R&S®SMW200A
Vector Signal Generator
Instrument Security Procedures

ROHDE & SCHWARZ

Make ideas real

This document describes the types of memory and their use in the R&S®SMW200A.

While every effort has been made to ensure the accuracy of the information herein, it is provided without warranty. Design iteration and revisions may result in minor differences between the information provided here and your product.

Contents

1   Overview

Securing important information is crucial in many applications.

Generally, highly secured environments do not allow any test equipment to leave the area unless it can be proven that no user information leaves with the test equipment, e.g. to be calibrated.

"Regarding sanitization, the principal concern is ensuring that data is not unintentionally released" [1].

This document provides a statement regarding the volatility of the memory types used and specifies the steps required to sanitize an instrument.

The procedures in this document follow "NIST Special Publication 800-88: Guidelines for Media Sanitization" [1].

In addition, recommendations are provided to safeguard information on the product.

References

See the following literature for further information.

[1]   **Kissel Richard L. [et al.]** Guidelines for Media Sanitization = Special Publication (NIST SP) = NIST SP - 800-88 Rev 1. - Gaithersburg : [s.n.], December 17, 2014.

[2]   **National Industrial Security Program Authorization Office** Defense Security Service (DSS) Assessment and Authorization Process Manual (DAAPM). - May 6, 2019.

[3]   **ACSC Australian Cyber Security Centre** Australian Government Information Security Manual, January 2020.

2 Instrument models covered

Table 2-1: R&S SMW200A models

Product name	Order number
R&S SMW200A	1412.0000.02

3 Security terms and definitions

Terms defined in Guidelines for Media Sanitization

According to NIST Special Publication 800-88 [1]: "Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort." It defines the following categories of sanitization:

- **"Sanitization"**
  "Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort."
- **"Clear"**
  "Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported)."
- **"Purge"**
  "Purge applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques."
- **"Destroy"**
  "Destroy renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data."

Control of media

Another option to secure sensitive information is to keep physical media within the classified area, see [1], paragraph 4.4.

Volatile memory

"Memory components that do not retain data after removal of all electrical power sources, and when reinserted into a similarly configured system, are considered volatile memory components." [2]

Typical examples are RAM, e.g. SDRAM.

Non-volatile memory

"Components that retain data when all power sources are discontinued are non-volatile memory components." [2].

In the context of this document, non-volatile memory components are non-user accessible internal memory types, e.g. EEPROM, Flash, etc.

Media

Media are types of non-volatile memory components. In the context of this document, media are user-accessible and retain data when you turn off power.

Media types are Hard Disk Drives (HDD), Solid State Drives (SSD), Memory Cards, e.g. SD, microSD, CFast, etc., USB removable media, e.g. Pen Drives, Memory Sticks, Thumb Drives, etc. and similar technologies.

4 Statement of volatility

The R&S SMW200A contains various memory components. See the subsequent sections for a detailed description regarding type, size, usage and location.

Notes on memory sizes

Due to the continuous development of memory components, the listed values of memory sizes may not represent the current, but the minimal configuration.

This document uses the common notation kbyte, Mbyte and Gbyte for memory sizes, although the prefix multiplication factor is 1024.

4.1 Volatile memory

Volatile memory modules refer to non-accessible internal storage devices, as described in Security terms and definitions > Volatile memory.

Table 4-1: Types of volatile memory

Memory type	Location	Size	Content / Function	User modifiable
SDRAM	CPU board	up to 8 Gbyte	Temporary information storage for: • Operating system • Instrument firmware • User data	Yes
SDRAM	Wideband baseband board	8 Gbyte	Temporary information storage for arbitrary waveforms	Yes
SDRAM	Baseband board			

4.2 Non-volatile memory

Non-volatile memory modules refer to non-accessible internal storage devices, as described in Security terms and definitions > Non-volatile memory.

Table 4-2: Types of non-volatile memory

Memory type	Location	Size	Content / Function	User modifiable
EEPROM	CPU board	256 byte	Board identification data	No
Flash	CPU board	up to 8 Mbyte	BIOS	No
EEPROM/Flash	One per module	up to 32 Mbyte	Module-specific data: • Board identification data • Board internal calibration data (if applicable) • FPGA configuration (if applicable)	No

4.3 Media

Media memory modules refer to non-volatile storage devices, as described in Security terms and definitions > Media.

Table 4-3: Types of media memory modules

Memory type	Location	Size	Content / Function	User modifiable

Hard disk drive (HDD) (removable)
 	
or
 	
Solid-state drive (SSD, option R&S SMW-B93) (removable)
	Rear of the R&S SMW200A	from 160 Gbyte
		
		256 Gbyte
			• Operating system
			• Instrument firmware
			• User data:
			  – Instrument settings and setups
			  – Waveform data
			  – Generic user data storage
			  – HUMS data
				Yes

5 Instrument sanitization procedure

(i) **Risk of losing operability**

The HDD/SSD memory module holds the operating system. Removing the HDD/SSD memory module makes the instrument unusable.

We recommend that you keep a second non-classified HDD/SSD memory module for use outside the secured area.

5.1 Volatile memory

You can purge the volatile memory by following the procedure below. The sanitization procedure complies with the definition of NIST [1], see "Terms defined in Guidelines for Media Sanitization" on page 4.

To turn off and remove power

1. Turn off the R&S SMW200A.

2. Disconnect the power plug.

   Leave the instrument powered off at least for five minutes to make sure that all volatile memory modules lose their contents, see [3].

5.2 Non-volatile memory

The non-volatile memories do not contain user data. Therefore no sanitization procedure is required.

5.3 Media

To purge the non-volatile memory, you have the following options:

- Enable the volatile mode, provided by the instrument, see Chapter 9.1, "Volatile mode", on page 11
- Execute the sanitization function to purge the user data, see "To sanitize the internal memory" on page 8
- Remove the media memory form the R&S SMW200A, see "To remove the HDD/SSD memory module at the rear of the instrument" on page 8.

The sanitization procedures comply with the definition of NIST [1], see "Terms defined in Guidelines for Media Sanitization" on page 4.

To sanitize the internal memory

As an alternative, you can purge the HDD/SSD memory module by executing the sanitization procedure provided on the instrument.

Access:

1. Select "System Config > Setup > Security".

2. Select "Security".

3. In the "General" tab, select the "Disk & Memory" side tab.
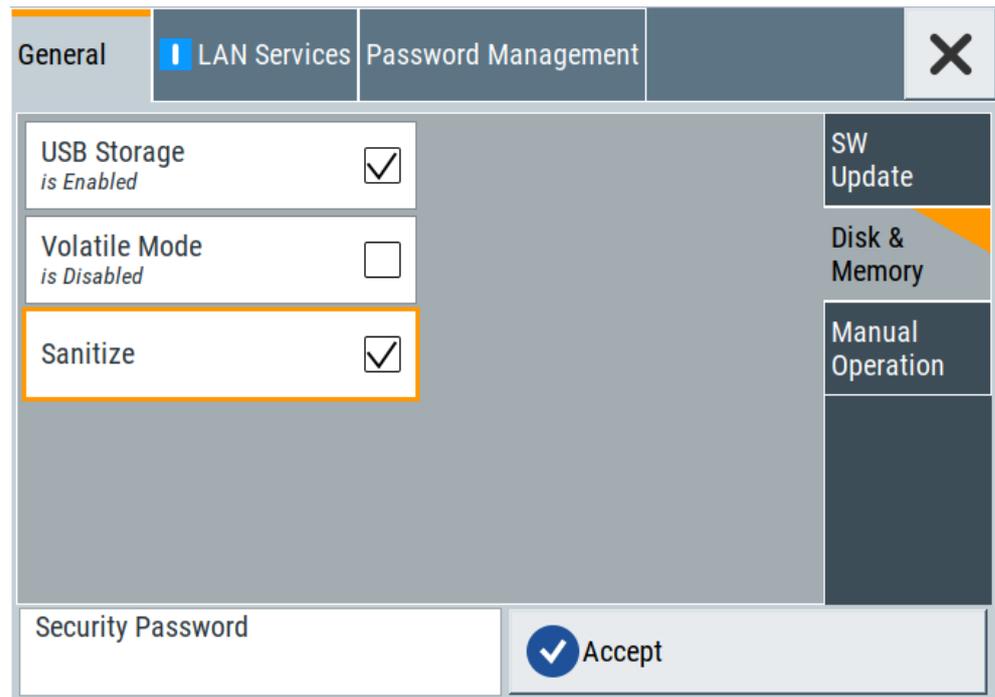
4. Enable "Sanitize".

5. Enter the "Security Password".

6. Confirm with "Accept".

7. **NOTICE!** Risk of losing instrument operability when interrupting the sanitization procedure. Do not turn off or disconnect the R&S SMW200A from the mains while the sanitization procedure is running.

   The sanitization procedure takes approximately 30 minutes.
   Wait until the instrument confirms the completed sanitization.

To remove the HDD/SSD memory module at the rear of the instrument

1. **NOTICE!** Risk of losing data. Do not remove the HDD/SSD memory module during operation as data can get lost.

   Turn off the R&S SMW200A and disconnect the power plug.

2. **NOTICE!** Risk of losing operability. The HDD/SSD memory module holds the operating system. Removing the HDD/SSD memory module makes the instrument unusable.
Use a second non-classified HDD/SSD memory module for use outside the secured area.

Locate the HDD/SSD memory module.

Figure 5-1: Location of the hard disk drive / solid-state drive

3. Unscrew the two knurled screws.

4. Remove the HDD/SSD memory module from the R&S SMW200A.

5. Keep the memory device under organizational control.

6 Operability outside secured area

As the HDD/SSD memory module holds the operating system, the R&S SMW200A cannot be operated without a HDD/SSD memory module. For servicing and calibration, Rohde & Schwarz provides a separate HDD/SSD memory module (option R&S SMW-B93) that contains the operating system and required instrument data.

To restore operability outside the secured area

1. Install a non-classified HDD/SSD memory module (option R&S SMW-B93).

2. Turn on the R&S SMW200A.

The R&S SMW200A can start the operating system.

To return to the secured area

► Before reentering the secured area, remove the non-classified HDD/SSD memory module.

To restore operability inside secured area

1. Install the classified HDD/SSD memory module.

2. Connect the instrument to the power supply.

    The R&S SMW200A is ready for use.

7   Validity of instrument calibration

The EEPROM and Flash memories are the only memory types used to hold permanent adjustment values required to maintain the validity of the R&S SMW200A's calibration. Therefore, the sanitization procedures do not affect the validity of the instrument's calibration.

8   Security features

This section leads you to the information on how to use the security features to protect the R&S SMW200A from unauthorized access of classified information saved or displayed in the instrument.

8.1   Considerations for USB interfaces

USB ports can pose a security risk in high-security locations. Generally, this risk comes from small USB pen drives, also known as memory sticks or key drives. They can be easily concealed and can quickly read/write several Gbyte of data.

The R&S SMW200A enables you, to disable the USB storage to prevent data being written to a USB memory device.

How to: Recommended security settings > USB interfaces12

8.2   Considerations for LAN interfaces

In a LAN, the interface can pose a security risk due to unauthorized data access during operation.

The R&S SMW200A enables you, to disable the LAN interface and individually enable or disable the supported LAN interface services.

How to: Recommended security settings > Chapter 9.3, "LAN interfaces and services", on page 13

8.3 Considerations for the user interface

To prevent unauthorized personnel from reading the display, you can disable the user interface, e.g. when you remotely control the instrument from a different location. You can lock only the status bar in the display, the entire screen and also the control elements on the front panel.

How to: see Recommended security settings > Chapter 9.4, "Graphical user interface (GUI)", on page 15.

9 Recommended security settings

Basically, see the user manual, chapter "General Instrument Functions > Using the Security Settings" for the security concept of the R&S SMW200A, including instructions on how to prevent unauthorized access.

The user manual is provided for download on the product page.

See www.rohde-schwarz.com/manual/smw200a.

The following sections describe measures that protect from unauthorized access during operation, and procedures that enable you to remove user data before issuing the instrument outside the secure environment.

9.1 Volatile mode

To activate the volatile mode

You can protect the internal memory of the HDD/SSD memory module (hard disk drive / solid state drive) from saving user data permanently by activating the volatile mode on the instrument:

Access:

1. Select "System Config > Setup > Security".

2. Select "Security".

3. In the "General" tab, select the "Disk & Memory" side tab.
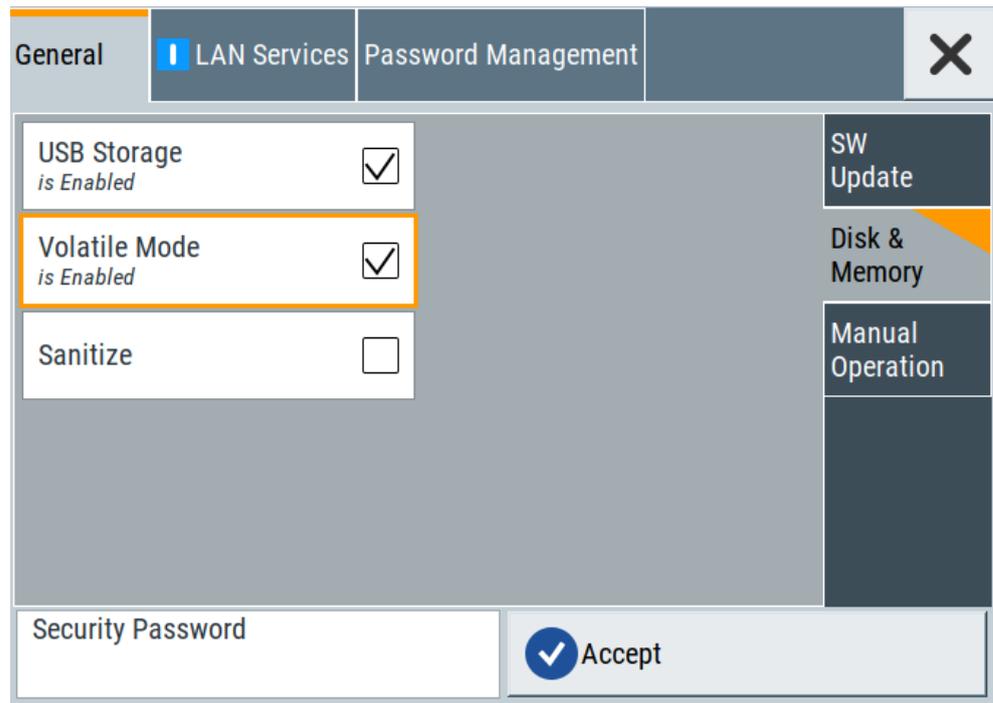
4.   Enable "Volatile".

5.   Enter the "Security Password".

6.   Confirm with "Accept".

     When enabled, the R&S SMW200A saves user data and instrument setups on the
     volatile memory (SDRAM).

9.2 USB interfaces

There are special considerations for R&S SMW200A USB ports to avoid unauthorized
data access in a high-security location.

To disable USB ports for writing user data

To disable the write capability on the USB ports of the R&S SMW200A:

1.   Select "System Config > Setup > Security".

2.   Select "Security".

3.   In the "General" tab, select the "Disk & Memory" side tab.

4.   Disable "USB Storage".

5.   Enter the "Security Password".

6. Confirm with "Accept".
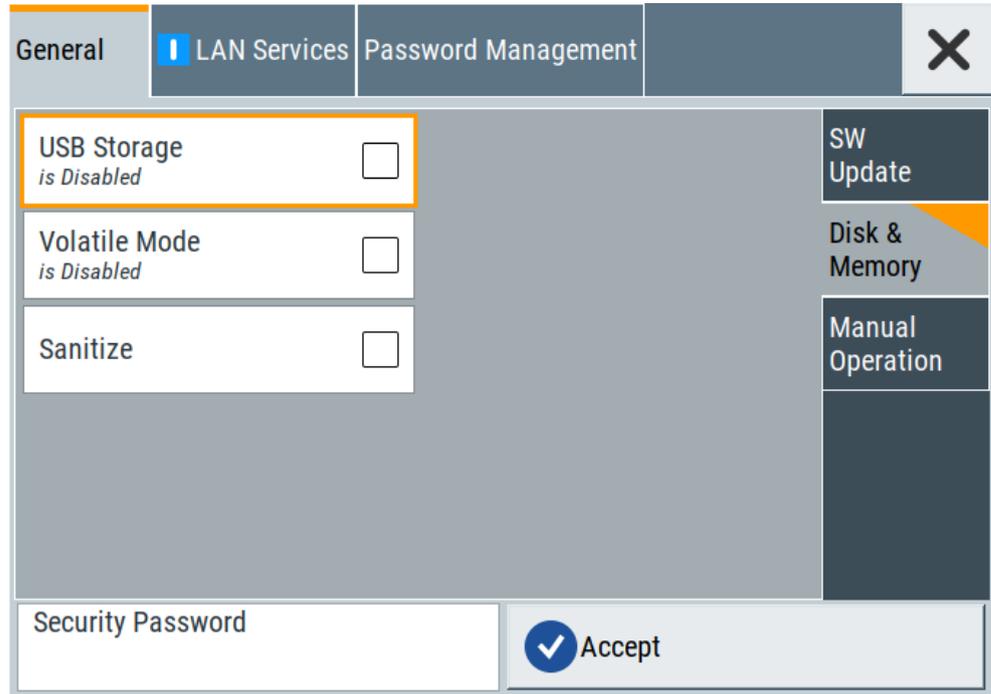
When disabled, the R&S SMW200A does not accept any USB memory device. After reboot, it also disables the USB write capability.

The setting does not affect USB devices without memory, such as a connected mouse or keyboard.

ⓘ Remove all USB memory devices before disabling the USB storage. If any USB memory device remains connected, disabling is blocked, and the instrument returns a warning message.

9.3 LAN interfaces and services

To protect the instrument against unauthorized data access in a high-security location, you can disable the LAN interface and individually enable or disable the supported LAN interface services.

We recommend that you disable all unused LAN ports and services.

To disable LAN ports and services

To disable the LAN ports and services of the R&S SMW200A:

1. Select "System Config > Setup > Security".

2. Select "Security".

3. Select "LAN Services".

4. In the "Common Services" side tab, disable the "LAN Interface".
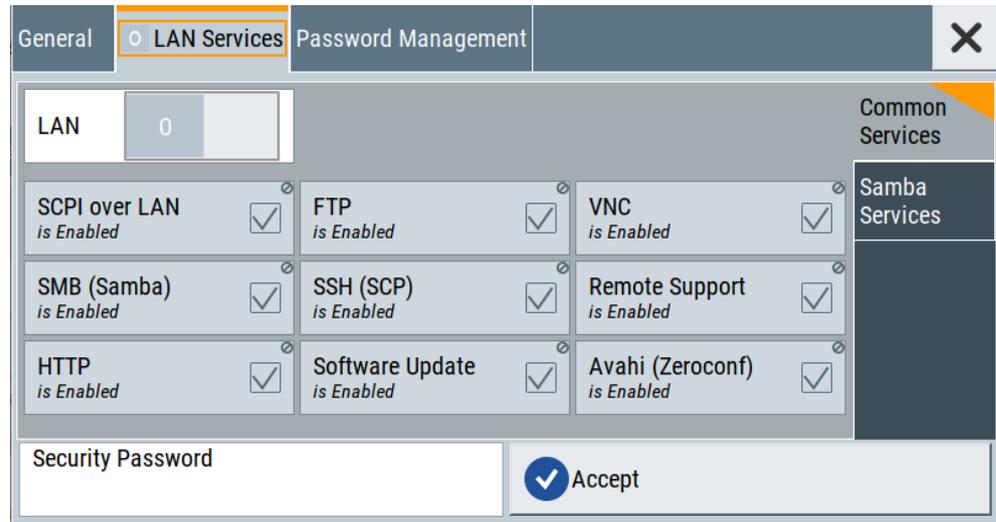
You can also enable or disable LAN services individually, e.g. select "FTP > Off" or "VNC > Off".

5. Select the "Samba Services" side tab.
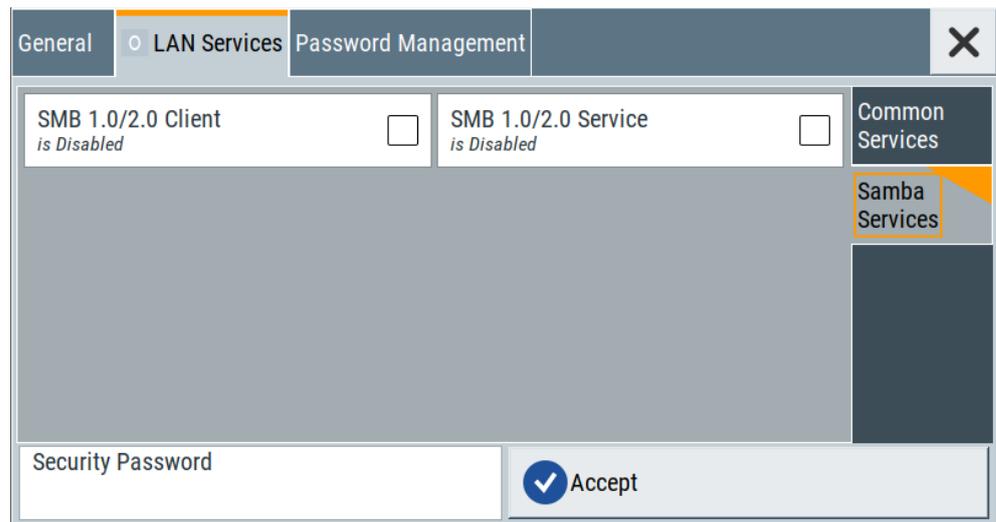
In this tab, you can enable or disable predecessor versions of the SMB client and SMB server.

6. Enter the "Security Password".

7. Confirm with "Accept"

When disabled, it is not possible to establish a LAN connection to the R&S SMW200A, or over the individually disabled services.

9.4 Graphical user interface (GUI)

To protect the instrument against unauthorized personnel from reading the display, you can lock the display and the front panel controls.

To disable frequency and level indication in the status bar

These settings are useful to prevent unauthorized personnel from reading the display, when you remotely control the instrument from a different location.

1. Select "System Config > Setup > Security".

2. Select "Security".

3. In the "General" tab, select the "Manual Operation" side tab.
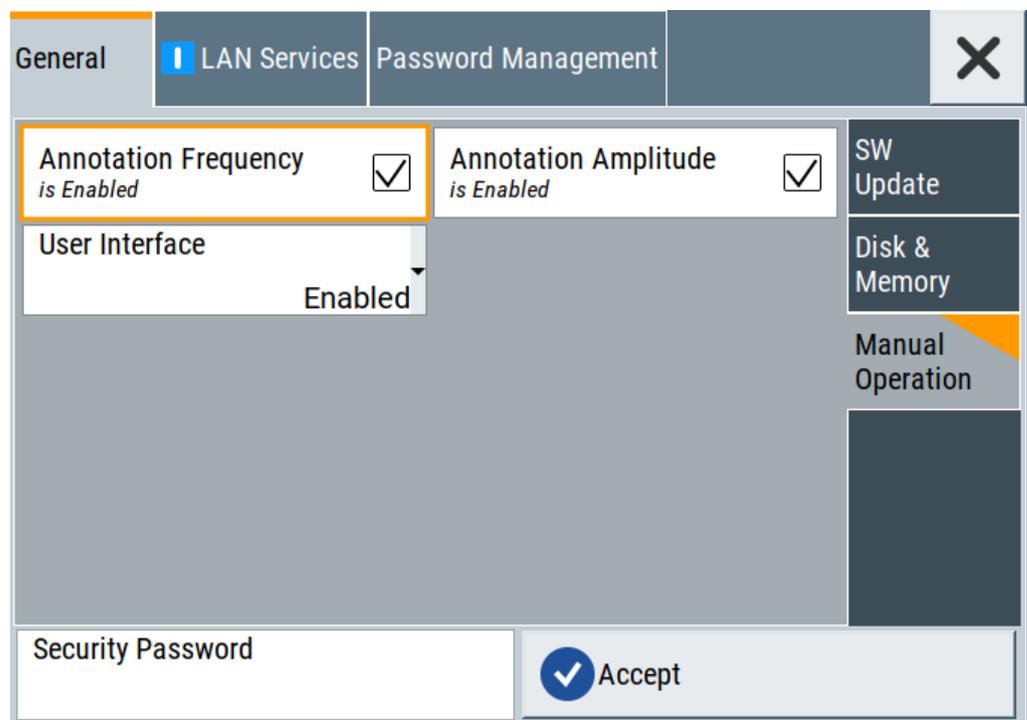
4. Disable "Annotation Frequency" and "Annotation Amplitude".

5. Enter the "Security Password".

6. Confirm with "Accept"

   The R&S SMW200A displays asterisks instead of the frequency and level settings in the status bar.

To disable control over the user interface

To lock the user interface:

1. Select "System Config > Setup > Security".

2. Select "Security".

3. In the "General" tab, select the "Manual Operation" side tab.

4. Select "User Interface > Disabled".

   This setting locks the display and all controls for manual operation.
   As an alternative, you can lock the display and controls individually for manual and remote operation:

5. Select "User Interface" > ...

UI selection	Locked	Still enabled	Unlockable with:
"Touchscreen Off"	Touchscreen functionality Displays the touchscreen locked icon 🔒.	Front panel controls External mouse and keyboard Remote operation	External mouse and keyboard Remote operation Remote control
"VNC only"	Front panel controls External mouse and keyboard Displays the VNC icon 🔒.	Screen display Remote operation	Remote operation Remote control
"Display only"	Touchscreen functionality Front panel controls External mouse and keyboard Displays a padlock icon 🔒.	Screen display	Security password.
"Disabled"	Display Touchscreen functionality Front panel controls External controls Remote operation Displays a padlock icon 🔒.	---	Security password. Remote control. See To unlock the user interface for manual and remote operation

6. Enter the "Security Password".

7. Confirm with "Accept".

To unlock the user interface for manual and remote operation

1. In manual operation:

a) On the instrument's keypad or external keyboard, press any key.
The instrument prompts you to enter the security password for unlocking.
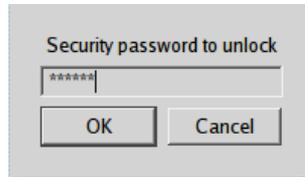
Note: The R&S SMW200A immediately inserts the character of the first key you pressed into the input field.

b) Delete the entry before inserting the password.
Enter the security password.

2. In remote control mode:

a) Send the command `SYST:ULOC ENABled` to release all locks at once.
b) Send the command `SYST:KLOC OFF` to unlock the keyboard and touchscreen.
c) Send the command `SYST:DLOC OFF` to release all locks.

There is no password required.

Glossary

C

CFast: Compact Fast - compact flash mass memory device.

D

DRAM: Dynamic Random Access Memory.

H

HDD: Hard disk drive.

M

microSD: Micro Solid-state Drive - memory card.

S

SD: Solid-state drive - memory card.

SSD: ATA Solid-state drives (including PATA, SATA, eSATA, mSATA,...).