ITAS WebSerives – Secure Ports

1st November 2021

Notice to switch all ports to the secure https protocol for ITAS APIs

Hivedome will be switching support from the non-secure http protocol to the secure https protocol on ITAS APIs from November 2021.

Background

Trader Desktop includes several rest APIs: these include APIs used internally by the application, APIs used to integrate ITAS with other third-party systems and a Web Portal option that enables users to access ITAS data via the web.

Historically these APIs have been delivered using the insecure http protocol, but support for the secure https version was introduced earlier this year within Trader Desktop version 8.10.4.1617. ITAS will continue to support the APIs over the existing insecure http protocol for the time being, to allow for a smooth transition for all customers to switch to the secure https systems, but http will eventually be made redundant. Hivedome plan to begin switching all clients to the http protocol from November 2021 as we roll out Trader Desktop version 8.12.0.

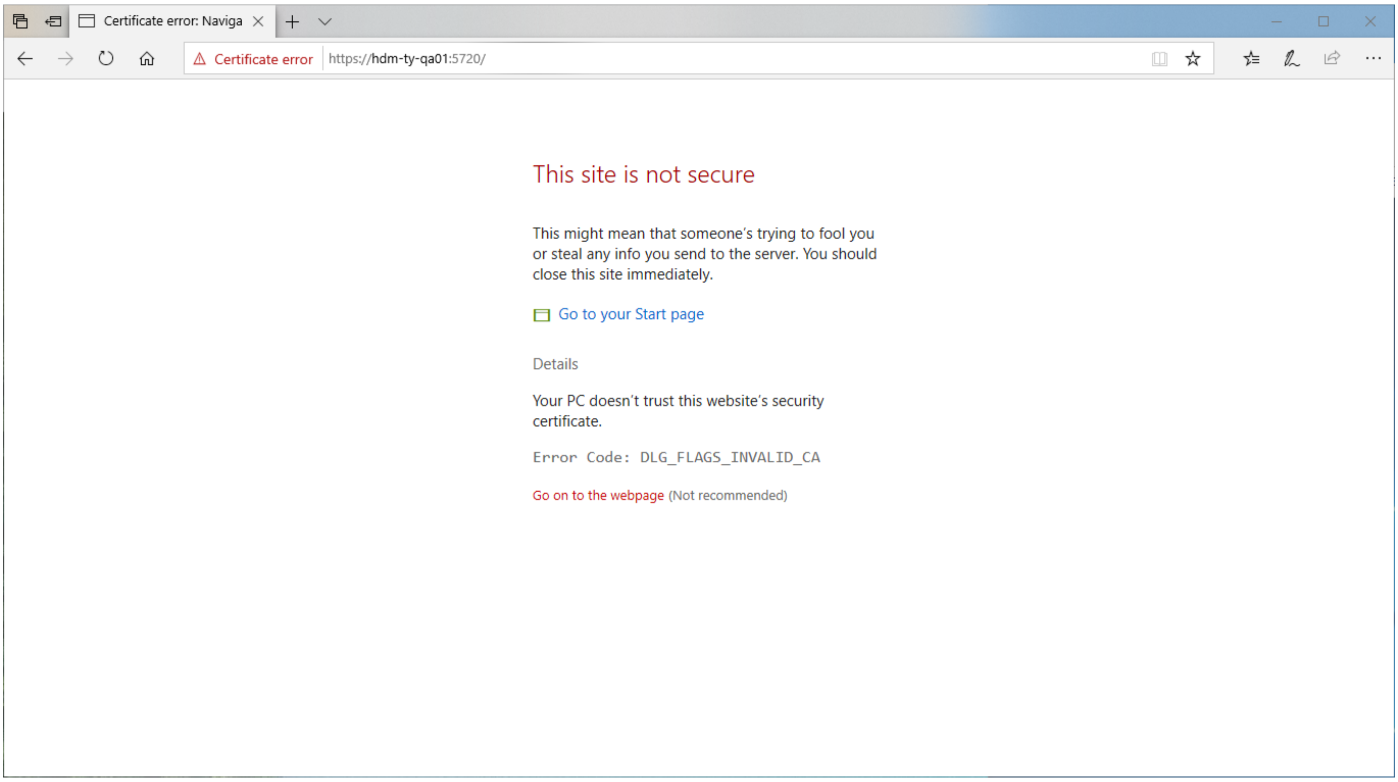
Requirements

Part of the challenge with the change is to manage the (SSL) certificate associated with https. The good news is that for the most basic ITAS installations, where Trader Desktop is run on a single server and where the ITAS application is also installed on that same server, this will be done for you. However, if your users run Trader Desktop from a separate server or from workstations then action will need to be taken.

The https certificate serves two purposes. Firstly, it provides keys by which the data may be encrypted by the sender end and decrypted by the receiver. This is intended to prevent anybody on the network from eavesdropping or altering the data. Secondly it can provide assurance that the sender is indeed the computer you think it is. This is because no unauthorised computer should have access to the key that encrypts the data.

The secure versions of the API endpoints have already been created using a self-signed certificate: a certificate that serves the first of these purposes, to encrypt the traffic. However, it will not necessarily provide assurance as to the sender’s identity. If the receiver has no way to verify that the certificate is the real deal, then it cannot use that certificate to verify the identity of the sender, as demonstrated on the next page:

Browsing to the web address of a site secured with a certificate that your computer does not trust results in an error like the one below:



This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Go to your Start page

Details

Your PC doesn't trust this website's security certificate.

Error Code: DLG_FLAGS_INVALID_CA

Go on to the webpage (Not recommended)

Similarly, secure API calls from Trader Desktop may fail if the computer running Trader Desktop does not trust the certificate.

The computer on which Trader Desktop and the ITAS web services reside already trusts this self-signed certificate, but other computers on your network will not unless you take one of the following two actions:

- Distribute the self-signed certificate to any client computer connecting to ITAS services.

  or

- If you already have a local certificate server trusted by computers on your network, then you may replace the self-signed certificate with one that is generated and signed by your own certificate server.

Switching To Secure Ports

Where APIs are already being accessed via the nonsecure http ports, following the deployment of 8.12.0, these will need to be accessed via their secure versions. Switching is simple, see below for an example.

Port in use prior to the deployment of Trader Desktop 8.12.0:

http://hdm-ty-dev01:4720/

Port to be used following the deployment of Trader Desktop 8.12.0:

https://hdm-ty-dev01:5720/

For more information or assistance with this change, please contact your ITAS representative or support team.