WPA2 Enterprise Configuration
(New Generation of Saveris 2 Loggers 0572 203x)

Table of Contents

1 The new generation of Saveris 2 loggers

1.1 Overview

An overview of the new and old generation of Saveris 2 loggers with related order numbers and availabilities is shown in the following table. The new generation is identifiable by order numbers 0572 203x instead of 0572 200x for the old loggers.

Name	Order number old	Available until (estimated)	Order number new	Available from
testo Saveris 2-T1	0572 2001	05/2017	0572 2031	01.01.2017
testo Saveris 2-T2	0572 2002	03/2017	0572 2032	01.01.2017
testo Saveris 2-T3	0572 2003	05/2017	0572 2033	01.01.2017
testo Saveris 2-H1	0572 2004	03/2017	0572 2034	01.01.2017
testo Saveris 2-H2	0572 2005	03/2017	0572 2035	01.01.2017

1.2 What is new?

The new generation of Saveris 2 loggers contains several significant improvements like an improved calibration process, more stable communication and prolonged battery life time (for details please see sales information no. 4275). Besides the design update the Saveris 2-H1 logger has received in order to improve the air circulation around the humidity sensor, the design of all other data loggers stays the same as before. For the new generation of data loggers the external probe list stays the same with the following exceptions and additions.

External probe	Order No.	Connectable to	Comment
Stump temp./ humidity probe	0572 2151	testo Saveris 2-H2	Existing analog probe, can only be used with data logger 0572 2005 (not compatible with 0572 2035)
Temp./humidity probe with cable	0572 6172	testo Saveris 2-H2	Existing analog probe, can only be used with data logger 0572 2005 (not compatible with 0572 2035)
Thin temp./humidity probe with cable	0572 6174	testo Saveris 2-H2	Existing analog probe, can only be used with data logger 0572 2005 (not compatible with 0572 2035)
Temp./humidity probe with cable	0572 2155	testo Saveris 2-H2	New digital probe, can only be used with data logger 0572 2035 (not compatible with 0572 2005)
Stump temp./ humidity probe	0572 2154	testo Saveris 2-H2	New digital probe, can only be used with data logger 0572 2035 (not compatible with 0572 2005)
Stump temp. probe	0572 2153	testo Saveris 2-T2	New digital probe, can only be used with data logger 0572 2032 (not compatible with 0572 2002)

The most significant improvement of the new generation of Saveris 2 loggers is characterized by the support of networks that work with WPA2 Enterprise. The aim of this document is to give an introduction into the WPA2 Enterprise standard, to provide instructions how the new Saveris 2 loggers can be incorporated in a WPA2 Enterprise network and to give examples of common errors that can occur.

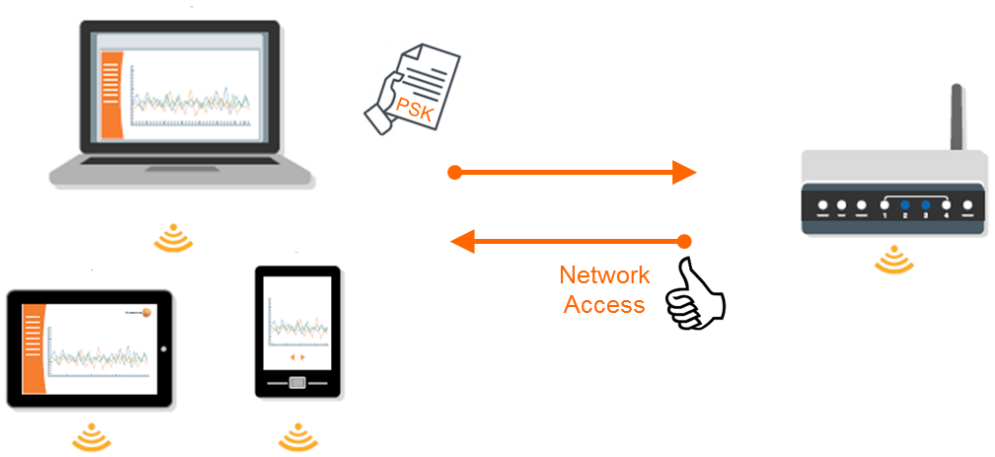
2 WPA2 Basics

2.1 Introduction

WPA2 (Wifi Protected Access 2) is an implementation of the IEEE 802.11i standard for authentication and encryption. It is based on AES, the Advanced Encryption Standard, which was developed in 2001. WPA2 replaced the more insecure WPA standard, which used TKIP (Temporal Key Integrity Protocol) as encryption method. Within WPA2 two modes are distinguished, which are both supported by the new generation of Saveris 2 Wifi loggers: WPA2 Personal and WPA2 Enterprise. The most fundamental difference between both WPA2 types is the way how the authentication of the client and the access point is performed.

2.2 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 the central role within the authentication process of WPA2 Personal since it has to be known both to the client and the access point. If the client wants to access the network via the access point, the access point asks for the PSK. In the case the the right PSK is stored on the device network access is granted. One weakness of the PSK principle is that security can only be guaranteed, if a strong password (i.e. complex and long) is used. A further disadvantage of WPA2 Personal lies in the fact that single users cannot be managed. Every user knows the same PSK for the particular Access Point (identifiable by its SSID).



2.3 WPA2 Enterprise authentication principle

During the authentication process of WPA2 Enterprise three participants are distinguished: supplicant (client), authenticator (access point) and an additional authentication server. In most cases this authentication server is a RADIUS server.

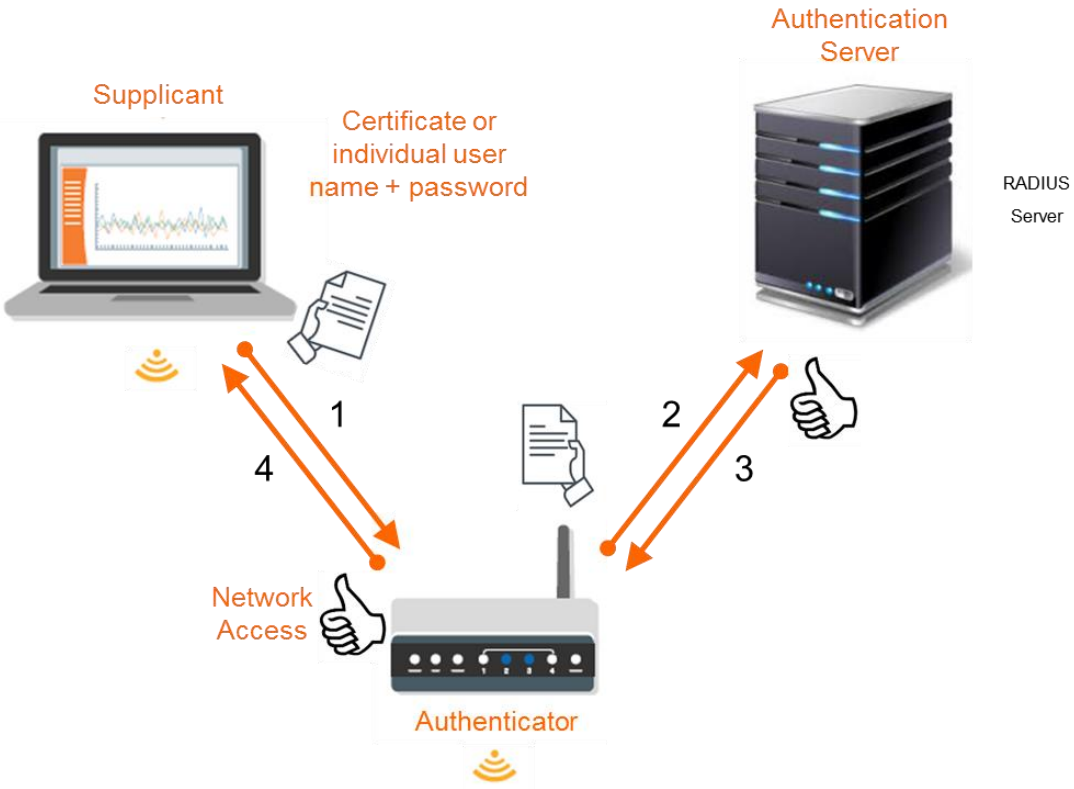
When the supplicant connects to the authenticator and applies for network access the authenticator asks for authentication. This authentication can be achieved by the right user name and password that are assigned to the supplicant and/or certificates. Certificates are data files that are not only used for authentication but contain also for example public keys that are used for the later encryption of the session data. The application of the supplicant to get access to the network is checked by the authenticator and forwarded to the authentication server, which decides if access is given to the supplicant.

There are multiple authentication methods that are supported by the new generation of Saveris 2 loggers. They are all based on Extensible Authentication Protocol (EAP) (a protocol, which ensures that access to the network is only possible after successful authentication and knows only authentication requests and authentication replies). EAP can be extended by other procedures, which leads to several authentication methods. One method that is most commonly used is EAP-TLS (Transport Layer Security). This method is a certificated based authentication where on both the client and authentication server the right certificates have to be stored.

The authentication methods that are supported by the new generation of Saveris 2 loggers are (in addition to 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

It is important to use the appropriate certificates and/or individual user names and passwords dependent on the particular method that was chosen. The two most commonly used methods are EAP-TLS and EAP-PEAP0-MSCHAPv2.



3 Configuration of Saveris 2 loggers with WPA2 Enterprise

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

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

Since a since a “plug-and-play” configuration via Quick Start Guide as it is known from the old generation of loggers is not supported in a WPA2 Enterprise network. Moreover, the Testo Saveris 2 App does not support WPA2 Enterprise networks, yet. This limits the integration of the loggers the two mentioned methods, which are described in detail in the following sections.

Note: Regarding the integration of the new loggers into a network using the **WPA2 Personal** security standard (with **PSK**), everything stays as it is known from the old generation.

3.1 Configuration via PDF form (mass storage mode)

To be able to configure the logger via the PDF form from the mass storage of the logger you need to have your Account ID at hand. After logging in to your Saveris 2 account, you can find it under **Configuration → Account ID**. Then execute the following steps to get to the PDF configuration file.

1. Connect the data logger to the PC´s USB port.
2. The notification “**USb**” on the logger´s 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 (summarized 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 authentication method that was chosen 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 that are used 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 PC
10. The logger then is ready to connect to the network and accesses the Testo Cloud.


testo Saveris 2 Configuration PDF
Fill in the form using the client´s data
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
Save configuration
Configuration is finished AFTER disconnecting the logger from the USB port

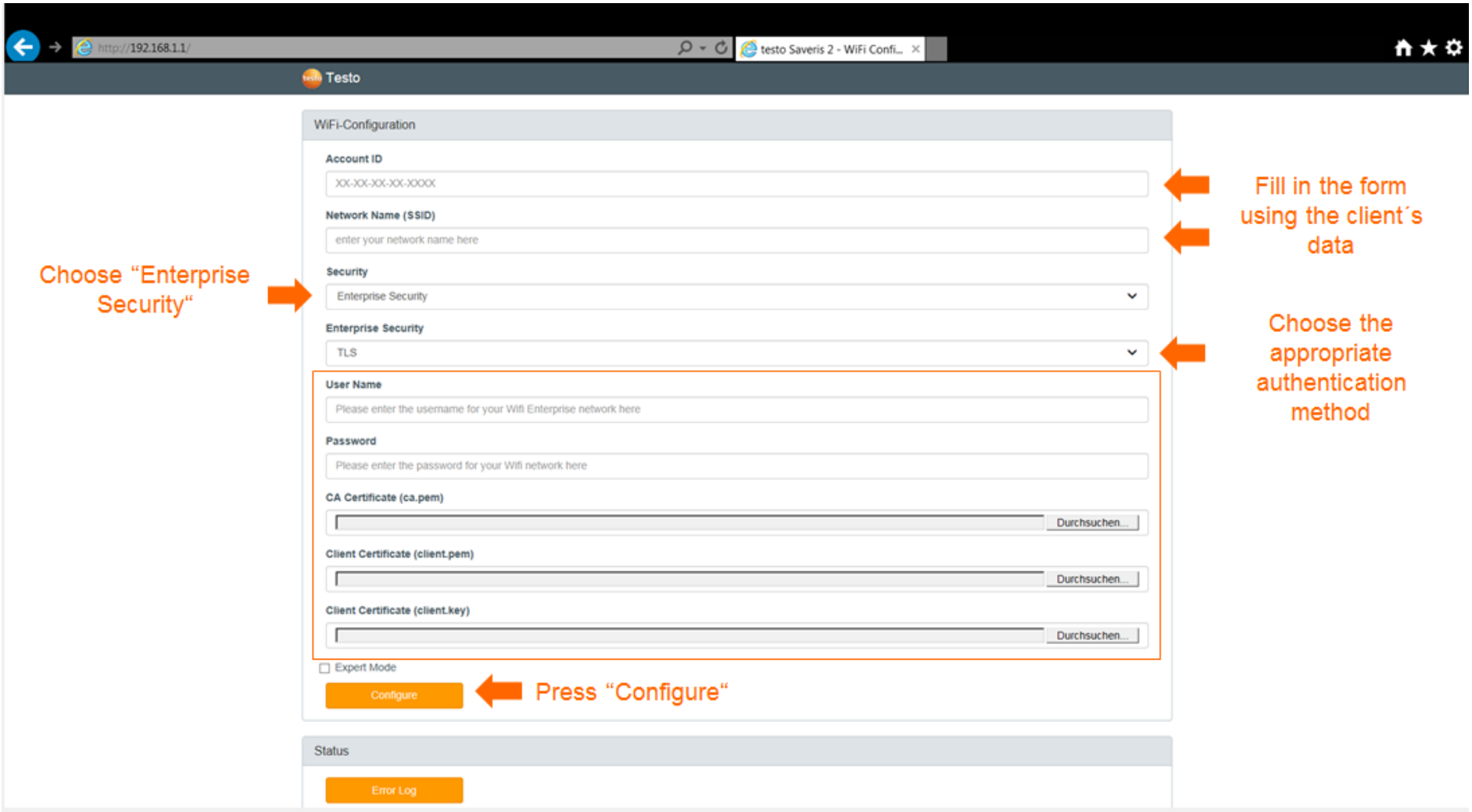
3.2 Configuration via web interface (hotspot mode)

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 again 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 PC or tablet to the open network with the name **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 field to open the web interface.
5. Copy your Account ID and paste it in the relevant field on the PDF form.
6. Enter the Network Name (SSID)
7. Choose the appropriate **authentication method**
8. Depending on the authentication method that was chosen 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 that are used are **EAP-TLS** and **EAP-PEAP0-MSCHAPv2.**
   EAP-TLS needs certificates for authentication, **EAP-PEAP0-MSCHAPv2** needs login data.
9. Press the "Configure" button and the logger is ready to connect to the network and the Testo Cloud


http://192.168.1.1/
testo Saveris 2 - WiFi Confi...
Testo
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
Choose "Enterprise Security"
Fill in the form using the client´s data
Choose the appropriate authentication method
Press "Configure"

4 Troubleshooting – The most common mistakes

In the following section the most common mistakes that can occur during the configuration of Saveris 2 loggers in a Wifi network with WPA2 Enterprise are described. These mistakes can be a guideline to get a first idea of possible reasons why something might not work properly.

Several data has to be typed in manually (e.g. Account ID, SSID, user name, passwords,...), which can lead to **spelling mistakes**. This is a source of errors that can be avoided very easily but occurs in various cases. Even the smallest mistake can lead to problems.

Furthermore, it is very important that the **certificates** that are 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 methods that are supported are EAP-TLS, EAP-TTLS-TLS, EAP-TTLS-PSK, EAP-TTLS-MSCHAPv2, EAP-PEAP0-TLS, EAP-PEAP0-MSCHAPv2, EAP-PEAP0-PSK, EAP-PEAP1-TLS, EAP-PEAP1-MSCHAPv2, EAP-PEAP1-PSK. The two methods that are most commonly used are **EAP-TLS** and **EAP-PEAP0-MSCHAPv2**.

Infrastructural issues in the clients network can also lead to problems. An example for this kind of issues is a hidden SSID of the company´s network that supports WPA2 Enterprise, which occurs from time to time. Here you have to make sure that the right SSID is used.