User Guide

Endpoint Manager

1.0

User Guide – Endpoint Manager 1.0
Updated 27 May 2022

Contents

Introduction

Endpoint Manager is part of the Universal Search System.

Before using the Endpoint Manager, it is necessary to set up the Universal Search Server on a Windows Server using Microsoft Internet Information Services (IIS) and create indexes using dtSearch Desktop or the Database Indexer or 365 Indexer add-on products.

Normally Universal Search Clients connect to an endpoint via https, users are limited to what indexes they can search according to Active Directory (if used).

It is also possible for demonstration or test purposes to run a Universal Search Client and an Endpoint Manager on the same machine. This requires that Microsoft IIS is installed (e.g., Windows 10 Pro).

Install Universal Search

Follow these steps to install and configure Universal Search on Windows Server using Microsoft Internet Information Services (IIS).

Setup DNS Record for API

Create a new Domain Name Address (DNS) that points to your servers IP Address. This will be the address that search clients use to connect to the server e*.g., search.contoso.com*

Tip: Typically, this is achieved by using your hosting providers control panel to create an A-Name DNS record. Consult your website hosting provider if you do not know how to do this.

Ensure that TCP Port 80 and 443 are allowed inbound by your server's firewall.

Install Software

1. Extract UniversalSearch.zip on the server

Run the Universal Search msi file, it will extract the following files to the selected directory:

- • PDFHighlighterSetup.msi
- • EndpointManagerSetup.msi
- • Setup.exe

2. Run Setup.exe

The utility will check that necessary dependencies are installed and then install **PDF Highlighter** and **Endpoint Manager.**

Install any missing dependencies if prompted

Translation

The default language of the Endpoint Manager user interface is English. To translate the user interface, make a copy of the **EndpointManager – template.lang** file which is in the **\I18N** subfolder.

Place the untranslated copy of the template file in the same folder as the EndpointManager.exe file and run Endpoint Manager, you will see all the English text is replaced by pseudo-language with a width 30% wider than English to account for the typical expansion that occurs in translating from English to many other languages. Text Labels in Endpoint Manager will automatically expand to accommodate the length of the text.

Translate the appropriate text using a text editor (e.g., Notepad), save it in utf-8 format (we suggest you rename it using IETF language tags (e.g. **fr-CA.lang** for Canadian French) and place the file in the same folder as EndpointManager.exe.

If a file with filename extension **.lang** is found when Endpoint Manager is run, it will read the file to translate the user interface

Using Endpoint Manager

Before setting up an endpoint, create indexes using **dtSearch Desktop** and optionally the **Database Indexer** and/or **365 Indexer** add-ons. If using dtSearch Desktop use the Create Index (Advanced) option and select the options to **cache documents in the index** and **Cache text in the index.**

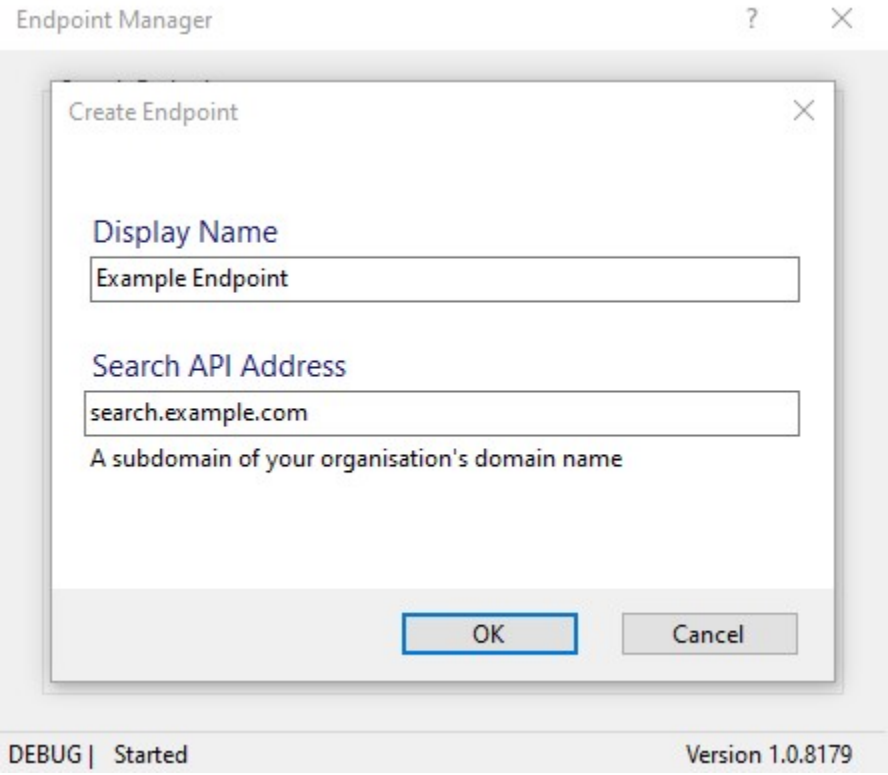
Use Endpoint Manager to create and manage the search endpoints.

Create new Endpoint

1. From the start menu, run **Universal Search Endpoint Manager**

2. Click ***New…***

3. Complete the steps:
a. Enter a ***Display Name***
Displayed to users connecting via Universal Search Client
b. Enter the ***Search API Address***
The DNS Address you configured earlier e.g., search.contoso.com
c. Click **OK**



Manage Endpoint

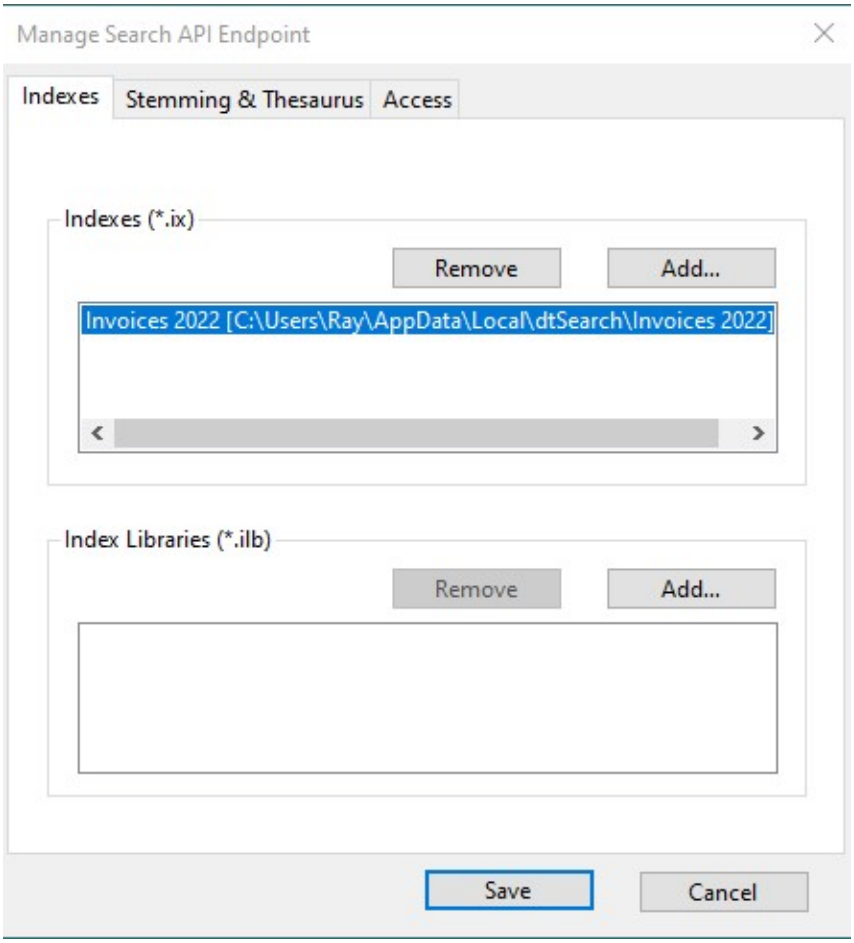
Use the **Manage Search API Endpoint** dialog to configure endpoint settings including Indexes, Stemming, Thesaurus and Access settings.

The dialog appears immediately after creating a new Endpoint, or when you select an existing endpoint and click the **Edit** button.

Indexes

Use the Indexes tab to add and remove dtSearch Indexes and Index Libraries to an Endpoint.

Indexes added are searchable to all users permitted by the *Access* tab.



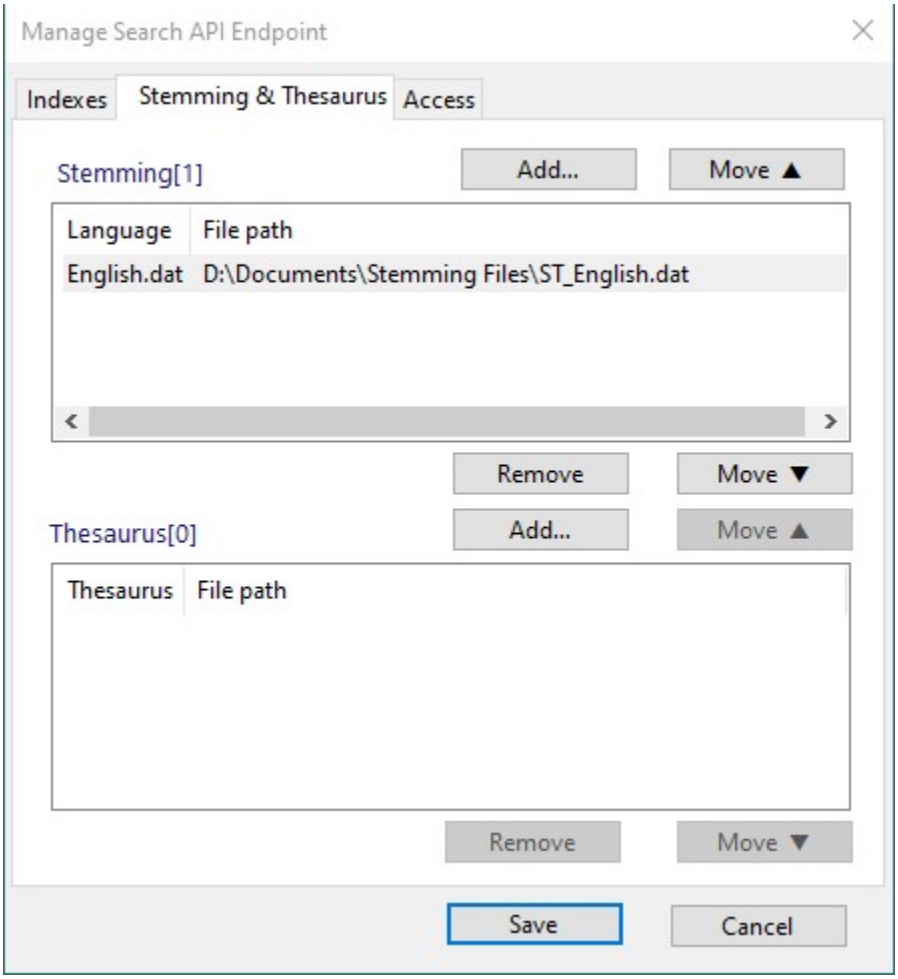
Use the **Stemming & Thesaurus** tab to add Stemming and Thesaurus files to your Endpoint

Stemming files

Add Stemming options to the Endpoint by adding Stemming files (*.dat)
Stemming is used to extend a search to cover grammatical variations of words.

Thesaurus files

Add Thesaurus options to the Endpoint by adding Thesaurus Files (*.xml)
Thesaurus files are used to add Synonym Search to an Endpoint.



Use User Thesaurus Plus to create and manage multiple Thesaurus files.

Access

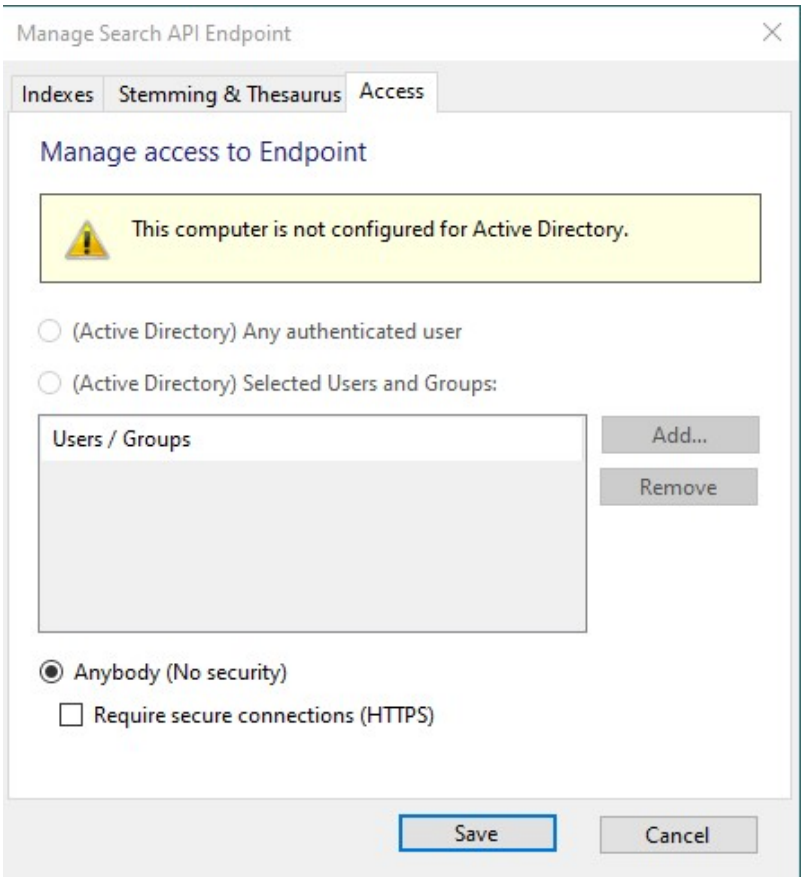
Use the access tab to control which Users and Groups can search Indexes added to the Endpoint.

Note: To use Active Directory options, the software must be running on a Windows Server configured with Active Directory.

(Active Directory) Any authenticated user
Any user that is part of the Server's Active Directory may search indexes assigned to the endpoint. Users connecting to the Endpoint will be required to log in with the credentials assigned to them in Active Directory. This option is disabled on computers that are not configured with Active Directory.

(Active Directory) Selected Users and Groups
Only selected users and groups of users may search indexes assigned to the endpoint. Users connecting to the Endpoint will be required to log in with the credentials assigned to them in Active Directory. This option is disabled on computers that are not configured with Active Directory

Anybody (No Security)
When chosen, anybody connecting to the Endpoint can search Indexes added to the endpoint without logging in.



Configure HTTPS Certificate (Required)

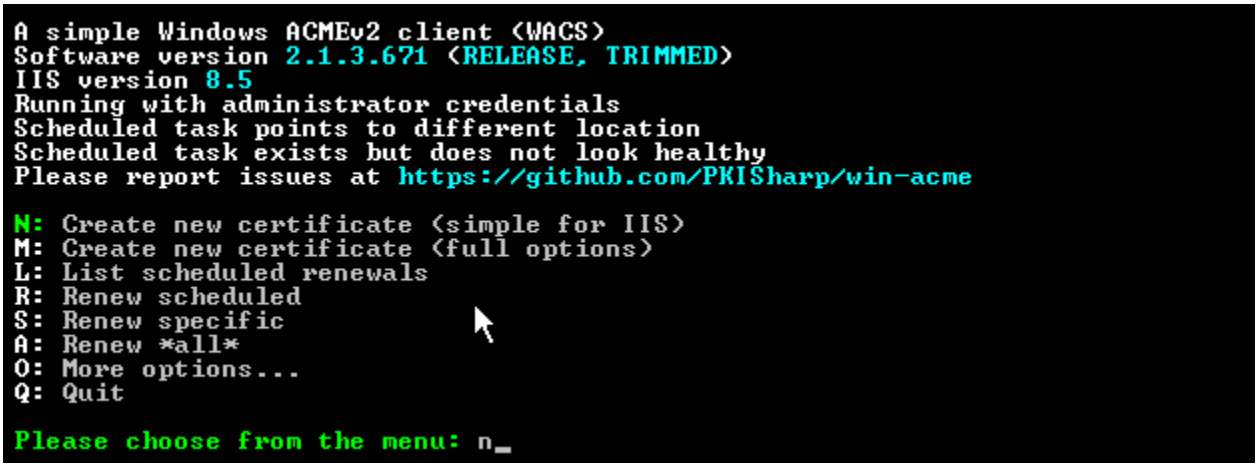
The Universal Search Client requires that HTTPS is configured on the endpoint for secure communications. There are two methods to obtain a certificate:

1. Obtain from a Certificate Authority
Obtain a certificate from a certificate authority if clients need to connect securely from outside the corporate network over the internet.
2. Self-Sign a Certificate
Sign your own certificate if all clients will connect over the local network.

Method 1. Obtain from Certificate Authority

To obtain a Certificate from a Certificate Authority, we recommend using the LetsEncrypt Certificate Authority 1 and use the included **Windows ACME Simple (WACS)** utility to automatically obtain and configure your Endpoint with the new certificate.

1. Run **wacs.exe**
2. When prompted, Select **Create new certificate (simple for IIS)**



3. When prompted, enter the number that corresponds to the Endpoint Name.

4. When prompted to pick bindings, select **All Bindings**

5. The utility will now perform the necessary steps to generate an HTTPS Certificate and configure IIS to use it on the given site.

6. Confirm you want a scheduled task to automatically renew the certificate, or update the existing scheduled task as required.

That's it, you're done. Your endpoint will now be HTTPS configured and certificate renewals will occur automatically in a scheduled task.

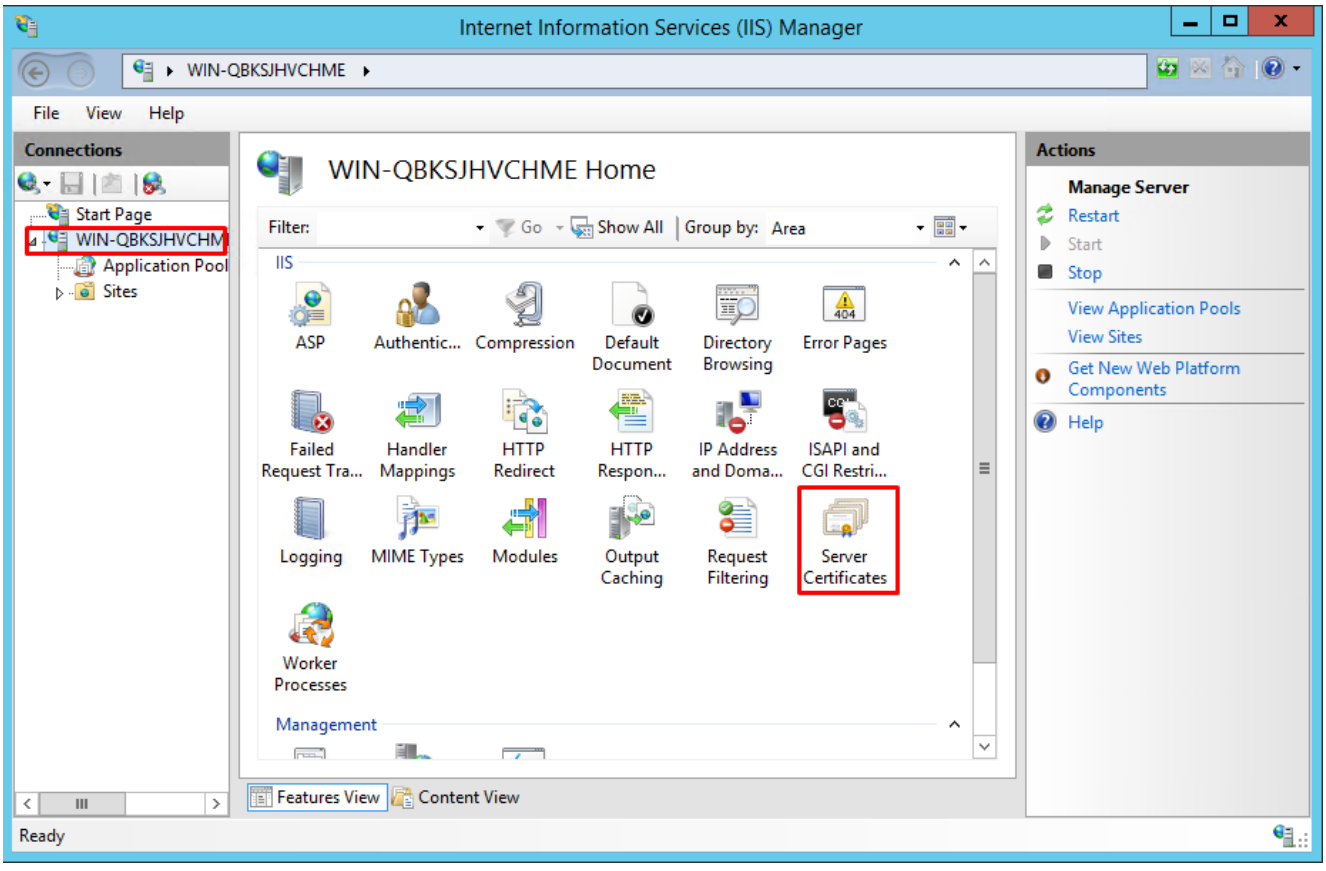
Method 2. Self-Sign a Certificate

There are three steps to create and use a self-signed certificate.
1. Use **IIS Manager** to Create the Self Signed Certificate
2. Bind the Certificate to the website
3. Trust the Certificate on client machines via Group Policy or manually install on all client machines.

Step 1. Create Certificate

1. From the Start menu, launch IIS Manager

2. In the Server Node, select Server Certificates



3. In the Actions Panel, select Create Self-Signed Certificate…

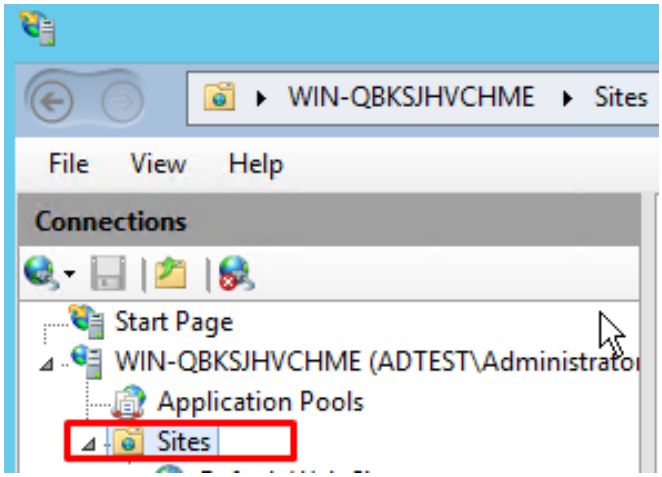
When prompted, enter a friendly name. This should be something memorable that describes the Endpoint. e.g., Contoso Search

Press OK

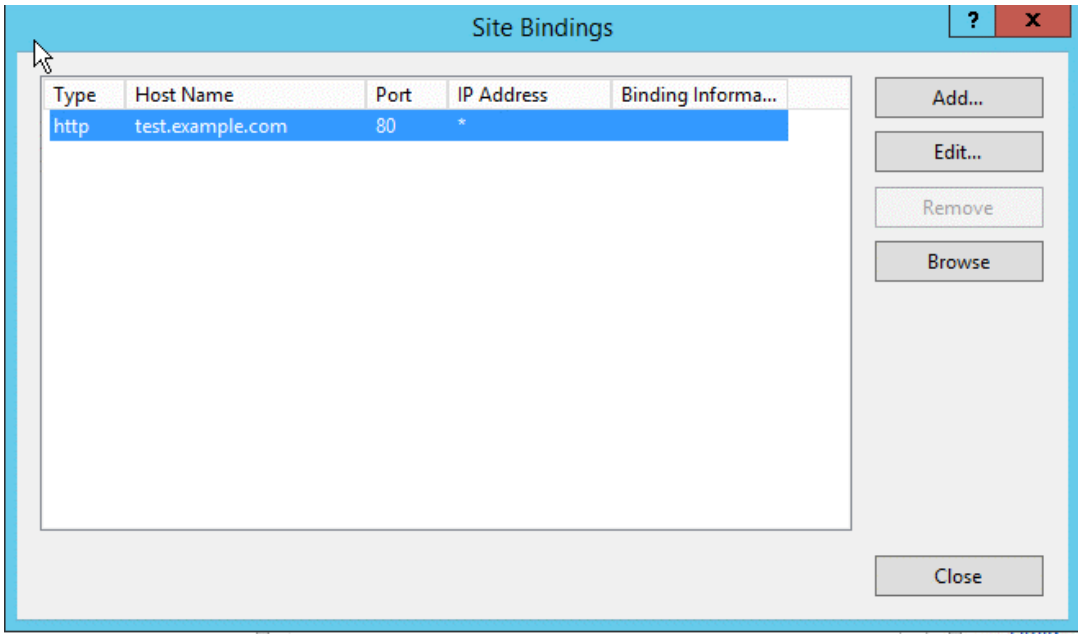
A new certificate has been created.

Step 2. Bind Certificate

1. In the Connections Panel, find your site inside the Sites Node

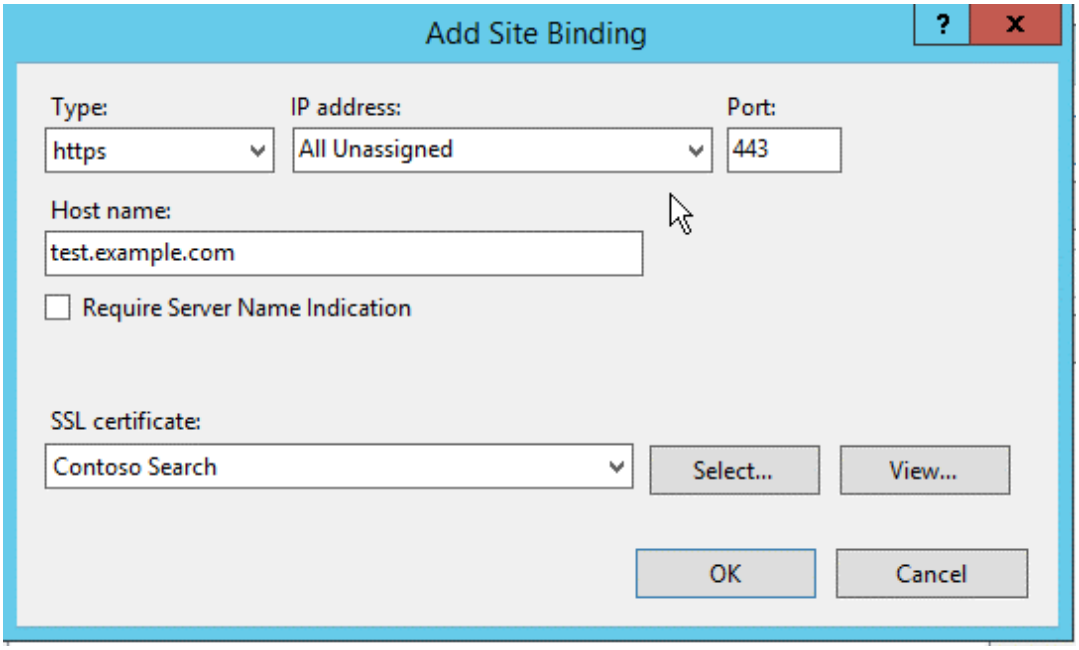


2. In the Actions Panel, under Edit Site, select **Bindings...**



Make a note of the **Host Name** bound to **Port** 80.

3. Click **Add...**

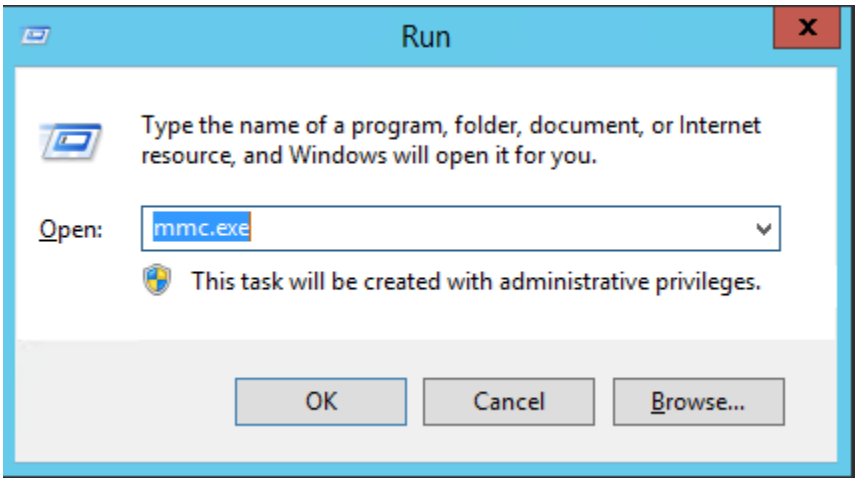


Do the following:
a. Set **Type** to ***https***
b. Set **Host Name** to the same as noted previously
c. Select the **SSL Certificate** you created.
d. Press **OK.** The binding already used warning can be safely ignored.

Step 3. Trust Certificate on Client Computers.

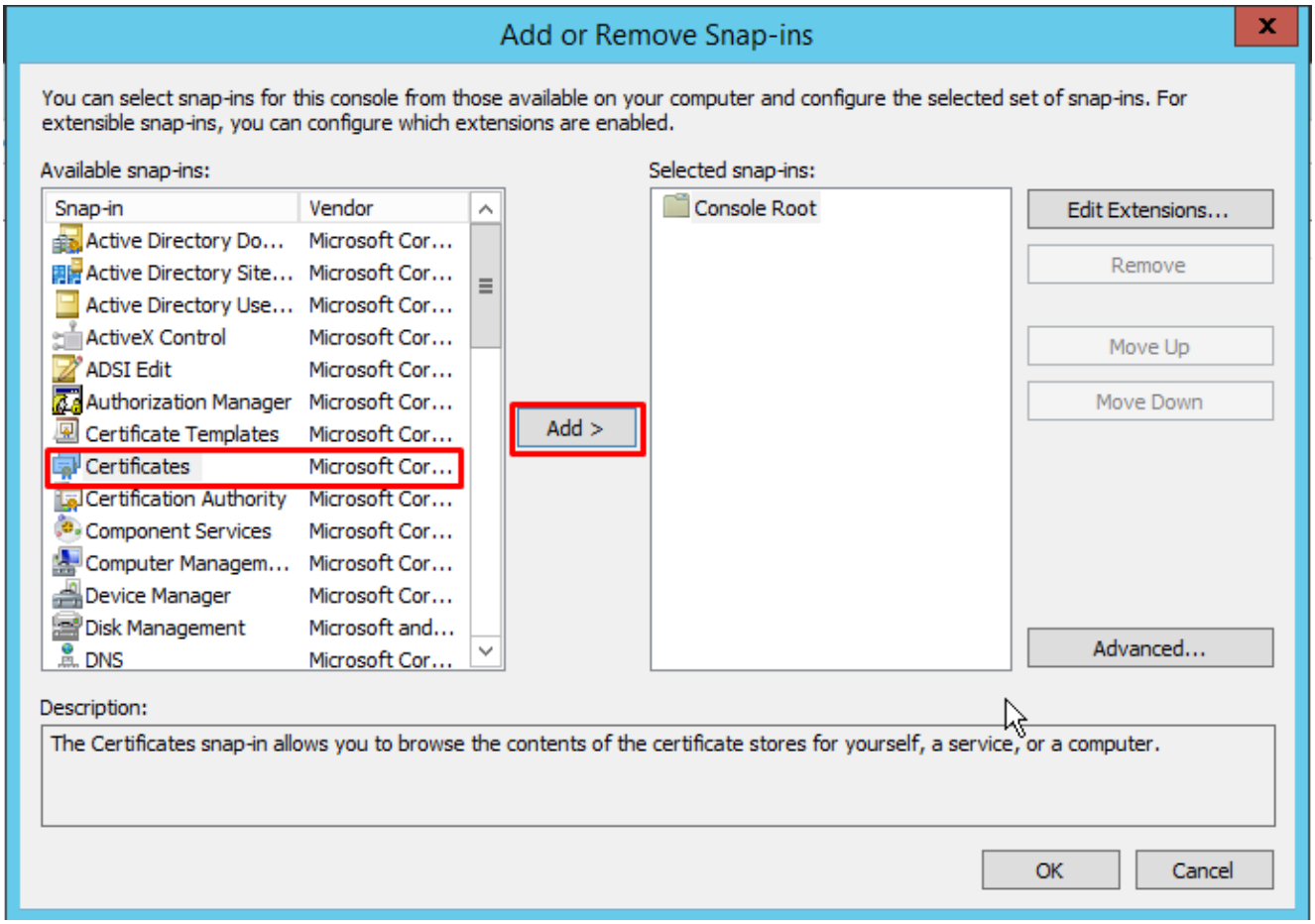
Export the Certificate

1. Run **mmc.exe**



2. Go to **File -> Add/Remove Snap In**

3. Add the **Certificates** Snap In



4. When prompted, select **Computer Account** and **Local Computer...** then finish.
Press **OK** to close the dialog.

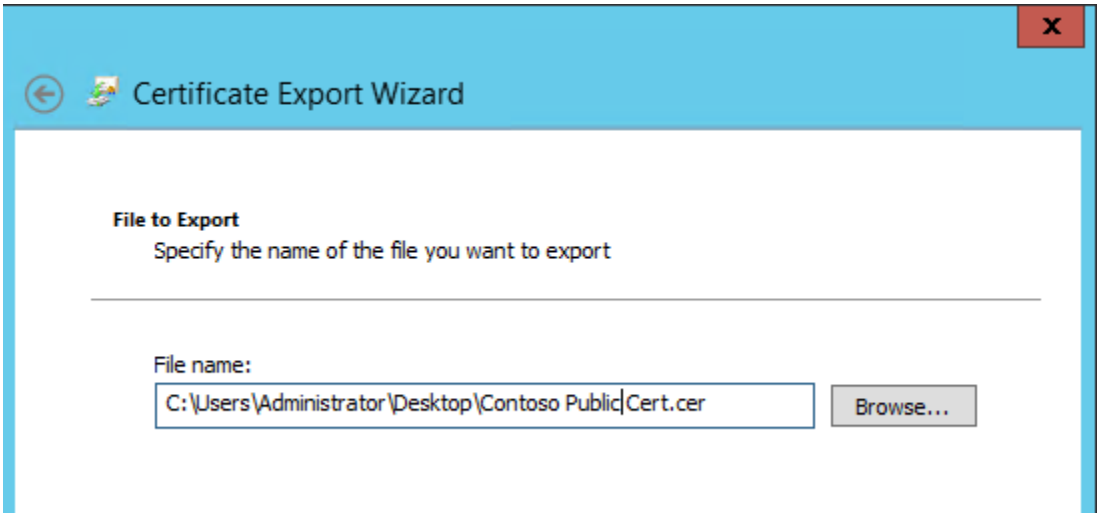
5. From the MMC Console, navigate to ***Certificates (Local Computer)\Personal\Certificates***

6. Find and select your certificate using the **Friendly Name** column

7. Go to **Action > All Tasks > Export...** to launch the Certificate Export Wizard.

8. When prompted, select **No, do not export the private key**

9. Select DER encoded binary X.509 (.CER).
Click Next and choose a location to save the certificate.



10. Click **Next** then **Finish** to export the Certificate.

The public certificate file is now created in the selected location.

Trust via Group Policy

If your server and client computers use Active Directory, follow the steps in this Microsoft Group Policy guide

https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/distribute-certificates-to-client-computers-by-using-group-policy

Trust Manually

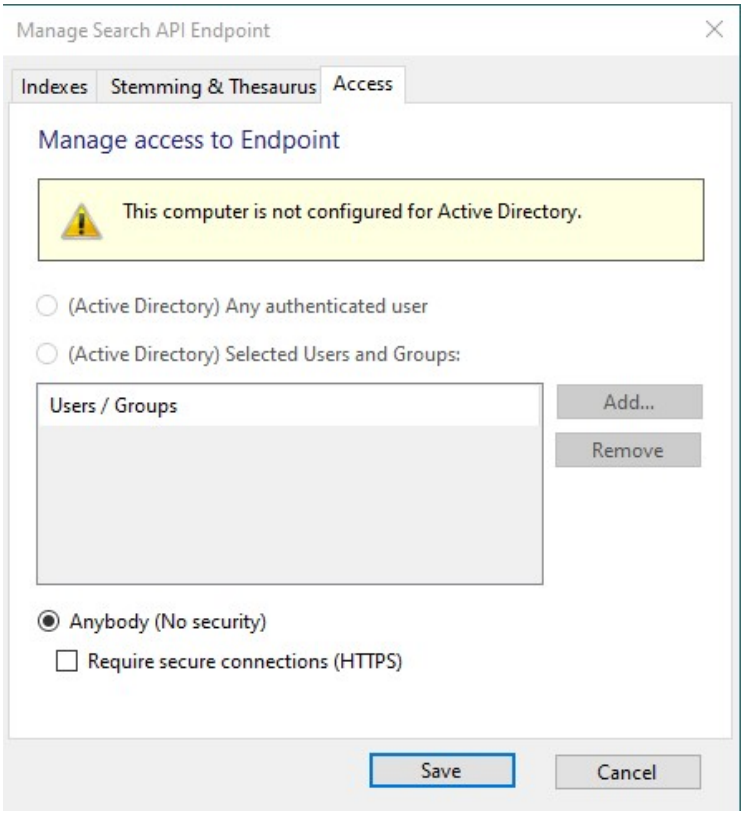
Distribute the created **.CER** file to client computers.

On each client computer, right click and **Install** the Certificate file.

Testing on a single machine

For demonstration or testing purposes it is possible to run a Universal Search Client on the same machine as the Endpoint Manager and Universal Search Server. This requires a machine that can run **Microsoft IIS** e.g., Windows 10 Pro. This will run over http instead of https.

1. Install **dtSearch Desktop**
2. Install (optionally) the **Database Indexer** and/or **365 Indexer** add-ons.
3. Create suitable indexes, if using dtSearch Desktop you need to use the Create Index (Advanced) options to **Cache documents in the index**, and **Cache text in the index.**
4. If you need to demonstrate faceted search you will need to use the Database Indexer add-on or 365 Indexer add-on, these will automatically use metadata to create fields that will be used for facets.
5. Install **Universal Search Server**
6. Setup Endpoint Manager to assign the indexes to the dummy endpoint ***search.example.com***
7. From Edit, open the **Access** tab and uncheck **Require secure connections**. Click **Save.**



8. Install and run the **Search Client**, choose the example endpoint.