Malware Protection
White Paper Embedded Linux

Products:

- R&S®SMW200A
- R&S®AREG100A
- R&S®SMBV100B
- R&S®SMB100B
- R&S®SMA100B
- R&S®SGS100A
- R&S®SGU100A
- R&S®SGT100A
- R&S®SMBV100A
- R&S®SMB100A
- R&S®SMA100A
- R&S®SMF100A

Rohde & Schwarz recognizes the potential risk of computer virus infection when connecting test instrumentation to Windows®-based computers via local area networks (LANs), or using removable storage devices.

This white paper introduces measures to minimize malware threats and discusses ways to reduce risks while ensuring that instrument performance is not compromised.

The paper also discusses the use of anti-virus software in combination with Embedded Linux based instruments.

Martin Runge
11.2016 – 1GP112_1E

ROHDE&SCHWARZ

Table of Contents

1 Introduction

Rohde & Schwarz is dedicated to ensuring that all products are shipped free of malware. Although the vast majority of malware existing out there is targeting the different versions of Windows, there is also malware trying to infect Linux-based systems, however by far less in numbers. Additionally, Linux is not Linux. Infecting a Linux-based Systems is very hard because there are many versions and flavors in use, each with a little different properties. This makes it very hard for malware to reach from one Linux system to another.

So the risk of a malware infection of an Embedded Linux based instrument is low but it is not zero. Additionally, an instrument could serve as a transport mechanism for a malware not trying to infect the instrument itself, but some standard PC reachable via the local area network the instrument is connected to. To minimize the remaining risk, Rohde & Schwarz is using a customized and hardened Embedded Linux OS on its instruments.

This paper discusses the measures taken to make instruments more resistant to malware infection and what the customer can do to further decrease the risk.

It is highly recommended that you work closely with your IT-department or system administrator to ensure compliance with your company policies when connecting instruments to your company’s network.

Rohde & Schwarz has established processes within the company to take all reasonable precautions to prevent the spread of viruses from instruments to our customers’ computers and networks:

- All computers used within Rohde & Schwarz that may be connected to instruments destined for customers are equipped with centrally managed firewall and anti-virus software and maintain the latest virus definitions. Computers and removable storage devices are scanned regularly to prevent the spread of computer viruses.
- Strict virus control protocols have been established in manufacturing, service, support, sales, distribution and demonstration environments. This includes the use of isolated LANs, scanning of instruments and removable storage devices and/or re-imaging hard drives, depending on instrument configuration.
- Procedures have been established for all Rohde & Schwarz employees who come in contact with customer instruments to reinforce anti-virus security protocols. This includes all personnel from manufacturing, service, support, sales and distribution.

2 System Design

Rohde & Schwarz instruments do not use a standard Linux distribution like Debian, RedHat or Ubuntu. Instead, a highly customized Linux OS is used, that is reduced to the needs of a measurement instrument.

Rohde & Schwarz uses the well proven Yocto Project [1] to build its custom Embedded Linux OS.

2.1 Reduce Software to the necessary only

The Rohde & Schwarz Embedded Linux based instrument OS is carefully reduced to the minimal set of software needed to operate the instrument. This significantly reduces the points of attack for potential malware.

Software that is not necessary for the operation or service of the instrument was permanently removed from the instrument's OS image and cannot accidently be activated.

Common standard OS installations usually include software like a web browser with flash player, a PDF reader and other add-ons that are expected to be needed by everybody anyway (on a desktop), so they are preinstalled for convenience and often not removable. In case of a measurement instrument, these programs are not needed for operation but unnecessarily offer additional points of attack for potential malware.

2.2 Read Only File System

Both, the Embedded Linux OS and the Rohde & Schwarz application, are located in a so called "read-only" file system. These file systems effectively prohibit possible modification of the instrument's firmware as well as installation of additional software.

Why is it important to prevent additional software to be installed on the instrument? There are two reasons:

- If an instrument should get in contact with malware once, the malware has no way to install itself permanently on the instrument and will be gone after the next reboot.
- A user cannot install additional software on the instrument and by doing so offer additional points of attack to any potential malware.

The only way to install new or additional software on an instrument is via the instrument's regular firmware update procedure (Rohde & Schwarz update package .rsu).

Only a few separated folders are writable to store the user's data and settings permanently. None of the instrument's firmware is located here.

3 User Accounts

Services exposed to the local network (LAN) by the operating system are accessible as user "instrument". This user is only granted limited access to the folders intended for storage of user data.

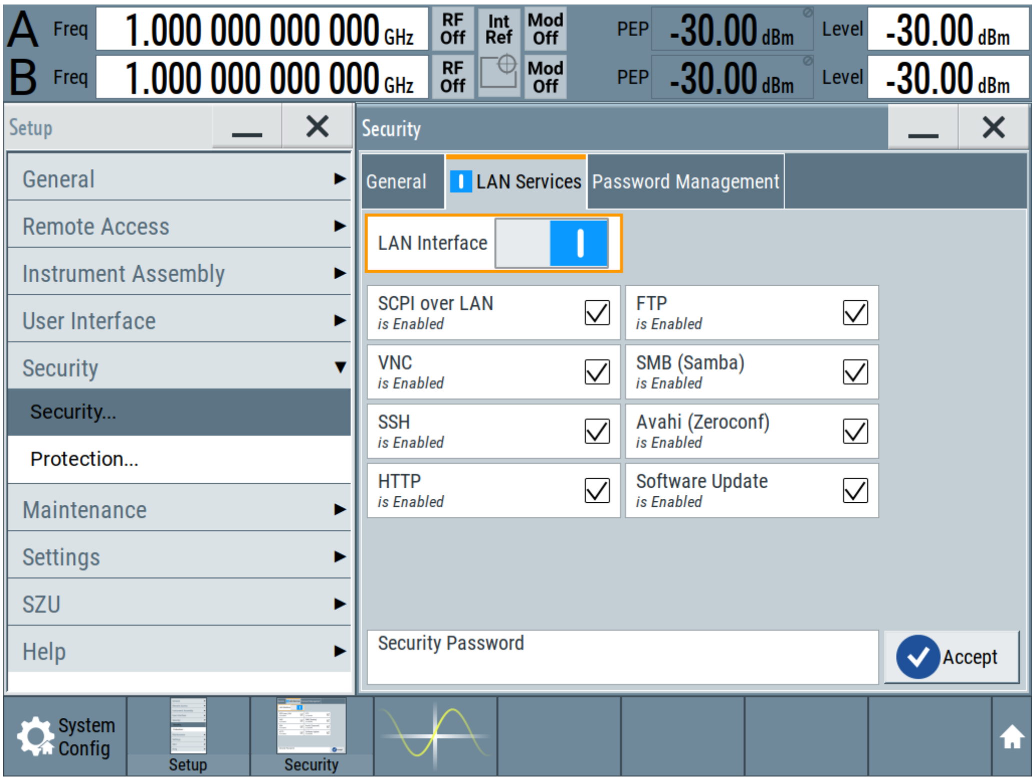
This separation ensures that the network services offer no access to software installation of the instrument.

4 Firewall / Network Services

Rohde & Schwarz Embedded Linux based instruments offer the following services to the local network (LAN):

Ports	Service	Description
21 TCP	FTP	Instrument FTP server File transfer of user data to and from the instrument.
22 TCP	SSH / SCP	Secure Shell File transfer of user data to and from the instrument
80 TCP	Web server	Instrument web server (LXI)
111 TCP & UDP	Port mapper	Port mapper service for VXI-11 / LXI
139 TCP	Netbios-ssn	Make the instrument visible on the LAN to pure Windows PC without Bonjour installed
5025 (data) **5125 (control)**	TCP Socket	'Raw SCPI' socket connection
5353 TCP & UDP **5354 TCP & UDP**	Bonjour	Multicast DNS responder (mDNS)
5900 TCP	VNC	Instrument soft front panel via web server (Browser interface)
13217 TCP & UDP	RS Installer	R&S Software distributor service
14142-16383 TCP & UDP (dynamic assignment)	ONC-RPC	SUN ONC-RPC protocol – VXI-11

To further decrease the risk of malware infection, the user can disable all unneeded LAN services via the instruments GUI:



LAN Interface: On

SCPI over LAN *is Enabled* ☑	FTP *is Enabled* ☑
VNC *is Enabled* ☑	SMB (Samba) *is Enabled* ☑
SSH *is Enabled* ☑	Avahi (Zeroconf) *is Enabled* ☑
HTTP *is Enabled* ☑	Software Update *is Enabled* ☑

Security Password

5 Anti-Virus Software

Rohde & Schwarz Embedded Linux based instruments do not have any anti-virus software preinstalled. Anti-Virus software is often respected as mandatory in Microsoft Windows environments like company networks. It is therefore important to understand how Rohde & Schwarz Embedded Linux based instruments differ from office PCs or servers and why Rohde & Schwarz decided, not to deploy Anti-Virus Software on Embedded Linux based instruments.

5.1 Timing considerations

Many measurement instruments need to keep tight timing limits to ensure not to miss any events or data. For example a signal generator is supposed to deliver a certain RF signal within a guaranteed maximal delay after it received the remote command to do so.

An on-access virus scanner that works in background would cause violations to these timing requirements and prohibit the correct operability of the instrument.

5.2 Instrument self-protection

The most important goal is to protect the instrument itself from malware.

Most Anti-Virus software available for Linux (remember: "Linux is not Linux") is intended for use on mail, file or web servers which usually use one of the classical Linux distributions like RedHat, Ubuntu or Debian. The main goal is to detect any malware before it is delivered to a client computer, be it a Linux, Windows, MacOS or mobile client. It is also easier to keep a single malware database up to date on a server than on all clients connected to it.

Due to this common use case, anti-virus software available for Linux would mainly scan for Windows malware. The small amount of malware targeting Linux is actually targeting RedHat, Debian or Ubuntu and will likely not be able to infect a highly customized Embedded Linux. That big advantage arises from the heterogeneous nature of Linux ("Linux is not Linux").

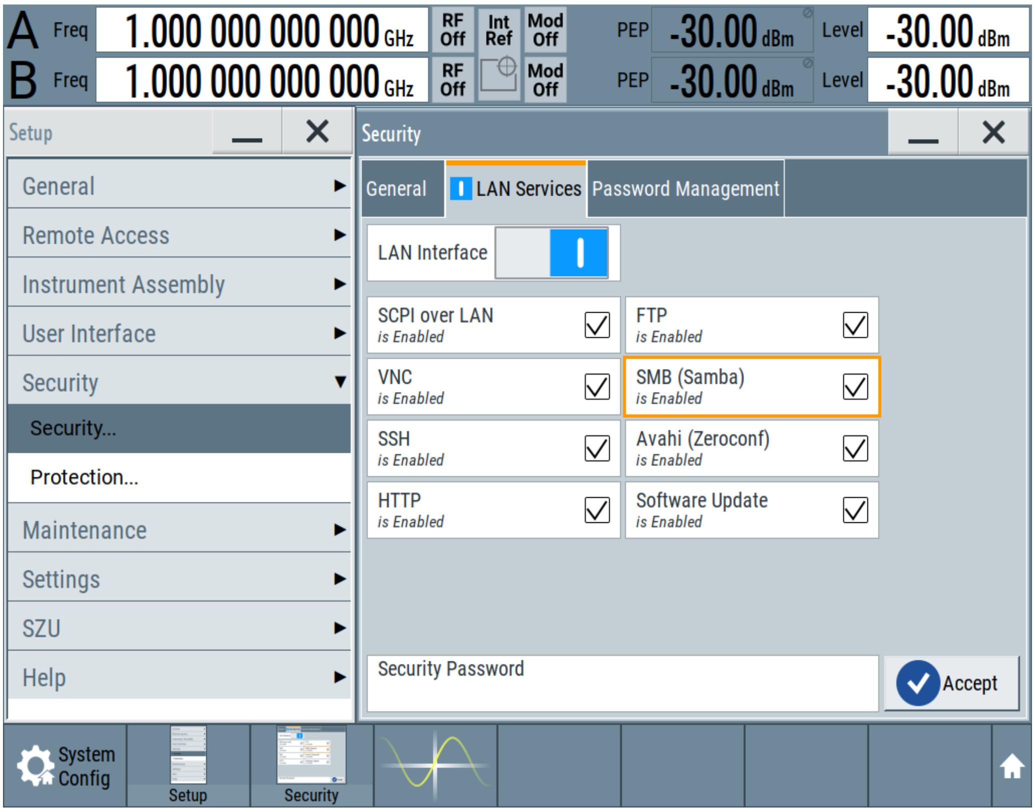
5.3 Scanning from an external PC

During normal operation of the instrument only the folders that are intended to store the nonvolatile user and instrument can be modified. These folder are also exported vial FTP, SSH and Samba if not disabled as shown above. A piece of malware placed here would not be able to infect the instrument itself but possibly another Desktop PC (for example a Windows PC) if it connects to that share.

These shares can be connected to Standard PC equipped with a Virus Scanner (for example a regular Windows office PC) and scanned for malware from outside. Please be aware that such a scan will influence the real-time behavior of an instrument. Please do only consider this option while the instrument is not in production use.

The following example illustrates how to export the nonvolatile storage from an R&S® SMW 200A to a Windows 10 PC for scanning.

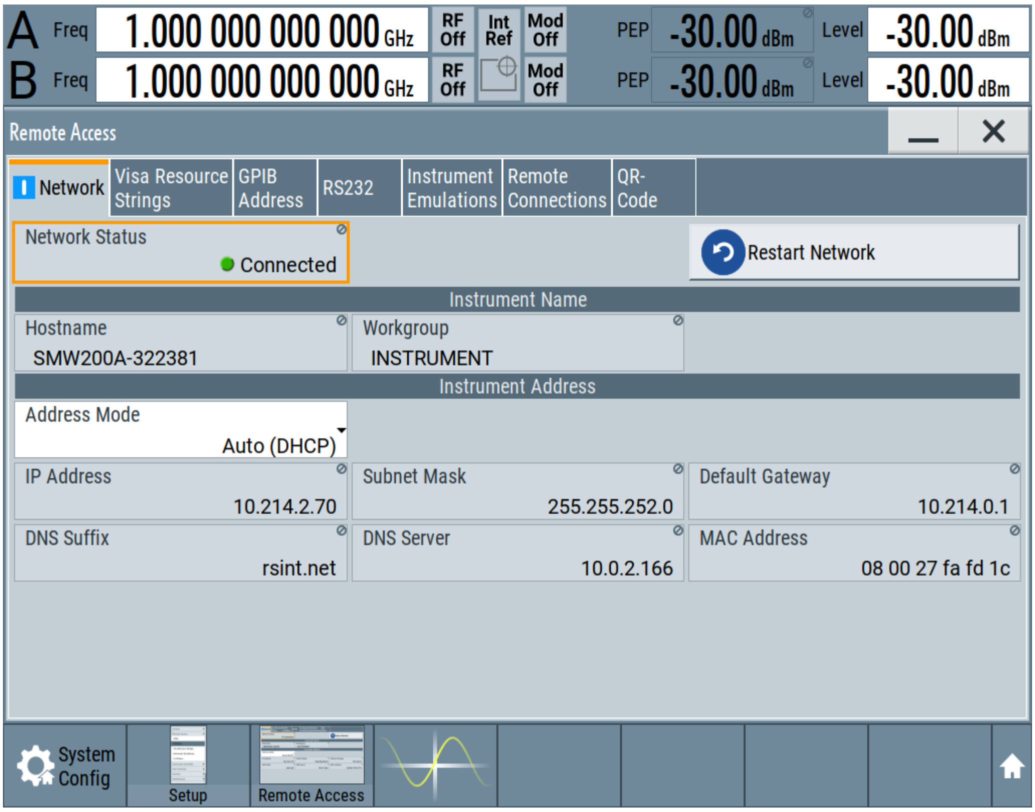
First, make sure that the nonvolatile file system is exported via the SMB (Samba) protocol:



LAN Interface: On

SCPI over LAN ☑ *is Enabled*	FTP ☑ *is Enabled*
VNC ☑ *is Enabled*	SMB (Samba) ☑ *is Enabled*
SSH ☑ *is Enabled*	Avahi (Zeroconf) ☑ *is Enabled*
HTTP ☑ *is Enabled*	Software Update ☑ *is Enabled*

Next, get the hostname or IP address of the instrument via "System Config" -> "Remote Access":



Network Status: Connected

Hostname: SMW200A-322381

Workgroup: INSTRUMENT

Address Mode: Auto (DHCP)

IP Address: 10.214.2.70

Subnet Mask: 255.255.252.0

Default Gateway: 10.214.0.1

DNS Suffix: rsint.net

DNS Server: 10.0.2.166

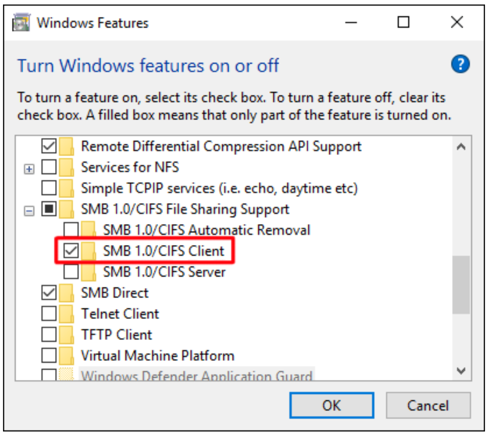
MAC Address: 08 00 27 fa fd 1c

In This example the hostname is "SMW200A-322381".

The instrument exports three shares that can be mounted as network drive:

- user (\\SMW200A-322381\user) (was “share” in versions < 4.30.xxx)
- update (\\SMW200A-322381\update)
- volatile (\\SMW200A-322381\volatile)

Current versions of Windows 10 do not support version 1.x of the smb protocol by default anymore. You need to activate it in “Turn Windows Features on or off” (search for “turn windows …” in Windows 10 start menu):

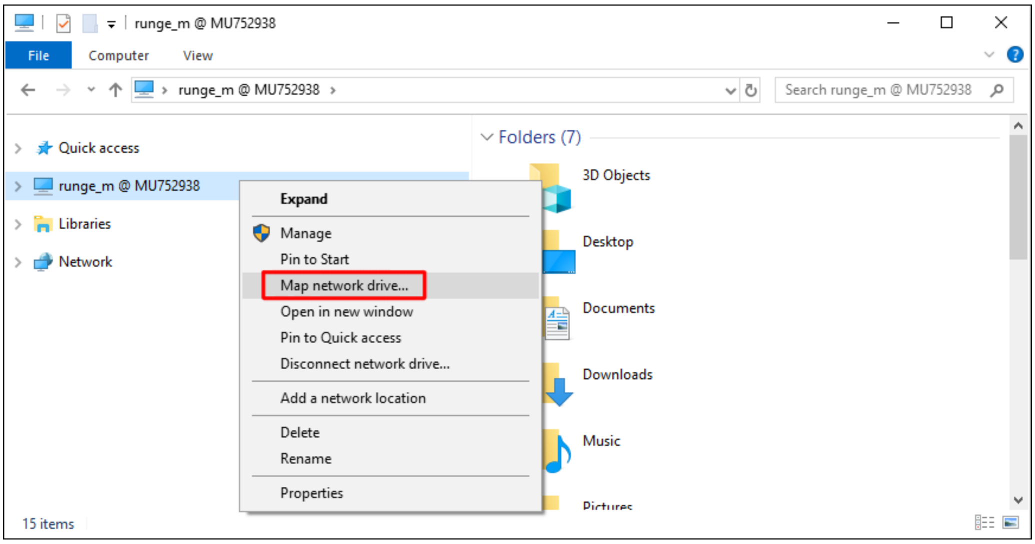


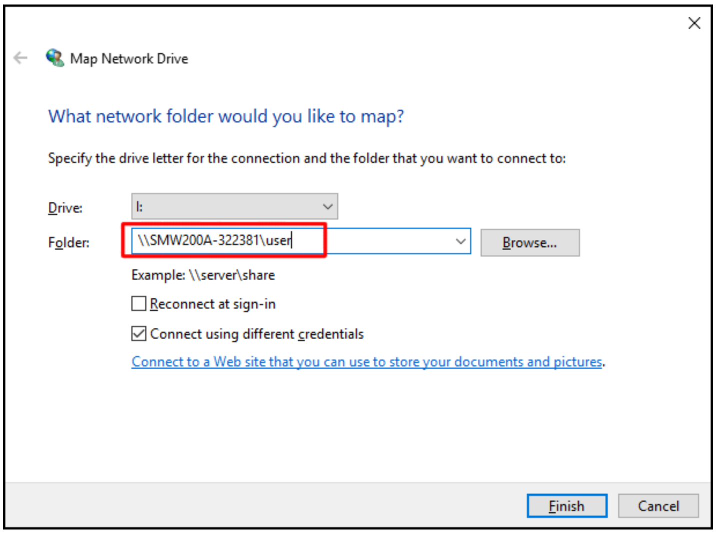
Turn Windows features on or off

To turn a feature on, select its check box. To turn a feature off, clear its check box. A filled box means that only part of the feature is turned on.

- ☑ Remote Differential Compression API Support
- ☐ Services for NFS
- ☐ Simple TCPIP services (i.e. echo, daytime etc)
- ■ SMB 1.0/CIFS File Sharing Support
  - ☐ SMB 1.0/CIFS Automatic Removal
  - ☑ SMB 1.0/CIFS Client
  - ☐ SMB 1.0/CIFS Server
- ☑ SMB Direct
- ☐ Telnet Client
- ☐ TFTP Client
- ☐ Virtual Machine Platform
- ☐ Windows Defender Application Guard

Each share can be mounted as network drive as follows:





What network folder would you like to map?

Specify the drive letter for the connection and the folder that you want to connect to:

Drive: I:

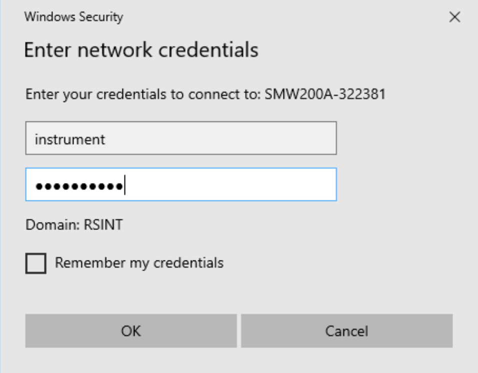
Folder: \\SMW200A-322381\user

Example: \\server\share

□ Reconnect at sign-in

☑ Connect using different credentials

Connect to a Web site that you can use to store your documents and pictures.



Enter network credentials

Enter your credentials to connect to: SMW200A-322381

instrument

••••••••••

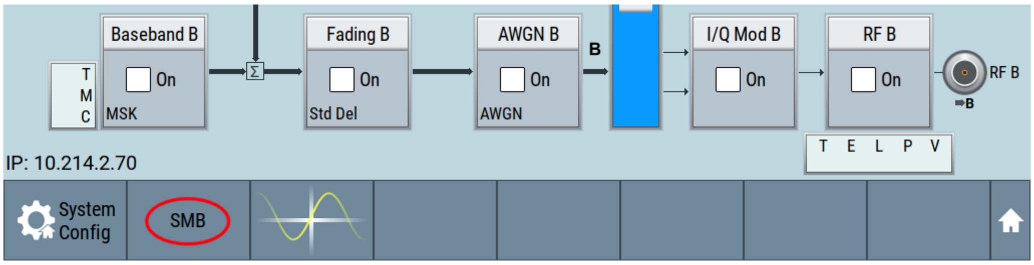
Domain: RSINT

□ Remember my credentials

The default password for the instrument's local user "instrument" is "instrument" if not changed by the customer, which is highly recommended.

The share "share" is now connected as drive i:

The active connection is also displayed in the instrument's status bar:



This network drive can be scanned with a virus scanner like any local or network drive. Please refer to the manual of your preferred virus scanner how to actively scan a drive.

5.4 Scanning from an external boot medium

For instruments which use a control PC based Intel's x86 or x86_64 architecture there is another way to scan for malware. These instruments can be booted from an external USB Pen drive or USB CD-ROM drive with an anti-virus software.

Instrument which make use of an x86 based computer are:

- R&S® SMW200A
- R&S® SMBV100B
- R&S® SMB100B
- R&S® SMA100B
- R&S® AREG100A
- R&S® SMA100A
- R&S® SMF100A

Note:

Many rescue CDs available are restricted to scan NTFS and FAT file systems used by Windows. Linux systems use ext3, ext4, xfs, btrfs or one of many other file systems. The R&S® Embedded Linux based signal generators use an ext3 and ext4 file system as container to store the images of the read-only squashfs file systems. These squashfs file systems contain the actual Embedded Linux OS and R&S® Firmware.

Make sure to use a rescue CD that supports at least the ext3 and ext4 file system.

If your rescue disk displays "no volume found" or something similar, it probably does not understand the Linux ext3/ext4 file system.

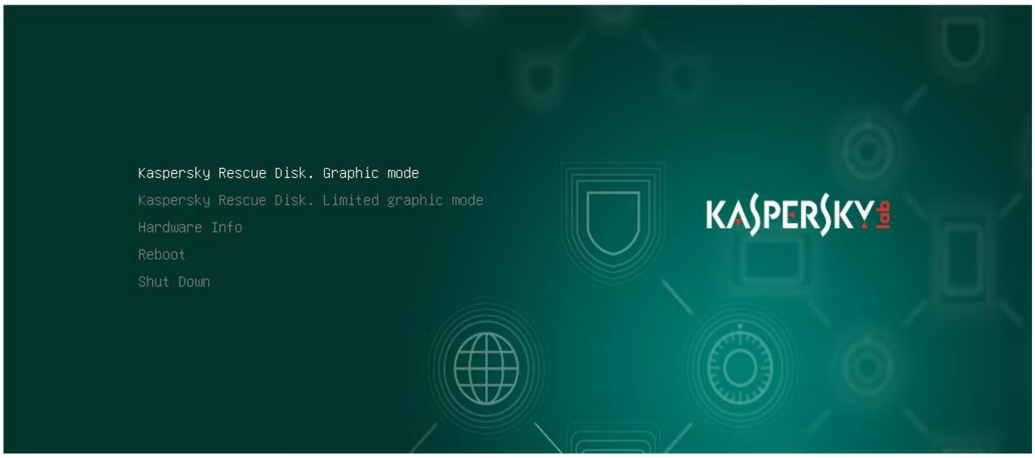
A rescue disk that supports scanning volumes with an ext3/ext4 file system is Kaspersky Rescue Disk 18 [2].

The following examples illustrates how to scan all internal storage media of an R&S® SMW200A with Kaspersky Rescue Disk 18.

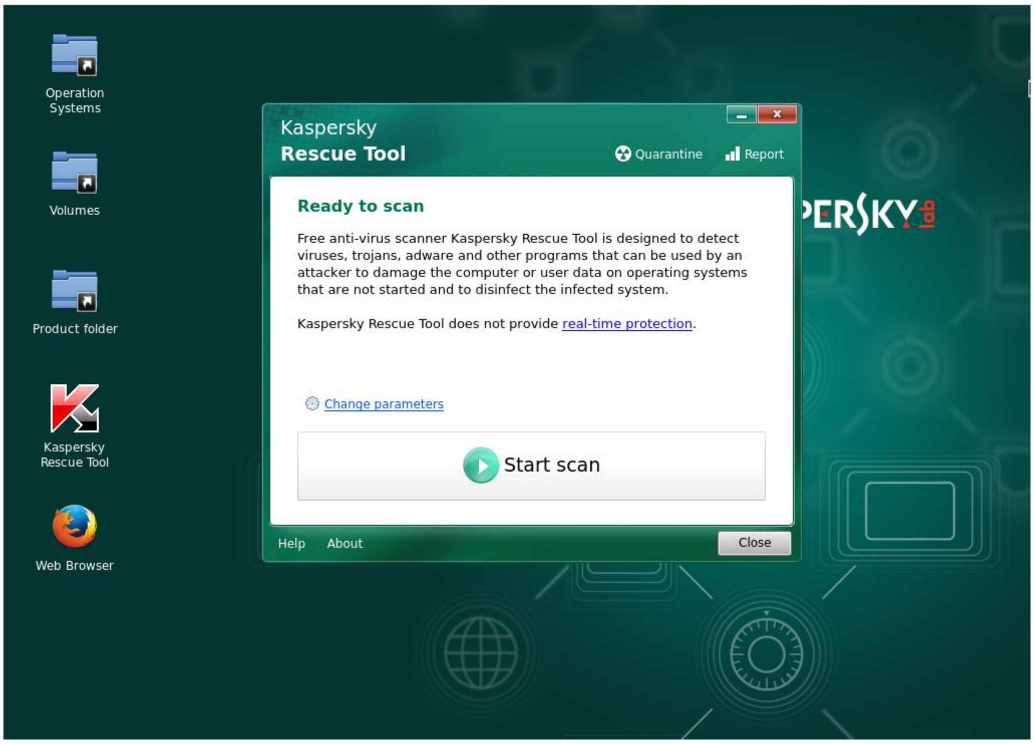
Kaspersky Rescue Disk 18 is offered in form of an iso image that can directly burned to a CD-R. Use this CD-R in an external USB CD-Rom drive to boot the instrument. At the same download address, there is also a handbook for the rescue disk available which explains in detail how to write the rescue disk's iso image to a CD-R or an USB pen drive.

After booting the instrument from the prepared external medium (USB CD-R or USB pen drive) the Kaspersky boot screen shows up and asks you to choose your language.

In the next menu choose “Graphic mode”:


Kaspersky Rescue Disk. Graphic mode
Kaspersky Rescue Disk. Limited graphic mode
Hardware Info
Reboot
Shut Down
KASPERSKY lab

After rescue disk booted up you need to accept the EULA and will then end up at a screen from where you can directly start the scan:

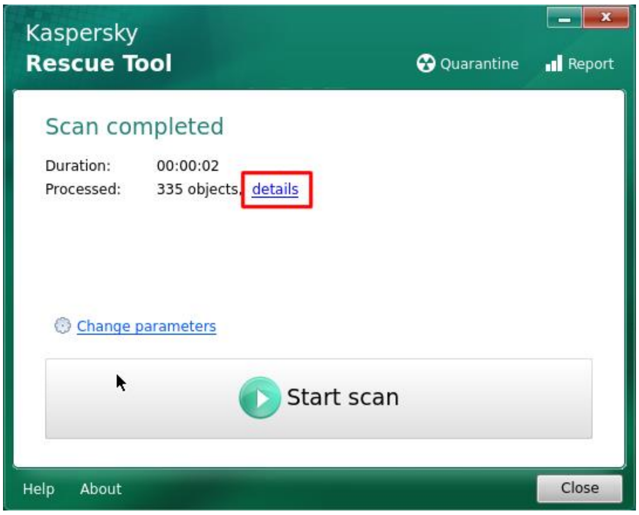


Ready to scan

Free anti-virus scanner Kaspersky Rescue Tool is designed to detect viruses, trojans, adware and other programs that can be used by an attacker to damage the computer or user data on operating systems that are not started and to disinfect the infected system.

Kaspersky Rescue Tool does not provide real-time protection.

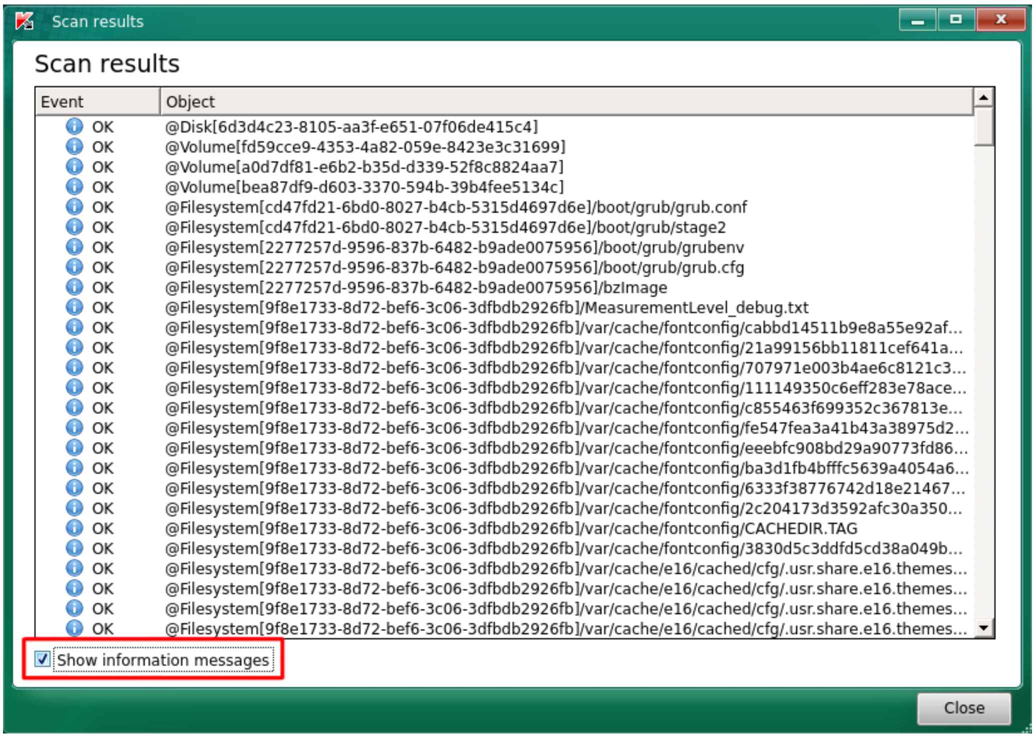
After the scan finished, click on "details" to see the results:



Scan completed

Duration: 00:00:02
Processed: 335 objects, details

In the “Scan results” window, click on “show information messages” to see every scanned file:



Scan results

Event	Object
OK	@Disk[6d3d4c23-8105-aa3f-e651-07f06de415c4]
OK	@Volume[fd59cce9-4353-4a82-059e-8423e3c31699]
OK	@Volume[a0d7df81-e6b2-b35d-d339-52f8c8824aa7]
OK	@Volume[bea87df9-d603-3370-594b-39b4fee5134c]
OK	@Filesystem[cd47fd21-6bd0-8027-b4cb-5315d4697d6e]/boot/grub/grub.conf
OK	@Filesystem[cd47fd21-6bd0-8027-b4cb-5315d4697d6e]/boot/grub/stage2
OK	@Filesystem[2277257d-9596-837b-6482-b9ade0075956]/boot/grub/grubenv
OK	@Filesystem[2277257d-9596-837b-6482-b9ade0075956]/boot/grub/grub.cfg
OK	@Filesystem[2277257d-9596-837b-6482-b9ade0075956]/bzImage
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/MeasurementLevel_debug.txt
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/cabbd14511b9e8a55e92af...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/21a99156bb11811cef641a...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/707971e003b4ae6c8121c3...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/111149350c6eff283e78ace...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/c855463f699352c367813e...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/fe547fea3a41b43a38975d2...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/eeebfc908bd29a90773fd86...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/ba3d1fb4bfffc5639a4054a6...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/6333f38776742d18e21467...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/2c204173d3592afc30a350...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/CACHEDIR.TAG
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/fontconfig/3830d5c3ddfd5cd38a049b...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/e16/cached/cfg/.usr.share.e16.themes...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/e16/cached/cfg/.usr.share.e16.themes...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/e16/cached/cfg/.usr.share.e16.themes...
OK	@Filesystem[9f8e1733-8d72-bef6-3c06-3dfbdb2926fb]/var/cache/e16/cached/cfg/.usr.share.e16.themes...

☑ Show information messages

Of course, booting the instrument from an external medium and scanning for malware is only possible while the instrument is not used in production.

6 Related Documents and Links

[1] The Yocto Project
https://www.yoctoproject.org/

[2] Kaspersky Rescue Disk 18
http://support.kaspersky.com/viruses/krd18

Trademarks

Microsoft and Windows are U.S. registered trademarks of Microsoft Corporation.

Kaspersky and Kaspersky Internet Security are U.S. registered trademarks of Kaspersky Lab ZAO.

Rohde & Schwarz

The Rohde & Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, radiomonitoring and radiolocation. Founded more than 80 years ago, this independent company has an extensive sales and service network and is present in more than 70 countries.

The electronics group is among the world market leaders in its established business fields. The company is headquartered in Munich, Germany. It also has regional headquarters in Singapore and Columbia, Maryland, USA, to manage its operations in these regions.

Regional contact

Europe, Africa, Middle East
+49 89 4129 12345
customersupport@rohde-schwarz.com

North America
1 888 TEST RSA (1 888 837 87 72)
customer.support@rsa.rohde-schwarz.com

Latin America
+1 410 910 79 88
customersupport.la@rohde-schwarz.com

Asia Pacific
+65 65 13 04 88
customersupport.asia@rohde-schwarz.com

China
+86 800 810 82 28 |+86 400 650 58 96
customersupport.china@rohde-schwarz.com

Sustainable product design

- Environmental compatibility and eco-footprint
- Energy efficiency and low emissions
- Longevity and optimized total cost of ownership

Certified Quality Management
ISO 9001

Certified Environmental Management
ISO 14001

This application note and the supplied programs may only be used subject to the conditions of use set forth in the download area of the Rohde & Schwarz website.

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG; Trade names are trademarks of the owners.

PAD-T-M: 3573.7380.02/02.05/EN/

1GP112_1E

Rohde & Schwarz GmbH & Co. KG
Mühldorfstraße 15 | 81671 Munich, Germany
Phone + 49 89 4129 - 0 | Fax + 49 89 4129 – 13777

www.rohde-schwarz.com