Installation Procedure

SSL Certificates in IIS 7

This document will explain the creation and installation procedures for enabling an IIS website to use Secure Socket Layer (SSL).

Check IIS for existing certificates

a. First open IIS Manager. Select Server Certificates while highlighted on the Server name node.

b. If no certificates exist in the list then you must continue to the Create Certificate Request section.
Create Certificate Request

How you create the SSL certificate depends on the type of certificate you are going to create.

1. Self-Signed Certificate

*NOTE: Qualtrax does not recommend self-signed certificates as they are not trusted by web browsers without additional support. You will need to manually add the certificate to any browser that wants to access Qualtrax. Alternatively, the self-signed certificate could be placed in a trusted store for the domain to apply to all machines on the domain. This option would require additional IT support.

a. This certificate is created on the Qualtrax web server.
b. Open IIS and choose the server where the certificate will be installed.
c. Double click the Server Certificates node in the browse pane.
d. Choose the Create Self-Signed Certificate option in the actions pane.

e. On the following screen, give the SSL certificate a name. Commonly the website URL is used but the certificate can be named whatever you like. Click ok and the certificate will be added to the list of available certificates.

f. Please move on to Set Website Bindings section.
2. Domain Certificate

*NOTE: This option requires a Certificate Authority (CA) server on your network.

a. Your IT team would need to generate this certificate from the CA server. This is commonly the same as the Domain Controller but is not always.

b. Once the certificate has been created and issued to the Qualtrax web server, it may show up in the certificates list. If it does not show up automatically the IT department will need to export the certificate from the CA server and provide a .pfx file and password that can be imported.

c. Open IIS and choose the server where the certificate will be installed.

d. Double click the Server Certificates node in the browse pane.

e. Chose Import from the Action pane.

![Image of Importing Certificate]

f. Browse to the .pfx file provided and enter the password. The certificate should now show in the certificate list.

g. Please move on to the Set Website Bindings section.
3. **Signed Certificate**

   *NOTE:* This is the simplest method to get a trusted certificate. You must pay a yearly subscription to keep the certificate valid. These types of certificates are normally used for sites accessed on the Internet.

   a. Open IIS and choose the server where the certificate will be installed.
   b. Double click the Server Certificates node in the browse pane.
   c. Choose Create Certificate Request from the Action pane.
   d. Fill out the information in the pop-up shown below and click next.

   ![Certificate Request Pop-up](image)

   e. On the following screen choose a Cryptographic service provider and a Bit length for the encryption and choose next. (We suggest Microsoft RSA as a service provider and 2048 as the bit length)
f. The final prompt will ask for a file name. Choose a location and save the file as a .txt file.

g. The .txt file that has been saved needs to be sent to the authority signing the certificate (ie: GoDaddy or Verisign). They will need to verify your identity.
h. The authority will then respond back, typically with 2 files. These file can have different extensions depending on which authority you use.

i. One of the files is used to complete the certificate request and the other is what is called an Intermediate Authority. More than likely the Intermediate Authority is already configured on the user’s browsers. You will be looking for the .cer or .crt that represents the completed certificate.

j. Once you have the completed certificate request, browse back to the Server Certificates feature in the server node in IIS. Choose Complete Certificate Request in the actions pane.

k. Browse to the .cer or .crt file provided by the certificate authority and give it a friendly name. This is typically the URL to be used but can be set to any name you would like.

l. The certificate should now be in the list.

m. Please continue to the Set Website Bindings section.
Set Website Bindings

1. Select the Qualtrax website in IIS Manager, choose Bindings in the Actions pane.

2. Bindings will configure IIS to only allow connections to the site when using a specific URL. This is required for SSL because the certificate is based on a URL.
   a. To enable SSL you simply need to add a new binding of the https type. Set the certificate you want to use and the URL of the website.

*Note: Hostname is not a required Site Binding field. However setting this will prevent users from being able to access the site by IP address. If both the http and https bindings have a hostname set they must be the same hostname, and you will only be able to access the site by using the hostname in the URL.
**URL Rewrite**

URL rewrite gives the ability to automatically redirect users connecting to [http://qualtrax](http://qualtrax) to [https://qualtrax](https://qualtrax). This forces all connections to be SSL. If URL rewrite is not currently installed you may need to download and install the correct server version from Microsoft.com

1. Browse to the Qualtrax website in IIS and double click URL Rewrite in the features pane.

2. Choose Add Rule(s) from the Actions pane.

3. Choose Blank rule from beneath the Inbound Rules Heading.

4. Enter a name for the rule.

5. Under the Match URL heading make sure that the Requested URL setting is ‘Matches the Pattern’ and that the Using setting is ‘Regular Expressions’. Type ‘(.*)’ into the Pattern field. Ensure that the Ignore case option is checked.
6. Expand the Conditions heading. Click Add. Enter '{HTTPS}' as your Condition input. For the
Check if input string option select Matches the Pattern. Enter '{^OFF$}' as your Pattern. Check the
Ignore case box. Click OK to add the Condition.

7. In the action tab set the Action Type option to Redirect. Enter 'https://{HTTP_HOST}' in the
Redirect URL field and make sure that the Append query string box is checked and that the
Redirect type is set to Permanent (301).

8. Your settings should match the screenshot on the following page.