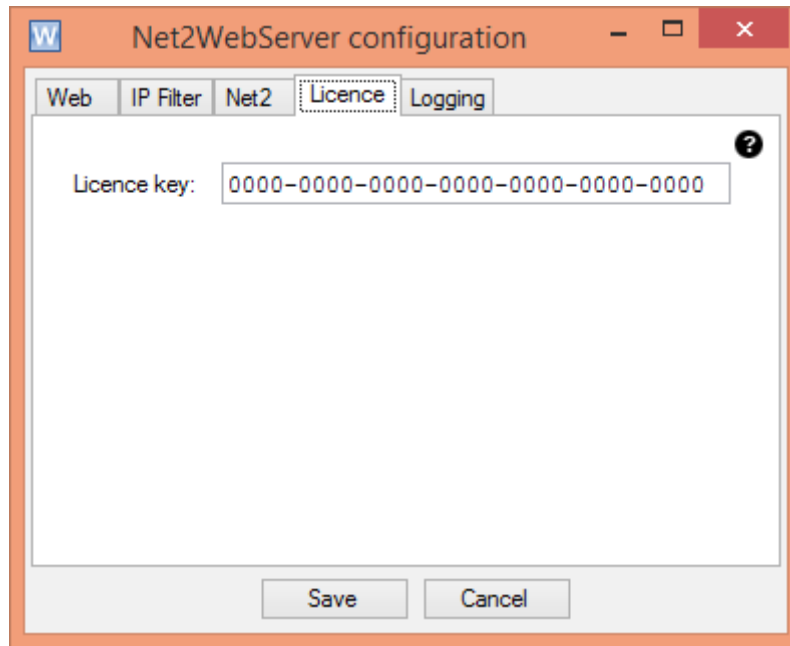
This tab is about entering a newly purchased licence code.

More information about licensing can be found in the section 'Licence'.

Configuration-tab: 'Logging'

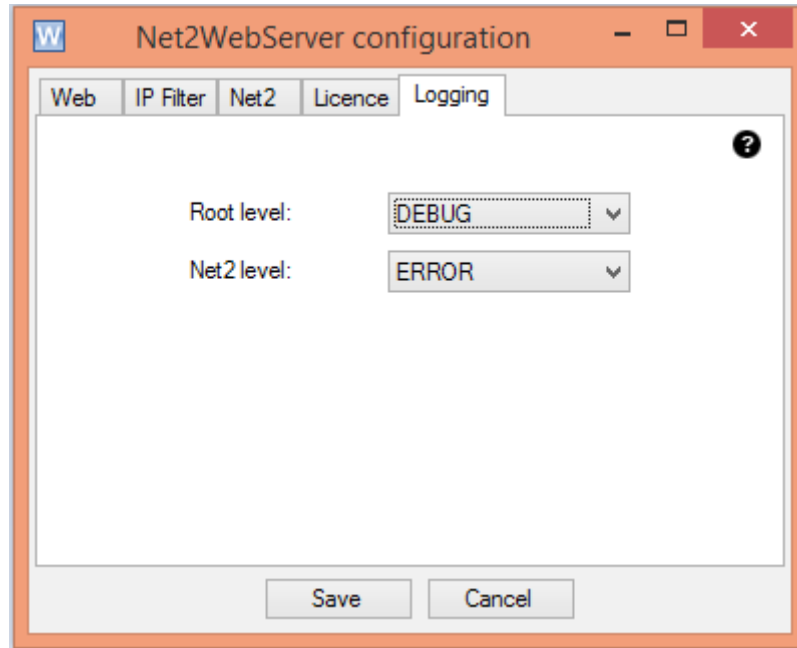On the last tab the amount of logging the application will generate can be stated. This option is important in case of trouble **only**.

Set the field 'Root level' to DEBUG in case the application refuses to start. After this change the log file will can hold valuable information about why the application didn't start.

The option 'Net2 level' is important in the (rare) case the communication between the Net2Server and the Net2WebServer is causing problems. It is not likely that this will ever be the case.

Leave both fields set on 'ERROR' under normal circumstances.

☑   Press 'Save' as soon as all parameters are set.

Starting the Net2WebServer
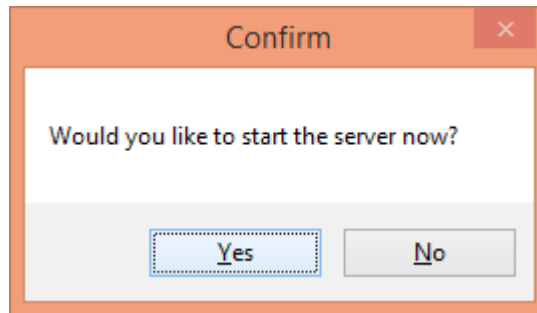
The manager application will ask whether it is OK to start the server once all initial settings are set.

The server can also be stopped- and started- manually.

☑ Open the Net2WebServer manager main menu by right-clicking the 'W'-icon and select option: 'Start Service'.
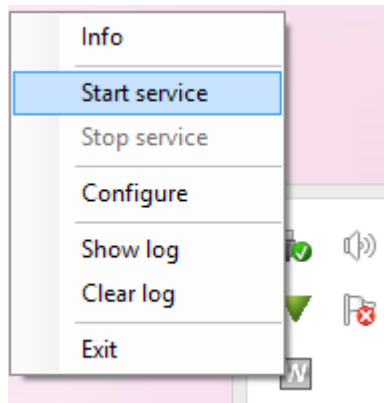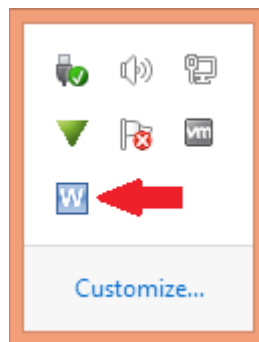
The, originally grey 'W'-icon, will become light blue when the Net2WebServer is successfully started. A message will be given if the Net2WebServer refuses to start. In that case, enable the logging and try again. Check the log-file to find out the cause of the trouble. We can help if necessary.

A first test

Start, on the same machine as the Net2WebServer is running, a web-browser. Any web-browser will do but the application is optimized for FireFox, Google Chrome and Safari. Internet Explorer can be a bit slow under certain circumstances.
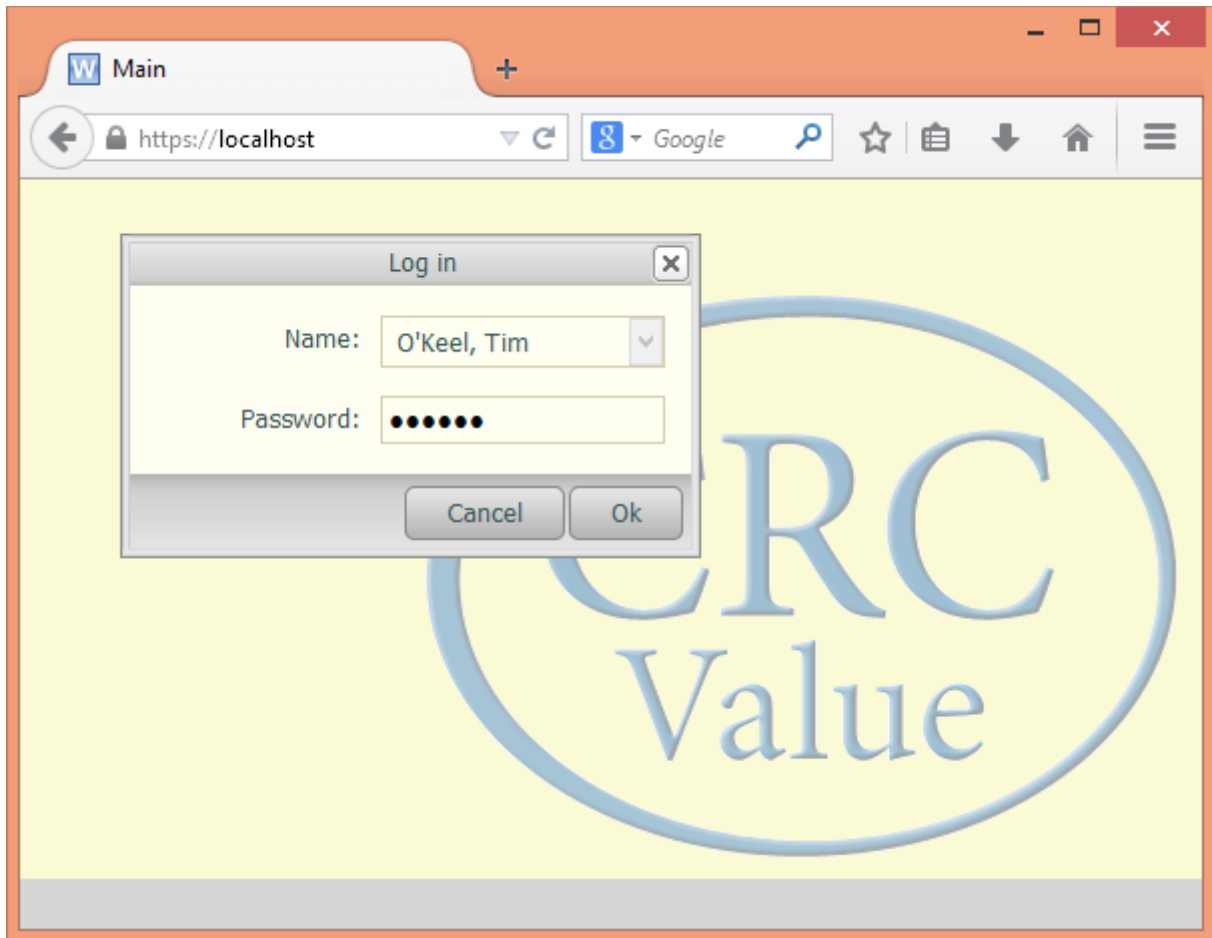
Type: http(s)://localhost on the URL bar.

More about this application can be found in the user manual.

Net2WebServer Security

The HTTP protocol is only suitable to be used on a 'trusted' (local) network. As soon as the application is to be accessed from a public location it is best to switch over to the HTTPS protocol.

Some background information about the HTTPS protocol

Certificates

During the initial connection setup process between a web-browser and a web-server the last one sends a so called 'certificate' to the browser. This certificate contains, besides information about how the communication is to be enciphered, the address of a 'trusted third party' who can confirm the site's identity. As soon as a browser receives a certificate it will always check the identity at this third party. There are several third parties that offer these certificates as a commercial service. Widely known third parties are for instance VeriSign and Thawte.

Self-signed certificates

As an alternative to buying a certificate it is also possible to create a certificate yourself. This self-created certificate will a so called 'self-signed' certificate. The drawback of this approach is that in this case the address of the 'trusted third party' is the same as the site who submits the certificate.

As a result, all browsers will therefore complain when they receive such self-signed certificate. This doesn't need to be a problem however because it is very well possible to let the browser accept these certificates. Once a certificate is accepted the connection will still be secure because all information about the enciphering is contained in the certificate also.

More about this subject can be found in the section: "Setting up your browser to accept Self-signed certificates".

Net2WebServer Security

The Net2WebServer manager is able to setup an infrastructure using a self-signed certificate as described above. Go through the following steps to enable this HTTPS infrastructure.
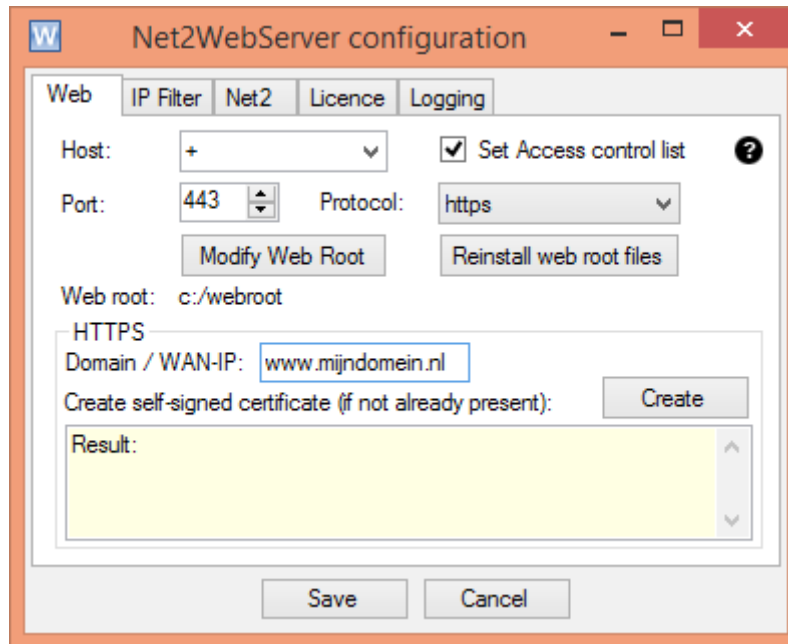
☑ Right-click on the icon of the Net2WebServer manager and select item 'Configure'.

☑ Select the tab page 'Web' and select 'https' as the desired protocol. The port number will automatically switch to 443 which is the standard HTTPS port.

☑ Supply the domain name or the (WAN)-IP address for which the certificate will be created.

☑ Press 'Create'.

The Net2WebServer manager will now go through all steps necessary to setup the right infrastructure. The result of all distinct steps will be shown in the (yellow) text-box.
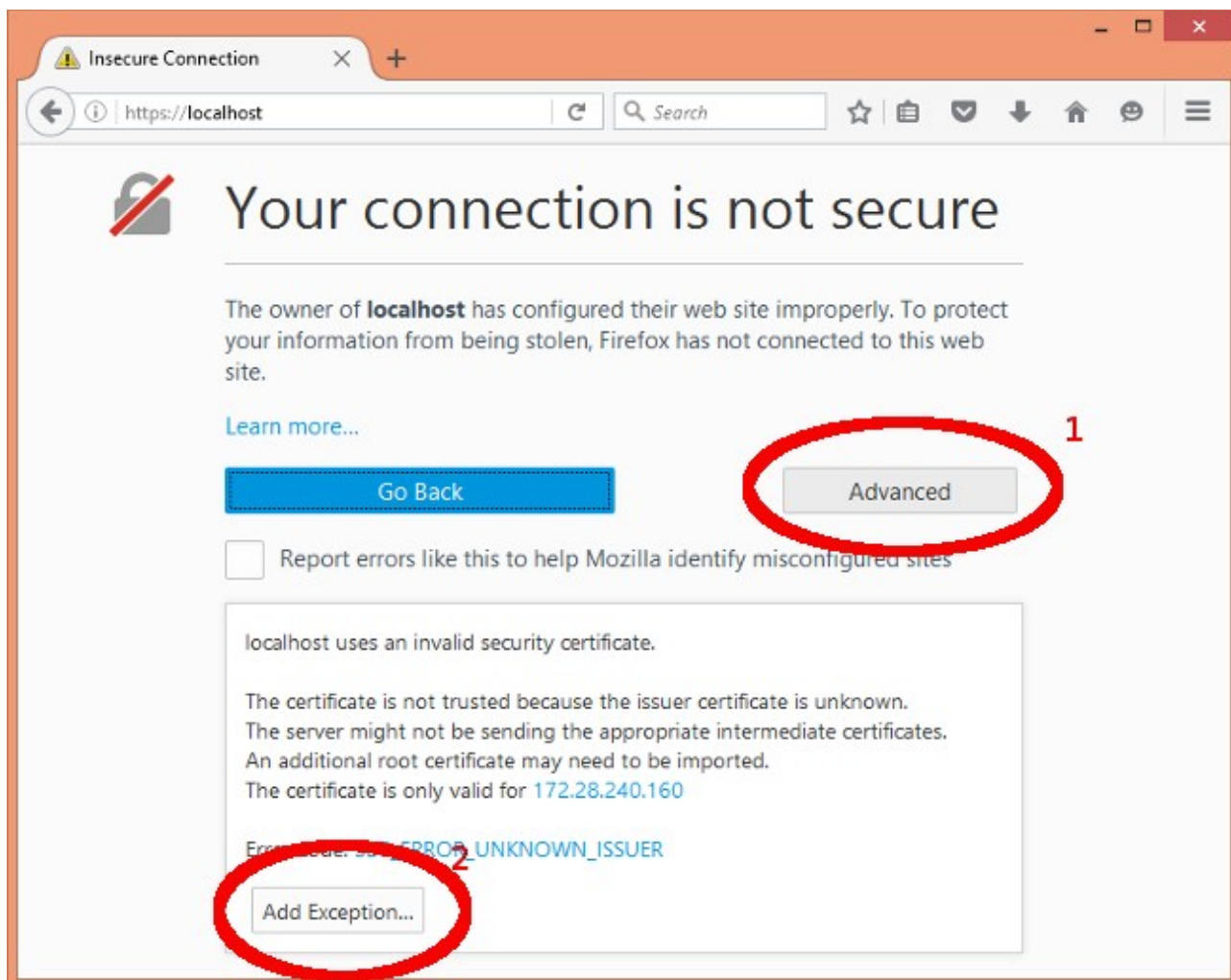
In case earlier created certificates are found you'll be questioned about what to do with these certificates.

When all steps are performed successfully the Net2WebServer needs to be restarted.

Setting up your browser to accept Self-signed certificates

Firefox

Go through the following steps to let Firefox accept a self-signed certificate permanently.

☑ Start Firefox on the same machine as on which the Net2WebServer is running and type: "https://localhost/" on the URL bar. Replace 'localhost' by the IP-number of the machine on which the Net2WebServer is running in case you started Firefox from a different machine.

Firefox will now respond with a message stating that the connection is not secure.
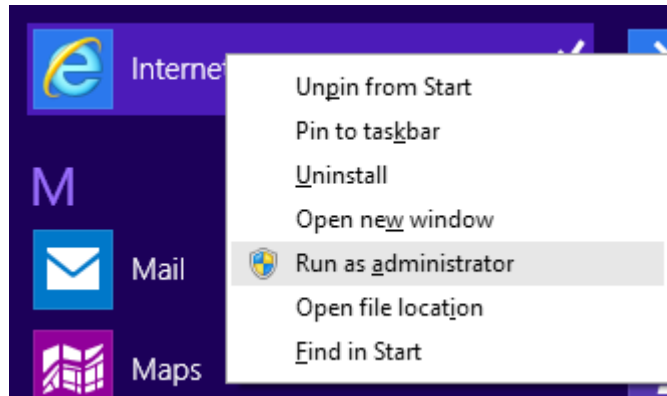
☑ Click: "Advanced".

A new message will be added now.

☑ Click: "Add Exception"

☑ Press 'Add Exception'.
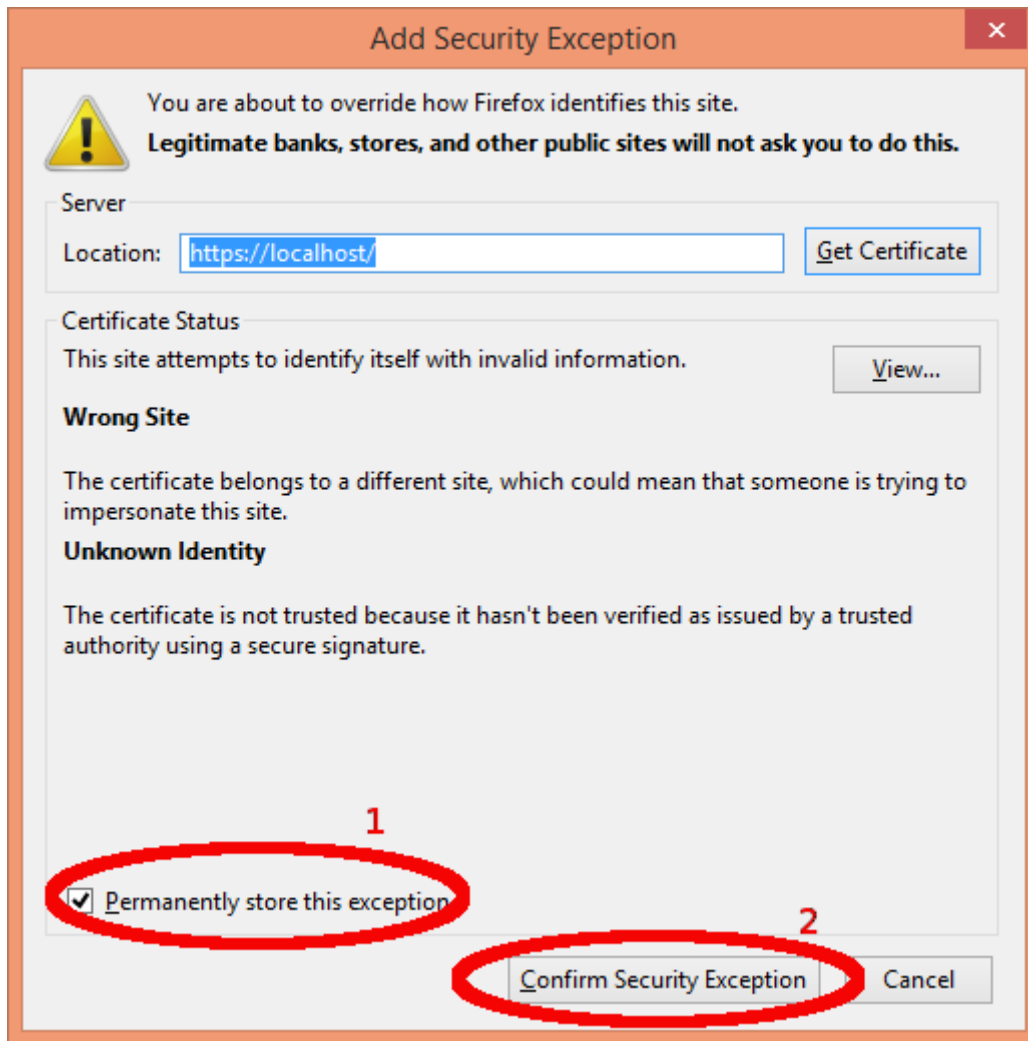
☑ Make sure the tick-box: 'Permanently store this exception' is checked,

☑ Press the button 'Confirm security Exception'.

These steps needs to be repeated on every machine from which you want to make contact with the Net2WebServer only once.

Internet Explorer

☑ Start Internet Explorer with Administrator rights.

☑ If you are on the same machine as which the Net2WebServer is running type: https://localhost in the URL bar. Replace 'localhost' by the IP-number of the machine on which the Net2WebServer is running in case you started Internet Explorer from a different machine.
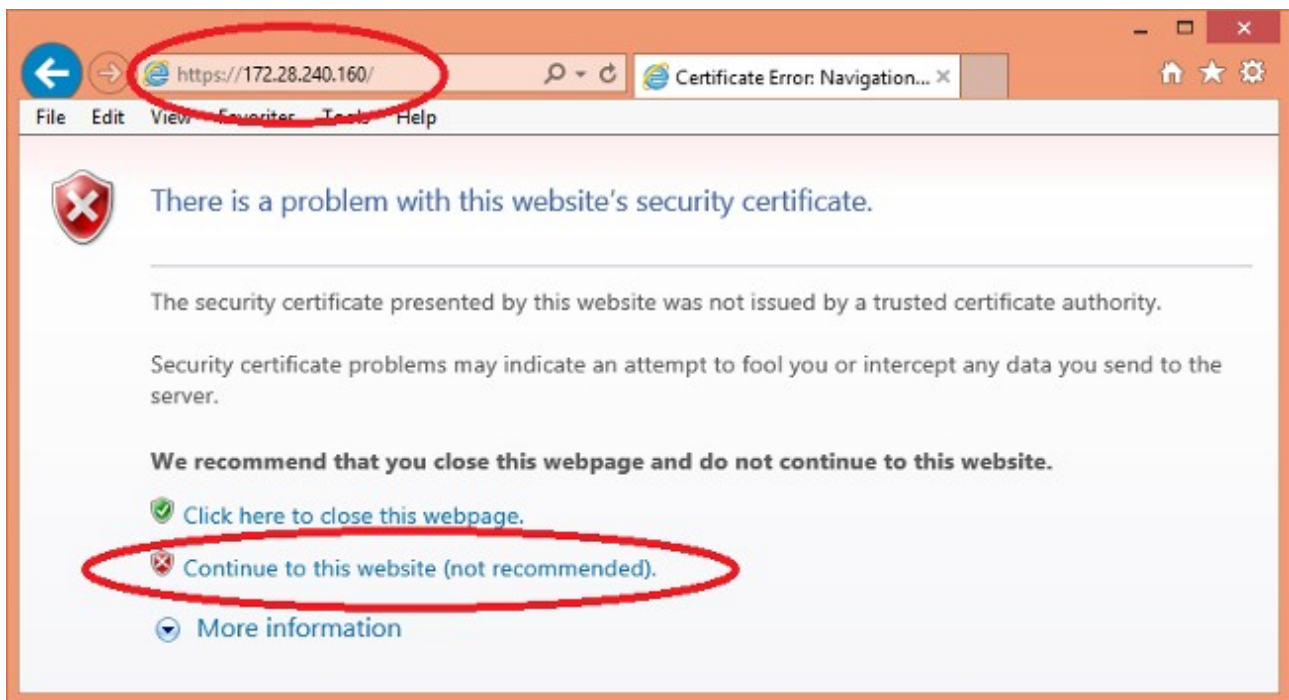
Internet Explorer will respond with a warning about the website's security certificate.
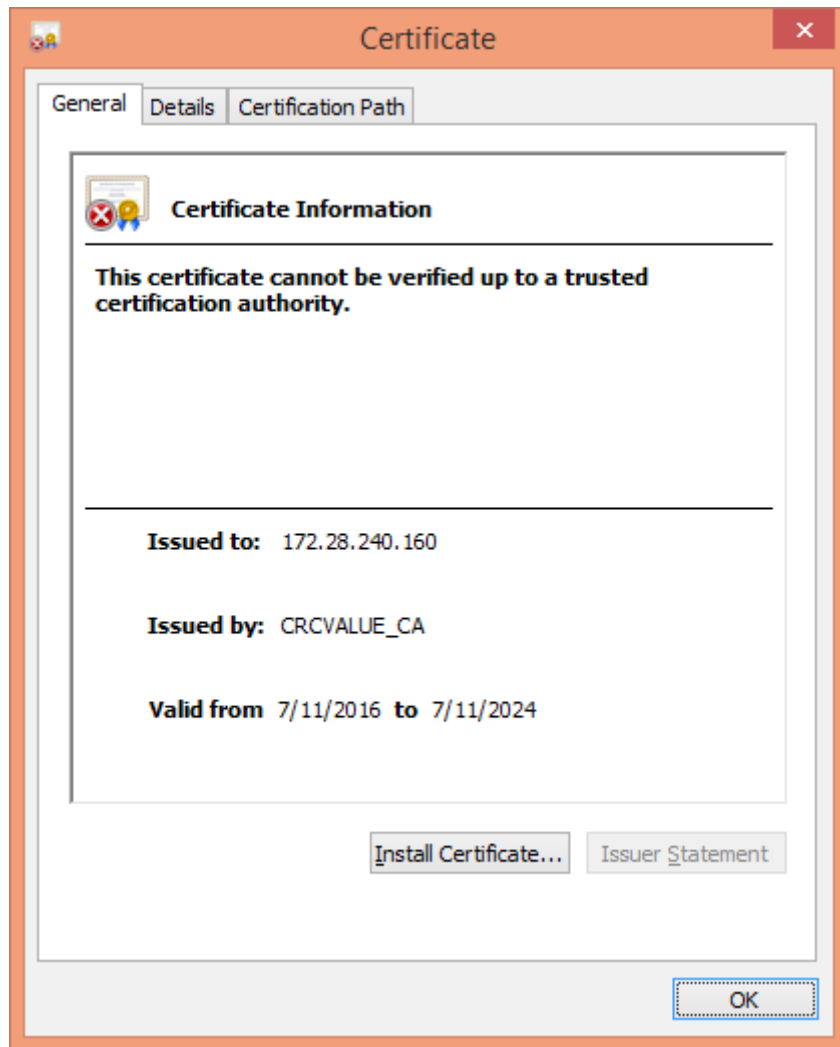
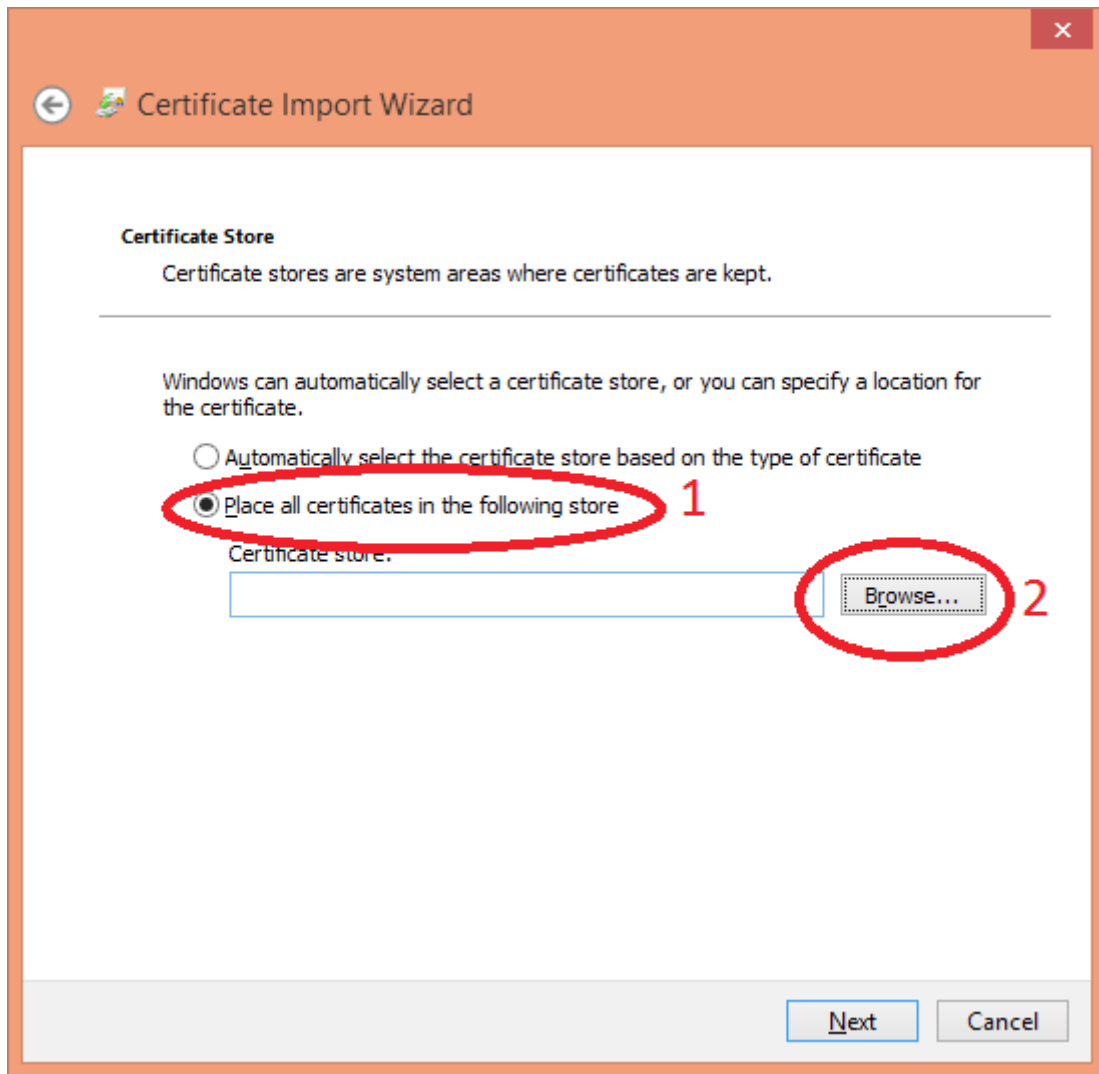☑ Click on 'Continue to this website (not recommended)'.
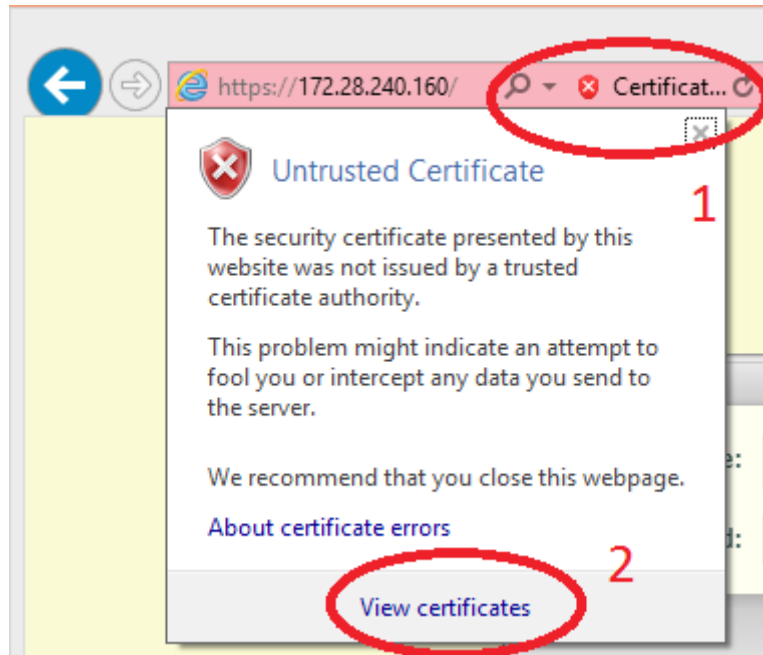
The program will now start and a message about a 'Certificate Error' will be visible in the URL bar.

☑ Click on that message. (1) A new window will now open.

☑ Click on 'View certificates' at the bottom of that window. (2)
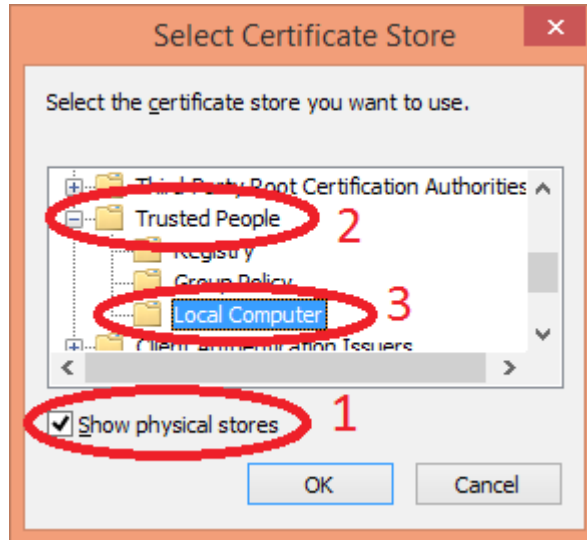
A new window will be opened.

☑ Click on 'Install Certificate...'.

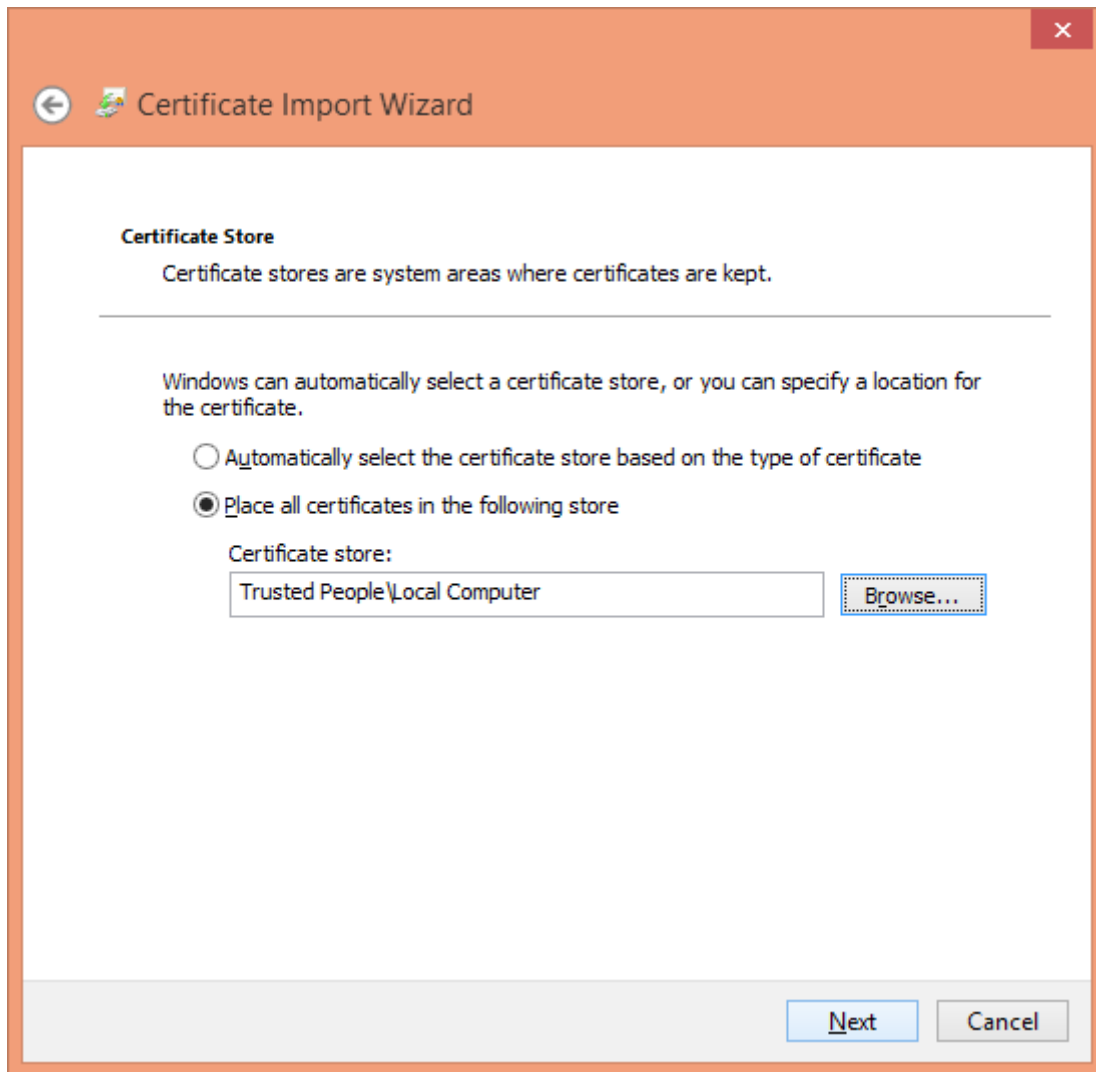This will start the 'Certificate Import Wizard'.

☑ Click 'Place all certificates in the following store' (1).

☑ Click 'Browse..' (2).

☑


☑   Click 'Show physical stores' (1).

☑   Select 'Trusted People' (2).

☑   Select 'Local Computer' (3).

And press OK.

Certificate Store
Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

◉ Place all certificates in the following store

Certificate store:

Trusted People\Local Computer   [Browse...]

[Next]   [Cancel]

IE will now show two more windows asking for confirmation.

Click 'Next'.
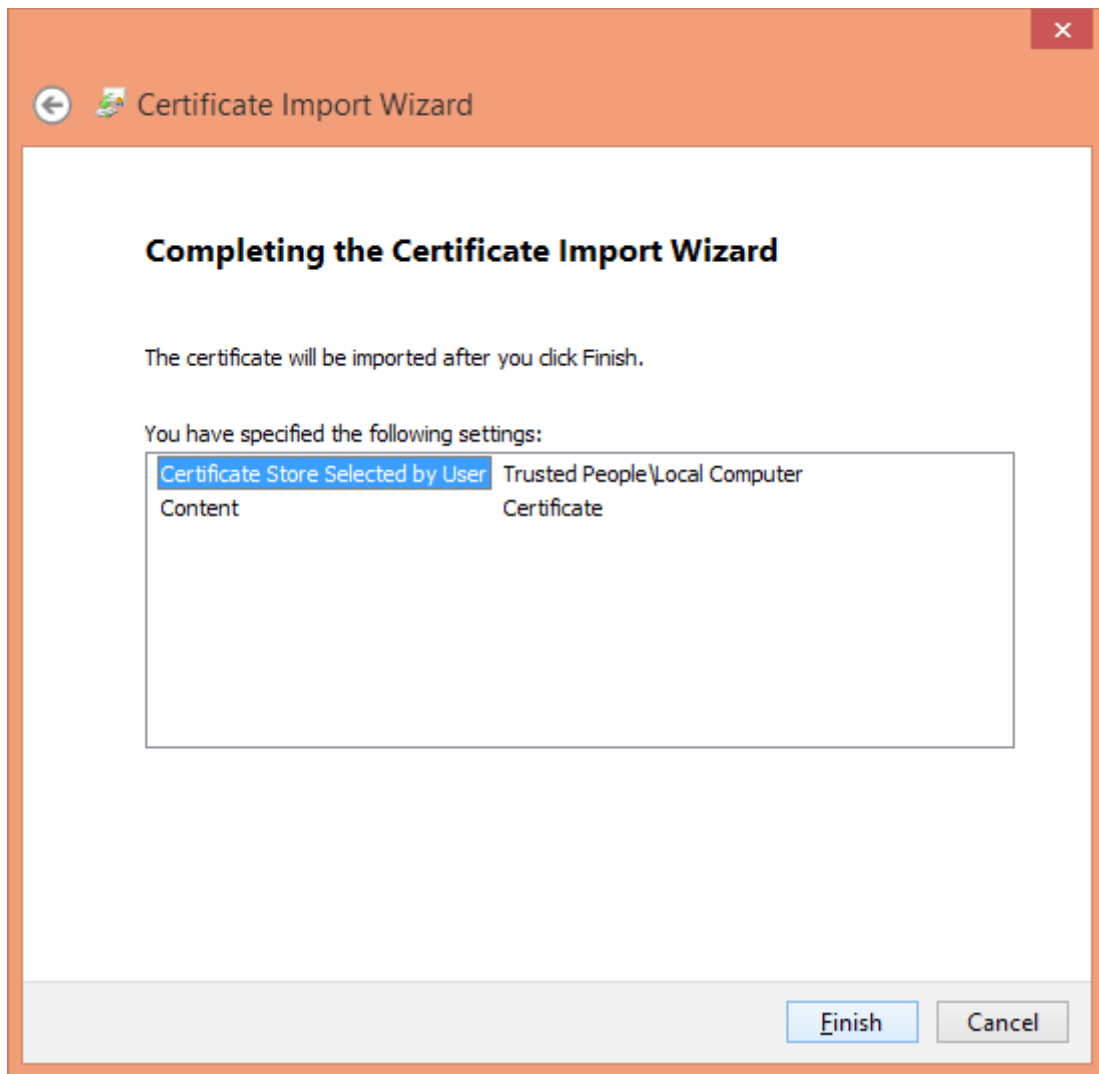
Click 'Finish'.

Internet Explorer will now accept this certificate in all future connections with the Net2WebServer.
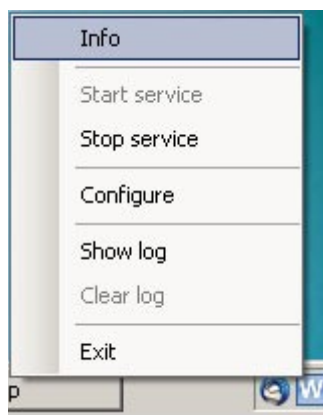
Licence

Trail period

An unlicensed version will be operational for 3 hours a day, starting from the first Net2WebServer request. After these 3 hours a message will be given at the client and the connection will closed. The Net2WebServer will become operational again for 3 hours the next day.
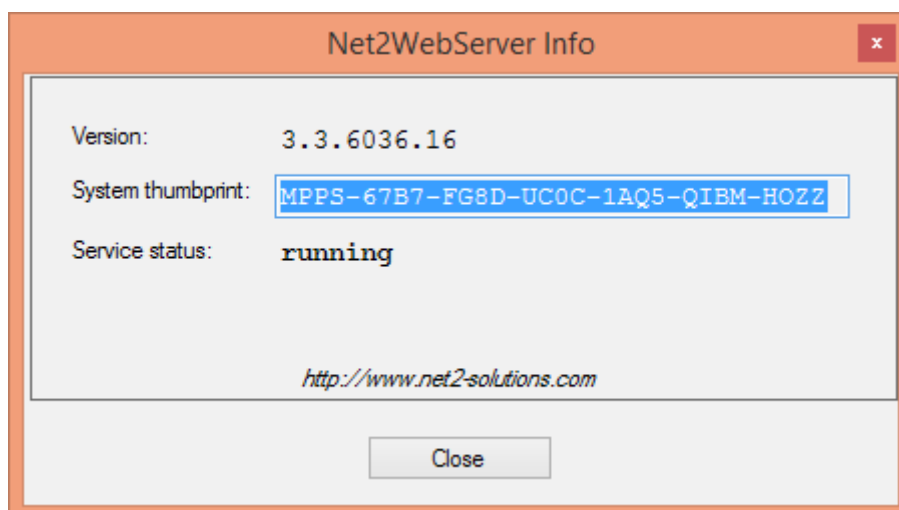
A licence will grant you the following:

• A licence key;

• Free updates, until the next major release;

• A year free technical support;

• Unlimited use.

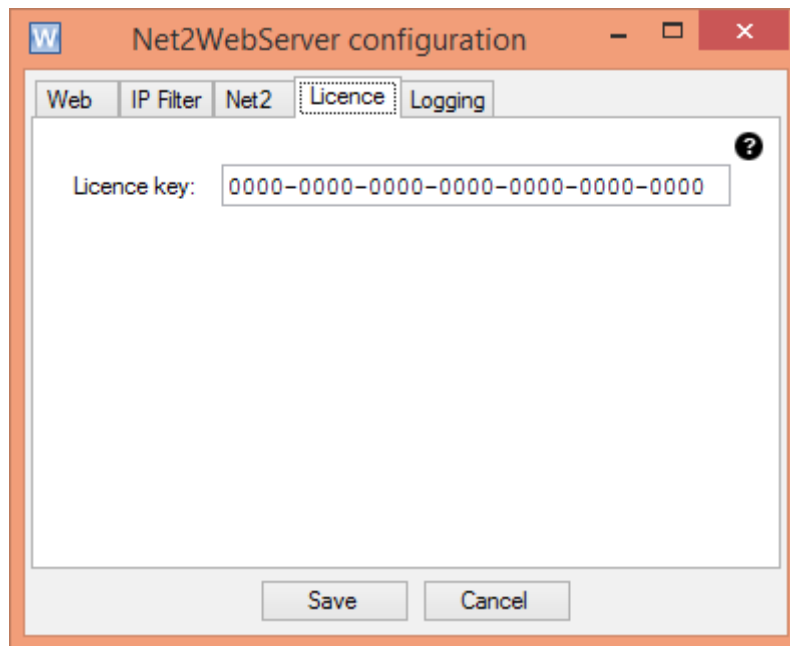### How do you get a licence

☑ Start the Net2WebServer manager

☑ Select menu item: 'info'.

☑ Note down the 'System thumbprint'. It is a requirement that this 'thumbprint' originates from the machine for which a licence is requested.

☑ Email this System Thumbprint to info@net2-solutions.com together with your name and address info.

☑ Transfer the right amount.

As soon as the payment is confirmed we will send you an licence key which can be entered at the tab page 'Licence' of the Net2WebServer manager.

Don't forget to restart the Net2WebServer once the new licence is entered.!