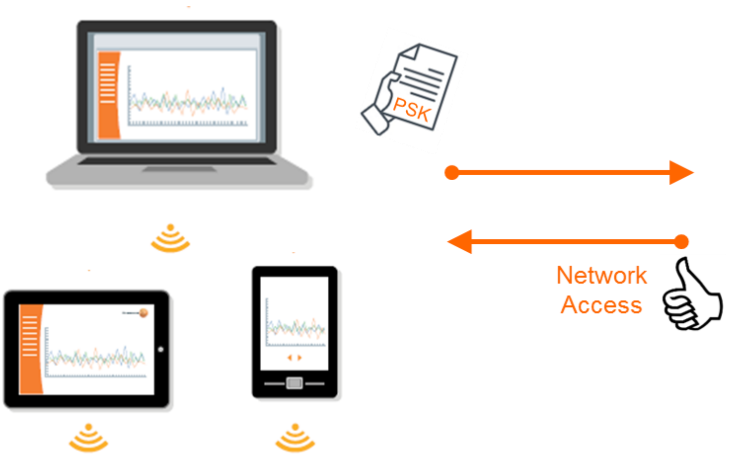
WPA2 Personal/Enterprise Configuration

1 WPA2 Basics

1.1 WPA2 Personal authentication principle

WPA2 Personal is most commonly used for private networks and networks of small companies. The Pre-Shared Key (PSK), also known as Wifi password, plays a central role in the authentication process of WPA2 Personal since it has to be known both by the client and the access point. If the client wants to access a network via the access point, the access point requires the PSK. In case the right PSK is stored on the device, network access is granted.

Note: Integration of loggers into a network using the **WPA2 Personal** security standard (with **PSK**) is possible using the Quick Start Guide on the Saveris 2 website.



1.2 WPA2 Enterprise authentication principle

There are multiple WPA2 Enterprise authentication methods that are supported by Saveris 2 loggers,which are all based on Extensible Authentication Protocol (EAP). EAP can be extended by other procedures, which leads to a variety of authentication methods. The most commonly used method is EAP-TLS (Transport Layer Security), a certificate-based authentication where the right certificates have to be stored on both the client and authentication server.

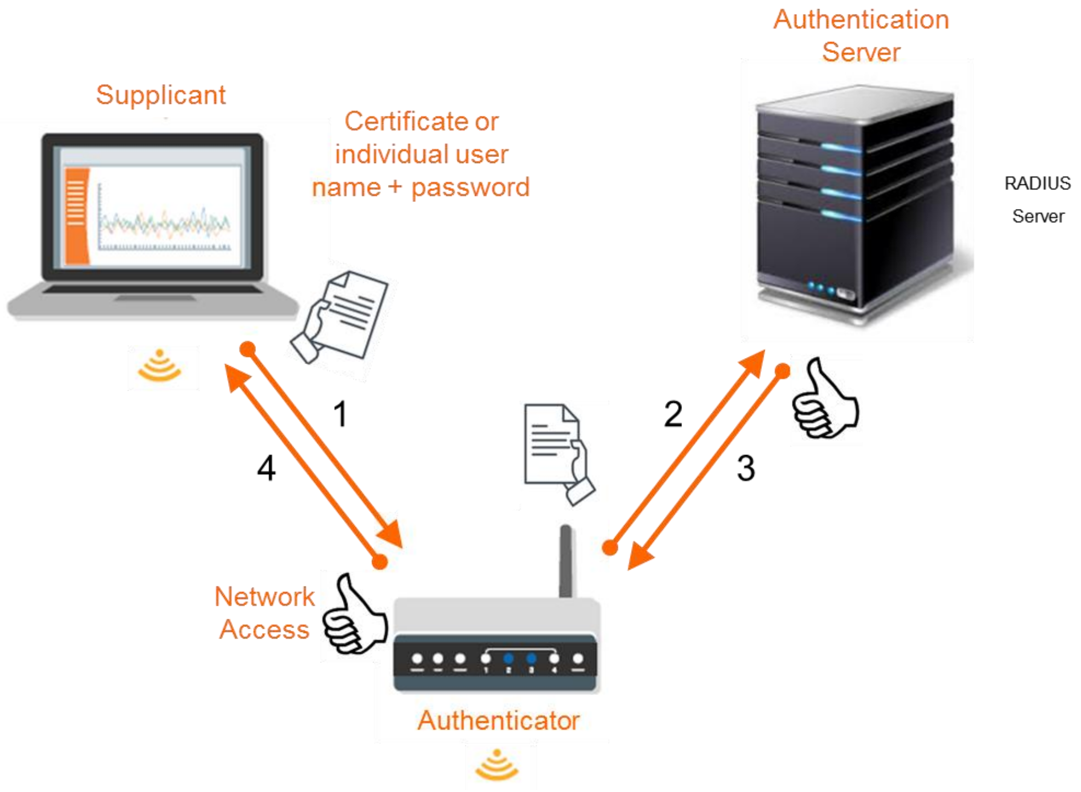
The authentication methods that are supported by Saveris 2 loggers are:

- EAP-TLS
- EAP-TTLS-TLS
- EAP-TTLS-MSCHAPv2
- EAP-TTLS-PSK
- EAP-PEAP0-TLS
- EAP-PEAP0-MSCHAPv2
- EAP-PEAP0-PSK
- EAP-PEAP1-TLS
- EAP-PEAP1-MSCHAPv2
- EAP-PEAP1-PSK

Please make sure to use the appropriate certificates and/or individual user names and passwords dependent on the chosen method.

Note: For EAP-TLS, only the following cryptographic types can be used:

- SHA1 with 160 Bit length
- SHA256 with 256 Bit length
- MD5 with 128 Bit length
- RSA with maximal 2048 Bit length
- DHE with 2048 Bit length
- ECDHE with 160 Bit length


Authentication Server
Supplicant
Certificate or individual user name + password
RADIUS Server
1
4
2
3
Network Access
Authenticator

2 Configuration of Saveris 2 loggers with WPA2 Enterprise

Generally, there are two ways to integrate Saveris 2 loggers into a WPA2 Enterprise network:

- PDF form on the logger´s mass storage
- Webpage (Hotspot mode)

2.1 Configuration via PDF form (mass storage mode)

In order to configure the logger via the PDF form from the mass storage of the logger, you need to have your Account ID at hand. In your Saveris 2 account, you can find it under **Configuration → Account ID**. Then proceed with the following steps to get to the PDF configuration file.

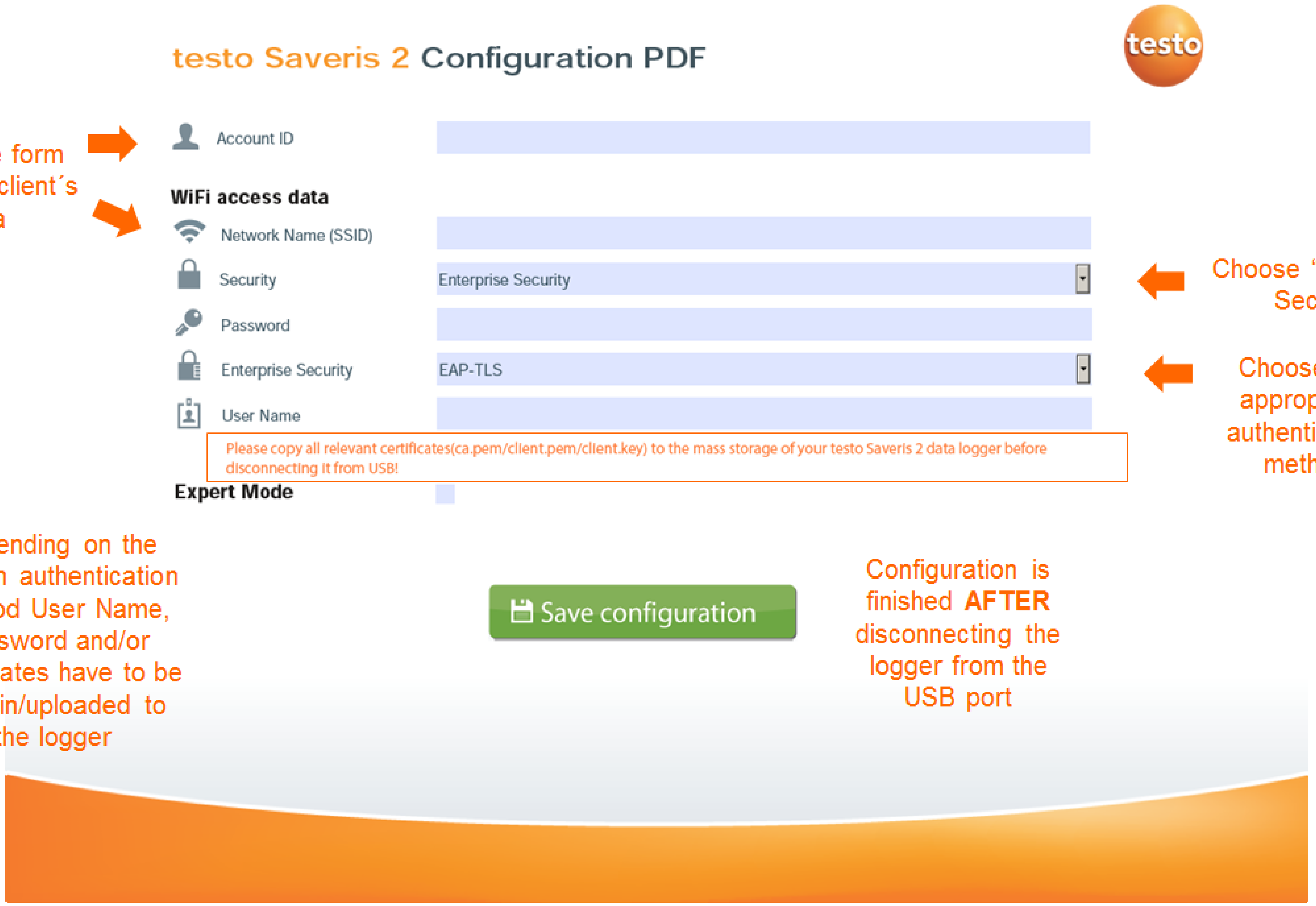
1. Connect the logger to the USB port of your computer.
2. The notification "**USb**" on the logger display shows that the logger is in mass storage mode.
3. Open the **WifiConf.pdf** file on the external drive **SAVERIS 2**.

The next steps are done in the PDF file (summarised in the figure on the next page).

4. Copy your **Account ID** and paste it in the relevant field on the PDF form.
5. Enter the network name (**SSID**).
6. Choose the appropriate **authentication method**.
7. Depending on the chosen authentication method, the individual **user name and password** have to be typed in and/or all relevant **certificates** have to be copied to the logger´s mass storage.

   Note: The two most common WPA2 Enterprise authentication methods are **EAP-TLS** and **EAP-PEAP0-MSCHAPv2.**
   EAP-TLS needs certificates for authentication; **EAP-PEAP0-MSCHAPv2** needs login data.
8. Press the **"Save Configuration"** button.
9. To finish the configuration, the logger has to be **removed from the USB port** of the computer.
10. The logger now connects to the network and accesses the Testo Cloud.

Fill in the form using the client´s data



testo Saveris 2 Configuration PDF

Account ID

WiFi access data

Network Name (SSID)

Security: Enterprise Security

Password

Enterprise Security: EAP-TLS

User Name

Please copy all relevant certificates(ca.pem/client.pem/client.key) to the mass storage of your testo Saveris 2 data logger before disconnecting it from USB!

Expert Mode

Choose “Enterprise Security“

Choose the appropriate authentication method

Depending on the chosen authentication method User Name, password and/or certificates have to be filled in/uploaded to the logger

Configuration is finished **AFTER** disconnecting the logger from the USB port

2.2 Configuration via web interface (hotspot mode)

To perform the configuration of the logger via web interface, the logger has to be brought into Hotspot mode. Before starting the configuration, you should have the Saveris 2 Account ID at hand. It can be found online in the testo Saveris 2 software under **Configuration → Account ID**. Then execute the following steps in order to access the web interface.

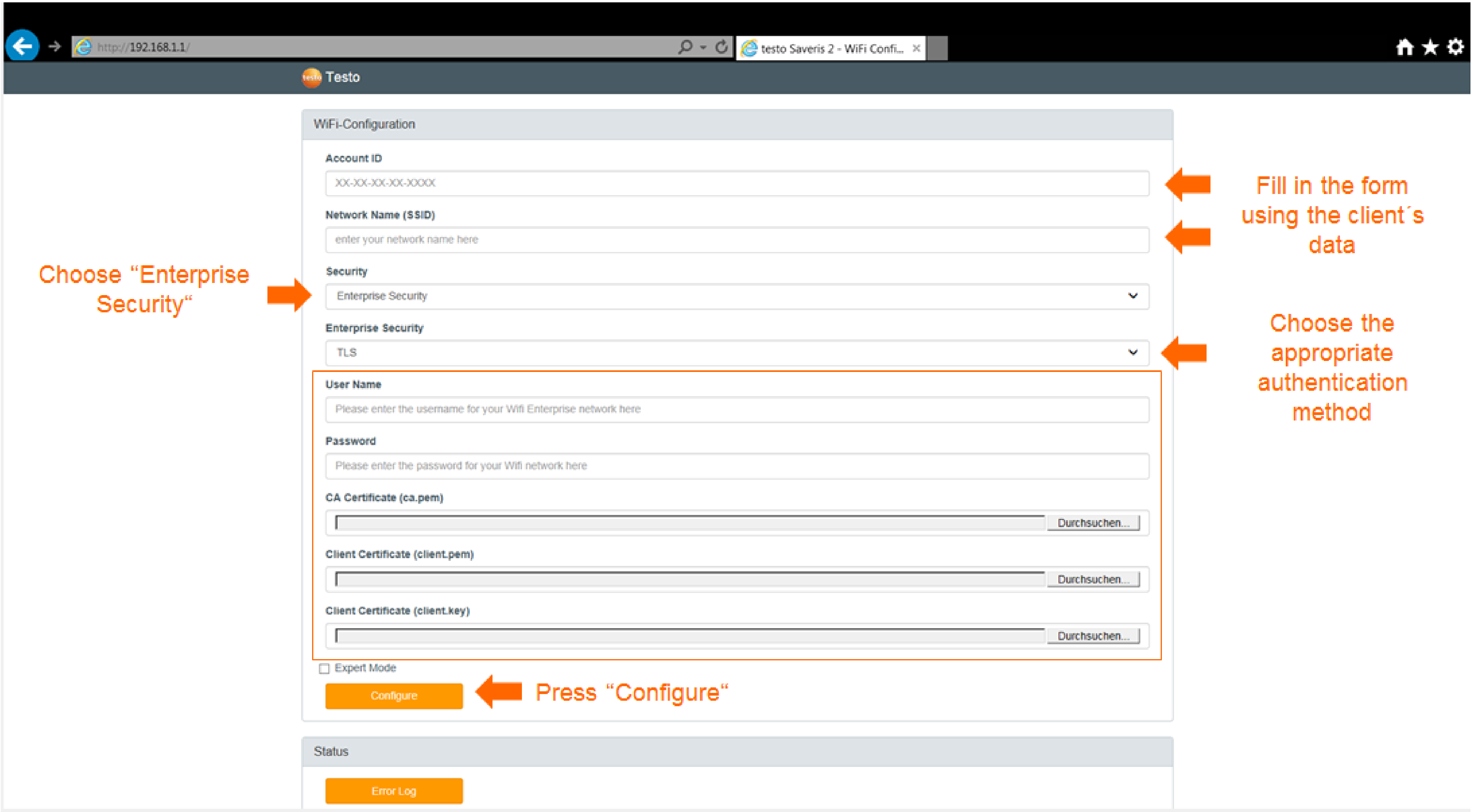
1. → If the logger has **not been configured before,** press the button on the front side of the logger **shortly.**

   → If the logger has **already been configured before,** press the button on the front side of the logger for **3 seconds.**
2. The logger changes to hotspot mode, indicated by the notification "**Conf**" on the display.
3. Connect your computer or tablet to the open network named **Saveris2 SNxxxxxxxx**. The 8-digit number at the end of the name is the serial number of the particular data logger.

   Note: Only one device can be connected to the logger´s hotspot. If someone connects to the hotspot by accident, the procedure has to be started again.
4. When you are connected to the hotspot, open your web browser and type the IP **192.168.1.1** into the address bar to open the web interface.
5. Copy your Account ID and paste it in the relevant array on the PDF form.
6. Enter the Network Name (SSID).
7. Choose the appropriate **authentication method**.
8. Depending on the chosen authentication method, the individual user name and password have to be typed in and/or all relevant certificates have to be copied to the logger´s mass storage.

   Note: The two most common WPA2 Enterprise authentication methods are **EAP-TLS** and **EAP-PEAP0-MSCHAPv2.**

   EAP-TLS needs certificates for authentication; **EAP-PEAP0-MSCHAPv2** needs login data.
9. The logger now connects to the network and accesses the Testo Cloud.



WiFi-Configuration

Account ID

XX-XX-XX-XX-XXXX

Network Name (SSID)

enter your network name here

Security

Enterprise Security

Enterprise Security

TLS

User Name

Please enter the username for your Wifi Enterprise network here

Password

Please enter the password for your Wifi network here

CA Certificate (ca.pem)

Durchsuchen...

Client Certificate (client.pem)

Durchsuchen...

Client Certificate (client.key)

Durchsuchen...

□ Expert Mode

Configure

Status

Error Log

Fill in the form using the client´s data

Choose “Enterprise Security“

Choose the appropriate authentication method

Press “Configure“

3 Troubleshooting – common mistakes during WPA2 Enterprise configuration

It is important that the **certificates** needed for certain authentication methods are not uploaded in the **wrong format**. Please make sure that the required certificates come in the right format (e.g. ca.pem, client.pem, client.key).

There is also the possibility that the **wrong authentication method** was chosen during the configuration. The supported methods are listed in chapter 1.2.

Infrastructural issues in the client’s network can also lead to problems; e.g. a hidden SSID of the company´s network. Always make sure that the right SSID is used.