

ITAS Certificate Management

1st November 2021

Support for https protocol for ITAS APIs

Hivedome now offer support for the secure https protocol to be used with ITAS APIs.

For Certificate installation instructions see below

Distribute A Self-Signed Certificate

This is a two-step process. Exporting the certificate from the ITAS Application Server and importing the exported certificate on to each of the client computers where Trader Desktop is used.

Exporting A Certificate

Log onto the ITAS Application server.

Run certlm.msc. Navigate to **Personal** > **Certificates** and find the certificate that bears the same name as the application server.

Right click on the certificate and choose All Tasks > Export.

🚡 certlm - [Certificates - Local Com	nputer\Personal	\Certificates]			_		×	
File Action View Help								
🗢 🔿 📶 🔚 🕷 🖬	1 📑 🛛 🖬							
🗊 Certificates - Local Computer 🔺	Issued To	^	Issued E	Зу			Ex	
✓ Personal	itasdemo		itasdem	10			21	
Certificates		Open						
> Interpretending in the second se		open	_					
> 📋 Enterprise Trust		All Tasks 🔅	> (Open				
> 📋 Intermediate Certification		C-4		D			I	
> Trusted Publishers		Cut		Request	Lertifica	ite with r	iew Key	·
> 📋 Untrusted Certificates		Сору	1	Renew Co	ertificate	e with Ne	ew Key	
> 📔 Third-Party Root Certifica		Delete		Managel	Drivate I	Cente		
> 📋 Trusted People		B	- '	, in the second s	- nvate i			
> 📔 Client Authentication Issu		Properties		Advance	d Opera	tions		>
> Preview Build Roots		Help		Export				
> 🧮 Test Roots	-							
> 📔 Remote Desktop								
> 📋 Certificate Enrollment Rec								
> Smart Card Trusted Roots								
> 📋 Trusted Devices								
Web Hosting								
Fundada and Gasta	•							
Export a certificate								

On the following screen, click Next.

÷	Certificate Export Wizard	×
	Welcome to the Certificate Export Wizard	
	This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, click Next.	
	<u>N</u> ext Can	cel

Ensure "No, do not export the private key" is selected and click Next.

		Х
←	F Certificate Export Wizard	
	Export Private Key	
	You can choose to export the private key with the certificate.	
	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
	Do you want to export the private key with the certificate?	
	○ Yes, export the private key	
	• No, do not export the private key	
	Next Canc	el

Ensure that "DER encoded binary X.509 (.CER)" is selected and Click Next.



Browse to the location where you want to save the exported file and click Next.

		×
← 🍃	Certificate Export Wizard	
	File to Export Specify the name of the file you want to export	
	File name:	
	C:\Users\HDMCS\Desktop\ITASDEMO.cer Brows	e
	Next	Cancel

Finally, click Finish.

÷	ş	Certificate Export Wizard		×
		Completing the Certificate Exp	port Wizard	
		You have successfully completed the Certificate	Export wizard.	
		You have specified the following settings:		
		File Name	C:\Users\HDMCS\Desktop\ITASDEMO.	
		Export Keys	No	
		Include all certificates in the certification path	No	
		File Format	DER Encoded Binary X.509 (*.cer)	
		<	>	
			<u>F</u> inish Car	ncel

Once the Certificate Export Wizard is closed, ensure that a .cer file is created in the location selected.

Importing A Certificate

Once the certificate is exported, it can be imported to each client machine that will connect to Trader Desktop and or ITAS web services.

Import the certificate by copying the exported .cer file to the client machine. **Double click** on this file to launch the Certificate Import Wizard, click "**Install Certificate**".

🛺 Certificate	×
General Details Certification Path	
Certificate Information	
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.	
Issued to: itasdemo	
Issued by: itasdemo	
Valid from 9/21/2020 to 9/21/2021	
Install Certificate Issuer Statement	
ОК	

On the next screen Select "Local Machine" and click Next.

;	×
 & Certificate Import Wizard 	
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location	
○ <u>c</u> urrent User	
To continue. dick Next.	
· · · · · · · · · · · · · · · · · · ·	
€ <u>N</u> ext Cancel	

If User Access Control is enabled, the following message should appear:



Click Yes and then select "Place all certificates in the following store" and Browse to Trusted Root Certification Authorities.

			×
←	🐓 Certificate li	mport Wizard	
	Certificate Stor	e	
	Certificate	stores are system areas where certificates are kept.	
	Windows of the certific	an automatically select a certificate store, or you can specify a location for ate.	
	Aut	pmatically select the certificate store based on the type of certificate	
	Place	Select Certificate Store X	
	Cer	Select the certificate store you want to use. Browse	
		Personal Trusted Root Certification Authorities	
		Enterprise Trust	
1		Trusted Publishers	
		Intrusted Certificates	
		Show physical stores	
		OK Cancel	
		Next Cance	ł

Click on **OK** and then **Next**.

On the final screen, click Finish.

← 🛿 🖗 Certificate Import Wizard	×
Completing the Certificate Import Wizard	
The certificate will be imported after you click Finish.	
You have specified the following settings:	
Certificate Store Selected by User Trusted Root Certification Authorities Content Certificate	
Finish Canc	el

Click **OK** to close Certificate Import Wizard.



Run certlm.msc. Navigate to **Trusted Root Certification Authorities** > **Certificates** and locate the certificate that was just imported.

If you have many machines which will need to connect to ITAS web services, then carrying out this procedure on each of them may be time consuming. This can be automated if required.

Using Your Own Local Certificate

If your organization has an internal certificate server that can produce and sign a certificate for your ITAS application server, and that will be trusted by machines on your internal network, you can use this certificate instead.

Your application server should already have a certificate in the certificate store for the local machine under **Personal**, this will bear the same name as the application server. If you simply replace this with the one generated by your internal certificate server and then run the ITAS deployment tool, it will deploy all web services using this certificate.

Follow the relevant instructions on the next page for Installing a Public or Local certificate:

Using Your Own Public Certificate

If you wish to have ITAS services accessed from outside of the local network, then there are a few ways to achieve this. You will need a public hostname address and a certificate to match. You may choose to have a web application firewall sit in-front of the ITAS Web Services. This can be configured with the public hostname address and the matching certificate. It can be set up to accept requests on the public address and forward those requests to the internal address. The configuration for this is outside of the scope of this document.

Alternatively, you may choose to set up your firewall to allow direct access to the ITAS application server from the outside. To do this Hivedome will need to be informed of the public address so that we can set the configuration files in order that the webservices are deployed with bindings to that hostname.

The ITAS deployment process will check if there is already a certificate available in the certificate store (in the local machine personal store) and use that certificate with the web bindings that it creates.

Follow the relevant instructions on the next page for Installing a Public or Local certificate:

Installing A Public or Local Certificate

This can be achieved as follows providing you have a pfx file and the password for that pfx file:

Launch certlm.msc and delete the existing certificate.

🚟 certlm - [Certificates - Local Com	puter\Personal\Certificates] —	×
File Action View Help		
🗢 🔿 🞽 📰 🔏 🛍 🗙 🖾		
 Certificates - Local Computer Personal Certificates Trusted Root Certification Enterprise Trust Intermediate Certification Trusted Publishers Untrusted Certificates Third-Party Root Certificat Trusted People Client Authentication Issu Preview Build Roots Test Roots Remote Desktop Certificate Enrollment Rec Smart Card Trusted Roots Trusted Devices 	Issued To Issued By Copen All Tasks Cut Copy Delete Properties Help	
< >>	<	>
Deletes the current selection.		1

Double click on the PFX file. Select "Local Machine" and then click Next.

 & Certificate Import Wizard 	×
Welcome to the Certificate Import Wizard	
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
Store Location	
O Current User	
Local Machine	
To continue, click Next.	
Next Cancel	

If User Access Control is enabled, the following message should appear:



Click Yes and the path to the pfx file you double clicked on should be displayed on the next screen.



Set a **Password** then tick "**Mark this key as exportable**" ensure that "**Include all extended properties**" is ticked before clicking on **Next**.

←	×
Private key protection To maintain security, the private key was protected with a password.	
Type the password for the private key.	
Password:	
Import options: Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.	1
Protect private key using virtualized-based security(Non-exportable) Indude all extended properties.	
Next	Cancel

Select "Place all certificates in the following store." Browse to Personal and click Next.

÷	😺 Certificate Import Wizard	×
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Automatically select the certificate store based on the type of certificate Ince all certificates in the following store		
	Personal Browse	
	Next Cano	el

Г

On the final screen, click Finish.

← 😺 Certificate Import Wizard		×	
Completing the Certific	cate Import Wizard		
The certificate will be imported after you click Finish.			
You have specified the following settings:			
Certificate Store Selected by User Content	Personal PEX		
File Name	C:\Users\HDMCS\Desktop\ITASDEMO.pfx		
	Finish Cance	el	

Allowing ITAS to generate a public certificate

The ITAS deployment process can create a certificate from 'Let's Encrypt' using WinACME. If no suitable certificate is found ITAS will attempt to use WinACME to generate a domain validation certificate. To do so it will need to demonstrate control of the public hostname included in the certificate. 'Let's Encrypt' will challenge WinACME to do so by publishing a particular code on the http website that responds at that hostname. If the firewall is forwarding http traffic (port 80) to the default website on the ITAS application server then this will work automatically.

For more information or assistant with this install, please contact your ITAS representative or support team.