

# **PAT REST APIs**

## **Configuration of HTTPS Access**

*© 2021 CONCEPT Data Systems Systemanalyse und Softwareentwicklung GmbH*



## General

The standard configuration of the PAT REST-APIs uses *http* as a protocol; as they all use user-login for authentication (+ an authorization token in the case of the WebAPI), for access within the company-LAN this should provide enough security.

But when accessing an API from outside the LAN, SSL/TLS-encryption will be desirable, leading to the usage of *https*.

Two of the PAT APIs can be operated on *https*:

- PAT Mobile
- PAT WebAPI

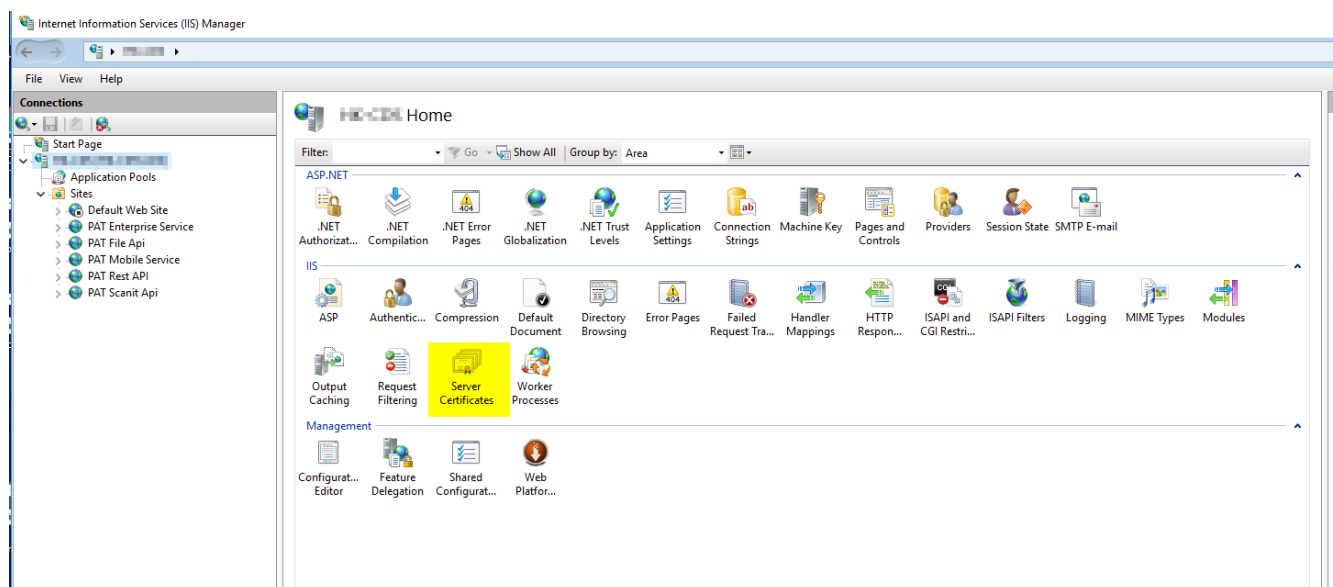
For the other APIs (PAT Enterprise, PAT Scan it, Pat File API), the clients are currently not configured to support *https*. If this is required, please contact CDS.

## Install Certificate

To use SSL/TLS, a valid certificate is needed; the issuing authority will depend on the IT-System of the customer and should be decided and acquired by the respective IT Admin department; most PAT users will already hold a certificate issued for their domain.

Alternatively, there are a number of CA (certification authorities) where the admin can acquire a free domain-certificate, e.g. [www.letsencrypt.org](http://www.letsencrypt.org); see there for further details and instructions.

To install the certificate in IIS, open the IIS-Manager start-page and choose option "Server Certificates":



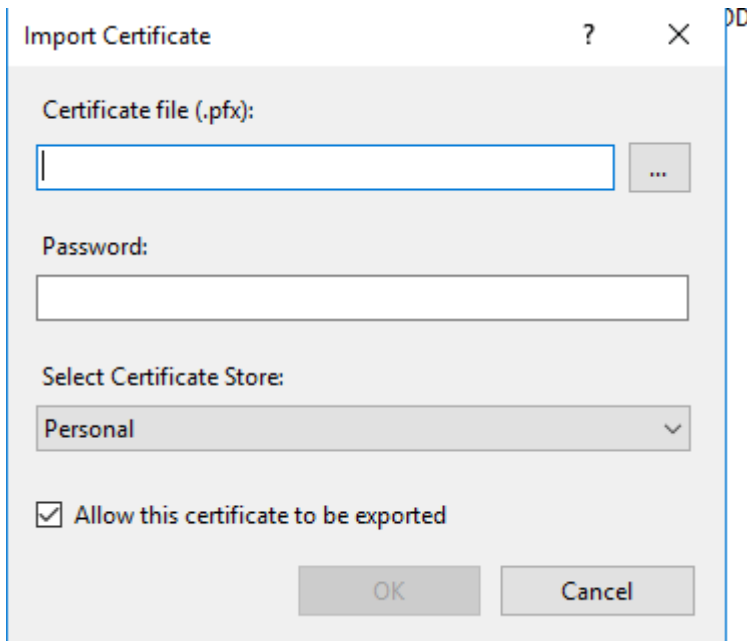
You will now see a list of installed certificates:

## Server Certificates

Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Filter:	Go	Show All	Group by:	No Grouping		
Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store	
	*.*****.com	Sectigo RSA Domain Validatio...	1/10/2022 12:59:59...	169DD3C9BB4A58C4B93F0F4...	Personal	

If the certificate does not show up yet, it has to be imported (Actions / Import Certificate...):



**Import Certificate**

Certificate file (.pfx):

Password:

Select Certificate Store:

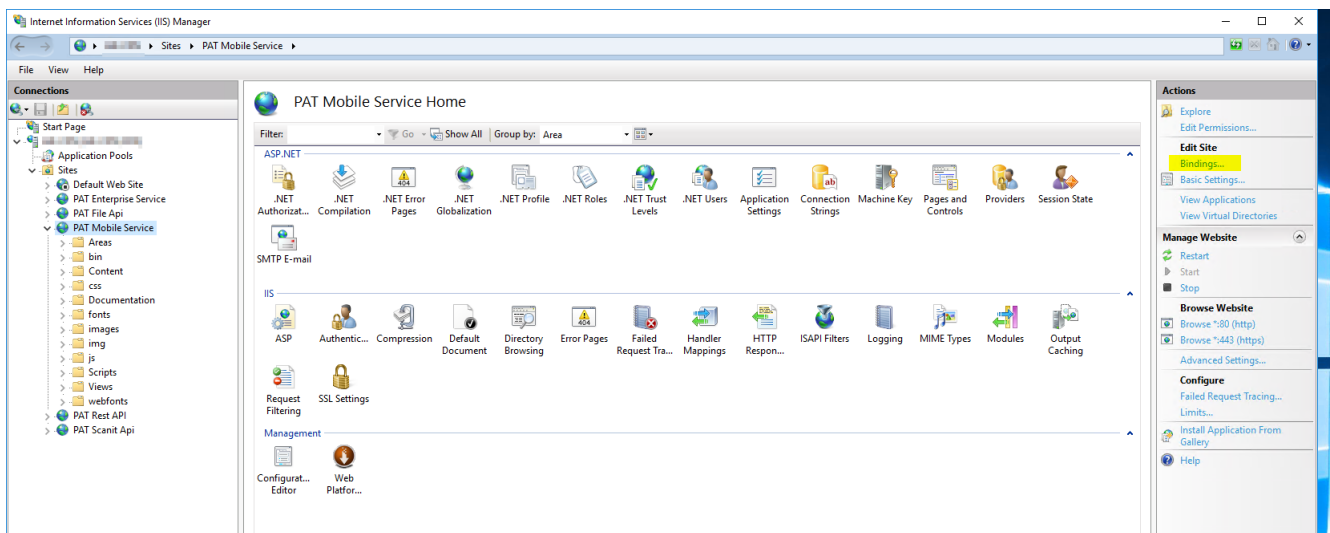
Personal

☒ Allow this certificate to be exported

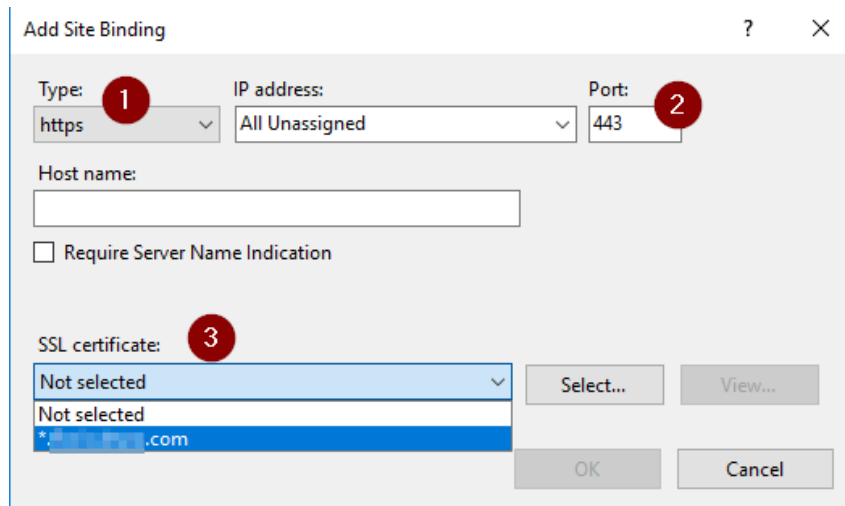
OK Cancel

## Add HTTPS-Binding

To add *https*-support to a PAT Api, an new binding has to be set up for its Application Pool:



To edit the bindings, either choose Actions/Bindings... on the right or in the local menu of the application pool (right mouse-click) and add a new binding:



The screenshot shows the 'Add Site Binding' dialog box. It contains the following fields and controls:

- Type:** A dropdown menu with 'https' selected. A red circle with the number 1 is next to it.
- IP address:** A dropdown menu with 'All Unassigned' selected.
- Port:** A text box containing '443'. A red circle with the number 2 is next to it.
- Host name:** An empty text box.
- Require Server Name Indication:** An unchecked checkbox.
- SSL certificate:** A dropdown menu with 'Not selected' selected. A red circle with the number 3 is next to it.
- Select...:** A button to the right of the SSL certificate dropdown.
- View...:** A button to the right of the 'Select...' button.
- OK:** A button at the bottom right.
- Cancel:** A button at the bottom right, to the left of the 'OK' button.

Select *https* in (1), choose a port in (2) and select your certificate in (3). 443 is the standard port for *https*, but of course any other available port can be chosen here.

Some versions of IIS show additional configuration-items in this dialog; those can safely be left on their defaults.

## Access the API via HTTPS

To access an API over *https*, any modern browser can be used here (Firefox, Edge, Chrome, ...). Depending on the chosen browser, you may have to add the certificate to the list of trusted certificates; see documentation of browser.

To choose *https*, prefix the url with *https:*, e.g. <https://192.168.1.7> in the address-field of the browser; if the binding was added to port 443, this port is automatically chosen when selecting *https*; if an alternative port has been added for the binding, it has to be specified in the url: e.g. <https://192.168.1.7:8081>.