R&S®NRX / R&S®NRT2 Power Meters Instrument Security Procedures

1179079702
Version 02

This document describes the types of memory and their usage of the R&S®NRX and R&S®NRT2 power meters.

© 2022 Rohde & Schwarz GmbH & Co. KG
Muehldorfstr. 15, 81671 Muenchen, Germany
Phone: +49 89 41 29 - 0
Email: info@rohde-schwarz.com
Internet: www.rohde-schwarz.com
Subject to change – data without tolerance limits is not binding.

1179.0797.02 | Version 02 | R&S®NRX / R&S®NRT2

Throughout this manual, products from Rohde & Schwarz are indicated without the ® symbol , e.g. R&S®NRX is indicated as R&S NRX. An R&S power meter is also referred to as instrument or 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 NRX / R&S NRT2 power meters

Product name	Order number
R&S NRX	1424.7005.02
R&S NRT2	1430.0509.02

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 Rohde & Schwarz power meters contain 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
R&S NRT2 power reflection meter / R&S NRX power meter				
OCRAM	Processor	256 kbyte	Boot code	No
SDRAM		1 Gbyte	RAM used by firmware to control the power meter operation	Yes
RAM	PLD	10 kbyte	Internal memory for trigger processing	Yes
R&S NRX-B1 (sensor check source)				
SRAM	MCU	160 kbyte	Internal memory for R&S NRX-B1	Yes
R&S NRX-B8 (GPIB/IEEE488 interface)				
SRAM	FPGA	60 kbyte	Internal memory for R&S NRX-B8	Yes

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
R&S NRT2 power reflection meter / R&S NRX power meter				
Flash	PLD	60 kbyte	Firmware for trigger processing	No

Memory type	Location	Size	Content / Function	User modifiable
eMMC		1 Mbyte	MBR and bootloader	No
		127 Mbyte	Temporary storage for firmware during sanitization	No
		256 Mbyte	Reserved for future use	No
		1460 Mbyte	ext4 file system: ● Operating system ● GUI application ● Instrument settings ● Product options	Yes
eMMC	boot partitions	2 x 16 Mbyte	not used	No
eMMC	RPMB partition	128 kbyte	not used	No
R&S NRX-B1 (sensor check source)				
Flash	MCU	2 x 512 kbyte	Firmware for R&S NRX-B1	No
R&S NRX-B8 (GPIB/IEEE488 interface)				
Flash	FPGA	4 Mbyte	Firmware for R&S NRX-B8	No

4.3 Media

The power meter does not contain media as defined in Security terms and definitions > Media.

5 Instrument sanitization procedure

Considerations on the sanitization procedure

- Maintaining operability
  Make sure that the instrument remains power supplied and switched on during sanitization. Turning off or disconnecting the instrument from the mains while the sanitization procedure is running results in loss of calibration data.
  Thus, the functionality of the product is no longer ensured.
- About the sanitization procedure
  To clear the non-volatile memory, the sanitization procedure executes several steps, see Sanitization process of the product.
- Starting the sanitization procedure

  You have several options to start the sanitization procedure:
  - On the instrument, see To sanitize the non-volatile memory
  - By I/O remote control commands, see Remote I/O
  - By the R&S power meter sanitization tool
- Security status after sanitization
  Sanitization clears all security settings. In particular, it resets all passwords to factory values.

5.1 Volatile memory

You can clear 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 7.

To turn off and remove power

1. Turn off the power meter.
2. Disconnect the power plug.

   Leave the instrument powered off at least for 10 minutes to make sure that all volatile memory modules lose their contents, see [3].

5.2 Non-volatile memory

You can clear the non-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 7.

Sanitization process of the product

The sanitization procedure implemented for the product executes the following actions:

1. Saves the instrument firmware (including the product options) temporarily.
2. Erases the ext4 partition (eMMC secure erase).
3. Overwrites each addressable location of the ext4 partition by 0xFF (binary one) characters.
4. Overwrites each addressable location of the ext4 partition by 0x00 (binary zero) characters.
5. Recreates the ext4 file system and restores the instrument firmware.

5.2.1 Graphical user interface

To sanitize the non-volatile memory

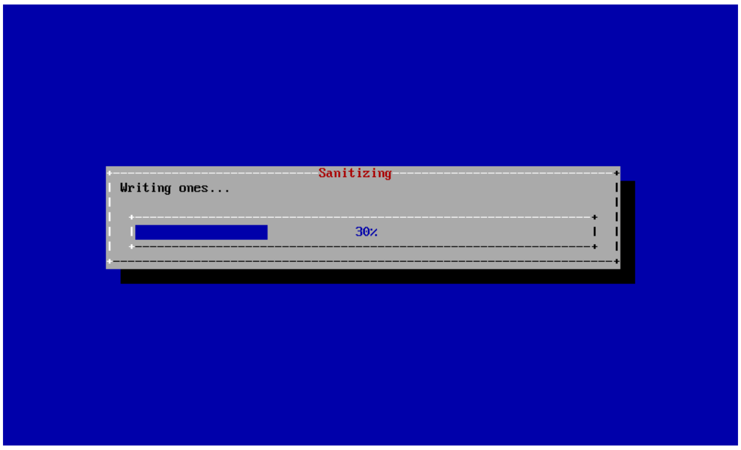
Access: [System] > "Instrument Info" > "Security"

1. Enter the security password.
2. Select "Sanitize".
3. **NOTICE!** Risk of loosing operability. Power interruption during the sanitization procedure leads to calibration data loss.
   Make sure that the instrument is continuously supplied with power as long as the process is running.

   NOTICE! The sanitization procedure clears all user data and resets the instrument.

   Confirm with "Erase all & Reboot".

   The sanitization lasts approximately 10 minutes.



Sanitizing

Writing ones...

30%

Figure 5-1: Example: Progress of sanitization process

See "Sanitization process of the product" on page 12 for information on the actions the sanitization procedure executes.

5.2.2 Remote I/O

To sanitize the non-volatile memory remotely

1. Connect the instrument to a controller device, either in a LAN or over USB.
   If the instrument is equipped with option R&S NRX/NRT2-B8 (GPIB/IEEE488 interface), you can also use this bus interface for remote control.
2. Start a controller application program on the controller.
3. Before starting the sanitization procedure, we recommend that you read out the status of the last sanitization.
   Send the following commands:
   ```
   SERVice:UNLock 1234                    // enables service functions
   SERVice:SECure:ERASe:STATus?
   ```
   Returns the number of the executed sanitization cycles so far, and the status/error information of the last sanitization, e.g. `"Counter:2","Error:none"`.
   Keep the counter in mind.
4. **NOTICE!** Risk of loosing operability. Power interruption during the sanitization procedure leads to calibration data loss.
   Make sure that the instrument is continuously supplied with power as long as the process is running.

   NOTICE! The sanitization procedure clears all user data and resets the instrument.

   Send the following remote I/O command sequence to the instrument:
   ```
   SERVice:UNLock 1234
   SERVice:SECure:ERASe
   ```
   The procedure "Sanitize internal memory" starts. The application indicates the currently performed action and its progress.
5. When completed, you can query the result with the following command sequence:
   ```
   SERVice:UNLock 1234
   SERVice:SECure:ERASe:STATus?
   ```
   Check if the counter has incremented by 1 after sanitization, e.g. `"Counter:3","Error:none"`.

5.2.3 R&S power meter sanitization tool

As an alternative to sending the sanitization commands to the instrument (as described in Chapter 5.2.2, "Remote I/O", on page 13), you can use the R&S power meter sanitization tool which is provided on the Rohde & Schwarz website.

The R&S power meter sanitization tool must be installed on a controller PC and requires Microsoft®Windows 7, Microsoft®Windows 10 or Microsoft®Windows 11 operating system and an installed VISA library.

Rohde & Schwarz provides the VISA library free of charge for download on the Internet, see http://www.rohde-schwarz.com/rsvisa.

For detailed information, including download and installation of the application, see Chapter 10, "R&S power meter sanitization tool", on page 22

To sanitize the non-volatile memory with the R&S power meter sanitization tool

It is assumed, that you have installed the R&S power meter sanitization tool on the controller PC. Therefore, the following section briefly outlines the main steps to execute the procedure.

1. Start the R&S power meter sanitization tool.

   The application scans automatically for instruments connected over USB. For instruments connected in the LAN, enter the corresponding address information to add the instrument to the list.

2. Select the instrument from the list.

3. **NOTICE!** Risk of loosing operability. Power interruption during the sanitization procedure leads to calibration data loss.
   Make sure that the instrument is continuously supplied with power as long as the process is running.

   NOTICE! The sanitization procedure clears all user data and resets the instrument.

   Start the sanitization procedure.

   The R&S power meter sanitization tool confirms with a message when completed.

5.3 Media

The power meter does not contain media memory modules. Therefore no sanitization procedure is required.

6 Operability outside secured area

The sanitization procedure saves the firmware temporarily and restores it for recreation, see the description of the sanitization steps in Chapter 5.2, "Non-volatile memory", on page 11.

Thus the operability of the instrument is maintained after sanitization.

7 Validity of instrument calibration

The santitzation procedure does not affect the calibration of the R&S power meters.

8 Special security features

This section leads you to the information on how to use the security features to protect the product 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.

Depending on the power meter model, you can block the USB storage to prevent data being written to a USB memory device.

See Chapter 9.2, "USB interfaces", on page 19.

8.2 Considerations for LAN interfaces

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

Depending on the power meter model, you can disable the LAN interface services, or individually enable or disable the access to the product over LAN.

See Chapter 9.3, "LAN interfaces and services", on page 19

8.3 Considerations for the user interface

To prevent unauthorized personnel operating the instrument, you can lock the touch functionality of the screen, e.g. when you remotely control the instrument from a different location.

See Chapter 9.4, "Graphical user interface (GUI)", on page 20.

9 Recommended security settings

Basically, see the user manual, chapter *System settings* > *Instrument info* > *Security settings* for the security measures the power meter provides.

The user manuals are is provided for download on the product page:

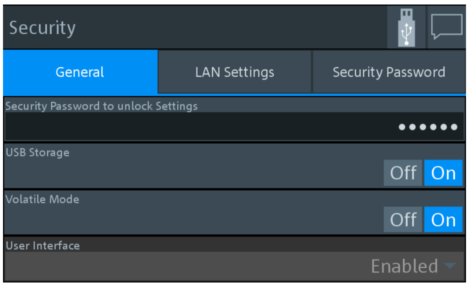
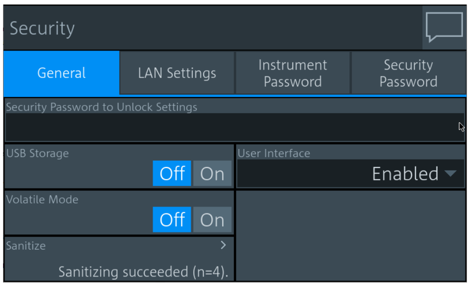
- www.rohde-schwarz.com/manual/NRX
- www.rohde-schwarz.com/manual/NRT2

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

You can protect the internal memory of the power meter from saving user-specific application settings permanently by enabling the volatile mode on the instrument.

Table 9-1: General instrument security settings

 Security General | LAN Settings | Security Password Security Password to unlock Settings: ●●●●●● USB Storage: Off [✓ On] Volatile Mode: Off [✓ On] User Interface: Enabled	 Security General | LAN Settings | Instrument Password | Security Password Security Password to Unlock Settings USB Storage: [✓ Off] On User Interface: Enabled Volatile Mode: [✓ Off] On Sanitize Sanitizing succeeded (n=4).
R&S NRT2	R&S NRX

To enable the volatile mode

Access: [System] > "Instrument Info" > "Security"

1. In the "General" tab, switch on "Volatile Mode".

   Changing the volatile mode setting requires the security password and a reboot.

2. Enter the security password.

3. Reboot the instrument.

   The product saves all user data and instrument setups in the volatile memory (SDRAM).

9.2 USB interfaces

To disable the USB interface for file transfer

There are special considerations for the USB ports to avoid unauthorized file transfer.

Access: [System] > "Instrument Info" > "Security"

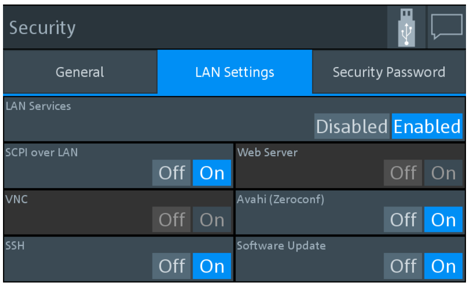
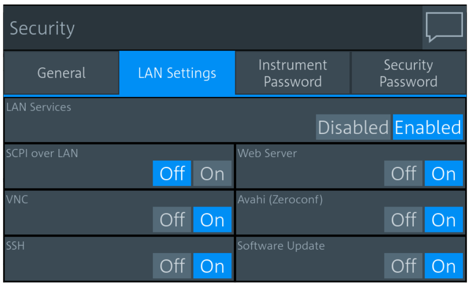
1. In the "General" tab, switch off "USB Storage".
2. Enter the security password.

   The product blocks file transfer over USB.

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.

Table 9-2: LAN security settings

 Security General | LAN Settings | Security Password LAN Services: Disabled [✓ Enabled] SCPI over LAN: Off [✓ On] Web Server: Off On VNC: Off On Avahi (Zeroconf): Off [✓ On] SSH: Off [✓ On] Software Update: Off [✓ On]	 Security General | LAN Settings | Instrument Password | Security Password LAN Services: Disabled [✓ Enabled] SCPI over LAN: [✓ Off] On Web Server: Off [✓ On] VNC: Off [✓ On] Avahi (Zeroconf): Off [✓ On] SSH: Off [✓ On] Software Update: Off [✓ On]
R&S NRT2	R&S NRX

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

To disable the LAN ports and services

There are special considerations for the LAN interface to avoid unauthorized access in a high-security location.

Access: [System] > "Instrument Info" > "Security"

1. Select the "LAN Settings" tab.
2. To disable all services, select "LAN Services > Disabled".

   This setting blocks all LAN services in general, i.e. it is not possible to access the instrument over the LAN connection.
   If enabled, it provides remote access over the unlocked services.
3. Switch off all not used access and services settings.

UI selection	Setting	Effect
"SCPI over LAN"	"Off"	Blocks remote control over LAN with SCPI commands.
"Web Serverf"*)	"Off"	Blocks remote access over a web application.
"VNC"*)	"Off"	Blocks remote access over a virtual network computing interface (VNC).
"Avahi (Zeroconf)"	"Off"	Disables automatic configuration of the instrument in a network environment.
"SSH"	"Off"	Disables the use of the network protocol for secure file transfer.
"Software Update"	"Off"	Blocks the access for updating the software LAN.
*) R&S NRX only		

The power meter applies the settings immediately. You do not have to confirm with the security password, nor reboot the instrument.

9.4 Graphical user interface (GUI)

To protect the instrument against unauthorized manual control, you can lock the display and the front panel controls.

This security measure applies to R&S NRX power meters. For the R&S NRT2, manual operation over the user interface and all manual controls is permanently possible and cannot be blocked.

To disable control over user interface

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

Access: [System] > "Instrument Info" > "Security".

1. In the "General" tab, select "User Interface".
2. You can lock the display and controls individually for manual and remote operation:

UI selection	Locked	Enabled	Unlockable with:
"Enabled"	---	Screen display Touchscreen functionality Front panel controls External mouse and keyboard Remote operation	---
"VNC only"	Touchscreen functionality External mouse and keyboard Front panel controls	Screen display Remote operation	Remote operation
"Display only"	Touchscreen functionality Front panel controls External mouse and keyboard Remote operation	Screen display	Security password.
"Disabled"	Screen display 🔒. Touchscreen functionality Front panel controls External mouse and keyboard Remote operation	---	Security password, see To unlock the user interface in manual and remote operation

3. Enter the security password.

To unlock the user interface in manual and remote operation

1. Select any control.

   The instrument prompts you to enter the security password for unlocking.

2. Enter the security password.

   The instrument sets the "User interface" to "Enabled".

10 R&S power meter sanitization tool

R&S power meter sanitization tool is a PC application that helps you to declassify a Rohde & Schwarz instrument before it leaves a secure environment. The application executes a procedure that removes all user data from the instrument.

This declassification procedure meets the needs of customers working in a secured area.

Instruments covered

You can use the R&S power meter sanitization tool to sanitize the following instruments:

- R&S NRX / R&S NRT2 power meters
- R&S NRP power sensors
- R&S NRQ6 power sensors
- NRPM3(N) power sensor modules
- R&S NRPCxx(-B1) / R&S NRPC-LS power sensor calibration kits

10.1 Setting up the R&S power meter sanitization tool

Prerequisites

The R&S power meter sanitization tool runs on PCs with Microsoft®Windows 7, Microsoft®Windows 10 or Microsoft®Windows 11 operating system with an installed VISA library.

Rohde & Schwarz provides the VISA library free of charge for download on the Internet, see http://www.rohde-schwarz.com/rsvisa.

The R&S power meter sanitization tool is available free of charge also. You can download the program file `NrpSanitizer_Installer_x.x.xxxx.xxxx.exe`[1] from the product page of any of the supported instruments, e.g. www.rohde-schwarz.com/software/nrp

[1] xx represents the current version of the application.

The installer program contains all components required for installation and operation of the R&S power meter sanitization tool.

To install the application

1. Download the latest version of the R&S power meter sanitization tool installer program.

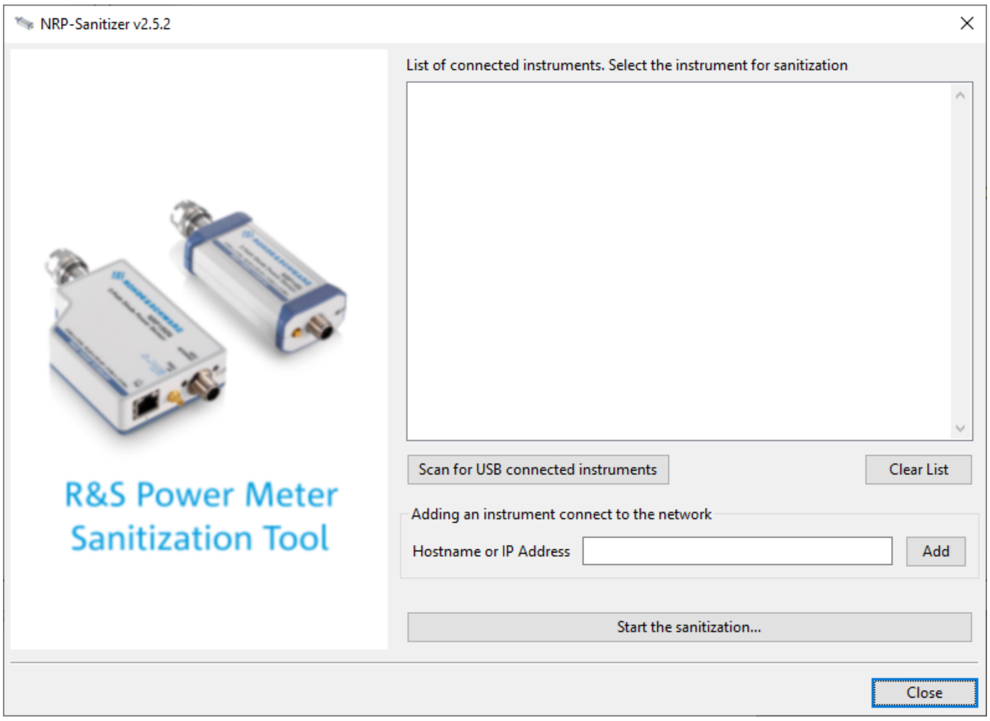
2. Execute `NrpSanitizer_Installer_x.x.xxxx.xxxx.exe` and follow the instructions of the installation wizard.

   The setup program checks if a VISA library is available and installs the application files.

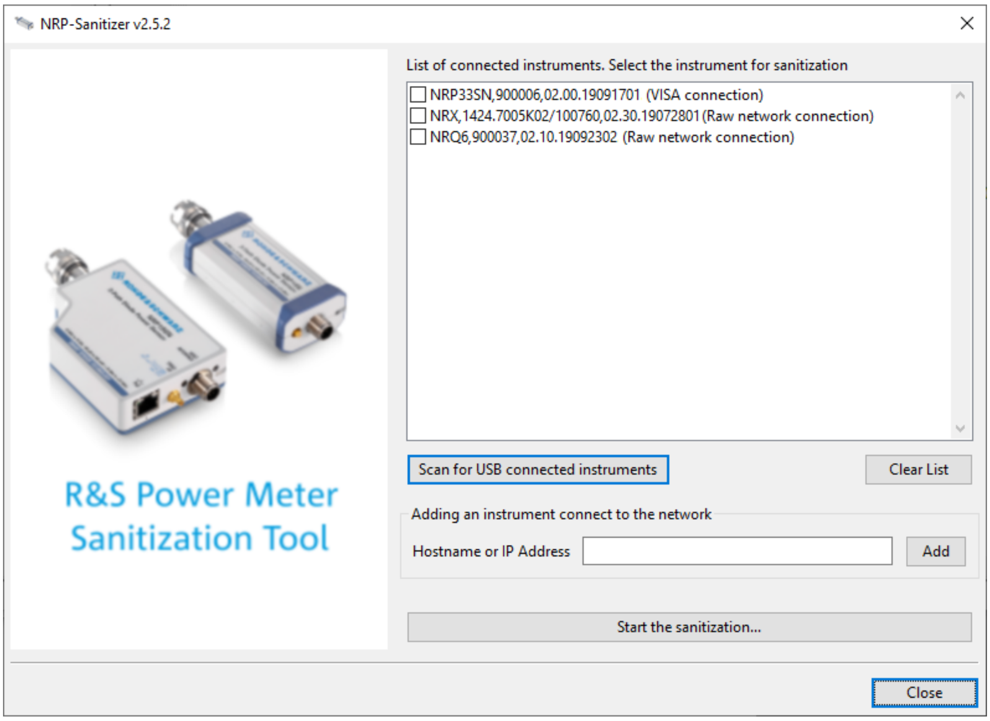
10.2 Starting the sanitization

After downloading the installer file to your PC and installing the R&S power meter sanitization tool, perform the following steps:

1. Start the application.


NRP-Sanitizer v2.5.2
List of connected instruments. Select the instrument for sanitization
Scan for USB connected instruments
Clear List
Adding an instrument connect to the network
Hostname or IP Address
Add
Start the sanitization...
Close
R&S Power Meter Sanitization Tool

2. To search for USB connected instruments, select "Scan for USB connected instruments".



NRP-Sanitizer v2.5.2

List of connected instruments. Select the instrument for sanitization

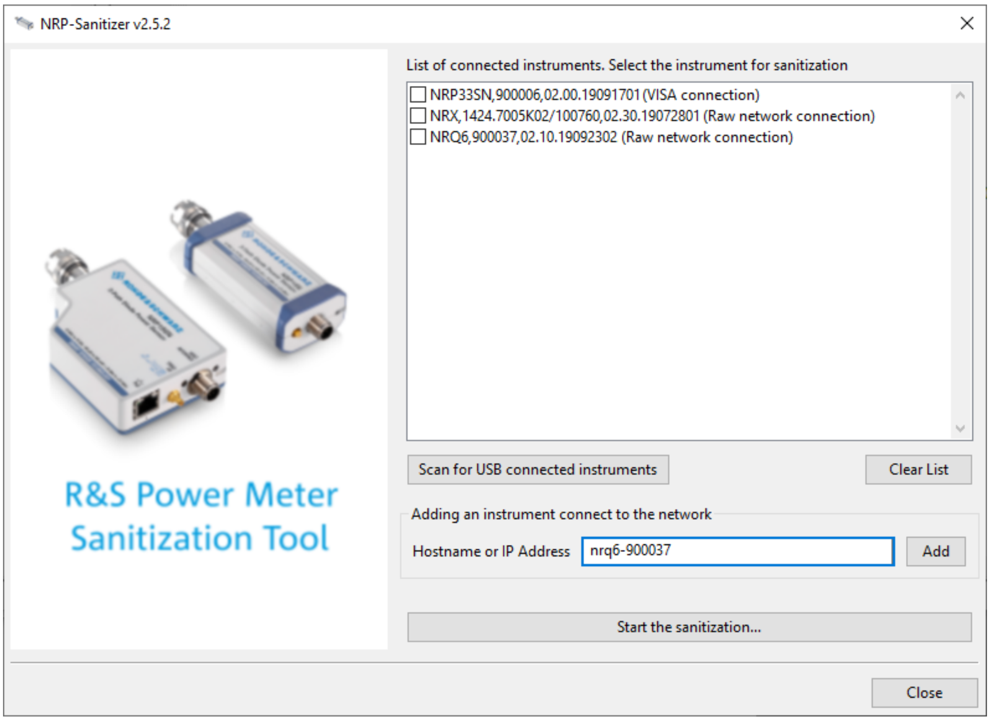
□ NRP33SN,900006,02.00.19091701 (VISA connection)
□ NRX,1424.7005K02/100760,02.30.19072801 (Raw network connection)
□ NRQ6,900037,02.10.19092302 (Raw network connection)

Adding an instrument connect to the network

Hostname or IP Address

The application lists all supported instruments connected to the USB interfaces.

3. For instruments connected to the LAN, enter the corresponding address information in the "Hostname or IP Address" field.



NRP-Sanitizer v2.5.2

List of connected instruments. Select the instrument for sanitization

□ NRP33SN,900006,02.00.19091701 (VISA connection)
□ NRX,1424.7005K02/100760,02.30.19072801 (Raw network connection)
□ NRQ6,900037,02.10.19092302 (Raw network connection)

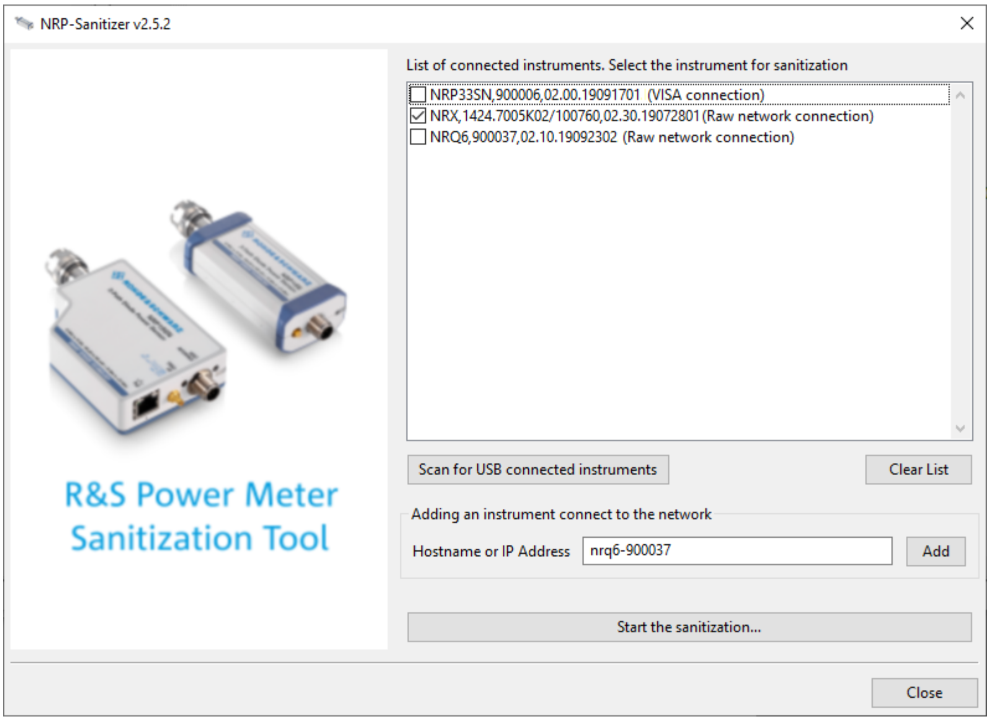
Adding an instrument connect to the network

Hostname or IP Address: nrq6-900037

4. Confirm with "Add".

   The application adds the instrument to the list.

5. Select the instrument you need to sanitize from the list.



NRP-Sanitizer v2.5.2

List of connected instruments. Select the instrument for sanitization

☐ NRP33SN,900006,02.00.19091701 (VISA connection)
☑ NRX,1424.7005K02/100760,02.30.19072801 (Raw network connection)
☐ NRQ6,900037,02.10.19092302 (Raw network connection)

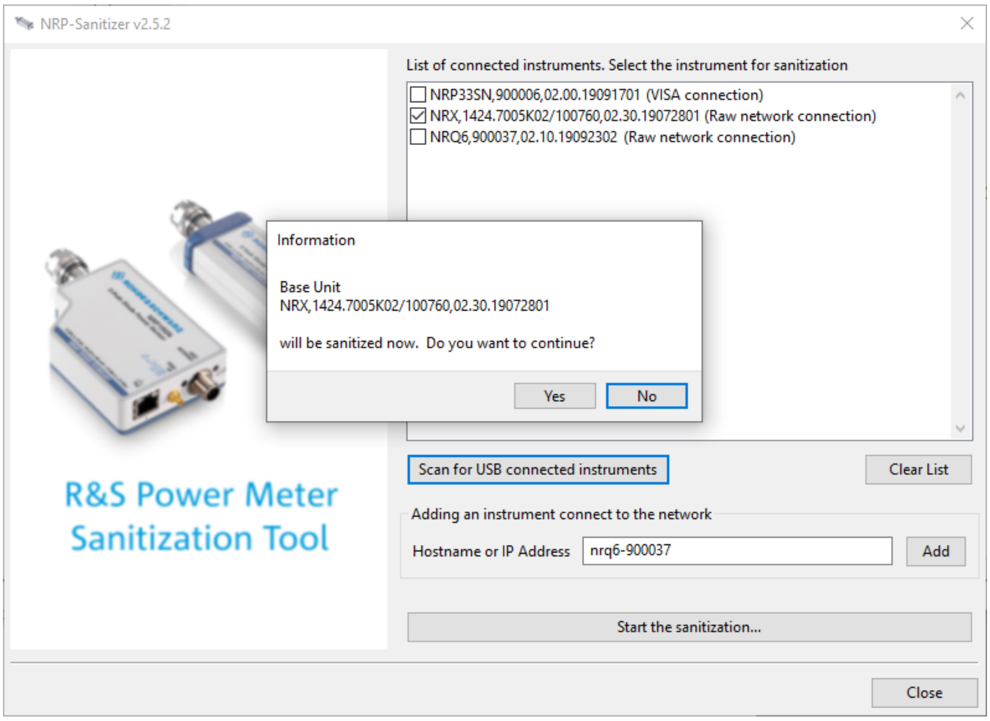
Adding an instrument connect to the network

Hostname or IP Address: nrq6-900037

6. **NOTICE!** Risk of loosing operability. Power interruption during the sanitization procedure leads to calibration data loss.
Make sure that the instrument is continuously supplied with power as long as the process is running.

   NOTICE! The sanitization procedure clears all user data and resets the instrument.

   "Start the sanitization..." and confirm the execution.



NRP-Sanitizer v2.5.2

List of connected instruments. Select the instrument for sanitization

☐ NRP33SN,900006,02.00.19091701 (VISA connection)
☑ NRX,1424.7005K02/100760,02.30.19072801 (Raw network connection)
☐ NRQ6,900037,02.10.19092302 (Raw network connection)

Information

Base Unit
NRX,1424.7005K02/100760,02.30.19072801

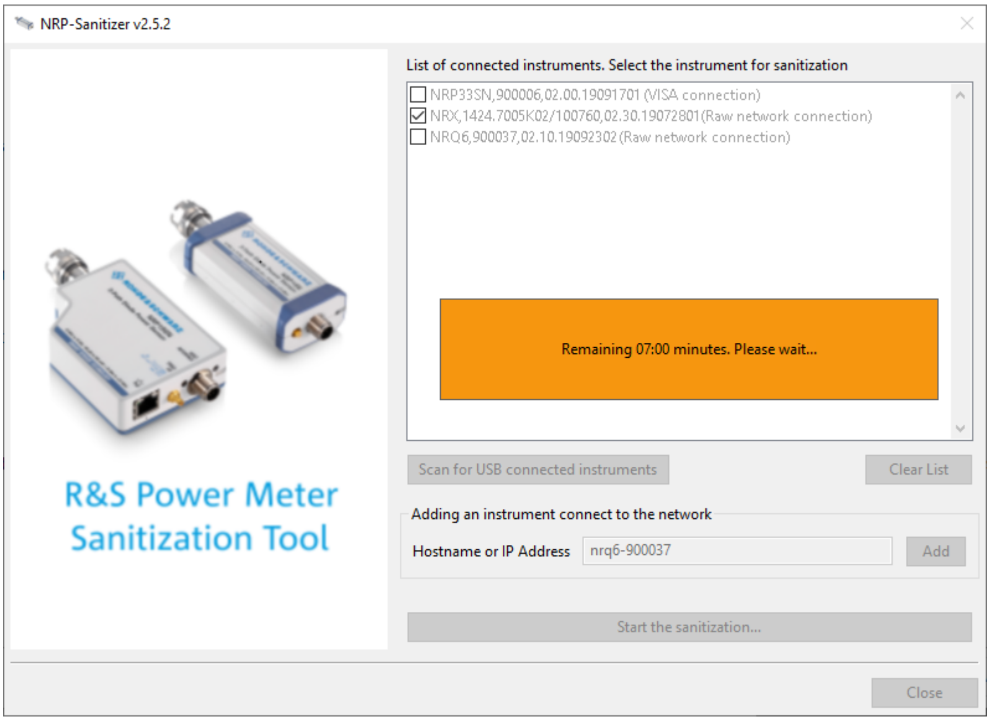
will be sanitized now. Do you want to continue?

Yes
No
Scan for USB connected instruments
Clear List
R&S Power Meter Sanitization Tool

Adding an instrument connect to the network

Hostname or IP Address: nrq6-900037

The sanitization lasts approximately 10 minutes.



NRP-Sanitizer v2.5.2

List of connected instruments. Select the instrument for sanitization

☐ NRP33SN,900006,02.00.19091701 (VISA connection)
☑ NRX,1424.7005K02/100760,02.30.19072801 (Raw network connection)
☐ NRQ6,900037,02.10.19092302 (Raw network connection)

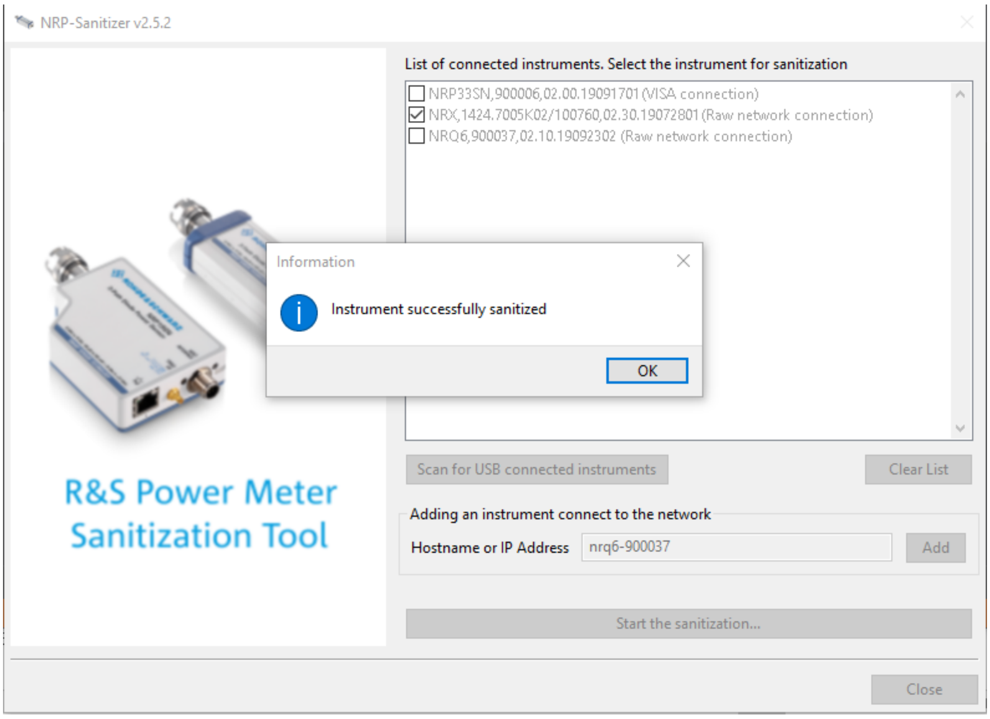
Remaining 07:00 minutes. Please wait...

Scan for USB connected instruments
Clear List
R&S Power Meter Sanitization Tool

Adding an instrument connect to the network

Hostname or IP Address: nrq6-900037

7. The R&S power meter sanitization tool also validates the sanitization and confirms with a message when completed.



NRP-Sanitizer v2.5.2

List of connected instruments. Select the instrument for sanitization

- □ NRP33SN,900006,02.00.19091701 (VISA connection)
- ☑ NRX,1424.7005K02/100760,02.30.19072801 (Raw network connection)
- □ NRQ6,900037,02.10.19092302 (Raw network connection)

Information

Instrument successfully sanitized

Adding an instrument connect to the network

Hostname or IP Address: nrq6-900037

OK
R&S Power Meter Sanitization Tool
Scan for USB connected instruments
Clear List
Add
Start the sanitization...
Close