MALWARE PROTECTION WINDOWS 10

White paper | Version 01.00

ROHDE&SCHWARZ

Make ideas real



CONTENTS

1	Introduction	4
1.1	Overview	4
1.2	General considerations	4
2	Active directory and group policies.	5
2.1	Change group policies	5
2.2	Computer configuration	б
2.3	User configuration	7
3	User accounts and groups	7
3.1	Administrators	8
3.2	Users	8
3.3	Remote desktop users	8
3.4	User account control	8
3.4.1	Levels	8
3.4.2	Changing UAC settings	g
3.5	Passwords	
3.5.1	Changing the account policies	10
4	Firewall	12
4.1	Default rules	12
4.2	Changing the network profile	
4.3	Adding and removing rules	14
5	Network shares	
5.1	Administrative network shares	
5.2	Creating and removing network shares	

6	Windows updates	25
6.1	Configuring Windows updates	25
6.1.1	Distribution of updates in local network	25
6.1.2	Distribution of updates using WSUS	28
6.2	Enabling the Windows Update service	
6.3	Installing Windows updates	32
6.4	Disabling the Windows Update service	33
6.5	Using the Windows Updater app	
7	Application control policies	
7.1	Default rules	
7.2	Enabling and disabling AppLocker	
7.3	Adding and removing rules	
8	Unified write filter	40
9	Windows apps	40
9.1	Microsoft OneDrive	40
10	Anti-virus software	41
10.1	Windows Defender	41
10.2	Scanning from a USB device	43
10.3	Scanning from a different PC	43
0.3.1	Mapping instrument drives on a computer with Windows 10	43

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

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

The white paper discusses the use of anti-virus software. It also outlines how to keep the Windows 10 operating system properly updated through regular installation of operating system patches.

For further information regarding malware protection please visit: www.rohde-schwarz.com/cybersecurity/malware-schutz

1 INTRODUCTION

Rohde & Schwarz is dedicated to ensure that all Rohde & Schwarz products are shipped virus-free. Instruments that run Windows 10 operating systems should be protected from malware just like any other PC. Users are strongly advised to take such measures to protect their instruments as using anti-virus software and installing Windows updates on a regular basis. We highly recommend 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. This document does not make any difference between 32-bit and 64-bit versions of Windows 10. When using anti-virus software make sure it is designed for your instrument's operating system.

1.1 Overview

Rohde&Schwarz recognizes the potential risk of computer virus infections on Windows based instrumentation that are connected to local area networks (LAN).

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.

1.2 General considerations

The steps described above help to guarantee that any instrument from Rohde&Schwarz will be virus-free when delivered to the customer. From that point on it is the user's responsibility to ensure the security of the instrument.

Before connecting the instrument to your company's network, please consult with your IT department or system administrator to determine what specific policies apply. Bear in mind that the instrument appears to be a standard computer to the network. If applicable, consider the possibility to connect the instrument to a network separated from your company's network (e.g. using virtual LANs, VLANs). Follow your company's policies with regard to computer security and virus protection.

If supported by the instrument, using an IEEE-488 (GPIB) connection for SCPI remote control can be considered as a secure alternative instead of connecting the instrument to your company's network.

Like any computer, all instruments face a possible threat by malware. Therefore it is essential to maintain a high level of security by installing the latest Windows updates, using anti-malware software and keep the system settings as restrictive as possible, while staying operational.

Windows 10 offers a lot of safety and security features to aid to that goal, including user account control (UAC), a built-in firewall and anti-malware protection. AppLocker application control policies make it possible to specify exactly what software can be used by a specific user account. In addition, the unified write filter (UWF) can prevent persistent changes to the data on the instrument's hard disk.

2 ACTIVE DIRECTORY AND GROUP POLICIES

Condition as supplied to customer

- Several group policies are preconfigured to ensure functionality and safety of the instrument
- Since group policies defined in an active directory take precedence over local group policies, it has to be ensured that local group policies aren't overwritten if the instrument is joined to a domain

Group policies are an easy way to manage system settings of instruments. Your local system administrator or IT department can set all settings concerning security from a central point for all instruments connected to your corporate network. If the instrument is joined to an active directory (AD), group policies that are defined in the AD take precedence over the group policies defined locally. By default Rohde&Schwarz instruments have several group policies preconfigured. Please ensure that no important policies conflict with group policies from your AD.

The group policies are subdivided into computer configuration and user configuration. User configuration only applies to a specific user account. Computer configuration applies to the system and includes all security-related settings. Some settings can be configured both in computer configuration and user configuration, for example "Turn off Autoplay". If these conflict, the setting in computer configuration takes precedence over the setting in user configuration.

2.1 Change group policies

To review or change local group policies open the Start menu and type "group policy". Select the option "Edit group policy". This requires administrator rights.



2.2 Computer configuration

The settings in computer configuration apply to all users. In particular the security settings are very important. They include password policies, firewall settings and application control policies. Their usage is described in the following chapters.

Local Group Policy Editor			_		×
File Action View Help					
🗢 🏓 🗖 📰 🗙 🗟 🖬 🖬					
 Local Computer Policy Computer Configuration Software Settings Windows Settings Windows Settings Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Local Policies Local Policies Software Restriction Polici Application Control Polici Advanced Audit Policy Cc Advanced Audit Policy Call 	Name Account Policies Local Policies Windows Firewall with Advanced Security Network List Manager Policies Public Key Policies Software Restriction Policies Application Control Policies FIP Security Policies on Local Computer Advanced Audit Policy Configuration	Description Password and account lockout policies Auditing, user rights and security options policies Windows Firewall with Advanced Security Network name, icon and location group policies. Application Control Policies Internet Protocol Security (IPsec) Administration. M Advanced Audit Policy Configuration	anage ll	Psec poli	icies
	1				

Administrative templates consists of 2019 settings. They are sorted in several categories and subcategories and use telling names, making it easier to find a specific setting. Regardless it is helpful to know the name of certain policies, because there is no search functionality. Group policies in administrative templates include for example Windows update, OneDrive and autoplay policies.

Jocal Group Policy Editor				:
File Action View Help				
🗢 🔿 📷 🗟 🖬 🖉 👘				
 Local Computer Policy Computer Configuration Software Settings Windows Settings Control Panel Control Panel Network Printers Server Start Menu and Taskbar System Windows Components All Settings User Configuration 	Setting Access data sources across domains Access data sources across domains Activate Internet printing Activate Shutdown Event Tracker S Add default Accelerators Add default Accelerators	State Not configured Not configured	Comment No No No No No No No No No No No No No	Path Windows Components\Internet Explorer\ Windows Components\Internet Explorer Windows Components\Internet Explorer Windows Components\Internet Explorer Windows Components\Internet Explorer
2019 setting(s)	Extended Standard			

2.3 User configuration

The settings in user configuration apply to a specific user. As mentioned above, settings in computer configuration take precedence over settings in user configuration. Most relevant settings are in administrative templates. Therein is a total of 1563 user-specific settings subdivided in several categories. The most important ones are described in the corresponding chapters.

State Not configured	Comment	Path	
State Not configured	Comment	Path	_
State Not configured	Comment	Path	
Not configured Not configured	No No No No No No No No No No No No No N	Windows Components/Microsoft Mana Network/Network Connections Network/Network Connections Network/Network Connections Network/Network Connections Network/Network Connections Windows Components/Interret Explorer Windows Components/Interret Explorer	
	Vot configured Vot configured Vot configured Vot configured Vot configured Vot configured Vot configured Vot configured Vot configured Vot configured Not configured Not configured Not configured	Vot configured No Vot configured No Not configured No Not configured No Not configured No Not configured No Not configured No	Vat configured No (Network/Network Connections Vat configured No (Windows Components/Interret Explorer Vat configured No (Windows Components/Interret Explorer Nat configured No (Windows Components/Interret Explorer)

3 USER ACCOUNTS AND GROUPS

Condition as supplied to customer

- ▶ The Instrument user account is logged on automatically
- ▶ The default passwords are commonly known and thus not secure

Most Rohde&Schwarz instruments with Windows 10 come preconfigured with two user accounts: the built in local "Administrator" account and a restricted user account called "Instrument". In most cases the user Instrument is in the remote desktop users group as well, allowing to connect to the instrument via remote desktop protocol (RDP). Members of the administrators group are allowed to connect remotely by default.

Rohde & Schwarz instruments offer an auto-logon feature that logs in the Instrument user account on startup. This behavior can be disabled by changing the data of the value "AutoAdminLogon" in the following registry key to "0":

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

The username and password of the auto login user are defined in the values "DefaultUserName" and "DefaultPassword" of the same registry key.

These values should be adjusted when passwords are changed. We strongly recommend that you neither add nor remove any user accounts on your instrument!

3.1 Administrators

Members of the administrators group have full access on all files excluding critical system files. They are allowed to install software, change system settings and connect to the instrument remotely.

3.2 Users

Members of the users group have limited access on most files. This means they can read but cannot delete, create or change files in the Windows and Program Files folders. They don't have access to files stored in the users folder of other users. It is possible to view system settings, registry keys and most event logs. The security event log is not visible. Changes to the registry are only allowed in HKEY_CLASSES_ROOT and HKEY_CURRENT_USER. Only changes to user-specific, non-critical system settings are allowed. Members of the users group are not allowed to connect remotely to the instrument by default.

3.3 Remote desktop users

Members of the remote desktop users are usually members of the users group as well and therefore have the same rights. Additionally they are allowed to connect to the instrument remotely.

3.4 User account control

On some Rohde&Schwarz instruments, the user account control (UAC) is active by default. In that case, we highly recommend keeping the UAC turned on, as it prevents undetected changes to the system's configuration. Nevertheless the UAC is considered rather a convenience feature than a security feature as it only prevents the user from changing a setting or installing software inadvertently.

3.4.1 Levels

There are four different levels that can be selected when configuring the UAC. The highest level (level 3), which is the default level for restricted users, notifies if apps try to install software or make changes to the computer as well as if the user changes Windows settings. The second highest level, which is default for users with administrator rights, doesn't notify if the user changes Windows settings. The third highest level doesn't dim the desktop when notifying. This setting should only be used if the system is unable to dim the desktop due to technical reasons. The lowest level doesn't notify if apps try to install software or make changes to the computer or when the user changes Windows settings.

UAC levels

	Level 3	Level 2	Level 1	Level 0
Notification if apps try to install software or change Windows settings	•	•	•	-
Dimming of the desktop when a notification is displayed	•	•	-	-
Notification if the user changes Windows settings	•	-	-	-

3.4.2 Changing UAC settings

In order to change UAC settings on your instrument, open the Start menu and type "user account control". Select the option "Change User Account Control settings". Administrator rights are required to change the UAC level.



The UAC level can be adjusted with the slider on the left. Click "OK" to confirm the setting.

👽 User Account Control Settings	8 <u>-</u> 8		×
Choose when to be notified about changes to your computer User Account Control helps prevent potentially harmful programs from making changes to Tell me more about User Account Control settings	your computer.		
Image: Notify me only when apps try to make changes to my computer (default) Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows settings Image: Don't notify me when I make changes to Windows setting			
Фок	Cancel]	

3.5 Passwords

Rohde&Schwarz instruments have default passwords for all user accounts. Please refer to the instrument's manual for details. It is important to change these passwords, because anybody with knowledge of the administrator's password has full control over the instrument, both locally and via network.

We recommend using a secure password and replacing it on a regular basis. A secure password should meet the complexity requirements. These define that a password must not contain the user's account name, and must be at least six characters in length and contain characters from three of the following four categories:

- English uppercase characters (A through Z)
- ► English lowercase characters (a through z)
- ► Base 10 digits (0 through 9)
- ▶ Non-alphabetic characters (for example !, \$, #, %)

There are group policies enforcing the use of a secure password. Among other things, they can define how often the password has to be changed and whether it has to meet the complexity requirements. These group policies can be set by your local system administrator or IT department if the instrument is in an active directory. Otherwise they can be configured locally on the instrument.

3.5.1 Changing the account policies

Open the local group policy editor as described in the chapter "Change group policies". Navigate to "Local Computer Policy" ▷ "Computer Configuration" ▷ "Windows Settings" ▷ "Security Settings" ▷ "Account Policies" ▷ "Password Policy".



As shown in the figure above, there are different policies that can be activated to force the use of a secure password. The policy "Enforce password history" can be configured to store between 0 and 24 passwords. This prevents the re-use of passwords.

"Maximum password age" defines after how many days a password has to be changed. This can be a value between 0 and 999, where 0 means disabled. "Minimum password age" defines after how many days a password can be changed. The value has to be lower than the maximum password age and should be combined with the "Enforce password history" policy.

"Minimum password length" can be a value between 1 and 14. When activated, the "Password must meet complexity requirements" policy enforces the use of a complex password as mentioned above. "Store password using reversible encryption" should not be activated, because it is less secure.



In addition, account lockout policies can be configured, so a user account is locked if too many failed logon attempts are made. "Account lockout threshold" determines after how many failed logon attempts a user account gets locked out. The value can be from 0 to 999, where 0 means this feature is disabled. The following policies can only be activated if a value larger than 0 is set.

"Account lockout duration" determines for how many minutes a user account gets locked out before it gets unlocked automatically. The value can be from 0 to 99999 minutes, where 0 means the user account gets locked out until an administrator explicitly unlocks it. "Reset account lockout counter after" determines the number of minutes that must elapse before the failed logon attempt counter is reset to 0. The value can be from 1 to 99999 minutes and has to be less than or equal to the account lockout duration.

4 **FIREWALL**

Condition as supplied to customer

- ▶ Windows firewall is enabled for all profiles
- ► Inbound connections are blocked by default
- ► Exceptions for all services used by the instrument's firmware are preconfigured
- ► Remote desktop is allowed for all profiles

Rohde & Schwarz instruments with Windows 10 use the built-in firewall to protect itself from attacks over the network. We highly recommend that you not turn off the instrument's firewall. Even in the controlled environment of a corporate network, malware infection over the network is a possible security threat.

There are three different firewall profiles in Windows 10: public, private and domain. By default the public profile is used when connecting the instrument to a network. It is possible to choose the private profile instead. If the instrument is joined to an active directory, the domain profile has to be used. This is done automatically.

4.1 Default rules

The following table shows the commonly used default firewall rules of Rohde&Schwarz instruments. These rules apply to all three different network profiles. The firewall rules of your instrument may vary.

Ports	Service	Description
21 TCP	FTP	Instrument web server, FTP port
80 TCP	Web server	Instrument web server (LXI)
111 TCP and UDP	Portmapper	Portmapper service for VXI-11/LXI
161, 162 UDP, 705 TCP	SNMP	Standard port for SNMP agent
319, 320 TCP and UDP	1588 PTP	LXI clock synchronization, IEEE 1588 precision pime protocol (PTP)
2525 TCP	RSIB	Rohde&Schwarz SCPI socket connection
4880 TCP, 48800 to 48840 UDP	HISLIP	High-speed LAN Interface protocol
5025 to 5030 TCP (data) 5125 to 5130 TCP (control)	TCP socket	'Raw SCPI' socket connection
5353 TCP and UDP, 5354 TCP and UDP	Bonjour	Multicast DNS responder (mDNS)
5044 TCP and UDP	LXI event messaging	LXI LAN messages and events, multicast address UDP: 224.0.23.159
5800 TCP	VNC	Instrument soft front panel via web server (browser interface)
13217 TCP and UDP	RS installer	Rohde&Schwarz software distributor service
14142 to 16383 TCP and UDP (dynamic assignment)	ONC-RPC	SUN ONC-RPC protocol, VXI-11

4.2 Changing the network profile

The network profile can be changed by using the Settings app. Please note that this option could be disabled by a group policy. Select the option "Network & Internet".

Setting	IS		—		×
<u>نې</u>	SETTINGS	Find a	setting		٩
				1	
	口				
	System Display, notifications, apps, power	Devices Bluetooth, printers, mouse	Network & Internet Wi-Fi, airplane mode, VPN		
				•	

Select "Ethernet" on the left side and open the option "Ethernet" on the right side. The option's name will differ when connected to a corporate network.

← Settings			×
🐯 NETWORK & INTERNET	Find a setting		٩
Data usage	Ethernet		
VPN			
Dial-up	Ethernet Connected		
Ethernet			
Proxy	Related settings		
	Change adapter options		

If the option "Find devices and content" is on, the network profile is private.



If the option "Find devices and content" is off, the network profile is public.



4.3 Adding and removing rules

When using additional software, it may be necessary to add exceptions to the firewall rules. Likewise, these exceptions should be removed if the software is uninstalled. Most installers set the necessary rules on their own, but in some cases it might be necessary to do this manually. To do so, open the firewall settings by typing "firewall" in the Start menu and select the option "Windows Firewall with Advanced Security".



Depending on requirements, select either "Inbound Rules" or "Outbound Rules" on the left side.

Pindows Firewall with Advanced	Security			_		>	<
File Action View Help							
Windows Firewall with Advance	Windows Firewall with Advanced Security on Local Computer		Acti	ions			_
Cuthound Rules		^	Win	ndows Firewall	with Adva	ince	•
Connection Security Rules	Windows Firewall with Advanced Security provides network security for Windows computers.			Import Policy			
> 🕾 Monitoring			6	Export Policy.	•		
	Overview 🔺			Restore Defau	It Policy		
	Domain Profile			Diagnose / Re	pair		
	Windows Firewall is on.			View			٠
	Inbound connections that do not match a rule are blocked.		a	Refresh			
	Outbound connections that do not match a rule are allowed.			Properties			
	Private Profile is Active		2	Help			
	Windows Firewall is on.		-				
	S Inbound connections that do not match a rule are blocked.						
	Outbound connections that do not match a rule are allowed.						
	Public Profile						
	Windows Firewall is on.						
	S Inbound connections that do not match a rule are blocked.						
	Outbound connections that do not match a rule are allowed.						
	Windows Firewall Properties						
< >	Gatting Started	~					

Select the option "New rule" on the right side. The process is the same for inbound rules and outbound rules.

e Action View Help								
🔿 🙋 🖬 🔒 👔 📷								
Windows Firewall with Advance	Inbound Rules						Actions	
K Inbound Rules	Name	Group	Profile	Enabled	Action	0 ^	Inbound Rules	
Outbound Rules	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No	Allow	N	New Rule	
Connection Security Rules	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach		No	Allow	N	New Kule	
s wonitoring	BranchCache Peer Discoveny (WSD-In)	BranchCache - Deer Discove	All	No	Allow	N	Filter by Profile	
	Contact Support	Contact Support	All	Vec	Allow	N	Filter by State	
	Core Networking - Destination Unreacha	Core Networking		Ves	Allow	N	Filter by Group	
	Core Networking - Destination Unreacha	Core Networking	All	Ves	Allow	N	10	
	Core Networking - Dynamic Host Config	Core Networking	All	Vec	Allow	N	view	
	Core Networking - Dynamic Host Config	Core Networking	All	Ves	Allow	N	Q Refresh	
	Core Networking - Internet Group Mana	Core Networking	All	Ves	Allow	N	Export List	
	Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Vec	Allow	N	12 Hale	
	Core Networking - IPv6 (IPv6-In)	Core Networking		Ves	Allow	N	мер	
	Core Networking - Multicast Listener Do	Core Networking	All	Vec	Allow	N	Your account	
	Core Networking - Multicast Listener Ou	Core Networking	All	Vec	Allow	N	Disable Rule	
	Core Networking - Multicast Listener Ren	Core Networking		Ves	Allow	N	W co	
	Core Networking - Multicast Listener Rep	Core Networking	All	Vec	Allow	N	d Cut	
	Core Networking - Neighbor Discovery A	Core Networking	All	Ver	Allow	N	Сору	
	Core Networking - Neighbor Discovery A	Core Networking	All	Ver	Allow	N	🗙 Delete	
	Core Networking - Packet Too Big (ICMP	Core Networking	All	Ver	Allow	N	Description	
	Core Networking - Packet 100 big (ichina.	Core Networking	All	Ver	Allow	N	Properties	
	Core Networking - Parameter Problem (I	Core Networking	All	Ver	Allow	N	🛛 🕜 Help	
	Core Networking - Kouter Advertisement	Core iveloworking	All	105	Andw	N V		

Select what kind of rule you want to create. The option "Custom rule" grants the most flexibility. Otherwise you can select to allow or block a certain program, a certain range of ports or to enable a predefined rule. Press "Next" to continue.

🔗 New Inbound Rule Wiza	ard
Rule Type	
Select the type of firewall rule to	o create.
Steps: Program Protocol and Ports Scope Action Profile Name	What type of rule would you like to create? Program Rule that controls connections for a program. Pott Rule that controls connections for a TCP or UDP port. Predefined: Remote Shutdown Rule that controls connections for a Windows experience.
	Custom rule. < Back Next > Cancel

If you chose "Custom", you can now select whether this rule applies to a specific program or all programs. In addition, you can specify what services this rule applies to by clicking "Customize".

💣 New Inbound Rule Wizar	d	×
Program		
Specify the full program path and	executable name of the program that this rule matches.	
Steps:		
Rule Type Recomm	Does this fulle apply to all programs or a specific program?	
Protocol and Ports Scope Action	 All programs Rule appies to all connections on the computer that match other rule properties. 	
 Profile 	This program path:	12
Name	Example c:\path\program.exe %Program.Files%\browser\browser.exe	1
	Services Customize Specify which services this rule applies to.	
	< Back Next > Canc	el

Here you can select either all programs and services, services only or a specific service. A specific service can either be chosen from a list of existing services or stated by its short name.

Apply to all programs and services		
Apply to services only		
Apply to this service:		
Name	Short Name	^
ActiveX Installer (AxInstSV)	AxInstSV	
🥋 AllJoyn Router Service	AJRouter	
S App Readiness	App Readiness	
Application Identity	AppIDSvc	
Sk Application Information	Appinfo	
Application Layer Gateway Service	ALG	
Sk Application Management	AppMgmt	
AppX Deployment Service (AppXSVC)	AppXSvc	
Background Inteligent Transfer Service	BITS	~
Apply to service with this service short name (example	e: eventlog):	

On the next page a protocol can be stated. The list of available options includes HOPOPT, ICMPv4, IGMP, TCP, UDP, IPv6, IPv6-Route, IPv6-Frag, GRE, ICMPv6, IPv6-NoNxt, IPv6-Opts, VRRP, PGM and L2TP. In addition, a custom protocol can be selected by stating its protocol number.

When creating an inbound rule, the local port is the port a certain datagram is received on your instrument and the remote port is the one the sender used.

In case you create a rule for either ICMPv4 or ICMPv6, you can limit it to specific ICMP types by clicking "Customize".

	New Inbound Rule Wizard		×	(
P	rotocol and Ports			
Sp	ecify the protocols and ports to	which this rule applies.		
S	leps:			
	Rule Type	To which ports and proto	cols does this rule apply?	
٠	Program			
٠	Protocol and Ports	Protocol type:	Any 🗸	
۲	Scope	Protocol number:	0 🜩	
۲	Action			
۰	Profile	Local port:	All Pots 🗸	
۲	Name			
			Example: 80, 443, 5000-5010	
		Remote port:	All Pots 🗸	
			Example: 80, 443, 5000-5010	
		Internet Control Message (ICMP) settings:	e Protocol Customize	
			< Back Next > Cancel	

The rule can be limited to apply only to certain IP addresses and interfaces.

Specify the local and remote IP	addresses to which this rule applies.	
Steps:		
Rule Type		
Program	Which local IP addresses does this rule apply to?	
Protocol and Ports	Any IP address	
Scope	O These IP addresses:	
Action		Add
Profile		Edit
Name		
		Remove
	Customize the interface types to which this rule applies:	Customize
	Which remote IP addresses does this rule apply to?	
	Any IP address	
	O These IP addresses:	
		Add
		Edit
		Remove

The interfaces are differentiated in "Local area network", "Remote access" and "Wireless". They can be specified by clicking "Customize".

Customize Interface Types	×
This rule applies to connections on the following interface type	S.
 All interface types These interface types: 	
Local area network Remote access Wireless	
OK Cancel	

The connection can either be allowed, blocked or allowed if it is secure when it matches the previous settings. Since the default inbound rule is to block all incoming connections, we recommend selecting "Allow the connection" or "Allow the connection if it is secure". In case an outbound rule is created, "Block the connection" should be selected, because all outgoing connections are allowed by default.

-	P New Inbound Rule Wizard		Х
A	ction		
Sp	pecify the action to be taken wh	en a connection matches the conditions specified in the rule.	
S	teps:		
	Rule Type	What action should be taken when a connection matches the specified conditions?	
۲	Program	 then a connection matches the conditions specified in the rule. What action should be taken when a connection matches the specified conditions? Allow the connection This includes connections that are protected with IPsec as well as those are not. Allow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customize. 	
۲	Protocol and Ports	Allow the connection This includes connections that are protected with IPsec as well as those are not.	
۲	Scope		
۲	Action	Allow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections	
۲	Profile	will be secured using the settings in IPsec properties and rules in the Connection Security Bule node	
۲	Name		
		Customize	
		C Block the connection	
		< Back Next > Cancel	

In case "Allow the connection if it is secure" is selected, additional options are available. Click "Customize" to specify whether the connection has to be authenticated or encrypted.



In addition, specific user accounts and groups can be stated to have access. If "Override block rules" is selected, a computer or a group of computer accounts has to be specified.

	114 	~
Specify the users that are allow	ed to make the connecton specified by this rule.	
Steps:	Authorized users	
Rule Type	Only allow connections from these users	
Program	Add	
Protocol and Ports	Permate	
Scope	Nellove	
Action		
Users		
Computers	Exceptions	
 Profile 	Skip this rule for connections from these users	
Name	Add	
	Remove	
	Note: user identities can only be verified if an authentication method	
	that carries user identity is used.	
	< Back Next >	Cancel

🔗 New Inbound Rule Wiza	ard	×
Computers		
Specify the computers that are	allowed to make the connection specified by this rule.	
Steps:	Authorized computers	
Rule Type	Only allow connections from these computers:	
Program		
Protocol and Ports	Add	
Scope	Remove	
Action		
Users		
Computers	Exceptions	
Profile	Skip this rule for connections from these computers:	
Name	Add	
	Remove	
	Note: computer identities can only be verified if an authentication	
	method that carries computer identity is used.	
	< Back Next >	Cancel

The next step is to decide which profiles the rule applies to. The choices are "Domain", "Private" and "Public".



Finally the rule has to be named. Choose a name that shows its purpose, for example include the name of the program or port that gets enabled. Writing a description is optional but recommended.

🔗 New Inbound Rule Wizard	1	×
Name		
Specify the name and description	of this rule.	
Steps:		
Rule Type		
Program		
Protocol and Ports		
Scope	Name:	
Action		
Profile	Description (optional):	
Name		
	< Back Finish Cancel	

5 NETWORK SHARES

Condition as supplied to customer

- Administrative network shares are enabled by default
- ► Administrative network shares grant full access to the instrument's hard disk

Network shares can be used to scan an instrument's hard disk drive from a different computer. Therefore, the chapter "Scanning from a different PC". describes how to connect to an instrument's network share.

5.1 Administrative network shares

As on any device with a Windows operating system there is an administrative share for every volume of the instrument by default. The volumes can be accessed by adding the character \$ after the drive letter of the volume. For example, the UNC path \\RS-100000\ C\$

can be used for the Windows partition of an instrument with the computer name "RS-100000". The username and password of an instrument's user with administrator rights is required to connect to an administrative share.

5.2 Creating and removing network shares

Besides administrative shares, custom network shares can be created with in-depth configuration of user permissions. Please note that permissions on network shares should be set as restrictive as possible. In order to create a new share, open the File tab in Windows Explorer and navigate to the folder you want to share. Right-click the folder and select "Share with" ▷ "Specific people".



Select the name of the user or group you want to give access to from the dropdown list or enter the name directly, for example "Everyone". Click "Add" to set the user's or group's permissions.

_	T File Sharing		-		Х
2	a rie snanng				
	Choose people to share with				
	Type a name and then click Add, or click the arrow to find	someone.			
				_	
	Everyone	~	Add		
	Name	Permission Lev	/el		
	8 instrument	Owner			
	l'm having trouble sharing				
		💡 S	hare	Can	icel

The default permission level is "Read". Change this setting according to requirements. The option "Remove" removes the user or group from the list.

hoose people to share with	
pe a name and then click Add, or click th	e arrow to find someone.
	✓ Add
Name	Permission Level
😢 Everyone 🙎 instrument	Read Read Read/Write Remove
m having trouble sharing	

🏪 | 🛃 📙 🖛 | Local Disk (C:) X ~ () Home Share View ← → ~ ↑ 🏪 → This PC → Local Disk (C:) ✓ ^さ Search Local Disk (C:) Q ~ Date modified Name Туре Size Ouick access PerfLogs 7/10/20154:04 AM File folder a OneDrive Program Files 7/1/2016 6:42 AM File folder This PC Program Files (x86) 7/10/2015 4:04 AM File folder Users 7/1/2016 4:25 AM File folder Petwork Windows 7/1/2016 7:24 AM File folder ExampleFolder 7/1/2016 8:54 AM File folder • Homegroup Open Cpen in new window Pin to Quick access Stop sharing Share with > Restore previous versions Create or join a homegroup Include in library > 2 Specific people... Pin to Start Send to > Cut Сору Create shortcut Delete Rename :::: 🖿 6 items 1 item selected Properties

In order to remove a network share, right-click the folder and select "Share with" \triangleright "Stop sharing".

Now you can select whether to remove all permissions or only permissions of single users and groups.



6 WINDOWS UPDATES

Condition as supplied to customer

- On some Rohde&Schwarz instruments, Windows updates are disabled by default to eliminate influence on the instrument's performance
- ▶ Windows updates are enabled by activating the service

Microsoft regularly creates security updates and other patches to protect Windows based operating systems. Instruments using Windows 10 – especially those that connect to a network – should be updated regularly. Usually Windows updates are released on the second Tuesday of each month, but critical updates may be released more frequently.

It is important to distinguish servicing updates from feature upgrades. Rohde&Schwarz instruments use the enterprise long-term servicing channel (LTSC). The servicing lifetime of each LTSC release is at least 10 years. There are no feature upgrades in LTSC to enable long-term deployment of Windows 10 releases in low-change configurations. It is not possible to switch to a different LTSC release by Windows update.

6.1 Configuring Windows updates

Windows updates are configured in the Settings app as well as by group policies. Among others things, it is possible to select where Windows updates shall be received from – this could be either a Microsoft server, your company's WSUS server, any computer on your local network or even any computer on the internet. Please comply with your company's guidelines. We recommend using a WSUS server if available. The receiving of updates from computers on the internet should be disabled.

6.1.1 Distribution of updates in local network

Windows 10 offers the possibility to receive and send Windows updates from and to other devices on the local network and even the internet. In order to disable this feature, open the Start menu und select the Settings app.



Select the option "Update & security" in the Settings app.



Select the option Windows update and click "Advanced options".

← Settings	-	×
ốȝ UPDATE & SECURITY	Find a setting	 ρ
Windows Update	Windows Update	
Windows Defender	Your device is up to date. Last checked: Today, 1:55 PM	
Backup	Check for updates	
Recovery		
Activation	Available updates will be downloaded and installed automatically.	
	Looking for info on the latest updates?	
For developers	Learn more	
	Advanced options	

Click "Choose how updates are delivered".

← Settings	-	×
ADVANCED OPTIONS		
Choose how updates are installed		
Keep everything running smoothly. We'll restart your device automatically when you're not using it. Updates won't download over a metered connection (where charges may apply).		
Give me updates for other Microsoft products when I update Windows.		
Defer upgrades Learn more		
View your update history		
Choose how updates are delivered		

By default the sending and receiving of updates from other devices on the local network is enabled. You can disable this by clicking the switch next to "On". The options below will then be shown grayed out.

÷	Settings		×
<u>ين</u>	CHOOSE HOW UPDATES ARE DELIVERED		
			^
Up Dov	odates from more than one place vnload Windows updates and apps from other PCs in addition		
to N Lear	/licrosoft. This can help speed up app and update downloads. rn more		
Whe dow netw belo	en this is turned on, your PC may also send parts of previously vnloaded Windows updates and apps to PCs on your local work, or PCs on the Internet, depending on what's selected w. On		
Get upd	updates from Microsoft, and get updates from and send lates to		
	PCs on my local network PCs on my local network, and PCs on the Internet		

Sharing Windows updates on the local network can save internet bandwidth when there is no WSUS server available. The option to share Windows updates with computers on the internet should never be used, because it significantly increases the usage of upload bandwidth.

6.1.2 Distribution of updates using WSUS

Your company may use Windows server update services (WSUS) to deploy updates. Contact your local system administrator or IT department for information about your company's update strategy and ensure that updates for Windows 10 are distributed via your company's WSUS server. The usage of a WSUS server can be configured in a group policy, either locally or in the active directory.

In order to set this group policy locally, open the local group policy editor as shown in chapter "Change group policies". Navigate to "Local Computer Policy" ▷ "Computer Configuration" ▷ "Administrative Templates" ▷ "Windows Components" ▷ "Windows Update".

Local Group Policy Editor			-6	٥	×
File Action View Help					
🗢 🔿 📰 🗟 🖬 🛛					
 Search Search Security Center Shutdown Options Smatt Card Software Protection Platfc Somy restings Tablet PC Task Scheduler Windows Color System Windows Color System Windows Color System Windows Color System Windows Defender Windows Logon Options Windows Kedia Digital Ri Windows Media Digital Ri Windows Remote Manage Windows Remote Shell Windows Remote Shell Windows Remote Shell Windows Retings Software Settings Windows Settings Windows Settings Windows Settings 	Windows Update Specify intranet Microsoft update service location Edit policy setting Requirements: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT Description: Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network. This setting lets you specify a server on your network. To use this service for updates that apply to the computers on your network. To use this setting, you must set two servername values: the server from which the Automatic Updates (and tapply to the servet to which updated workstations upload statistics. You can set both values to be the same server. If the status is set to Enabled, the	Setting Do not display 'Install Updates and Shut Down' option in Sh Chabling Windows Update Power Management to automati Chabling Windows Update Power Management to automati Chabling Windows Update Power Management to automati Chabling Windows Update Service location Charles Automatic Updates service location Charles Updates detection frequency Do not connect to any Windows Update Installation Charles Automatic Updates in Scheduled automat Charles Automatic Updates installations Charles Automatic Installations Charles Aut	State Not configured Not configured		
~	Automatic Updates client	<			>
< >	Extended Standard				
19 setting(s)					

Open the policy "Specify intranet Microsoft update service location" by selecting it and clicking "Edit policy setting".

By default this policy is set to "Not Configured". Select "Enabled" and fill the options with the information provided by your local system administrator or IT department. Usually the update service and the statistics server have the same address. The prefix can either be http or https, where the latter is encrypted and therefore the more secure option. The server address can either be a DNS name or an IP address. If the port number is different than 80, it has to be appended with a leading colon. The default port numbers are 8530 for http and 8531 for https. Apply the setting by clicking "OK".

💭 Specify intranet Microsoft	update service location	n – 🗆 X
Specify intranet Microsoft	update service location	n Previous Setting Next Setting
 Not Configured Common Enabled Disabled 	ent:	^ ~
Suppor	ted on: At least Win excluding W	dows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, Vindows RT
Set the intranet update service updates: https://server.company.com:8 Set the intranet statistics serve https://server.company.com	for detecting	Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network. This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on
(example: http://intranetUpd0	1)	To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.
		If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying
		OK Cancel Apply

Optionally the policy "Enable client-side targeting" can be enabled to determine the group the instrument shall be added to automatically. The group must already exist on the WSUS server. Multiple groups can be specified, separated by semicolons. If this policy is not enabled, a server administrator has to add the instrument to a group manually.

Enable client-side targeting	– 🗆 X
Enable client-side targeting	Previous Setting Next Setting
Not Configured Comment: Enabled	^
O Disabled Supported on:	tt least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, xcluding Windows RT
Options:	Help:
Target group name for this computer	Specifies the target group name or names that should be used to receive updates from an intranet Microsoft update service. If the status is set to Enabled, the specified target group information is sent to the intranet Microsoft update service which uses it to determine which updates should be deployed to this computer. If the intranet Microsoft update service supports multiple target groups this policy can specify multiple group names separated by semicolons. Otherwise, a single group must be specified. If the status is set to Disabled or Not Configured, no target group information will be sent to the intranet Microsoft update service. Note: This policy applies only when the intranet Microsoft update service to support client-side targeting. If the "Specify intranet Microsoft update service to support lient on to configured to support client-side targeting. If the "Specify intranet Microsoft update service is no effect. Note: This policy is not supported on Windows RT. Setting this

6.2 Enabling the Windows Update service

On some Rohde&Schwarz instruments, the Windows Update service is not active by default. This is intended to prevent disturbance of the instrument's functionality. In order to install Windows updates, you have to activate this service temporarily. To enable the Windows Update service, the service management console has to be started. Open the Start menu and type "services". Select the option "Services".



Once the "Services" console is displayed, search for the "Windows Update" service:

• 🔿 🔂 🔯 🤇	3 🗟 🚺 🏹 🕨 🔲 11 10					
Services (Local)	Services (Local)	Name ^	Description	Status	Startup Type	Log On As
	Description: Enables the detection, download, and installation of updates for Windows and other programs. If this service is disabled, users of this computer will not be able to use Windows Update or its automatic updating feature, and programs will not be able to use the Windows Update Agent (WUA) API.	Windows Management Inst Windows Media Player Net Windows Mobile Hotspot S Windows Modules Installer Windows Presentation Fou Windows Push Notification Windows Push Notification Windows Store Service (WS Windows Time	Provides a c Shares Win Provides th Enables inst Optimizes p This service Windows R Provides co Provides inf	Running Running	Automatic Disabled Manual (Trig Manual Manual Manual Automatic (D Manual (Trig.	Local Syste Network S Local Service Local Syste Local Syste Network S Local Syste Local Syste Local Syste
		Windows Update	Enables the		Disabled	Local Syste
		Wired AutoConfig Wired AutoConfig WULAN AutoConfig Work Folders Workstation WWAN AutoConfig Xbox Live Auth Manager Xbox Live Game Save Xbox Live Hetworking Service	WinHTTP i The Wired The WLANS Provides pe This service Creates and This service This service This service This service	Running	Manual Manual Manual Manual Automatic Manual Manual Manual Manual	Local Service Local Syste Local Syste Local Syste Local Service Network S Local Service Local Syste Local Syste Local Syste

If the service is disabled (as shown in the figure above), the service must be enabled. To do this, proceed with the next steps. If the service is enabled, you can proceed with installing Windows updates as described in the next chapter. To enable the service, select the "Windows Update" service, open the context menu and select "Properties".

	Þ				
Services (Local)					
Windows Update	Name	Description	Status	Startup Type	Log On As
Description: Enables the detection, downloa installation of updates for Wind and other programs. If this servi disabled, users of this computer not be able to use Windows Up or its automatic updating featu and programs will not be able t the Windows Update Agent (WI API.	d, and d, and d, and d, windows Media Player Net d, Windows Mobile Hotspot S d, Windows Mobile Hotspot S d, Windows Mobules Installer will Q, Windows Postention Fou date d, Windows Push Notification JA) d, Windows Sterestation Fou d, Windows Fou d, Windows Fou d, Windows Fou	 Provides a c Shares Win Provides th Enables inst Optimizes p This service Windows R Provides co Provides inf Maintains d 	Running Running	Automatic Disabled Manual (Trig Manual Manual Manual Automatic (D Manual (Trig Manual (Trig	Local Syste Network S Local Service Local Service Local Service Local Syste Network S Local Syste Local Service
	Windows	s the		Disabled	Local Syste
	WinHTTP Start Wined Aut Stop Wired Aut Stop Wined Aut Pause WMAN Aut Pause Work Folc Workstati Workstati MI Tasks Xbox Live Xbox Live Xbox Live Xbox Live Xbox Live Xbox Live Xbox Live Xbox Live Xbox	TP i ired LANS es pe rvice s and rvice es au rvice rvice	Running	Manual Manual Manual Manual Automatic Manual Manual Manual Manual	Local Service Local Syste Local Syste Local Syste Local Service Network S Local Service Local Syste Local Syste Local Syste

Afterwards the "Windows Update Properties" will be displayed, set "Startup type" to "Automatic" and confirm the dialog with "OK".

Windows	Update I	Properties ((Local Computer) X
General	Log On	Recovery	Dependencies
Service	name:	wuauserv	
Display	name:	Windows l	Update
Descrip	tion:	Enables th updates fo	he detection, download, and installation of or Windows and other programs. If this
Path to C:\Wind	executabl dows\syst	e: em32\svcho	ost.exe k netsvcs
Startup	typ <u>e</u> :	Automatic	~
Service	status:	Stopped	
5	itart	Stop	p <u>P</u> ause <u>R</u> esume
You car from her	n specify t re.	he start para	meters that apply when you start the service
Start pa	ira <u>m</u> eters:		
			OK Cancel <u>Apply</u>

Start the Windows Update service by clicking "Start".

Services (Local)	Services (Local)			2	0	
	Windows Update	Name	Description	Status	Startup Type	Log On As
		Windows Management Inst	Provides a c	Running	Automatic	Local Syste.
	Start the service	🖗 Windows Media Player Net	Shares Win		Disabled	Network S
		🖏 Windows Mobile Hotspot S	Provides th		Manual (Trig	Local Servic
	Description:	🖏 Windows Modules Installer	Enables inst		Manual	Local Syste.
	Enables the detection, download, and	🖏 Windows Presentation Fou	Optimizes p		Manual	Local Servic
	and other programs. If this service is	🖏 Windows Push Notification	This service		Manual	Local Syste.
	disabled, users of this computer will	🏟 Windows Remote Manage	Windows R		Manual	Network S
	not be able to use Windows Update	🏟 Windows Search	Provides co	Running	Automatic (D	Local Syste.
	or its automatic updating feature,	Windows Store Service (WS	Provides inf		Manual (Trig	Local Syste.
	the Windows Update Agent (WUA)	🎇 Windows Time	Maintains d		Manual (Trig	Local Service
	API.	🍓 Windows Update	Enables the		Automatic (T	Local Syste.
		WinHTTP Web Proxy Auto	WinHTTP i	Running	Manual	Local Servic
		🍓 Wired AutoConfig	The Wired		Manual	Local Syste.
		🖏 WLAN AutoConfig	The WLANS		Manual	Local Syste.
		🖏 WMI Performance Adapter	Provides pe		Manual	Local Syste.
		Work Folders	This service		Manual	Local Servic
		Workstation	Creates and	Running	Automatic	Network S
		WWAN AutoConfig	This service		Manual	Local Service
		🔍 Xbox Live Auth Manager	Provides au		Manual	Local Syste.
		🔍 Xbox Live Game Save	This service		Manual	Local Syste.
		Xbox Live Networking Service	This service		Manual	Local Syste.

6.3 Installing Windows updates

In order to install Windows updates, open the Start menu und select the Settings app.



Select the option "Update & security" in the Settings app.



Select "Windows Update" on the left side and click "Check for updates".

← Settings	- □ >	<
🔅 UPDATE & SECURITY	Find a setting	2
Windows Update	Windows Update	
Windows Defender	Your device is up to date. Last checked: Today, 1:55 PM	
Backup	Check for updates	
Recovery		
Activation	Available updates will be downloaded and installed automatically.	
	Looking for info on the latest updates?	
For developers	Learn more	
	Advanced options	
		_

Windows Update will search for updates and install them automatically. Once this is done a reboot may be required. In that case select "Reboot now". After the reboot, repeat the steps described above until all updates have been installed. Continue with stopping and disabling the Windows Update service.

6.4 Disabling the Windows Update service

To disable the Windows Update service, start the services management console as described in the chapter "Enabling the Windows Update service". Select the Windows Update service and press "Stop".

	à 🔒 🛛 🖬 📄 🖛 💷 🕪					
Services (Local)	Services (Local)				pa de la	
	Windows Update	Name	Description	Status	Startup Type	Log On As
		Windows Management Inst	Provides a c	Running	Automatic	Local Syste.
	Stop the service	🖏 Windows Media Player Net	Shares Win		Disabled	Network S
	Restart the service	Windows Mcbile Hotspot S	Provides th		Manual (Trig	Local Service
		Windows Mcdules Installer	Enables inst		Manual	Local Syste.
	Description:	🖏 Windows Presentation Fou	Optimizes p		Manual	Local Servic
	Enables the detection, download, and	Windows Push Notification	This service		Manual	Local Syste.
	and other programs. If this service is	Windows Remote Manage	Windows R		Manual	Network S
	disabled, users of this computer will	Windows Search	Provides co	Running	Automatic (D	Local Syste
	not be able to use Windows Update	Windows Store Service (WS	Provides inf		Manual (Trig	Local Syste
	or its automatic updating feature, and programs will not be able to use	🖏 Windows Time	Maintains d		Manual (Trig	Local Service
	the Windows Update Agent (WUA)	🍓 Windows Update	Enables the	Running	Automatic (T	Local Syste
	API.	WinHTTP Web Proxy Auto	WinHTTP i	Running	Manual	Local Service
		Wired AutoConfig	The Wired		Manual	Local Syste
		🖏 WLAN AutoConfig	The WLANS		Manual	Local Syste
		Sector WMI Performance Adapter	Provides pe		Manual	Local Syste
		Work Folders	This service		Manual	Local Service
		Workstation	Creates and	Running	Automatic	Network S
		WWAN AutoConfig	This service		Manual	Local Servic
		🔍 Xbox Live Auth Manager	Provides au		Manual	Local Syste.
		🔍 Xbox Live Game Save	This service		Manual	Local Syste.
		Kbox Live Networking Service	This service		Manual	Local Syste.

Right-click the Windows Update service to open the context menu and select "Properties". Change the startup type to "Disabled".

6.5 Using the Windows Updater app

Some Rohde&Schwarz instruments offer the Windows Updater app, a convenient and easy way to install Windows updates. Open the Start menu as the instrument user. Click the tile "Win10 Updates".

lnstrument		
Most used		
Snipping Tool		
🧭 Paint	Search	
Notepad	2	
	Contact Support	Win10 Updates
🛱 File Explorer >		
နိုင္တဲ့ Settings		
() Power		
E All apps		
Search Windows		

A dialog will ask whether you want to continue or not. Click "Yes" to continue.



Enter the administrator password in the user account control dialog and continue with "Yes". The app will automatically search for updates and security updates and install them. The progress is displayed on the tile in the Start menu.



In case a reboot is required, the following message is displayed and the instrument reboots automatically.



7 APPLICATION CONTROL POLICIES

Condition as supplied to customer

- The default AppLocker policies allow the execution of all files in the Windows and Program Files folders
- ► The administrator account is allowed to execute any software
- ► Any executables signed by Rohde&Schwarz are allowed to be executed
- ► Any other software cannot be executed by a standard user

AppLocker application control policies define which user account is allowed to run what software. It has two different modes of operation, determined by the default enforcement policy. One possibility would be to allow everything and block certain software. Rohde&Schwarz instruments use the opposite approach. By default the execution of any software is blocked and certain software is allowed to be executed.



7.1 Default rules

By default the execution of valid signed software from Rohde&Schwarz as well as software in the Program Files folder and the Windows folder is allowed for all users. All users with administrator rights are allowed to execute any software. These rules are divided into four categories:

Executable rules

Action	User	Name	Condition	Exceptions
🗸 Allow	Everyone	(Default Rule) All files located in the Program Files folder Path		
🕖 Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
🕖 Allow	BUILTIN\Administrators	(Default Rule) All files Path		
🐼 Allow	Everyone	Signed by O=ROHDE & SCHWARZ GMBH & CO. KG, L	Publisher	

Windows installer rules

Action	User	Name	Condition	Exceptions
🕖 Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
🕖 Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
🕖 Allow	BUILTIN\Administrators	(Default Rule) All files	Path	

Script rules

Action	User	Name	Condition	Exceptions
🕖 Allow	Everyone	(Default Rule) All files located in the Program Files folder Path		
🕖 Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
🕖 Allow	BUILTIN\Administrators	(Default Rule) All files	Path	

Packaged app rules

Action	User	Name	Condition	Exceptions
🐼 Allow	Everyone	(Default Rule) All files located in the Program Files folder	Path	
😻 Allow	Everyone	(Default Rule) All files located in the Windows folder	Path	
🐼 Allow	BUILTIN\Administrators	(Default Rule) All files	Path	

There are three different kinds of rules based on either signature, hash value or location of a file. The default rules are based on file location, as it is easy to allow all programs in the Windows folder. Since a user without admin rights isn't allowed to copy files there, this is considered secure. The same applies to the Program Files folder. Rules based on a file's hash value are a good way to allow a specific version of a software to run. The downside is that with each update a new AppLocker policy has to be created. We therefore recommend using rules based on signatures when adding new rules. These can allow some or all software signed by a certain publisher.

7.2 Enabling and disabling AppLocker

AppLocker can be configured in the local group policy editor. Navigate to "Local Computer Policy" \triangleright "Computer Configuration" \triangleright "Windows Settings" \triangleright "Security Settings" \triangleright "Application Control Policies" \triangleright "AppLocker". In the main window select "Configure rule enforcement". Select or deselect the categories of rules that shall be enforced and confirm your selection by clicking "OK".

AppLocker Properties	×
Enforcement Advanced	
Specify whether AppLocker rules are enforced for each rule collection.	
Executable rules:	
Enforce rules ~	
Windows Installer rules Configured	
Enforce rules V	
Script rules: Configured Enforce rules	
Packaged app Rules:	
Enforce rules ~	
More about rule enforcement	
OK Cancel Apply	0

7.3 Adding and removing rules

The easiest way to add new rules is to right-click one of the groups and select "Automatically Generate Rules". It is possible to generate specific in-depth rules by selecting "Create New Rule" as well.

Create New Rule	
Automatically Generate Rules	
Create Default Rules	
View	
Export List	
Help	

The dialog that opens is basically the same for each category of rules. In this example, executable rules shall be created. First select the user or security group the rules shall apply to. Second, select the folder containing the software you want to allow. Enter a name for this set of rules and proceed by clicking "Next".

Automatically Generate Executable Rules	×
Folder and Permissions	
This wizard helps you create groups of AppLocker rules by analyzing the files within a folder that you select.	
User or security group that the rules will apply to:	
Everyone Select	
Folder that contains the files to be analyzed:	
C:\Program Files\MyProgram Browse	
Name to identify this set of rules:	
MyProgram	
More about these settings	
< Previous Next > Create Cancel	

Now you can specify how the rules shall be generated. The default settings are recommended for most use cases. Rules are generated for each valid signature. If no signature is found, a rule based on the file's hash value is generated. Proceed by clicking "Next".

Automatically Generate Executable Rules	×
Rule Preferences	
Select the type of rules that you want to create. You should only create file hash rules when necessary. A file hash rule must be revised every time that the file is updated and a large number of file hash rules might affect system performance.	
Create publisher rules for files that are digitally signed	
If a file is not signed, create the following type of rule:	
File hash: Rules are created using a file's hash	
O Path: Rules are created using file's path	
○ Create file hash rules for all files	
Reduce the number of rules created by grouping similar files	
More about rule preferences	
< Previous Next > Create Cancel	

You can review the analyzed files and the rules to be generated. Finish the operation by clicking "Create".

Automatically Generate Executable Rules X							
	Review Rules						
	The folder analysis is comp	lete and the follow	ving rules will	be added to the J	policy.		
	Rule Type	Rules		Files			
	Publisher	1		1			
	File Hash	0		0			
	Total	1		1			
	Review files that wer View rules that will b Click Create to close the v	e analyzed e automatically cro vizard and create tl	eated he rules.				
			< Previous	Next >	Create	Cancel	

In case the default rules are not present, the system queries whether to create them automatically.

AppLocke	r	×
	The default rules are currently not in the rule list for this rule collection. When creating rules, it is recommended that you also create the default rules to ensure that important system files will be allowed to run.	
	Yes No	

Any rules can be removed by right-clicking a rule and selecting "Delete". You will be prompted to confirm the deletion by clicking "Yes".

8 UNIFIED WRITE FILTER

Condition as supplied to customer

- ► Unified write filter (UWF) is optional and not applicable to all instruments
- ▶ If enabled, UWF prevents persistent changes to the hard disk

UWF is included in every Windows 10 IoT Enterprise image but by default not active on all instruments. It provides the capability to redirect any write access on the hard disk drive to a virtual overlay. This means all changes to the system are wiped when turning off or rebooting the instrument. Note that UWF cannot be used to protect any removable devices, USB devices or flash drives. Individual files, folders and registry keys can be excluded from the overlay. UWF replaces the previously used file based write filter (FBWF) and enhanced write filter (EWF).

UWF can be configured by using Windows management instrumentation (WMI, for example in a PowerShell script) or the command line tool uwfmgr.exe. We do not recommend changing the UWF's configuration on your own, as it affects the instrument's functionality.

9 WINDOWS APPS

Condition as supplied to customer

- There are no Windows apps on Rohde&Schwarz instruments because of usage of long-term servicing channel (LTSC)
- The browser Microsoft Edge is not available
- Cortana is not available
- ► Apps from the Microsoft Store cannot be installed
- Microsoft OneDrive is disabled by default

Rohde&Schwarz instruments with Windows 10 use the long-term servicing channel (LTSC), where no Microsoft Store apps are included. This includes Cortana, the browser Microsoft Edge and the Microsoft Store itself. Therefore no new apps can be installed using the store mechanic. Instead of Microsoft Edge, the included Internet Explorer 11 can be used. Otherwise any third-party browser can be installed and used.

9.1 Microsoft OneDrive

Microsoft OneDrive is disabled by group policy on all Rohde&Schwarz instruments to prevent the upload of sensitive data to the cloud.

10 ANTI-VIRUS SOFTWARE

Condition as supplied to customer

- Windows Defender is disabled by default
- ► No additional anti-virus solution is installed

Anti-virus software is an essential part of software security on Rohde & Schwarz instruments as well as on any PC or server. While Windows 10 comes with a reasonable anti-virus software included (i.e. Windows Defender), We recommend using third-party software to protect your instrument from malware.

There are different anti-virus software solutions available from different manufacturers that offer good protection against malware. Although they differ in their requirement of system resources and handling, they have quite equally good detection rates. Please abide by your company's policy and use the anti-virus software solution provided by your IT department.

General recommendation

- Disable any on-access scanner and additional features to prevent performance influences on the instrument's firmware
- ► Always update virus definitions before performing a scan
- ▶ Perform a full system scan at least once a week

10.1 Windows Defender

Windows Defender is built-in anti-virus software that provides reasonable protection against malware. It offers real-time scans as well as the option to scan the hard disk on demand. In order to perform a scan, type "defender" in the Start menu and select "Windows Defender".



In the main dialog you can select whether to perform a "Quick", "Full" or "Custom" scan. By selecting "Quick", Windows Defender will scan for viruses, spyware and unwanted software on certain parts of the hard disk. This scan will take a few minutes. By selecting "Full", Windows Defender will scan the entire hard disk as well as all running programs. This scan can take more than one hour. You can scan a subset of folders by selecting a "Custom" scan. The virus and spyware definitions are automatically updated through the Windows Update service on a weekly basis.



Windows Defender can be configured in the Settings app. The real-time scanner can only be disabled temporarily.

← Settings	– 🗆 X
OPDATE & SECURITY	Find a setting ρ
Windows Update	Real-time protection
Windows Defender	This helps find and stop malware from installing or
Backup	running on your PC. You can turn this off temporarily, but if it's off for a while we'll turn it back on automatically.
Recovery	On
Activation For developers	Cloud-based Protection Get better, faster protection by sending Microsoft info about potential security problems Windows Defender finds. The output of the
	Sample submission Help us make Windows Defender better by sending Microsoft malware samples so we can learn about potential security problems and catch them earlier. The privacy Statement

Please note that Windows Defender will be disabled if third-party anti-virus software is installed.

10.2 Scanning from a USB device

Most anti-virus software solutions offer the possibility to create bootable USB flash drives. This is a safe way to scan your instrument outside production time. Please refer to the manual of your anti-virus software for further information.

10.3 Scanning from a different PC

Scanning your instrument's hard disk drive from a different PC is an easy and convenient way to scan multiple instruments in an automated way. This only works if the instruments are connected to the same network as the scanning PC.

10.3.1 Mapping instrument drives on a computer with Windows 10

Open the File tab in Windows Explorer and right-click the folder "This PC" on the left side to open the context menu and select "Map network drive".

💻 🛃 📄 🖛 Thi	is PC		5 <u>07</u>	ΟX	
File Computer	View			~ 🕐	
← → • ↑ 💻	This PC	ٽ ~	Search This PC	٩	
> 📌 Quick access	> Folders (6)) nd drives (3) —			
	Local Disk (C:)				
This PC	Expand				
> 💣 Network	Manage Pin to Start Map network drive Open in new window Pin to Quick access Disconnect network drive Add a network location Delete				
9 items	Rename Properties		_		

Select the drive, folder and the option "Connect using different credentials" and confirm the dialog with the "Finish" button. We recommend using the administrative share "C\$".

			×
~	Map N	etwork Drive	
	What ne	etwork folder would you like to map?	
	Specify the	e drive letter for the connection and the folder that you want to connect to:	
	<u>D</u> rive:	S: ~	
	F <u>o</u> lder:	\\RS-100000\C\$ <u>B</u> rowse	
		Example: \\server\share	
		<u> </u>	
		Connect using different credentials	
		Connect to a Web site that you can use to store your documents and pictures.	
		<u> </u>	el

Enter the login information of your instrument's administrator account. Please refer to the instrument's manual for details. It might be necessary to add the instrument's computer name in front of the name of the instrument's administrator account name.

Windows Security	×
Enter network credentials Enter your credentials to connect to: RS-10000	
\\RS-100000\Administrator A	
Domain:	
ок с	ancel

To scan the instrument's hard drive, start the anti-virus software on the control PC. Select one of the mapped drives of the instrument and run a virus scan. Please refer to the anti-virus software's user manual for how to scan a network drive.

In order to return the PC to its original state, the network share should be removed. Open the File tab in Windows Explorer and expand the folder "This PC" to see all drives. Rightclick the network share to open the context menu and select "Disconnect".



11 REFERENCES

- [1] Mitigate threats by using Windows 10 security features https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-10-security-guide
- [2] Security policy settings https://technet.microsoft.com/en-us/itpro/windows/keep-secure/security-policy-settings
- [3] Changes to Group Policy settings for Windows 10 Start https://technet.microsoft.com/en-us/itpro/windows/manage/changes-to-start-policies-in-windows-10
- [4] New policies for Windows 10 https://technet.microsoft.com/en-us/itpro/windows/manage/new-policies-for-windows-10
- [5] Windows firewall with advanced security https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/ windows-firewall-with-advanced-security
- [6] Update Windows 10 in enterprise deployments https://technet.microsoft.com/en-us/itpro/windows/manage/introduction-to-windows-10-servicing
- [7] AppLocker https://technet.microsoft.com/en-us/itpro/windows/keep-secure/applocker-overview
- [8] Next-generation protection in Windows 10, Windows Server 2016, and Windows Server 2019 https://technet.microsoft.com/en-us/itpro/windows/keep-secure/windows-defender-in-windows-10

Trademarks

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

Rohde & Schwarz

The Rohde&Schwarz electronics group offers innovative solutions in the following business fields: test and measurement, broadcast and media, secure communications, cybersecurity, monitoring and network testing. Founded more than 80 years ago, the independent company which is headquartered in Munich, Germany, has an extensive sales and service network with locations in more than 70 countries.

www.rohde-schwarz.com

Rohde & Schwarz customer support

www.rohde-schwarz.com/support



3608.6454.52 01.00 PDP 1 en