Aquaforest

Searchlight
Troubleshooting Guide

Aquaforest

Making Content Findable

Searchlight
Troubleshooting Guide

Version 2.1
May 2021

© Aquaforest Ltd 2001 - 2021

Content

1 INTRODUCTION 3

1.1 Installation 3

2 POST INSTALLATION 3

2.1 SharePoint URL format 3

2.2 Running the Diagnostic Tool 4

2.3 Long Path Support 5

2.4 Empty drop down lists 6

2.5 Certificate Error 9

2.5.1 Retrieving certificate thumbprint/fingerprint 9

2.6 HTTP Error 500.19 – Internal Server Error 14

1 Introduction

This brief guide is intended to summarize the most common configuration issues that can affect the operation of Aquaforest Searchlight version 2.x. The Release Notes has more information on more specific errors. You can also check Searchlight blogs for even more information.

1.1 Installation

The installation process is relatively straight forward by following the steps on the GUI. The installation should be carried out whilst being logged in as a System Administrator. In cases where the logged-on user does not have full admin privileges some components will fail to install.

A recommend approach is to run the Aquaforest_searchlight.msi through the command prompt. You will need to open an instance of command prompt with the 'Run as Administrator' option.

2 Post Installation

2.1 SharePoint URL format

Below is an example of how to set the SharePoint URL format when setting up a document library in Searchlight.

Sharepoint 2010:

- Actual URL:
  https://SharePoint2010/site/myLibrary/myForms/AllItems.aspx

- Supported URL format in Searchlight:
  https://SharePoint2010/site/myLibrary

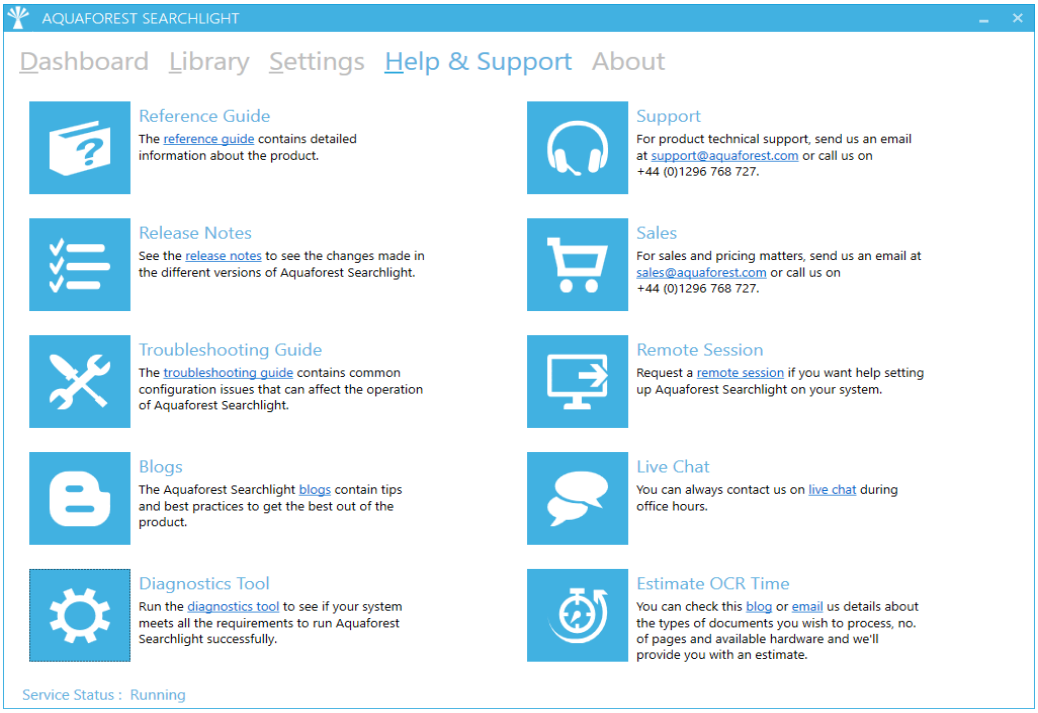
SharePoint 2013:

- Actual URL:
  https://SharePoint2013/site/Library/_layouts/15/start.aspx#/mylibrary/Forms/AllItems.apsx

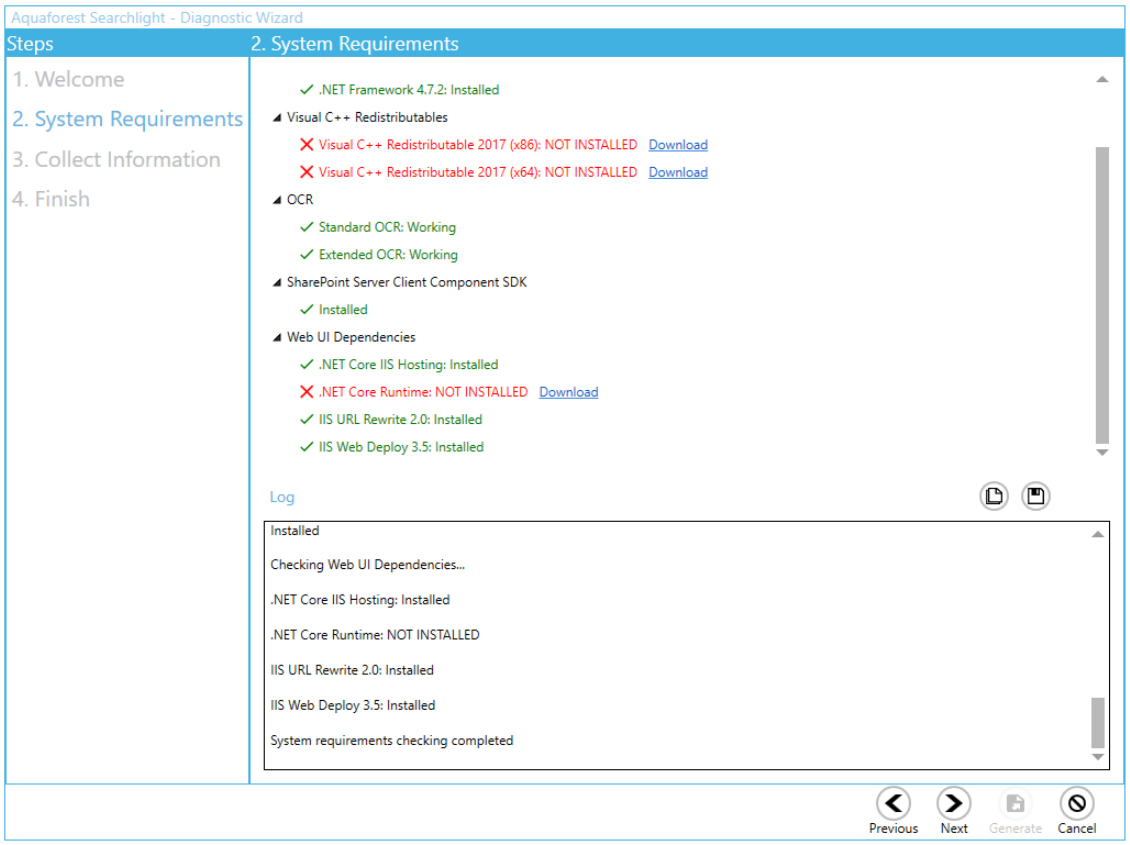
- Supported URL format in Searchlight:
  https://SharePoint2013/site/Library/mylibrary

2.2 Running the Diagnostic Tool

Once installed you can run the **Diagnostic Tool** which can be accessed from the **Help & Support** tab on the main screen.



This will initiate the diagnostic wizard which will run various checks to determine if your system meets all the requirements needed to run Searchlight. If there are dependencies that are not installed, download them using the link in the diagnostic tool and install them. If you notice any failures during the run contact the support team.

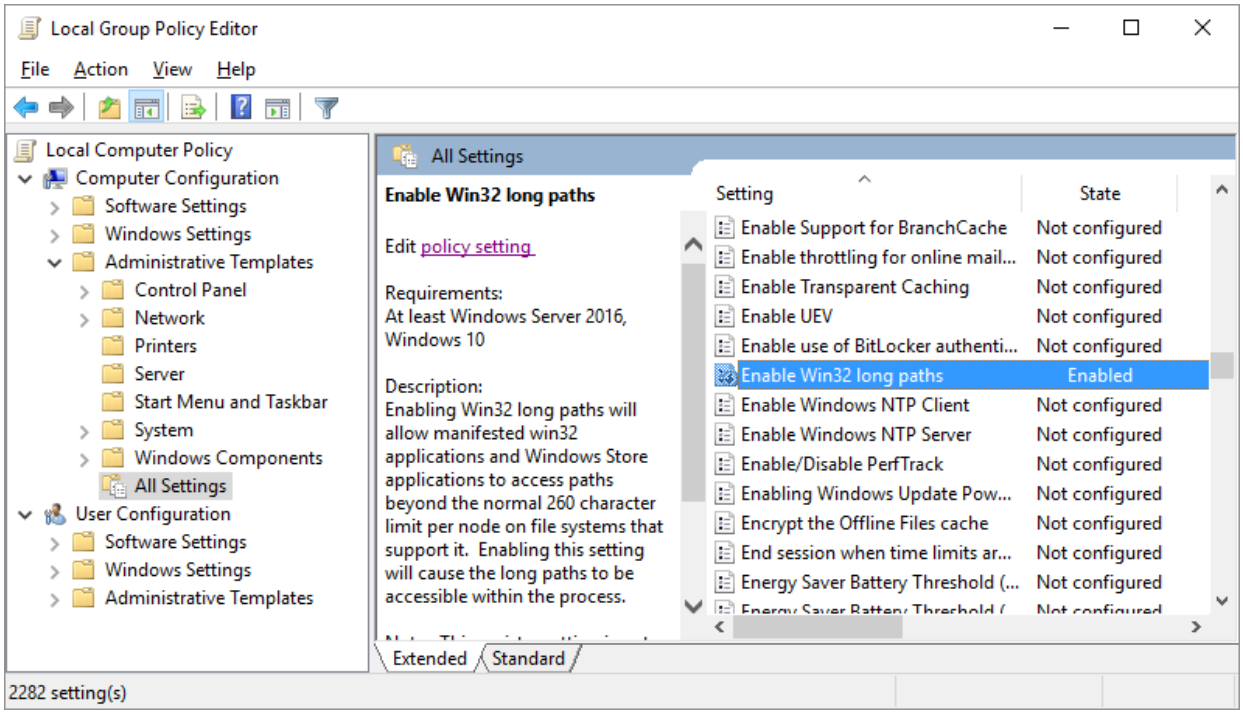


2.3 Long Path Support

When enumerating documents to process, Searchlight can come across documents that exceed the file path length enforced by windows. These files are skipped and not processed.

Starting from Windows 10 and Windows Server 2016, there is now support for long paths. However, long paths support is not enabled by default. You need enable the following policy to take advantage of this new feature.

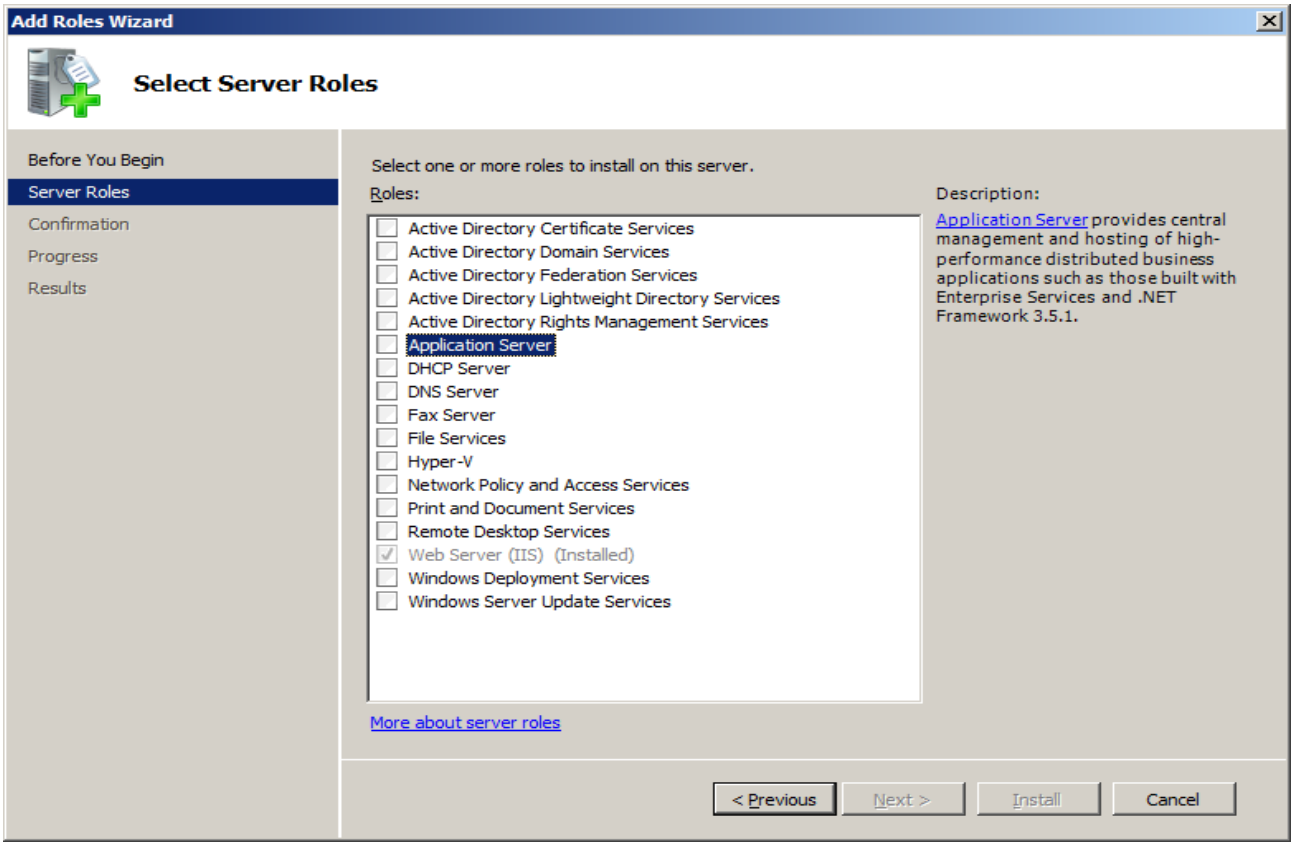
Open Global Policy Editor (**Start > Run > gpedit.msc**) and enable "**Enable Win32 long paths**".

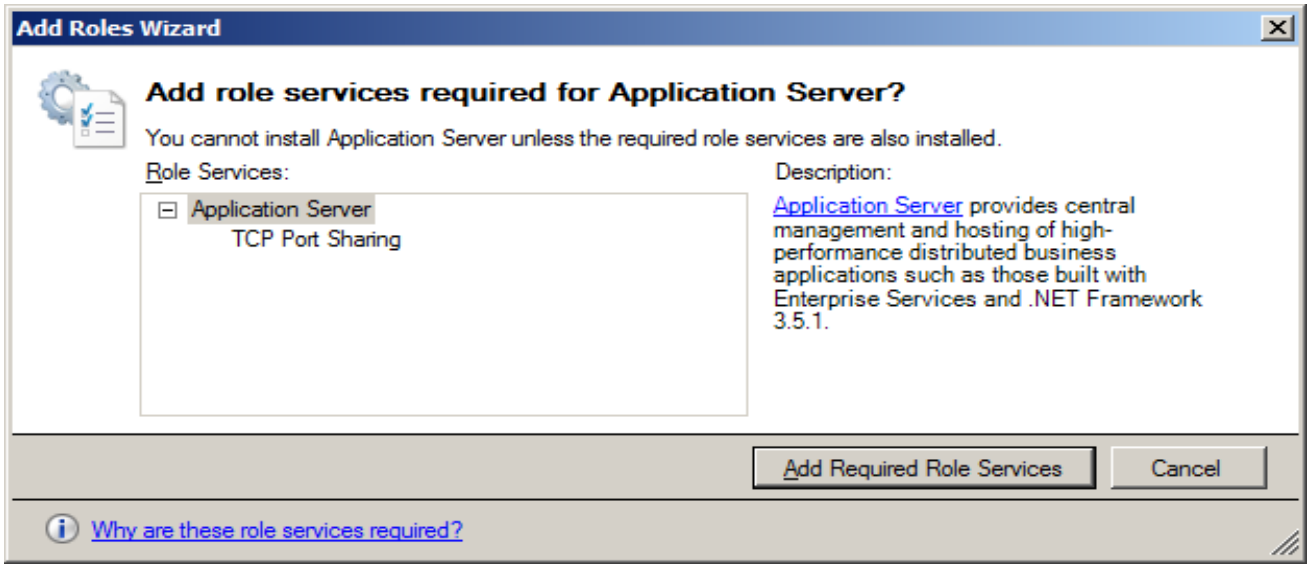


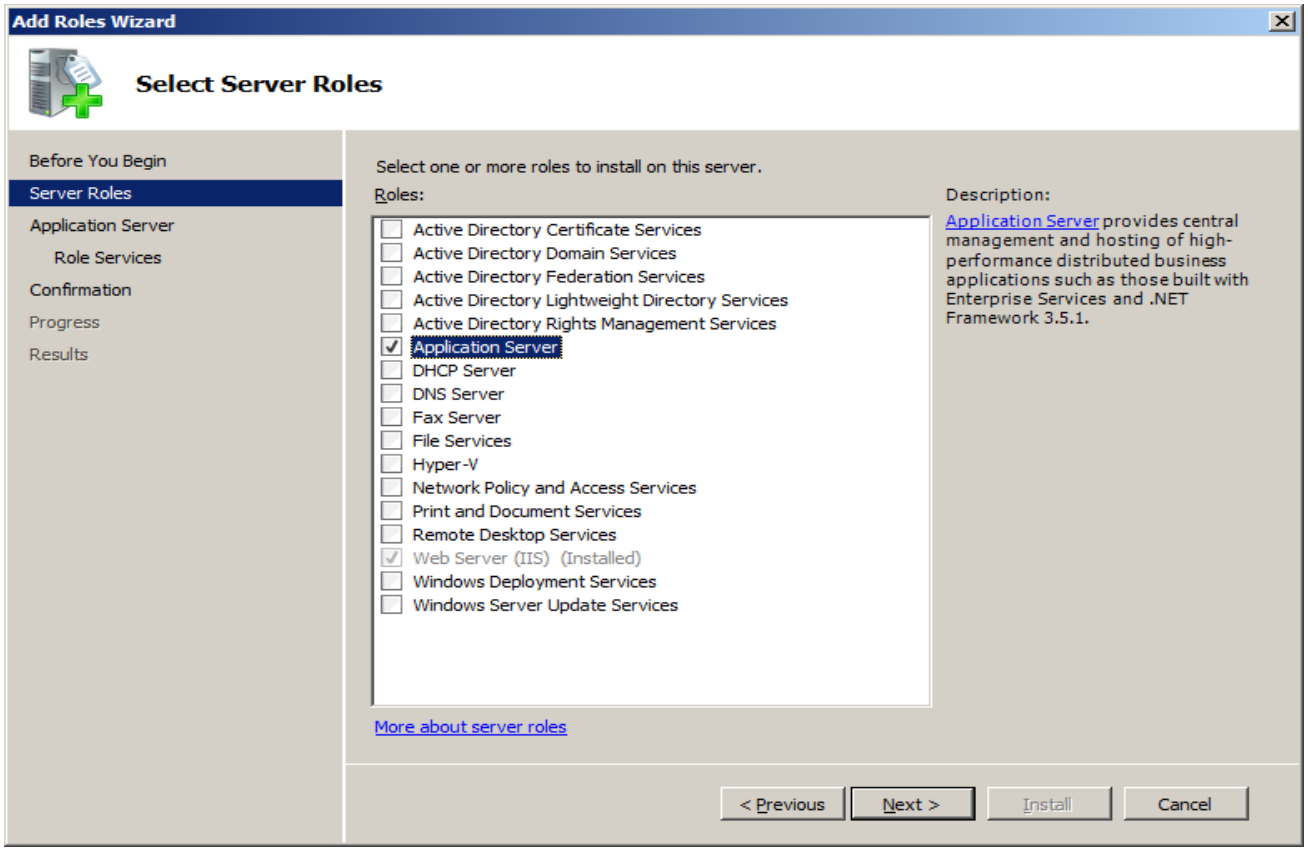
Restart the Searchlight UI and service after making changes to this policy.

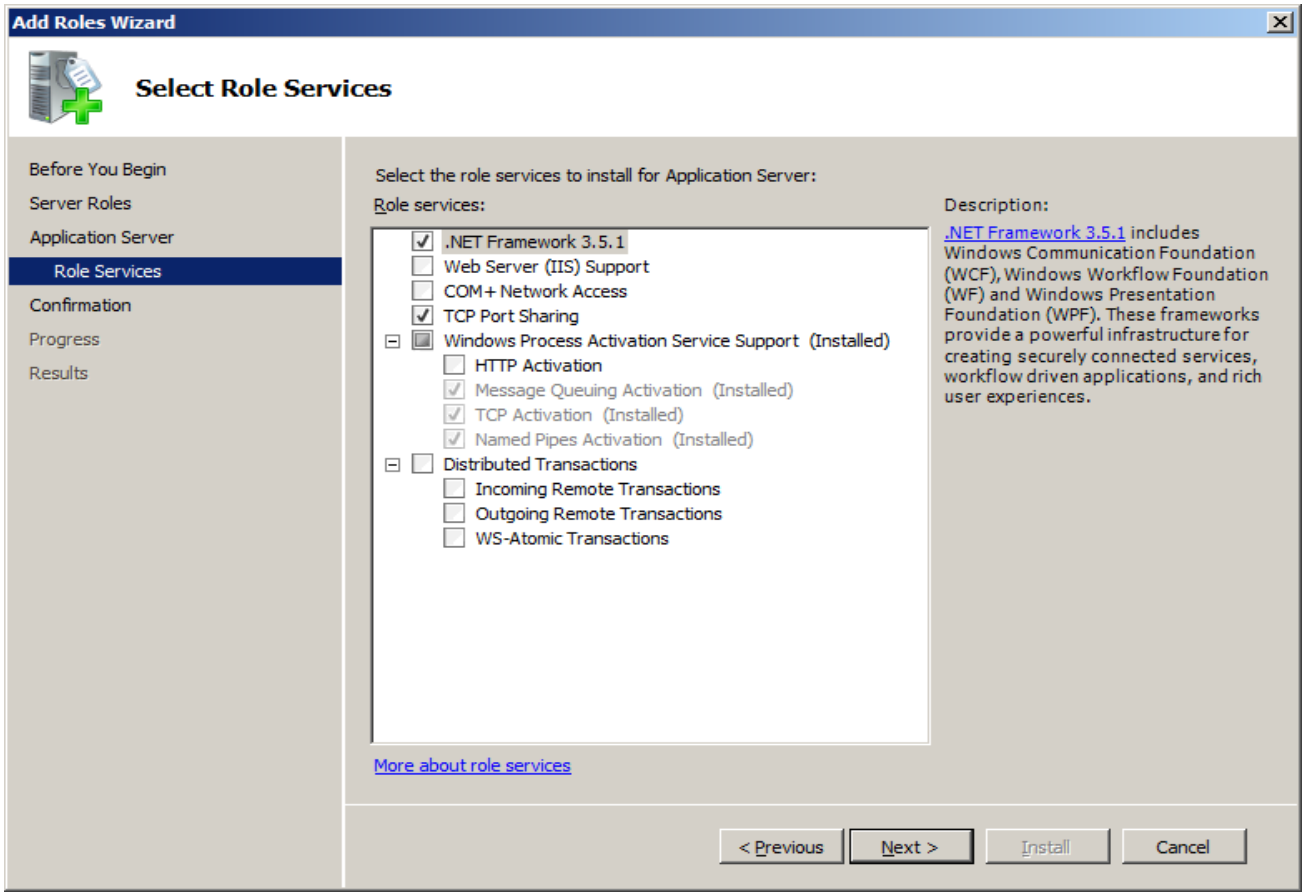
2.4 Empty drop down lists

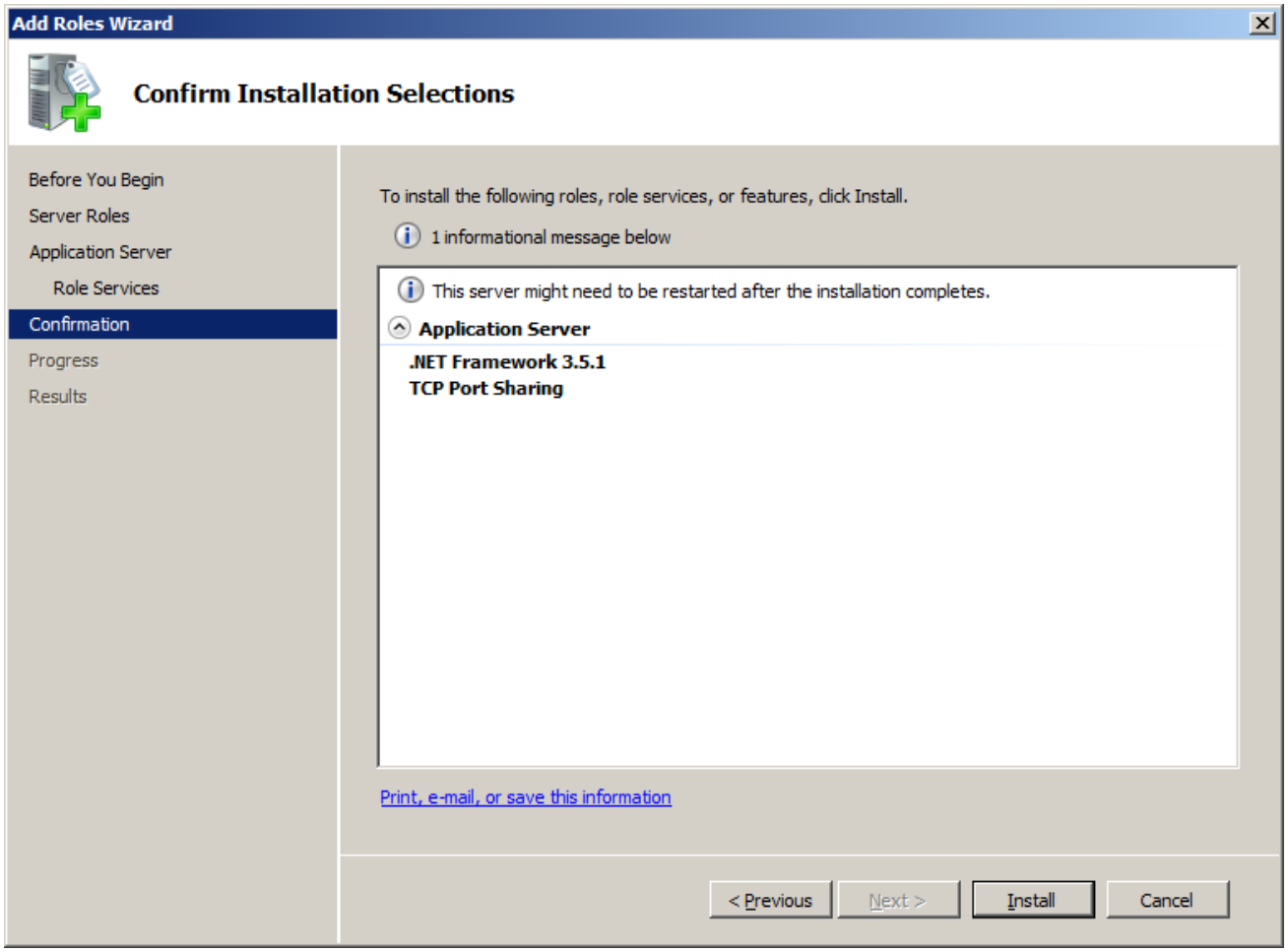
This is a symptom seen on Windows Server 2008 and Windows Server 2012. If you experience the dropdown lists being empty within Aquaforest Searchlight and are using one of the above operating system, then you will need to enable the "Application Server" Role. The following screenshots illustrate how to enable the "Application Server" Role:






Add Roles Wizard
Select Server Roles
Before You Begin
Server Roles
Application Server
Role Services
Confirmation
Progress
Results
Select one or more roles to install on this server.
Roles:
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Application Server
DHCP Server
DNS Server
Fax Server
File Services
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Desktop Services
Web Server (IIS) (Installed)
Windows Deployment Services
Windows Server Update Services
Description:
Application Server provides central management and hosting of high-performance distributed business applications such as those built with Enterprise Services and .NET Framework 3.5.1.
More about server roles
< Previous
Next >
Install
Cancel


Add Roles Wizard
Select Role Services
Before You Begin
Server Roles
Application Server
Role Services
Confirmation
Progress
Results
Select the role services to install for Application Server:
Role services:
.NET Framework 3.5.1
Web Server (IIS) Support
COM+ Network Access
TCP Port Sharing
Windows Process Activation Service Support (Installed)
HTTP Activation
Message Queuing Activation (Installed)
TCP Activation (Installed)
Named Pipes Activation (Installed)
Distributed Transactions
Incoming Remote Transactions
Outgoing Remote Transactions
WS-Atomic Transactions
Description:
.NET Framework 3.5.1 includes Windows Communication Foundation (WCF), Windows Workflow Foundation (WF) and Windows Presentation Foundation (WPF). These frameworks provide a powerful infrastructure for creating securely connected services, workflow driven applications, and rich user experiences.
More about role services
< Previous
Next >
Install
Cancel


Add Roles Wizard
Confirm Installation Selections
Before You Begin
Server Roles
Application Server
Role Services
Confirmation
Progress
Results
To install the following roles, role services, or features, click Install.
1 informational message below
This server might need to be restarted after the installation completes.
Application Server
.NET Framework 3.5.1
TCP Port Sharing
Print, e-mail, or save this information
< Previous
Next >
Install
Cancel

2.5 Certificate Error

If Searchlight tries to access a site that has an invalid SSL certificate, it will fail with an error message like "*Could not establish trust relationship for the SSL/TLS secure channel.*"

There are 2 settings in the **Searchlight.config** file that can be used to fix this.

```
<!--
To enable Searchlight to process sites that have invalid certificates or certificates with errors,
enter a comma separated list of all thumbprints of certificates that you recognize
in the setting below to make Searchlight ignore them and continue processing. Alternatively, set
"ignoreAllCertificateErrors" to "true" (use at your own risk!).
-->
<add key="recognizedCertificateThumbprints" value="" />
<add key="ignoreAllCertificateErrors" value="false" />
```

- **recognizedCertificateThumbprints**

  Use this setting to add the thumbprint/fingerprint (SHA-1) of the certificate that is causing the issue. More thumbprints can be added by separating each one with a comma. This is recommended way as it instructs Searchlight to only ignore errors of recognized certificates.

  See how to retrieve the thumbprint or fingerprint of the invalid certificate using Chrome, Firefox and Edge web browser below.

- **ignoreAllCertificateErrors**

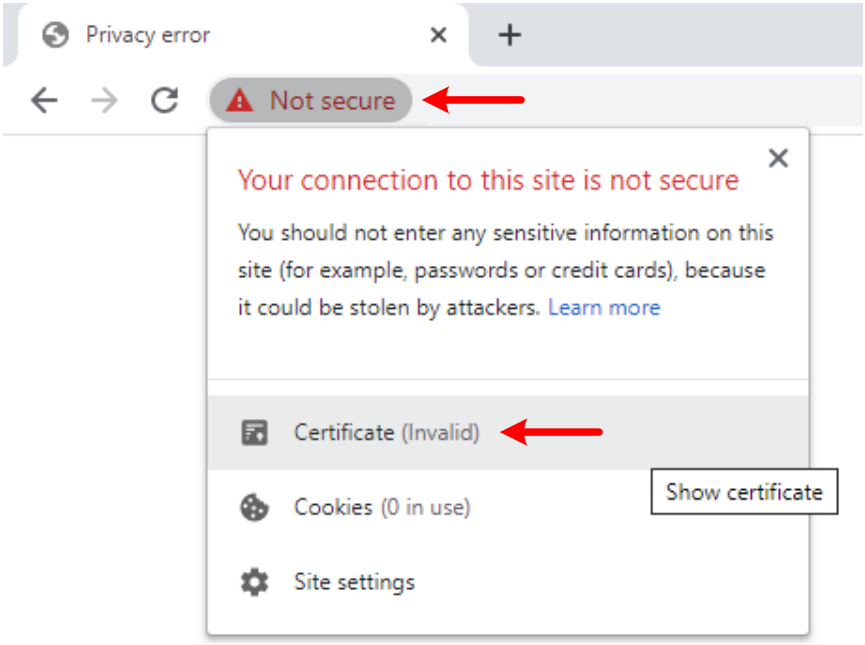
  Set this setting to true to ignore all errors for all certificates.

NOTE: The Searchlight UI and service must be restarted after making the change.

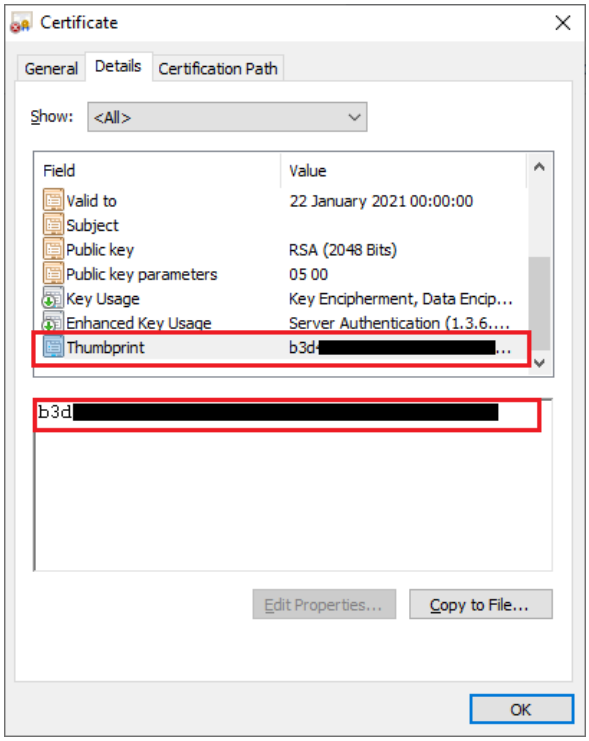
2.5.1 Retrieving certificate thumbprint/fingerprint

To retrieve a site's certificate's thumbprint, first open the site in a web browser. If the certificate is invalid, a warning will be shown in the address bar.

- **Chrome**

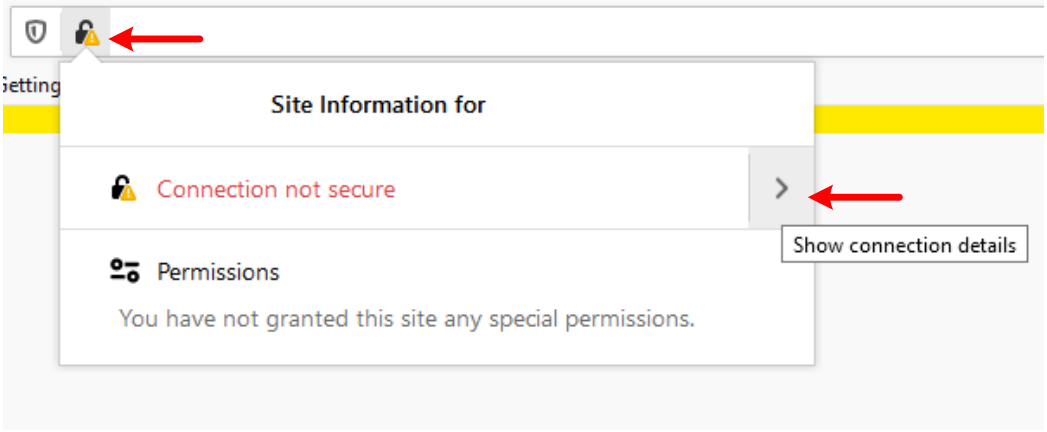


1. Click on **Not secure** > **Certificate (Invalid)**
2. A popup window will appear

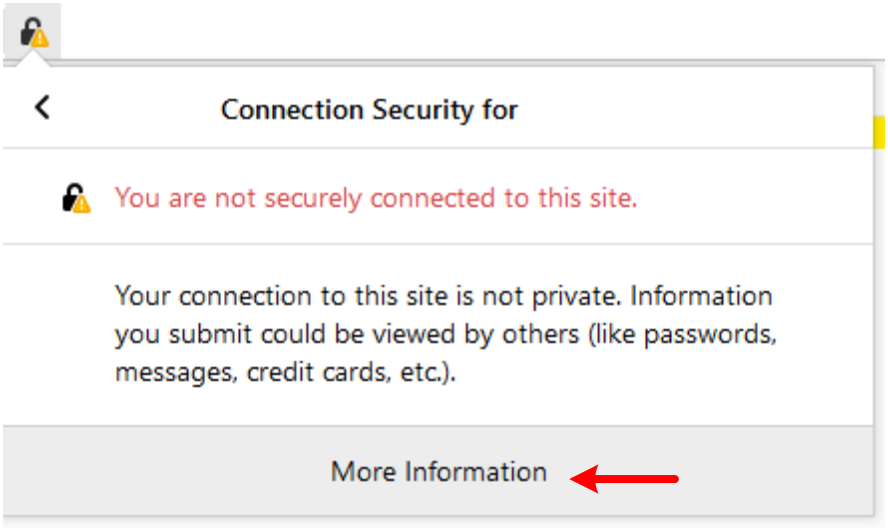


3. On the **Details** tab, select **Thumbprint** and copy the value in the **recognizedCertificateThumbprints** setting in **Searchlight.config**.

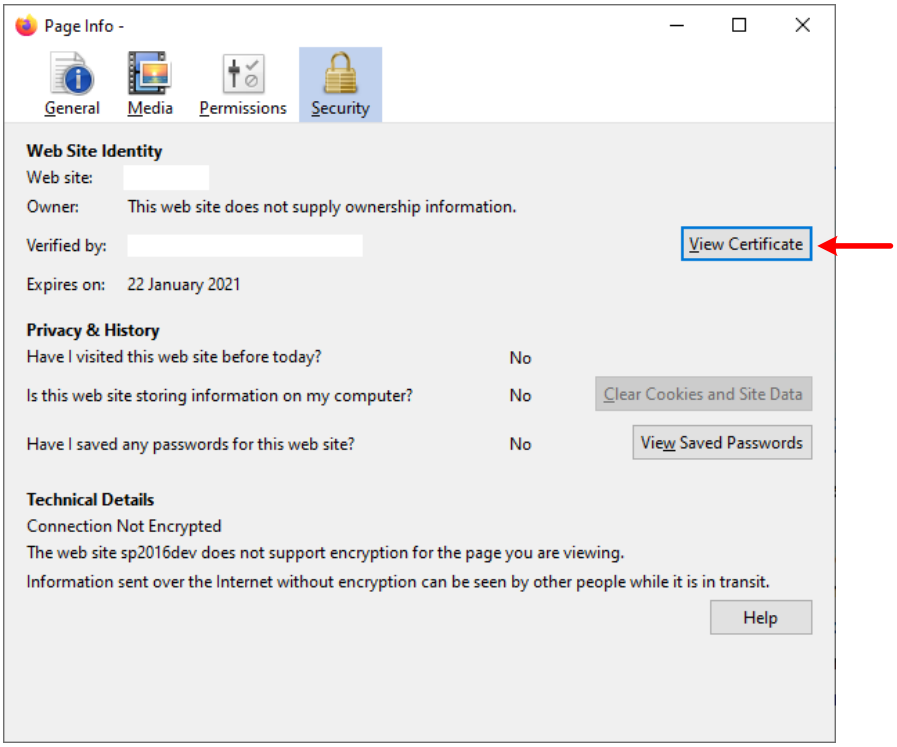
- **Firefox**



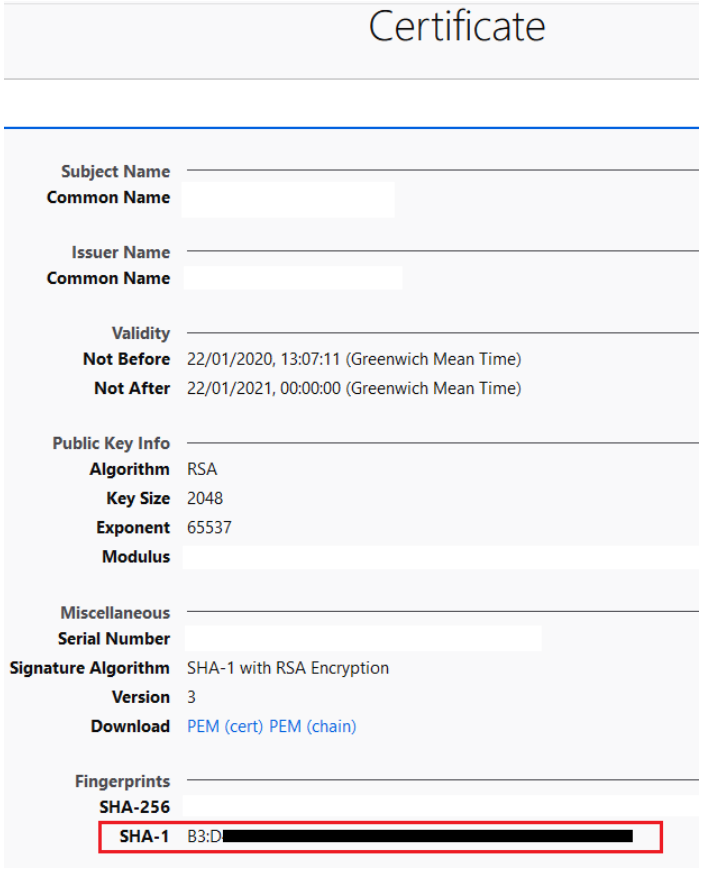
1. Click on the padlock icon with an exclamation mark
2. Click on the arrow new to **Connection not secure**
3. A new popup will be shown. Click on **More Information**



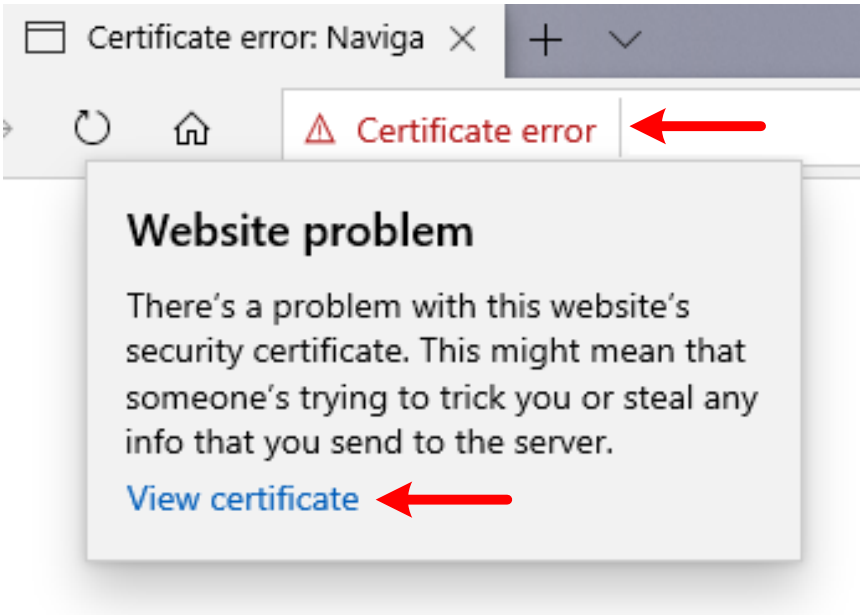
4. In the new popup window, under **Security**, select **View Certificate**



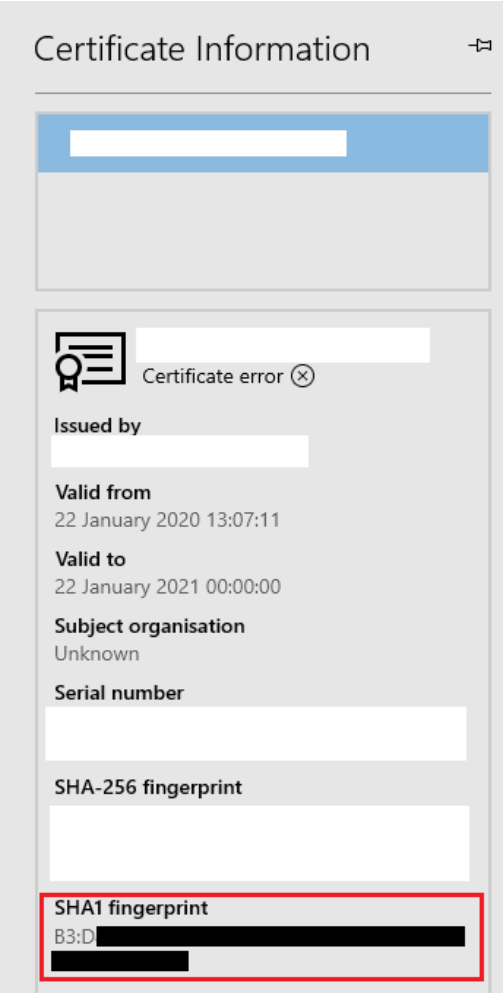
5. Copy the value of **SHA-1** under **Fingerprints** and paste it in the **recognizedCertificateThumbprints** setting



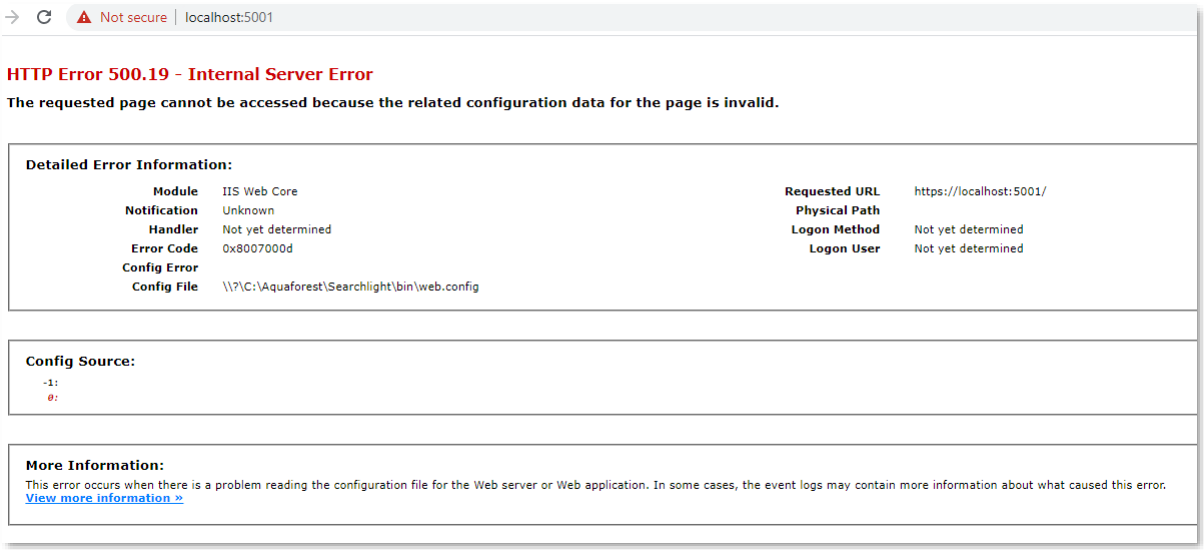
- **Edge**



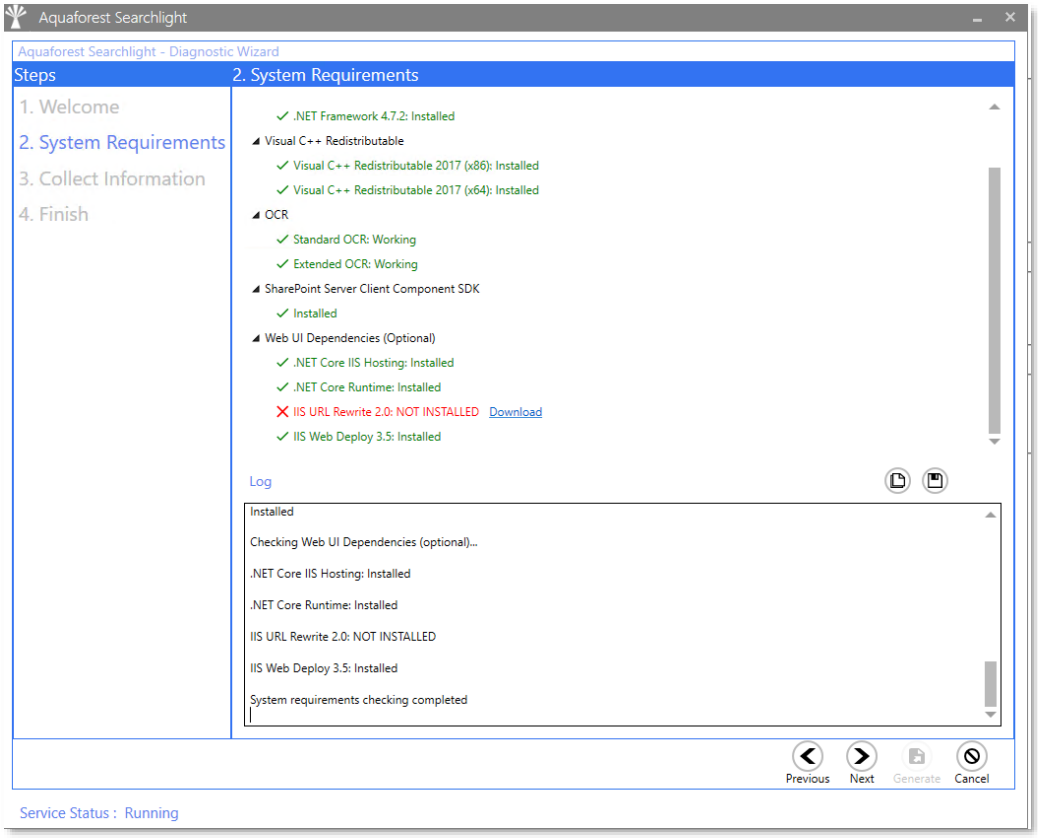
1. Click on **Certificate error** > **View certificate**
2. In the popup window, copy the value of **SHA1 fingerprint** and paste it in the **recognizedCertificateThumbprints** setting.


Certificate Information
Certificate error
Issued by
Valid from
22 January 2020 13:07:11
Valid to
22 January 2021 00:00:00
Subject organisation
Unknown
Serial number
SHA-256 fingerprint
SHA1 fingerprint
B3:D

2.6 HTTP Error 500.19 – Internal Server Error



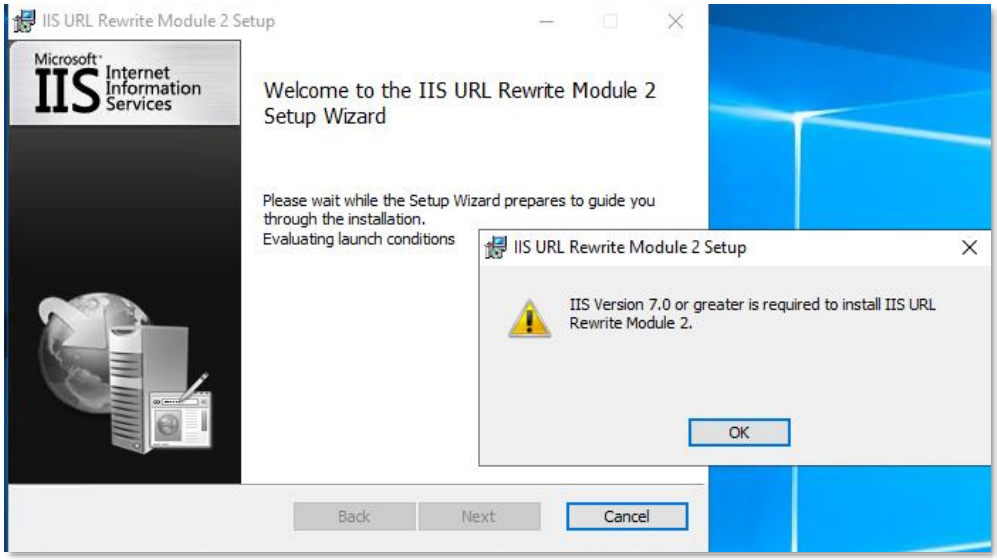
The cause of this error can be found by running the **Diagnostic Tool**



As shown above, the **URL Rewrite module** is not installed. This is required if you use the web interface.

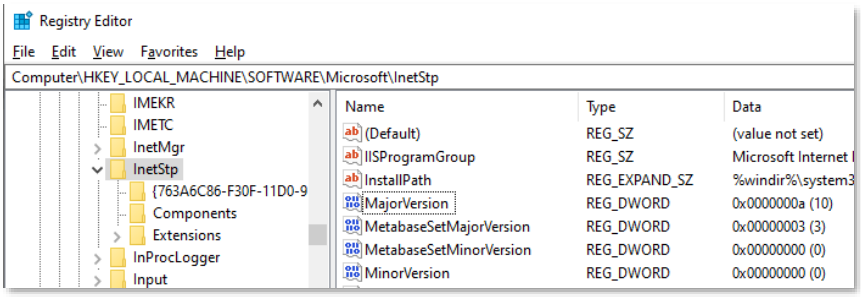
Download and install it.

You may encounter the following error when installing the URL Rewrite module “IIS Version 7.0 or greater is required to install IIS URL Rewrite Module 2”:

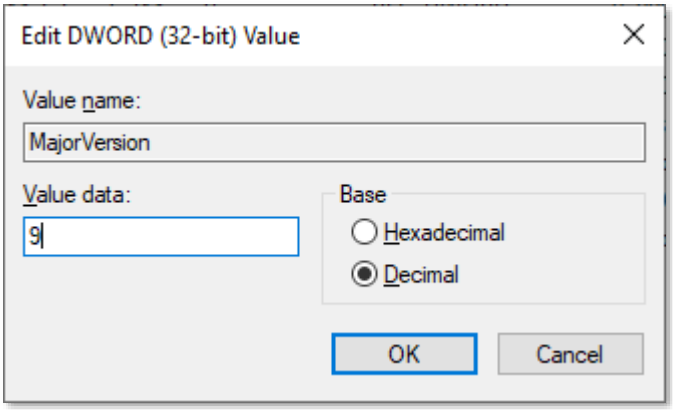


To fix this:

1. Open Registry Editor (Regedit)
2. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\InetStp**



3. Modify the **MajorVersion** and set the **Decimal** value to **9**



4. Install the URL Rewrite Module
5. Go back to the registry editor and change the **MajorVersion** back to **Decimal** value of **10**