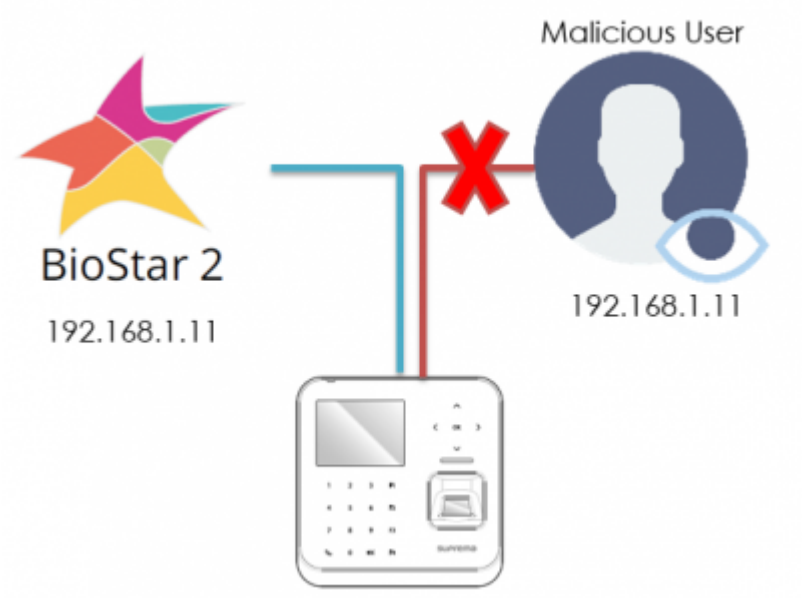
Table of Contents

System Configuration, BioStar 2, TLS, secure communication

How to configure Secure Communication between Device and Server (TLS/SSL)

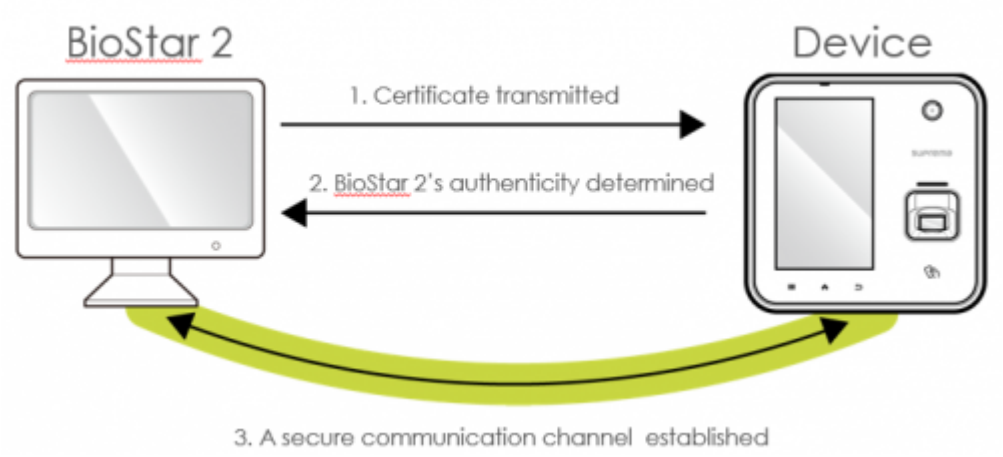
Concept

A transport layer security (TLS/SSL) feature for the communication between the server and device has been implemented in BioStar 2.4.
This feature would stop malicious users from connecting to the device by pretending to be the server with the same server IP.



1)

This security is achieved by storing a digital certificate in the device.
When the device connects to the server, it will exchange an encryption key (session key) using the digital certificate to provide server identity verification.



BioStar 2 supports TLS version 1.1 and 1.2. For more generic security information refer to the FAQ article

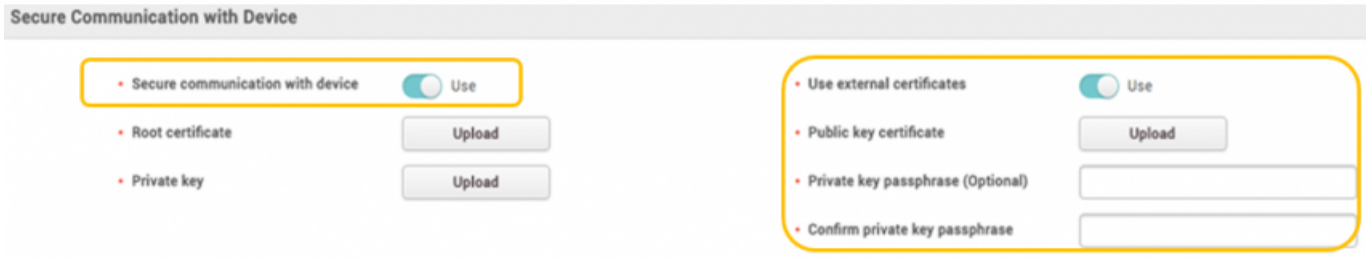
Configuration

Access to the devices can be limited while this feature is turned on.
It will take several minutes for the devices to reconnect to the server.
Port 51213 should be enabled if TLS/SS: is used.

Supported Devices / Firmware versions
- BioEntry W2 FW 1.1.0 or later
- BioStation L2 FW 1.2.0 or later
- BioStation A2 FW 1.3.0 or later
- BioStation 2 FW 1.4.0 or later
- FaceStation 2 FW 1.1.0 or later (to be released in 2018)
- CoreStation FW 1.0.0 or later
- P2 FW 1.0.0 or later

Follow the steps below to configure the secure communication. It is not turned on by default.
1. Log in to BioStar 2.
2. Click **Setting**.
3. Click **Server**.
4. On the **Secure Communication with Device** tab, set **Secure communication with device** as **Use**

If you want to use a external certificate from a CA (certificate authority) such as VeriSign, Comodo, GoDaddy and etc, check **Use external certificates** and **Upload** the file.



Caution
Do not turn off the secure communication option if the device is physically disconnected from the network while using the secure communication feature.
If the feature is turned off, the certificate of BioStar 2 will be deleted and the device will not be able to connect to the server again.
To connect the device to the server again, the certificate saved in the device must be deleted

> or the device must be reset to factory default.
> For devices without LCD such as W2 or P2 you can factory default the device with the reset buttons as shown in the device manual.
> Refer to the FAQ article: Factory Default W2 / P2

1)

icon designed by Madebyoliver from Flaticon