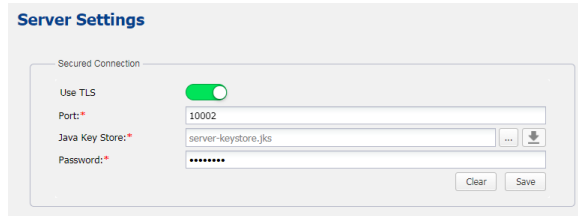


Enabling a secure connection

To enable a secure connection to Teamwork Cloud (TWCloud), you must enable TLS (Transport Layer Security) on the TWAdmin's **Server Settings** page. This page also allows you to disable the option if you do not need to use a secure connection (see the following figure). You can always enable it whenever necessary.

- [Setting up TLS in TWAdmin](#)
- [Setting up client-side TLS](#)



The screenshot shows the 'Server Settings' page in TWAdmin. Under the 'Secured Connection' section, the 'Use TLS' toggle switch is turned on and is green. Below it, the 'Port' is set to 10002. The 'Java Key Store' is set to 'server-keystore.jks', with a file selection icon to its right. The 'Password' field is masked with asterisks. At the bottom right of the settings area are 'Clear' and 'Save' buttons.

Enabling TLS protocol in TWCloud (when the option is turned on, the color changes to green).

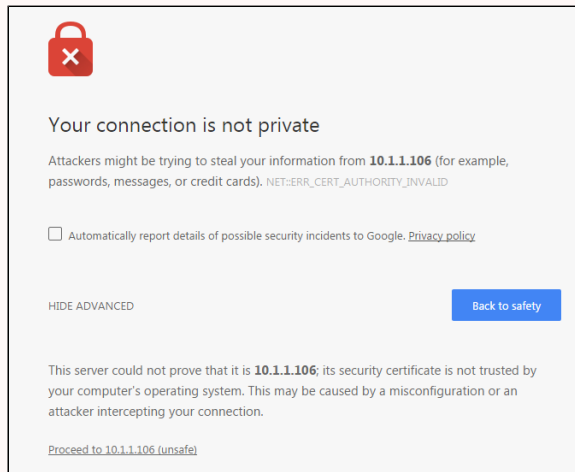


Self-signed TLS certificate warning

Teamwork Cloud Admin (TWAdmin) uses TLS (Transport Layer Security) as the security protocol to keep any information you enter on TWAdmin private and secure.

By default, your server generated an TLS certificate and signed it as being valid (self-signed certificate). The self-signed TLS certificate allows a secure connection to be established, but does not verify the authenticity of the server like the TLS certificate issued by a valid Certificate Authority (CA) does.

Trusted root certificates are embedded into popular browsers such as Internet Explorer, Firefox, and Chrome. They are used to verify all TLS certificates that the browsers encounters. If a certificate is not signed by one of these roots, the browsers display an error or warning message stating that it is untrusted. Thus, when you try to access the server via the self-signed one, you will get the error or warning in your web browser. The following figure below shows an example of the "TLS certificate not trusted" warning in Chrome.



A self-signed TLS certificate error in Google Chrome.





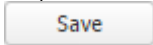
This warning tells you the TLS certificate installed on your server was self-signed and cannot be verified by the browser. You may simply let your browser accept it and continue using the server. If you are using Firefox, you can accept it and the error or warning will no longer appear. If you are using Chrome, the error or warning will appear every time you try to access your server.

To permanently mitigate this situation to avoid having the self-signed TLS certificate error or warning appear when accessing your server via TLS, it is recommended that you either:

- Replace the self-signed TLS certificate with a dedicated one issued by a trusted certificate authority.
- Establish your own root certificate authority and manually import it to each browser on all workstations.

Setting up TLS in TWAdmin

To enable a secure connection using the TLS protocol in TWAdmin

1. Click . The **Server Settings** page will open.
2. Click  to enable the TLS protocol. The TLS option will be enabled  (in green).
3. Input the port, select a **Java Key Store** file by clicking , and type the password.
4. Click .

At this point, you will be able to use MagicDraw to connect to TWCloud via the TLS connection.

Setting up client-side TLS

To enable a secure connection using the TLS protocol on the client side

1. Locate the client certificate manually.
2. Create a folder named **certs** under the MagicDraw install folder. Place the following files into the newly created **certs** folder:
 - A client certificate named **cert.jks**.
 - A file named **cert.pass** wherein the certificate password is typed.