



BOSCH

Invented for life

Intelligent Insights Certificate handling

Author: Hepting Manuel (BT-VS/PAS4-MKP)
Date: 24 July, 2020

1	Introduction	3
1.1	About TSL	3
1.2	About TLS/SSL certificates	3
1.3	Self signed and trusted certificates	4
2	Managing certificates in Intelligent Insights	5
2.1	Signing request	5
2.2	Uploading a certificate	5
2.3	Creating a self-signed certificate	6
2.4	Using self-signed certificates with BVMS	7

1 Introduction

This technical note describes how to install and configure certificates with Intelligent Insights. It also describes the different security options.

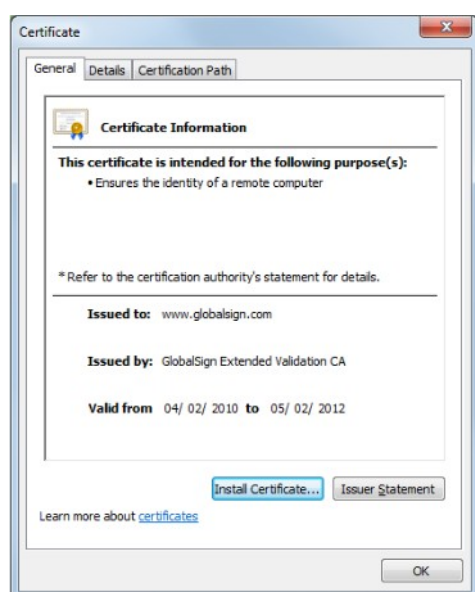
TLS (Transport Layer Security) is a common security protocol that most web servers use to ensure a secure machine-to-machine connection via an unsecure network like the internet. This white paper helps you choosing the most suitable type of certificate for your business's requirements, whether an internal network or external website. It informs about the features and benefits of using TLS, describes the different available types of certificates and also recommends the appropriate use of each type.

1.1 About TSL

The Transport Layer Security (TLS) along with Secure Sockets Layer (SSL) is the most common security protocol today. Essentially, it provides a secure channel between two machines operating via the internet or an internal network. TLS/SSL is used when a web browser needs to securely connect to a web server via the unsecure internet.

The key success of TLS/SSL is the simplicity to the end user. Technically, TLS/SSL is a transparent protocol, which requires little interaction from the end user when establishing a secure session. In the instance of a browser, the end user is alerted about the use of TLS/SSL as they see a yellow padlock. In the case of Extended Validation TLS/SSL, the address bar displays a padlock, also switches the address bar green and displays the URL as HTTPS. Websites use HTTP as standard, which is unsecure and subject to eavesdropping attacks. Especially if critical information like credit card details and account logins are transmitted, the websites can give attackers access to online accounts and sensitive information, leading to fraud or even identity theft.

1.2 About TLS/SSL certificates



A TLS/SSL certificate is required in order to access and use a TLS/SSL protocol. A TLS/SSL certificate is a small data file issued by one of a limited number of trusted certificate authorities (CAs), such as GlobalSign, that digitally bind a cryptographic key to organizations corporate details. Such details can include domain, server or host name, company name and location and in some cases organizational contact details.

Organizations need to install the certificate on their web servers to initiate SSL sessions with browsers.

An individual or an organization can apply for varying levels of vetting for each type of certificate. Once a certificate is installed, it is possible to connect to a website using a HTTPS connection. A HTTPS connection establishes a secure connection with the browser. When the secure connection is established, all web traffic between server and browser is secure.

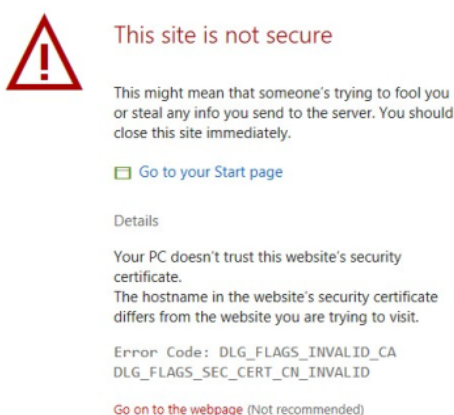
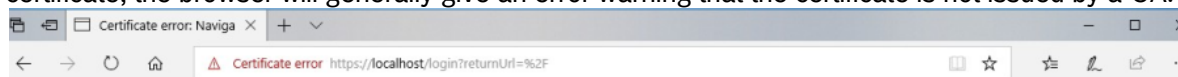
Anyone can view a TLS/SSL certificate in a browser by clicking on a padlock symbol and selecting **View Certificate**. Different browsers display the certificate in different ways, but the information is the same.

1.3 Self signed and trusted certificates

Security wise, both certificates work in the same way. Data transferred through a SSL or HTTPS connection is encrypted to provide a high level of security. The difference is getting customers' trust. A certificate from a CA implies that your website is secure as it is certified by a trusted source. CAs, like Verisign, verify the ownership of the domain and even check the trustworthiness of the business before issuing an SSL security certificate. That is why customers trust Verisign certificates when providing sensitive information such as credit card details to e-commerce sites.

Security certificates from a certificate authority are not free of charge. You have to pay for an SSL security certificate. To optimize costs, you can use a self-signed certificate whenever possible. For instance, webpages that do not require credit card information or sensitive data can be handled with a self-signed certificate. More specifically, when developers are working on a secure website, they can test the site using a self-signed SSL security certificate.

The primary operational difference between a self-signed certificate and a CA certificate is that with a self-signed certificate, the browser will generally give an error warning that the certificate is not issued by a CA.



This is the same warning message you receive when connecting to Intelligent Insights using a self-signed certificate. Generally, this warning should occur only once per browsing session.

1.3.1 Risk of using self-signed on public sites

The security warnings associated with self-signed SSL certificates could scare potential clients that the website does not secure their credentials. Both, brand reputation and customer trust, could be damaged.

1.3.2 Risk of using self-signed on internal sites

While the dangers of using self-signed certificates on public sites may be obvious, there is also a risk of using them internally. Self-signed certificates on internal sites (for example employee portals) still result in browser warnings. Many organizations advise employees to simply ignore the warnings, since they know the internal site is safe. But this can encourage dangerous public browsing behavior. Employees accustomed to ignore warnings on internal sites may be inclined to ignore warnings on public sites as well, leaving them, and your organization, vulnerable to malware and other threats.

2 Managing certificates in Intelligent Insights

2.1 Signing request

SSL secures all website traffic between two points, ensuring that any data shared between your customers and your webserver is safe and secure. It achieves this in two ways:

- It encrypts the data between the two computers, preventing anyone from eavesdropping on your communications.
- It confirms the identity of the website you are communicating with.

In order to confirm your identity it is important that a "trusted authority" that vouches for your identity, signs your SSL certificate. You can ask a "trusted authority" to sign a certificate confirming your identity by creating a certificate signing request and submitting it to a certified agent. The certificate signing request will generate the private and public keys that are needed to encrypt data between yourself and your customers. It will also record information regarding your company or organization.

A certificate signing request (CSR) is a message that an applicant (usually a person or organization who owns a website that needs to be secured) sends to a certification authority in order to apply for a specific digital identity certificate.

A CSR is usually generated by the server software, which the certificate uses on. The request contains a block of encrypted text which contains specific information that will be included in the certificate such as the owner or organization name, domain name or common name, country, locality, email address, etc.

For details on the included information, see chapter 2.3 Create self-signed certificate. To start a signing request provide at least the "Country code" and "Common Name".

Create certificate signing request

* Country

State (optional)

Locality (optional)

* Organization

Organizational unit (optional)

* Common name

Save

Cancel

Certificate signing request creation was successful.

```

-----BEGIN CERTIFICATE REQUEST-----
MIICszCCAZsCAQAwPDELMAkGA1UEBhMCREUxDjAMBgNVBAoMBUJvc2NoMR0wGwYD
VQQDDBRJbnRibGxpZ2VudCBJbnNpZ2h0czCCASlwdQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAMQzzqMhGnSUgaSC/WkK4bj1Ez/DS056/ft+nOfTDFpaSd348Hb
o2+eaX3B7iLnyqxEBi3II9I1TnAwHlw/v2qjHrv9N1GfVUUensDZ9LwJH3JgJB
dK+b9FcrJiA2iuFFhpcYsX854PxYcV7pBZ8IfT6QzyOVq+tY21Uo+H4kOOG+YBEU
LAFp/j7vLKvePpwCgVa6IZMOUOzboj2uYrITN3gTKXmX/HDElhPLVQaEC1/nAuF
GeKmQZzh5JzRv+WJITJON43tVAZJFOli+60IZhSUUrBhOfD/s4GodsfrBxc1yWp
hZ88dbeWXnuXRjaITbEU5Y8dPQT7sHLgHGKCAwEAaAaMDAGCSqGSIb3DQEJJDJj
MCEwHwYDVRRBggwFolUSW50ZWxsaWdlbnQgSW5zaWdodHMwDQYJKoZIhvcNAQEL
BQADggEBABGE2FpMcfn1rrLrMz3MXrd4uucR9SrOgBrOz1OQLhZc7qn+/ODmPy35
CLmPZht+NPax8VDWRbZqXn8GzAdtHS0lcUE1hQ19vKwqo8ER68Gz1fSoJ37Qoiz
xV30DyP36D3lrOSw7uGaWITP8+qQ8sYf3ZBO0b//lIO//nQJEFPwr+KFPms7vZJb
haWeyw48HfBDhQOVNE0Z9BOuEtGZ8TN47zrE2/ok9GRXrt5ckmF1vHSJ+eFMJLHN
3yYl+BAjrunXFU+ETRVqVuH4y2u5CNerXGRKcrg6HWG/1Mq/QvnxlWZuL0cykaN
AEaDMQwrrE06fxCbupGAdNP7YEbtsLI=
-----END CERTIFICATE REQUEST-----

```

OK

Download

2.2 Uploading a certificate

A TLS/SSL Certificate is a text file with encrypted data that you install on your server to be able to secure or encrypt sensitive communications between your site and your customers.

After you create a CSR and purchase a certificate, you need to upload the certificate to the server in order to let the server use the certificate for the encryption. With the function **Upload certificate** you can upload the issued certificate from the "trusted authority" to be used by Intelligent Insights. The uploaded certificate is used by the Intelligent Insight webservice. The HTTPS communication from client web browsers to Intelligent Insights is encrypted by the uploaded certificate.

Upload certificate

Choose file

* Certificate file path

Choose file

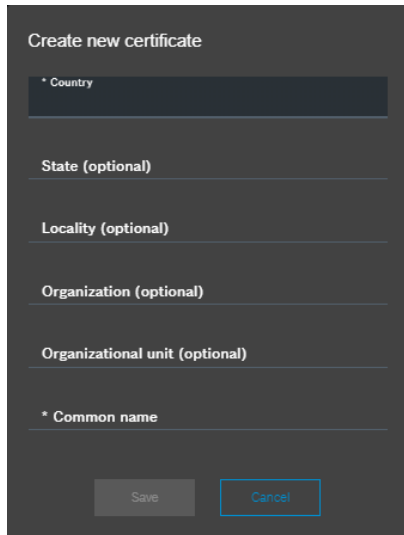
* Certificate authority file path

Upload

Cancel

2.3 Creating a self-signed certificate

When using a self-signed certificate, there is no chain of trust. The certificate has signed itself. The web browser will then issue a warning, telling you that the web site certificate can not be verified. Therefore you should not use self-signed certificates for professional usage, as your visitors will not trust your web site to be safe.



Create new certificate

* Country

State (optional)

Locality (optional)

Organization (optional)

Organizational unit (optional)

* Common name

Save Cancel

In order to create a self-signed certificate you need to enter:

2.3.1 Country:

Enter your Country code from the list of valid country codes. For example: US for United States of America, DE for Germany or NL for Netherlands.

2.3.2 State:

Enter a state or a province name. For example: Bavaria, California, North Holland

2.3.3 Locality:

Enter a city name. For example: Munich, San Francisco, Rotterdam

2.3.4 Organization:

Enter the organization name.

2.3.5 Organizational unit:

Enter the organization unit name.

2.3.6 Common name:

The common name (CN) is the computer or server name associated with your TLS/SSL certificate. For example: MyComputer.

The generated certificate is valid for 3 years.

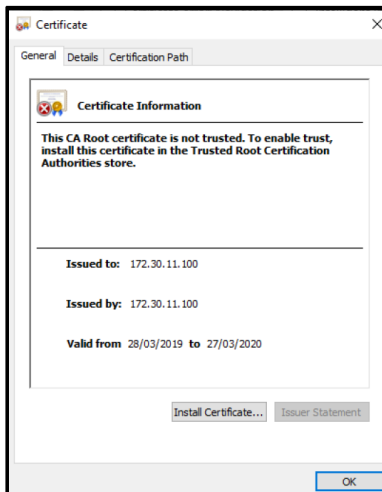
To create a self-signed certificate, provide at least the "Country code" and "Common Name".

2.4 Using self-signed certificates with BVMS

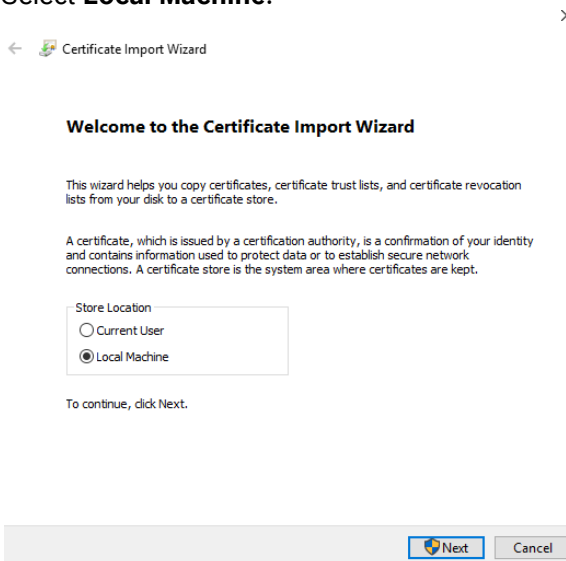
When integrating Intelligent Insights with a self-signed certificate, the BVMS operator client always shows an error message when opening a widget in the BVMS operator client image pane. In order to solve this issue, install the self-signed certificate in the trusted root certificate store of the local machine.

To install the certificate in the root certificate store of the local machine, connect to Intelligent Insights with a web browser and download the certificates. Once downloaded, install the certificate in the trusted root certificate store.

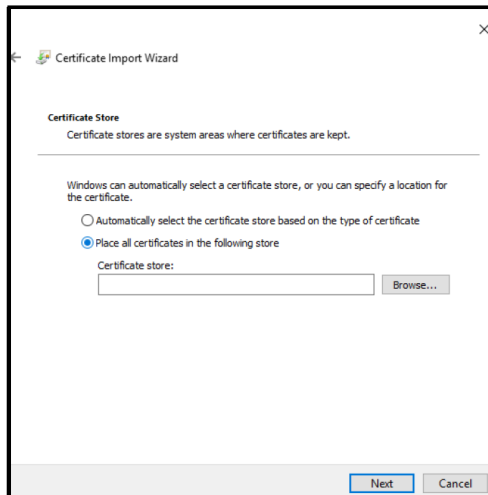
1. Double-click the downloaded certificate.
2. Click **Install certificate**.



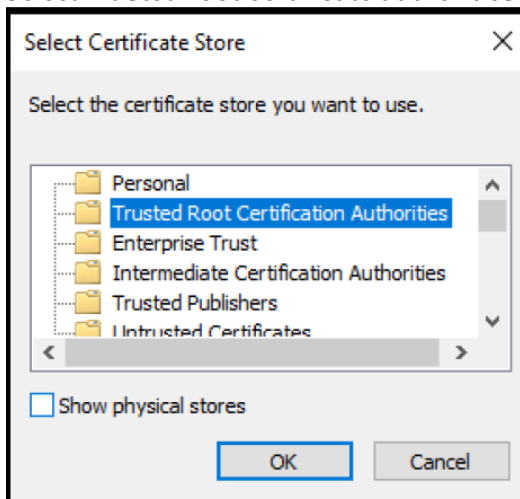
3. Select **Local Machine**.



4. Select the certificate store.



5. Select **Trusted root certificate authorities**.



6. Click **Finish** to complete the certificate installation

