MALWARE PROTECTION WINDOWS 8

ROHDE & SCHWARZ

Make ideas real

CONTENTS

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 8 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 ensuring that all Rohde & Schwarz products are shipped virus-free. Instruments that run Windows 8 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 8. 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 8 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.

Please refer to the "Group Policy Settings Reference for Windows and Windows Server" linked in References (page 35) for more information about the functionality of specific group policies.

2.1 Change group policies
To review or change local group policies open the start screen and type "group policy". Click "Settings" and select the option "Edit group policy". This requires administrator rights.
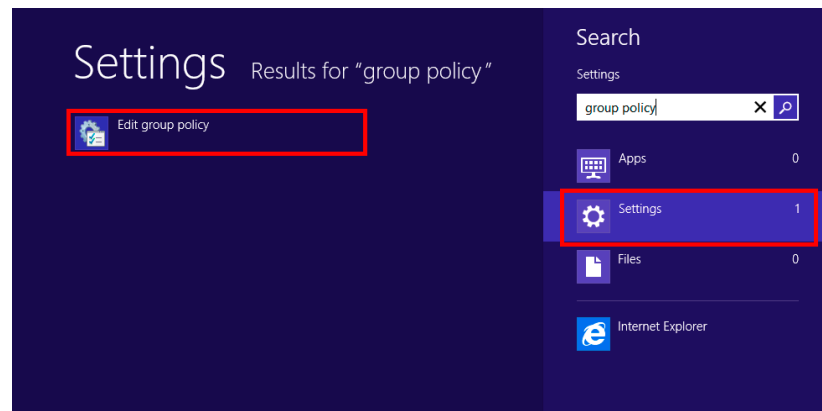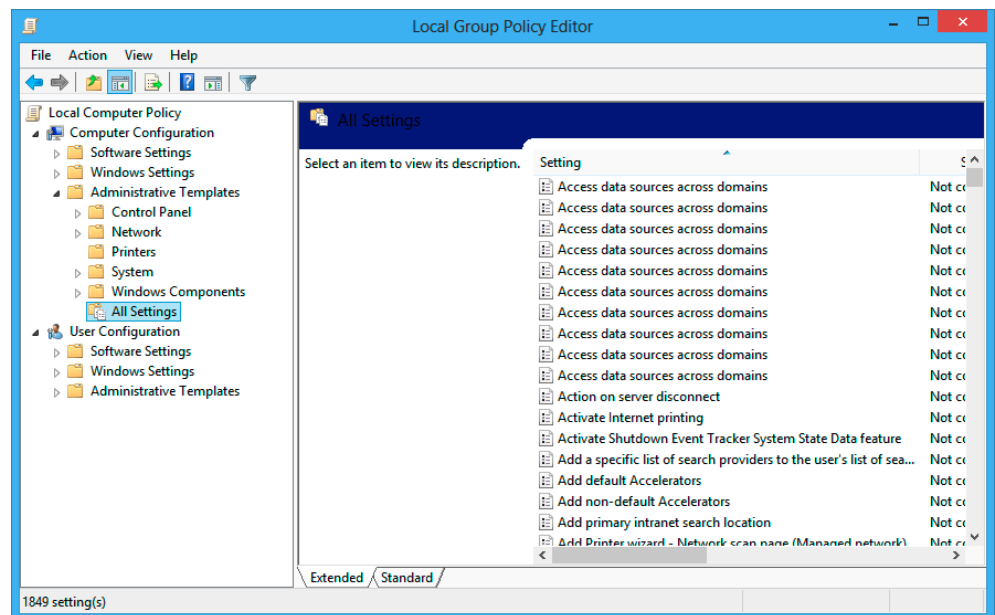
2.2 Computer configuration

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.
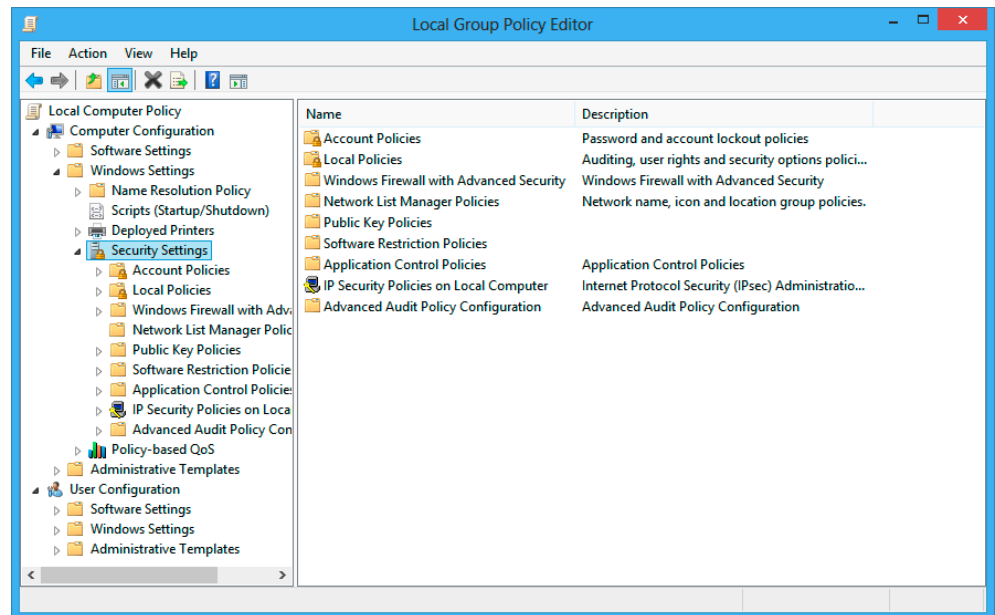

Administrative templates consists of 1849 settings. They are sorted in several categories and subcategories and use telling names, making it easier to find a specific setting. Regardless it is helpful to know the name of certain policies, because there is no search functionality. Group policies in administrative templates include for example Windows Update, OneDrive and autoplay policies.

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 1528 user specific settings subdivided in several categories. The most important ones are described in the corresponding chapters.
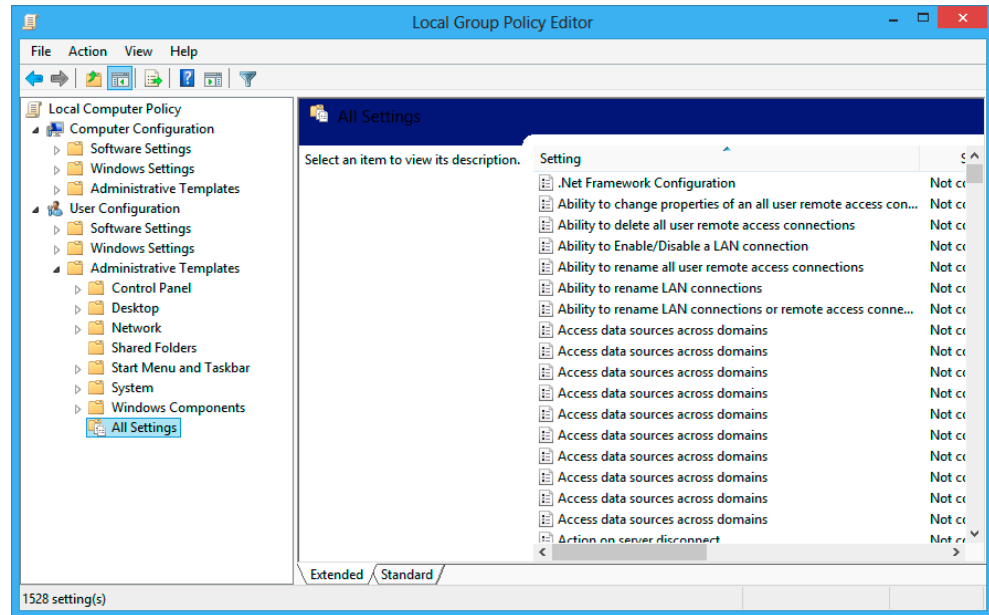
3　USER ACCOUNTS AND GROUPS

Condition as supplied to customer
▶ User account control (UAC) is disabled by default
▶ The instrument user account is logged on automatically
▶ The default passwords are commonly known and thus not secure

Most Rohde & Schwarz instruments with Windows 8 come preconfigured with three user accounts: the built in local "Administrator" account, an administrator account called "Instrument" and a restricted user account called "NormalUser". In most cases the user NormalUser 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. It is strongly recommended to 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

The user account control (UAC) is disabled by default on all Rohde & Schwarz instruments using Windows Embedded 8 Standard. We highly recommend keeping the UAC turned off as it is required for the instrument's functionality. 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 screen and type "user account control". Click "Settings" and select the option "Change User Account Control settings". Administrator rights are required to change the UAC level.
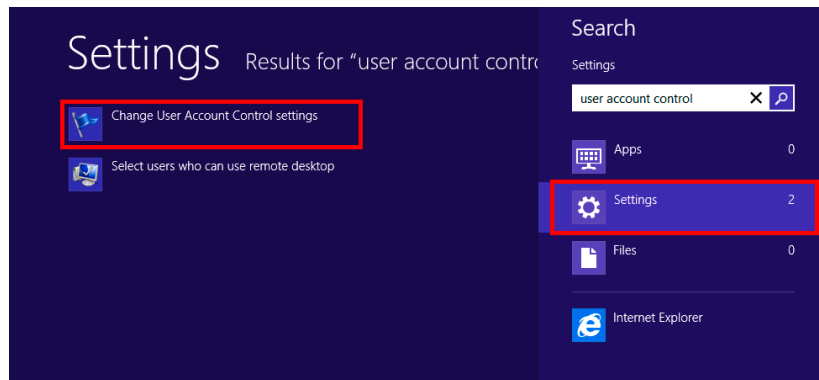
The UAC level can be adjusted with the slider on the left. Click "OK" to confirm the setting.
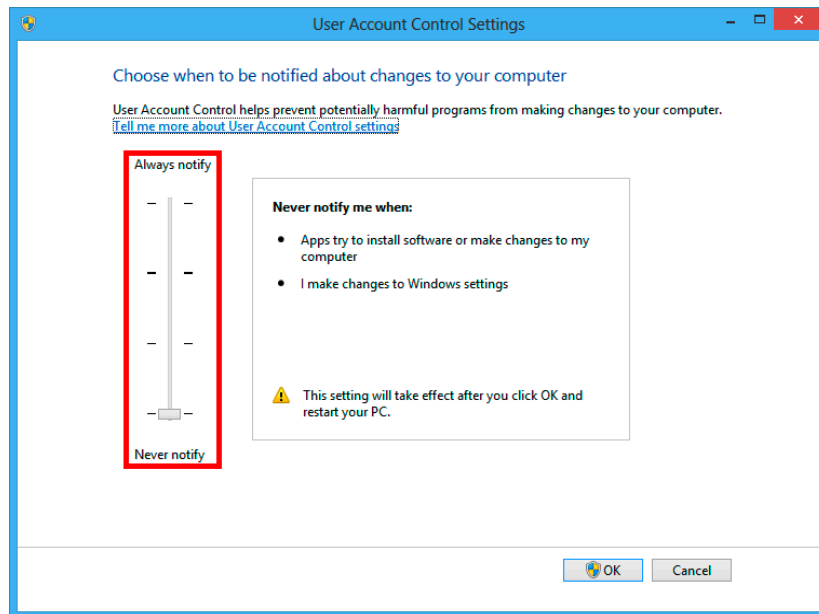
3.5 Passwords

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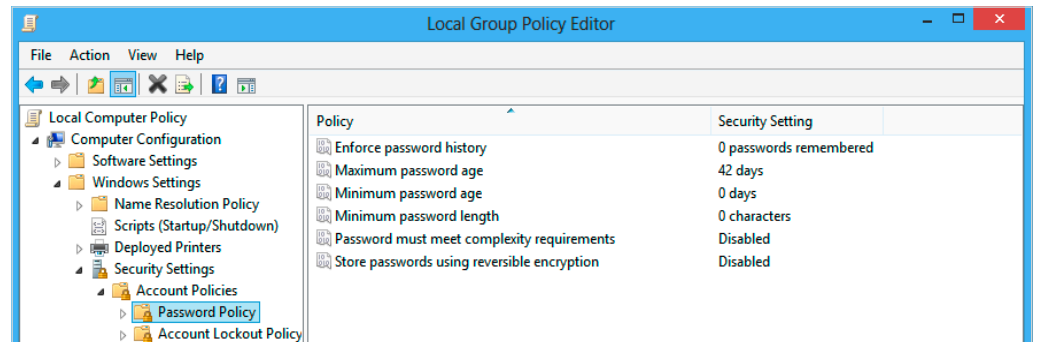
As shown in the figure above, there are different policies that can be activated to force the use of a secure password. The policy "Enforce password history" can be configured to store between 0 and 24 passwords. This prevents the re-use of passwords.

"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.
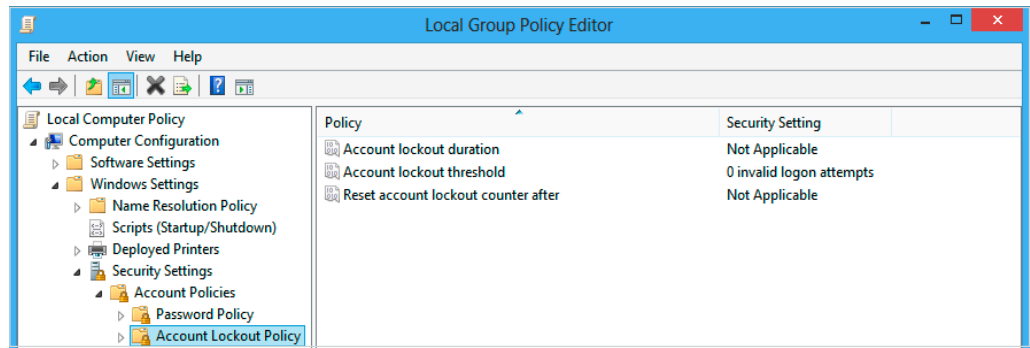
In addition, account lockout policies can be configured, so a user account is locked if too many failed logon attempts are made. "Account lockout threshold" determines after how many failed logon attempts a user account gets locked out. The value can be from 0 to 999, where 0 means this feature is disabled. 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 99 999 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 99 999 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 8 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 8: 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.
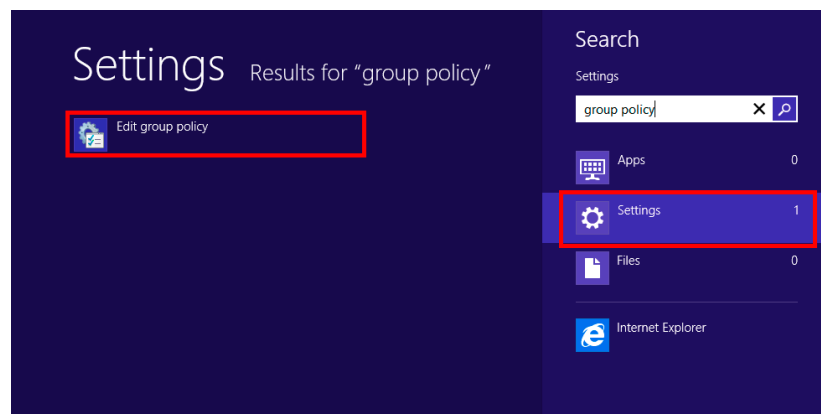
4.1 Default rules

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 ports 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

In order to change the network profile open the charms bar by pressing Windows + C. Select "Settings" and click the Ethernet icon shown in the middle picture below. Perform a right click and then click "Turn sharing on or off".
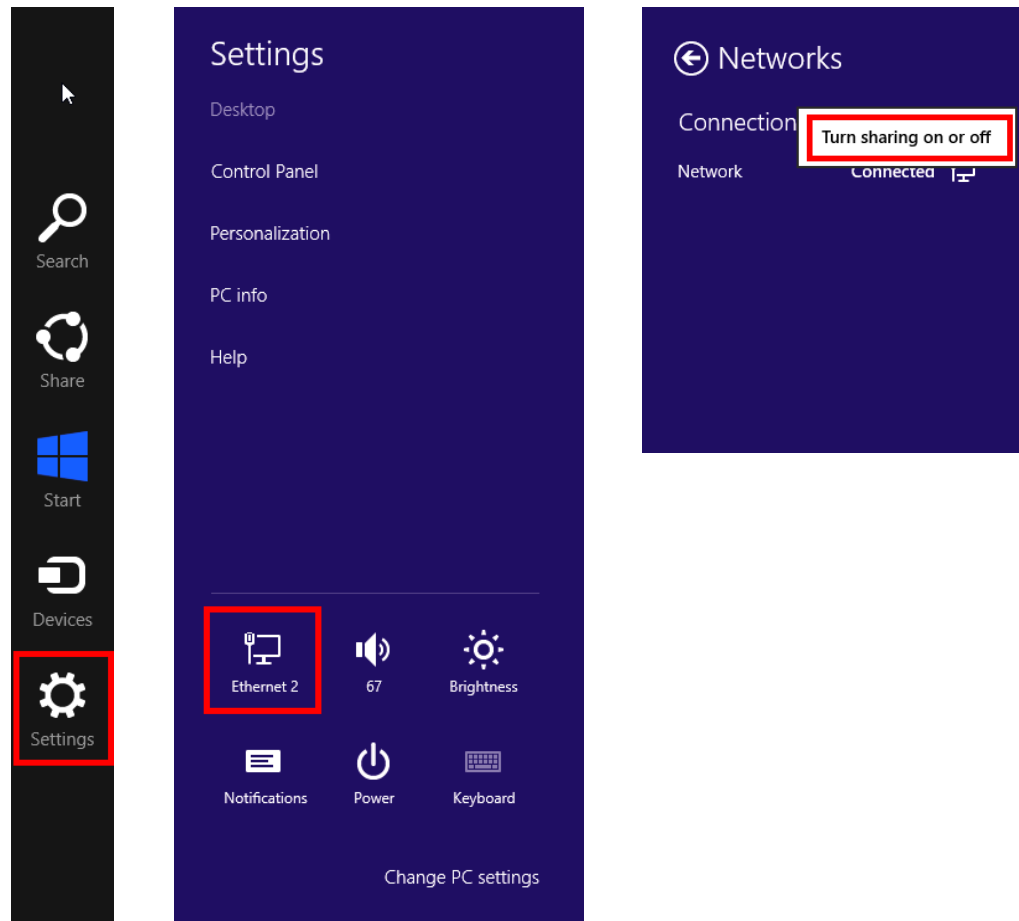
Select the option "Yes, turn on sharing and connect to devices" to switch to the private network profile or select the option "No, don't turn on sharing or cennect to devices" to switch to the public network profile.
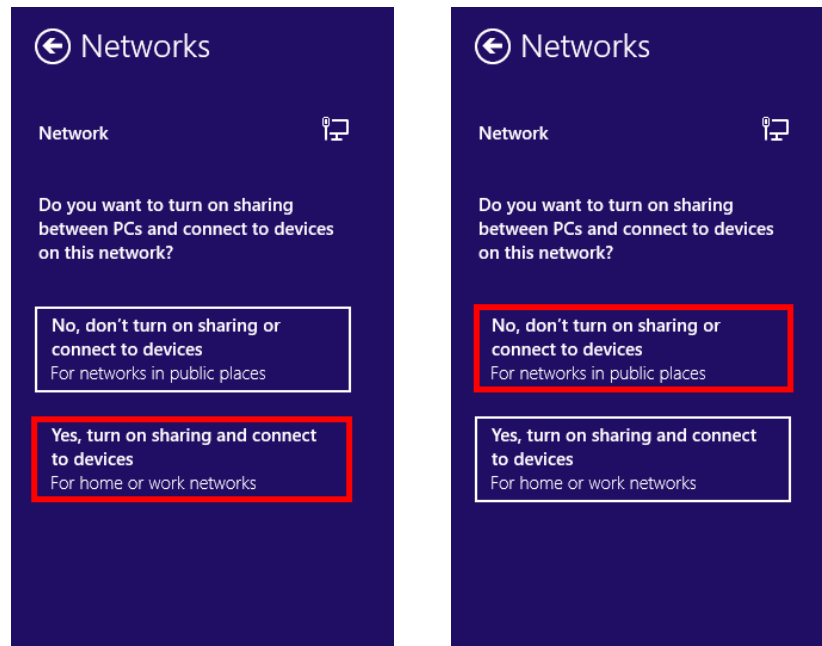
4.3 Adding and removing rules

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 neces-sary to do this manually. To do so, open the firewall settings by typing "firewall" in the Start menu, click "Settings" and select the option "Windows Firewall".
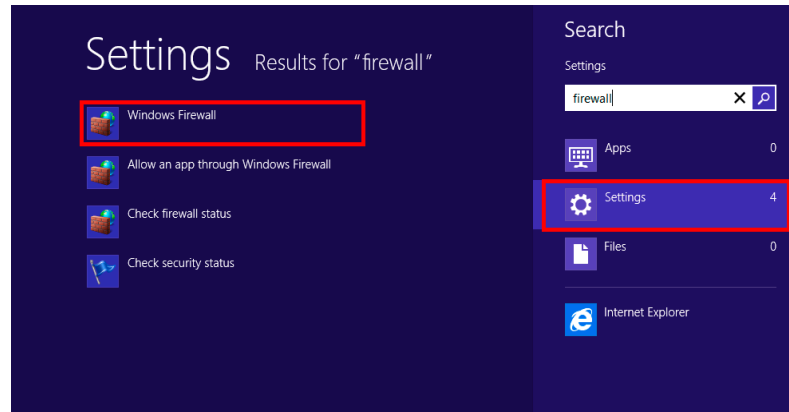
Click "Advanced settings" on the left side of the screen.
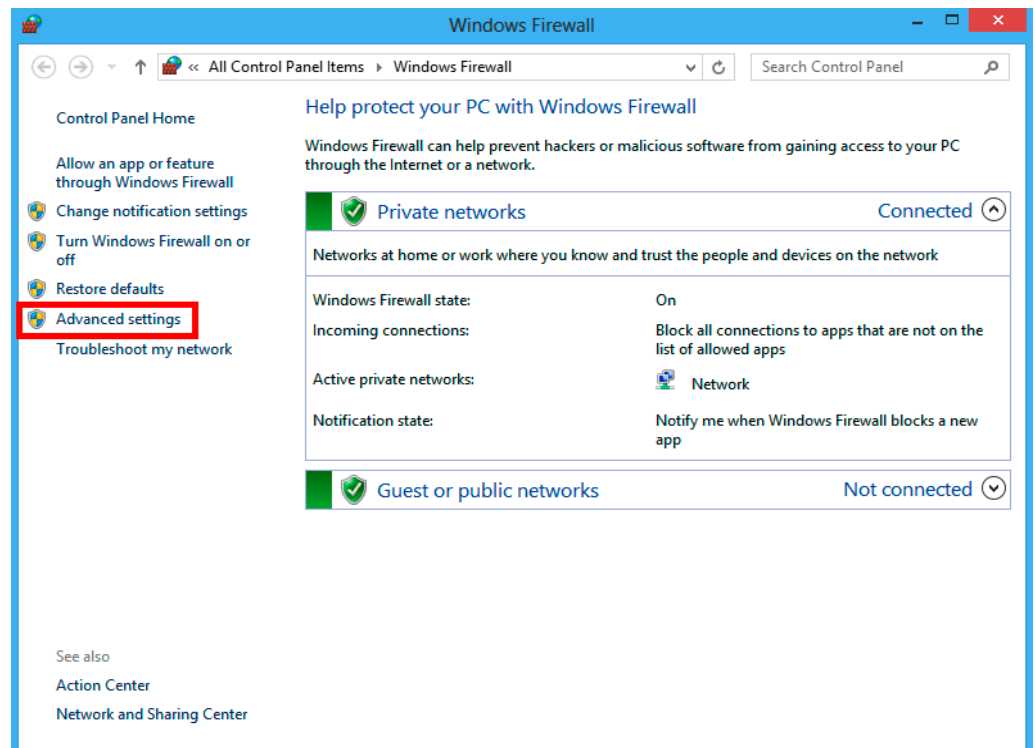
Depending on requirements, select either "Inbound Rules" or "Outbound Rules" on the left side.
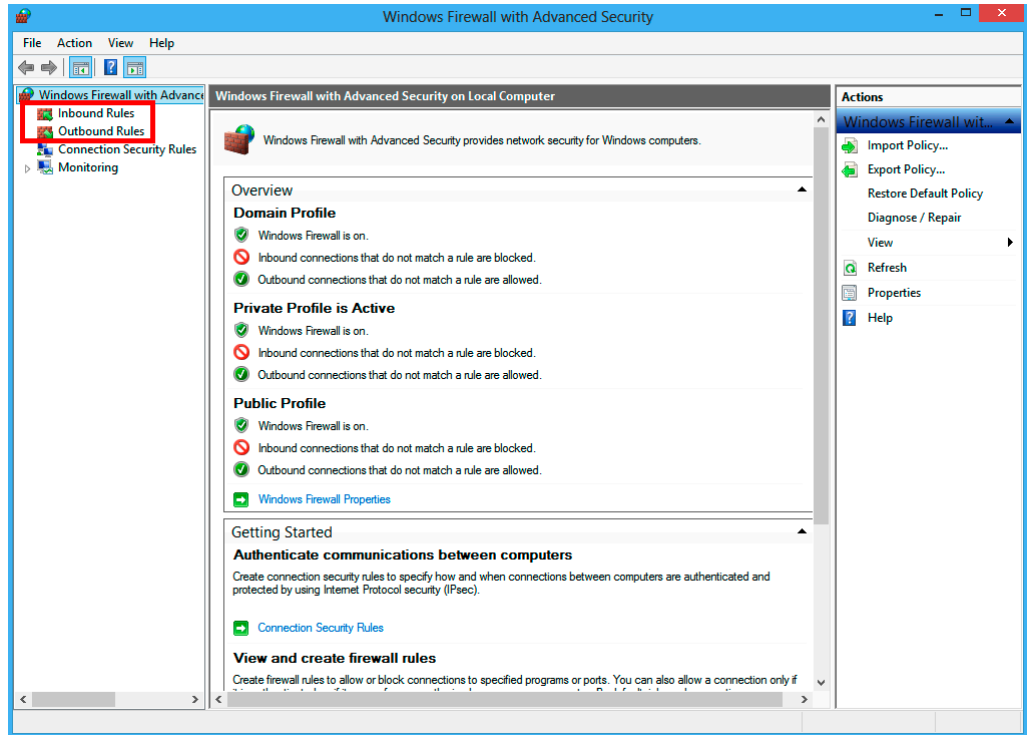
Select the option "New rule" on the right side. The process is the same for inbound rules and outbound rules.
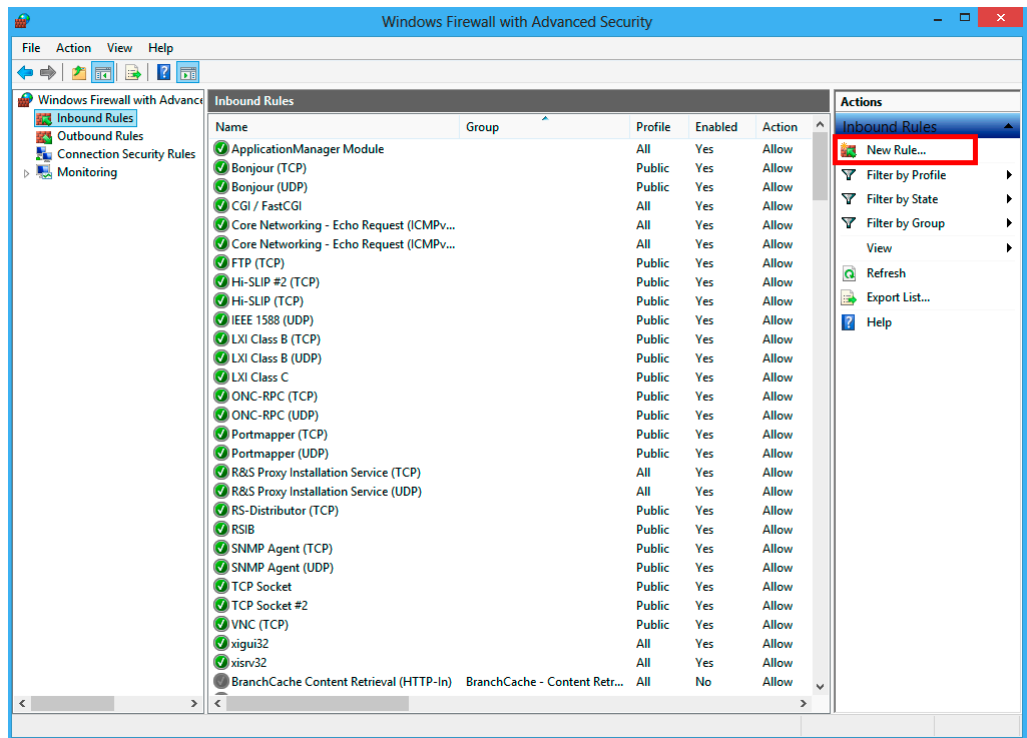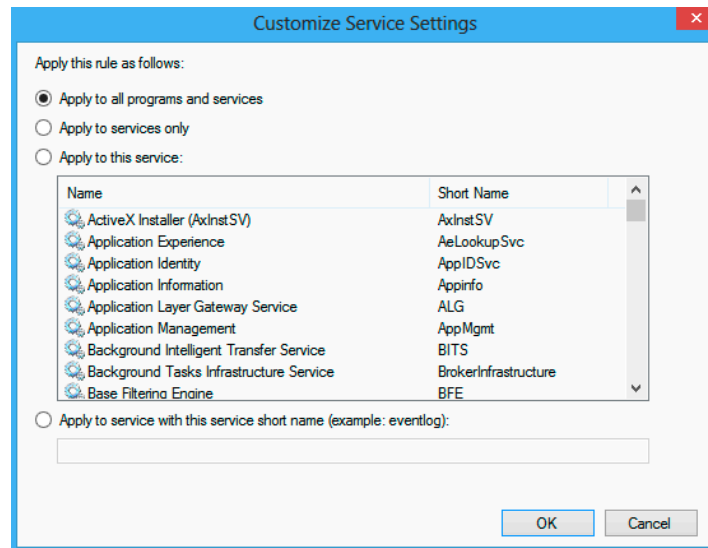
Select what kind of rule you want to create. The option "Custom rule" grants the most flexibility. Otherwise you can select to allow or block a certain program, a certain range of ports or to enable a predefined rule. Press "Next" to continue.

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".

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.

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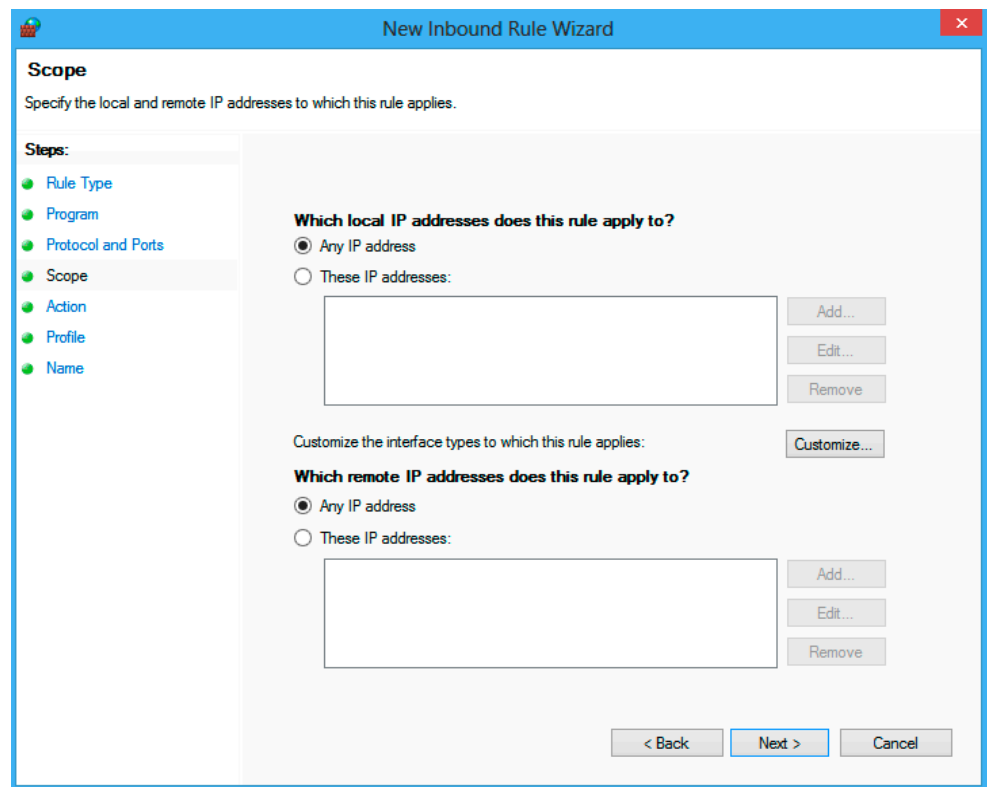
The rule can be limited to apply only to certain IP addresses and interfaces.

The interfaces are differentiated in "Local area network", "Remote access" and "Wireless". They can be specified by clicking "Customize".
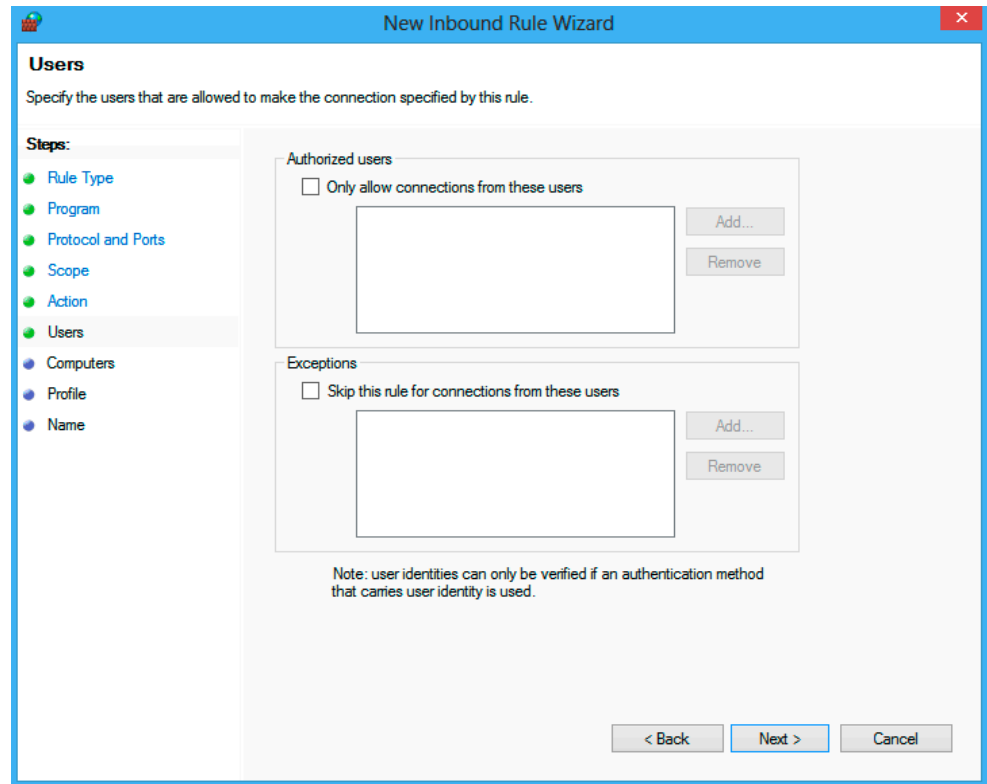
The connection can either be allowed, blocked or allowed if it is secure when it matches the previous settings. Since the default inbound rule is to block all incoming connections, we recommend selecting "Allow the connection" or "Allow the connection if it is secure". In case an outbound rule is created, "Block the connection" should be selected, because all outgoing connections are allowed by default.
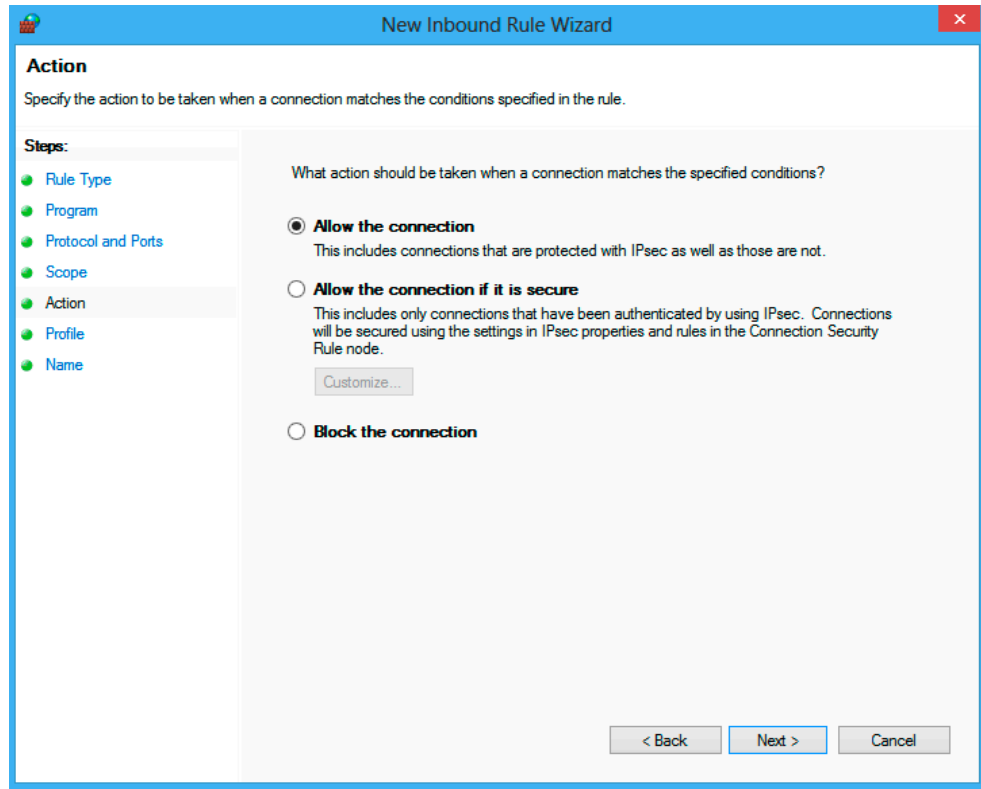
In case "Allow the connection if it is secure" is selected, additional options are available. Click "Customize" to specify whether the connection has to be authenticated or encrypted.
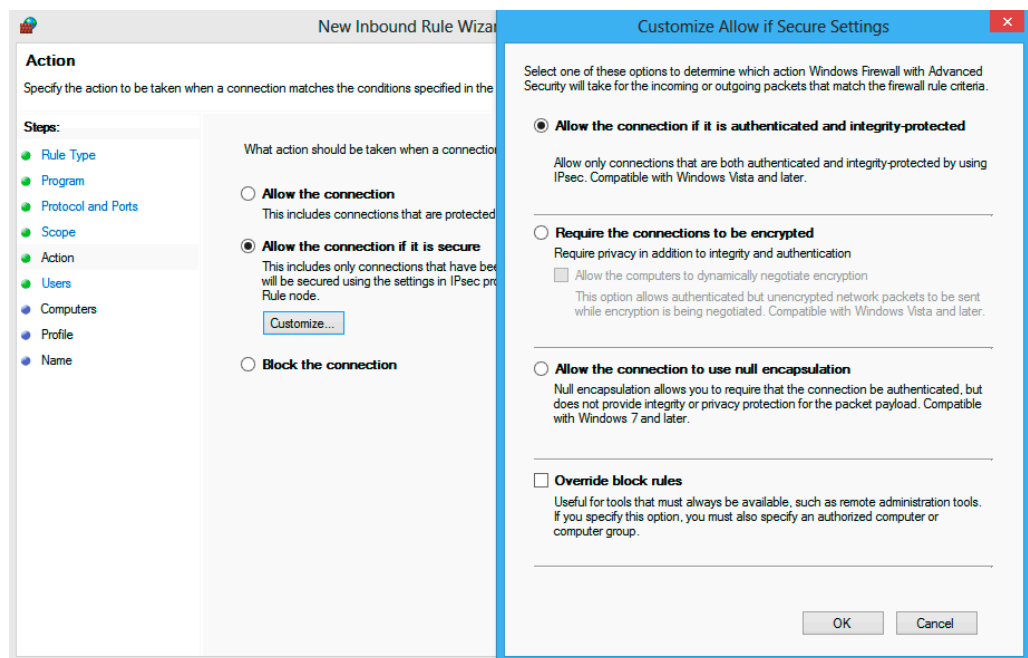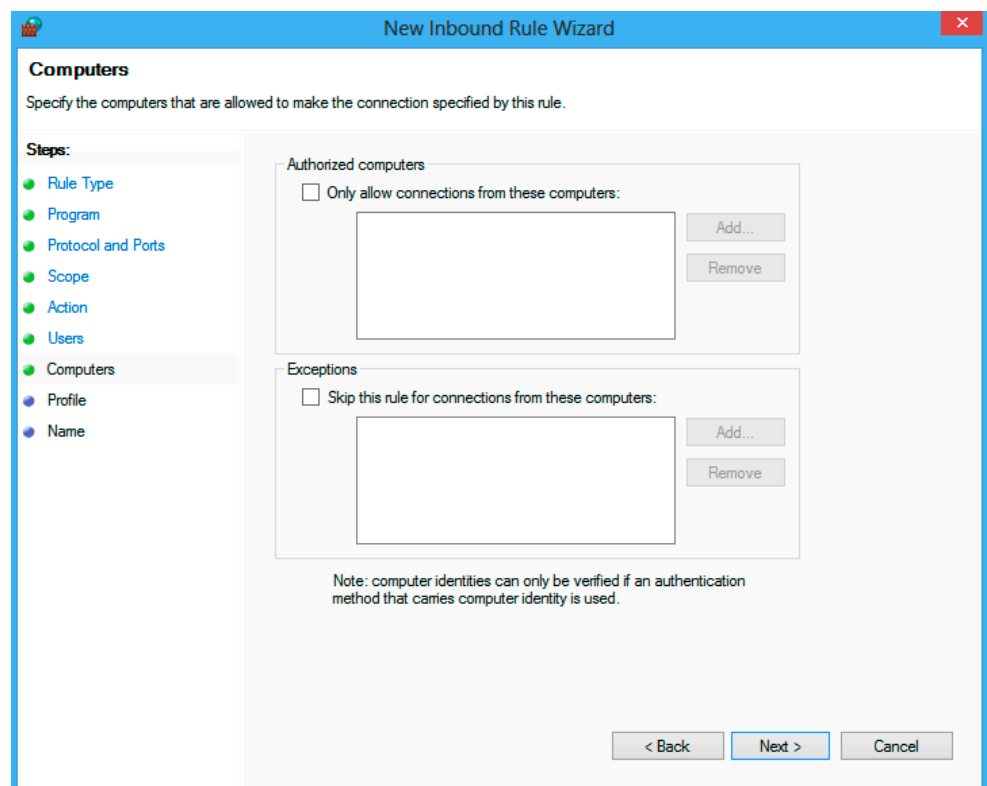
In addition, specific user accounts and groups can be stated to have access. If "Override block rules" is selected, a computer or a group of computer accounts has to be specified.

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.

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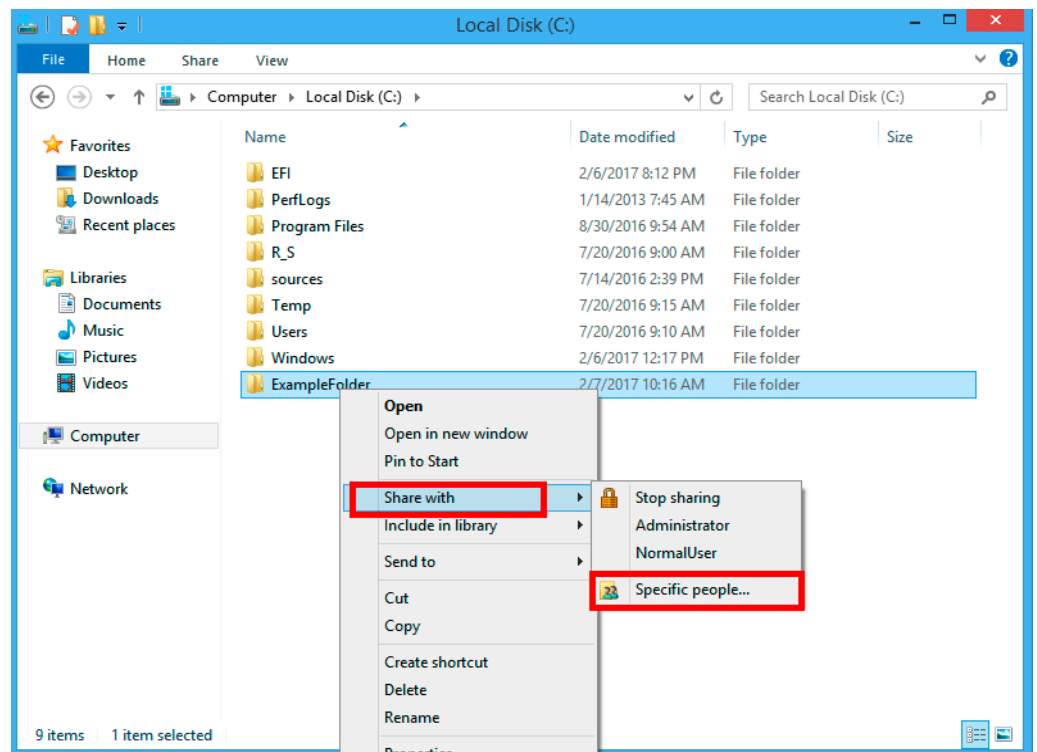
Select the name of the user or group you want to give access to from the dropdown list or enter the name directly, for example "Everyone". Click "Add" to set the user's or group's permissions.
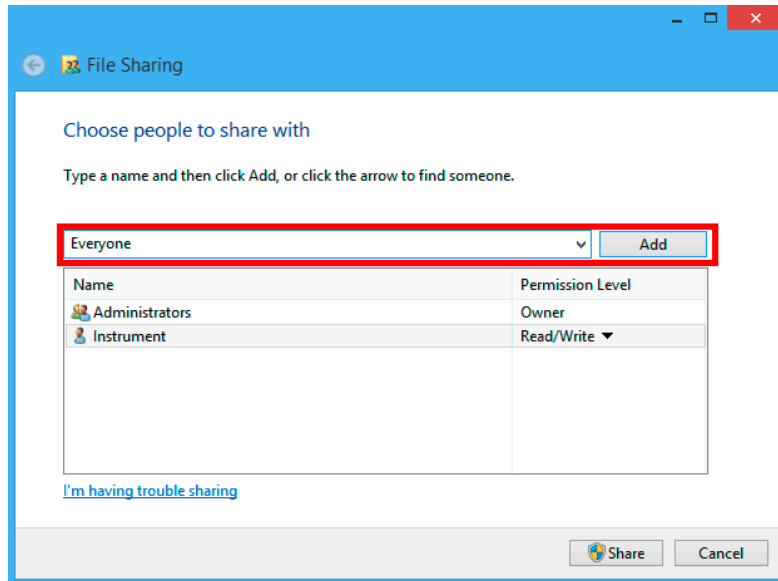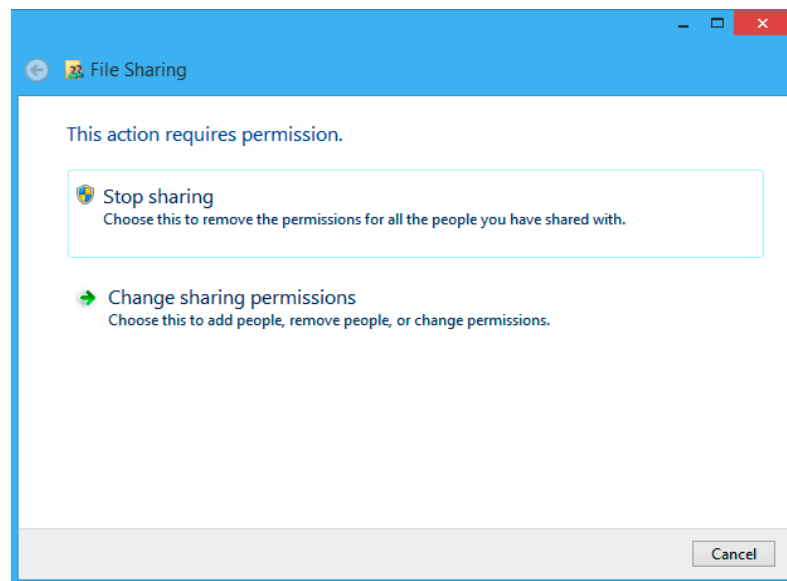

The default permission level is "Read". Change this setting according to requirements. The option "Remove" removes the user or group from the list.
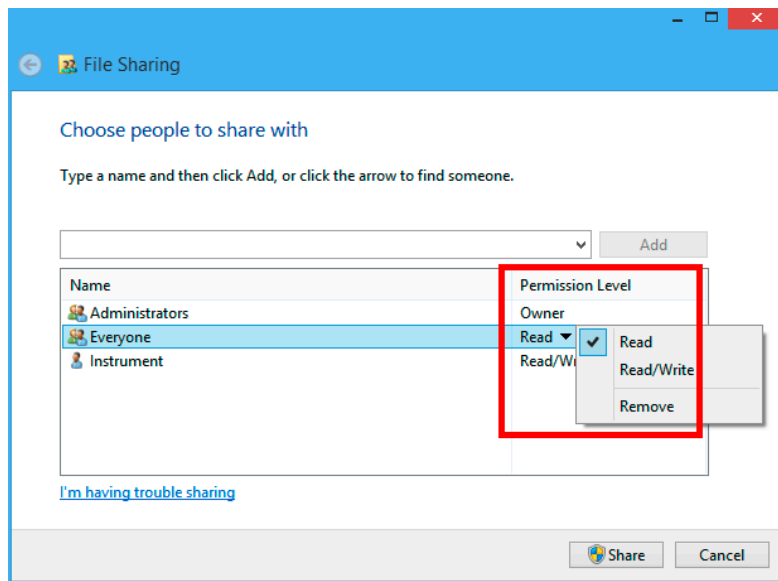
In order to remove a network share, right-click the folder and select "Share with" ▷ "Stop sharing".
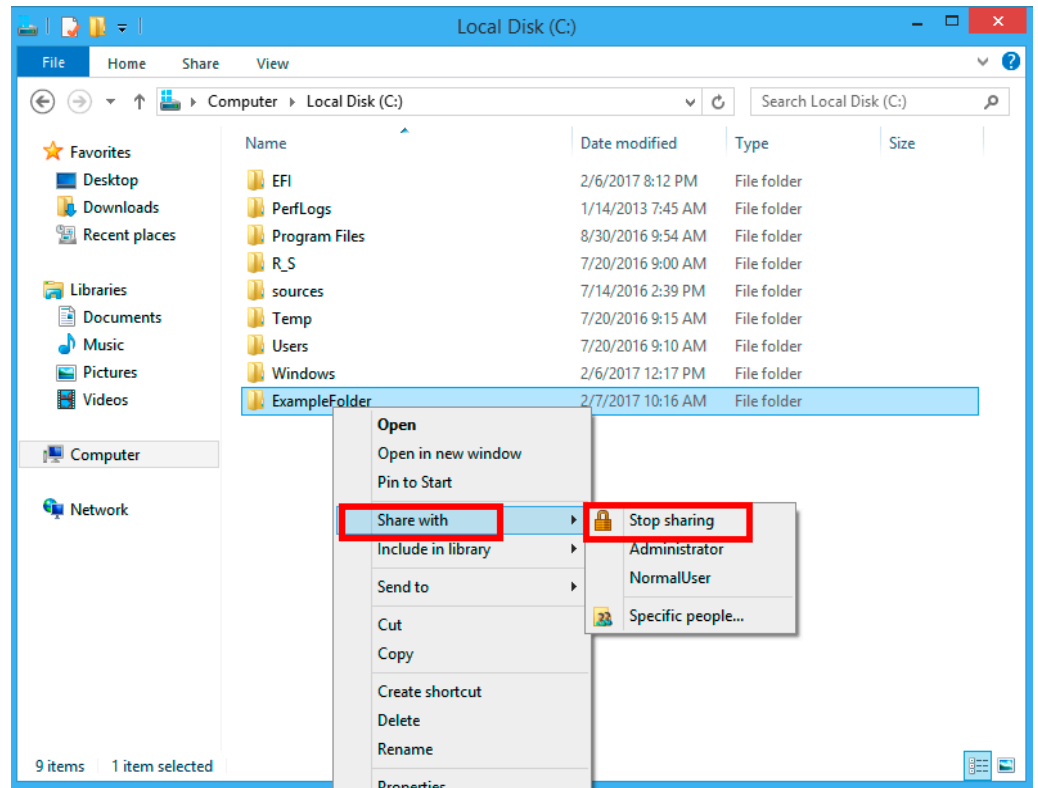
Now you can select whether to remove all permissions or only permissions of single users and groups.

6 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.
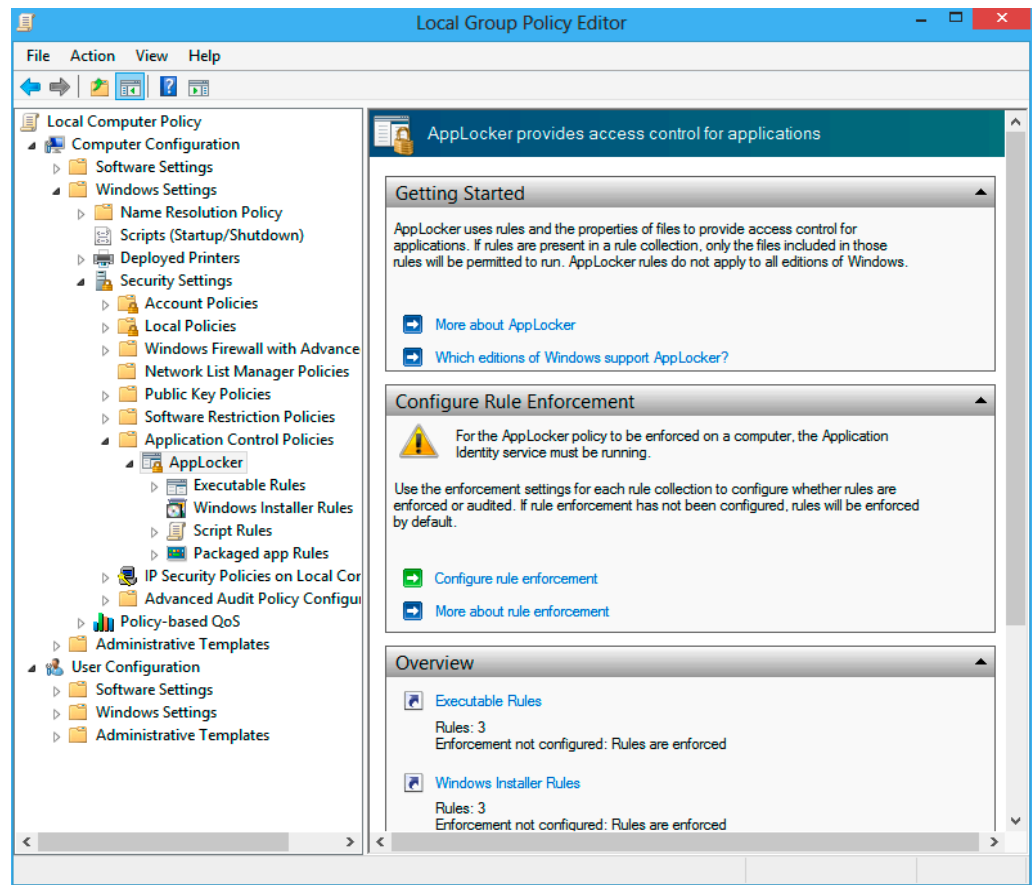
6.1 Default rules

By default the execution of 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 three categories:

Executable rules

Action	User	Name	Condition	Exceptions
✅ Allow	Everyone	(Default Rule) All files located in the Pro…	Path	
✅ Allow	Everyone	(Default Rule) All files located in the Wi…	Path	
✅ Allow	BUILTIN\Administrators	(Default Rule) All files	Path	

Windows installer rules

| Action	User	Name	Condition	Exceptions
✅ Allow	Everyone	(Default Rule) All digitally signed Wind…	Publisher	
✅ Allow	Everyone	(Default Rule) All Windows Installer files…	Path	
✅ Allow	BUILTIN\Administrators	(Default Rule) All Windows Installer files	Path	

Script rules

Action	User	Name	Condition	Exceptions
✅ Allow	Everyone	(Default Rule) All scripts located in the …	Path	
✅ Allow	Everyone	All scripts located in the Windows folder	Path	
✅ Allow	Everyone	(Default Rule) All scripts located in the …	Path	
✅ Allow	BUILTIN\Administrators	(Default Rule) All scripts	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.

6.2 Enabling and disabling AppLocker

AppLocker can be configured in the local group policy editor. Navigate to "Local Computer Policy" ▷ "Computer Configuration" ▷ "Windows Settings" ▷ "Security Settings" ▷ "Application Control Policies" ▷ "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".
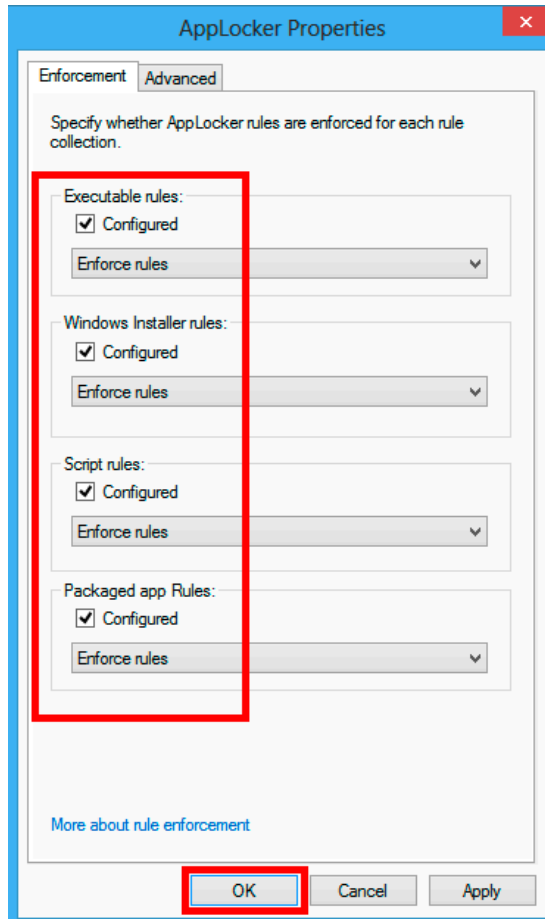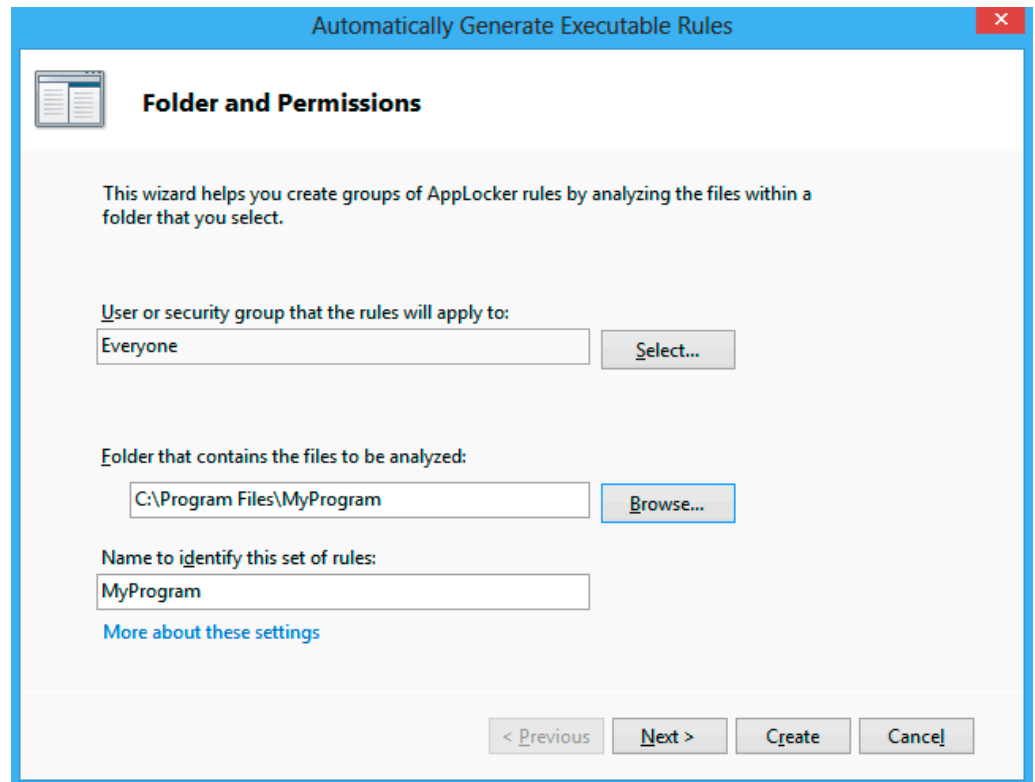

6.3 Adding and removing rules

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.
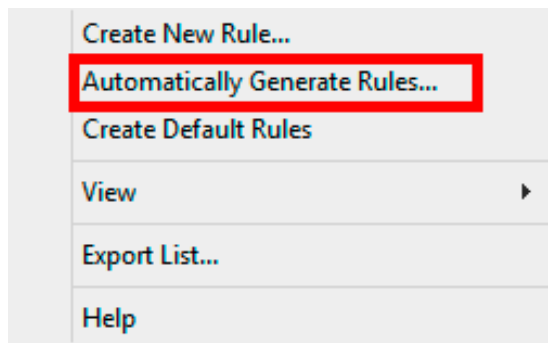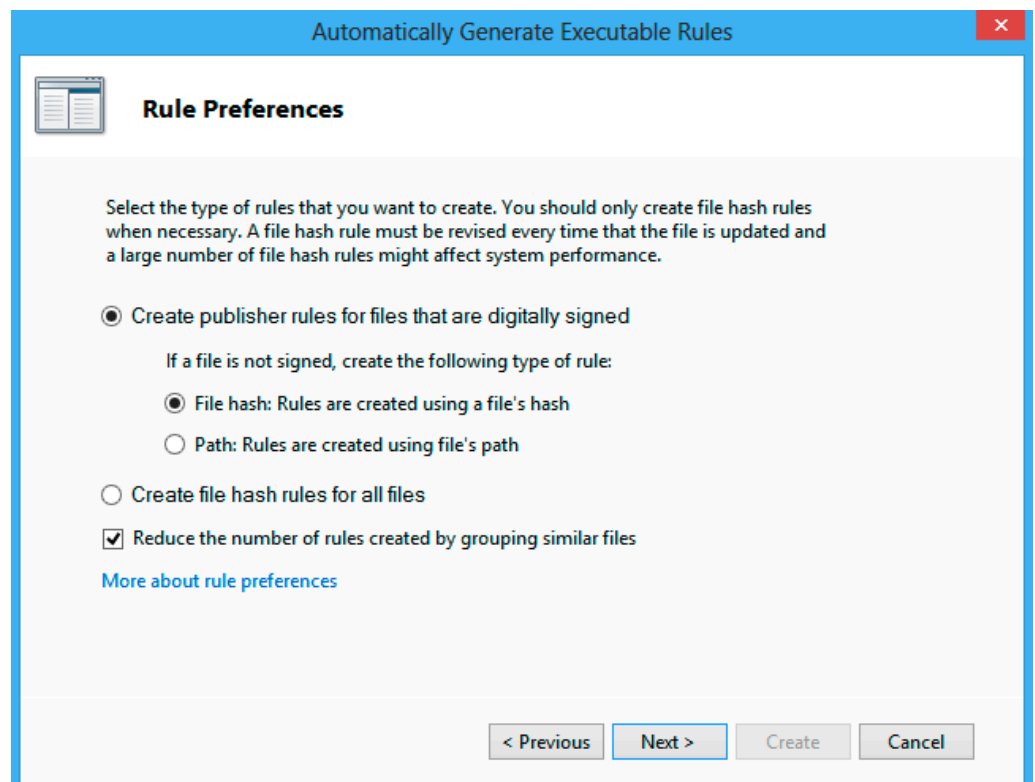
The dialog that opens is basically the same for each category of rules. In this example, executable rules shall be created. First select the user or security group the rules shall apply to. Second, select the folder containing the software you want to allow. Enter a name for this set of rules and proceed by clicking "Next".
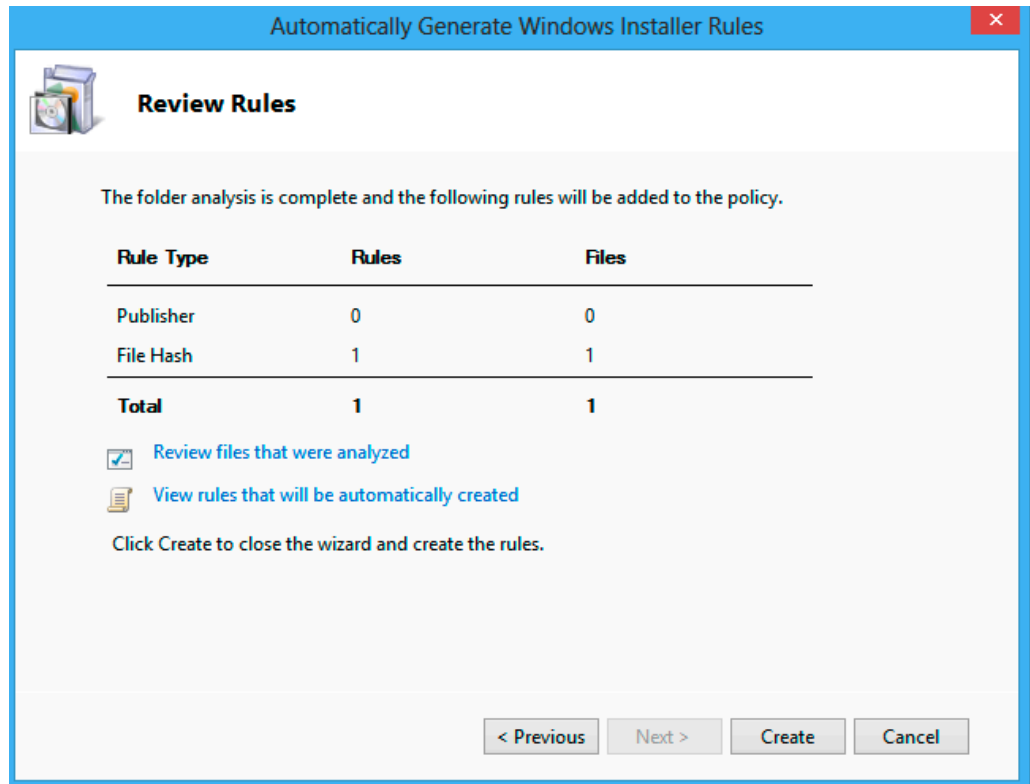
Now you can specify how the rules shall be generated. The default settings are recommended for most use cases. Rules are generated for each valid signature. If no signature is found, a rule based on the file's hash value is generated. Proceed by clicking "Next".

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

In case the default rules are not present, the system queries whether to create them automatically.
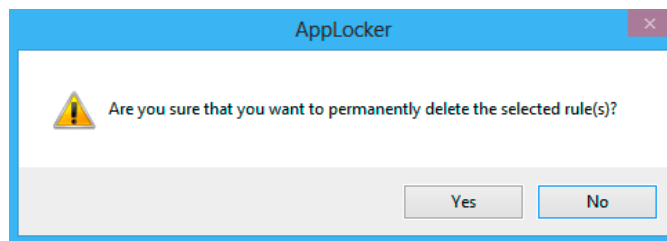
Any rules can be removed by right-clicking a rule and selecting "Delete". You will be prompted to confirm the deletion by clicking "Yes".

7 ANTI-VIRUS SOFTWARE

Condition as supplied to customer
▶ Windows Defender is enabled 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 Embedded 8 Standard 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

7.1 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 "windows defender" in the start screen and select "Windows Defender".
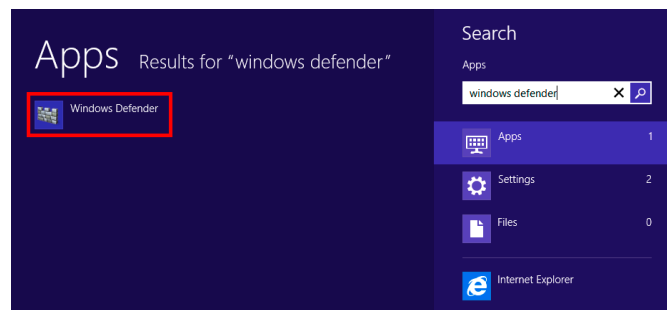
In the main dialog you can select whether to perform a "Quick", "Full" or "Custom" scan. By selecting "Quick", Windows Defender will scan for viruses, spyware and unwanted software on certain parts of the hard disk. This scan will take a few minutes. By selecting "Full", Windows Defender will scan the 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.
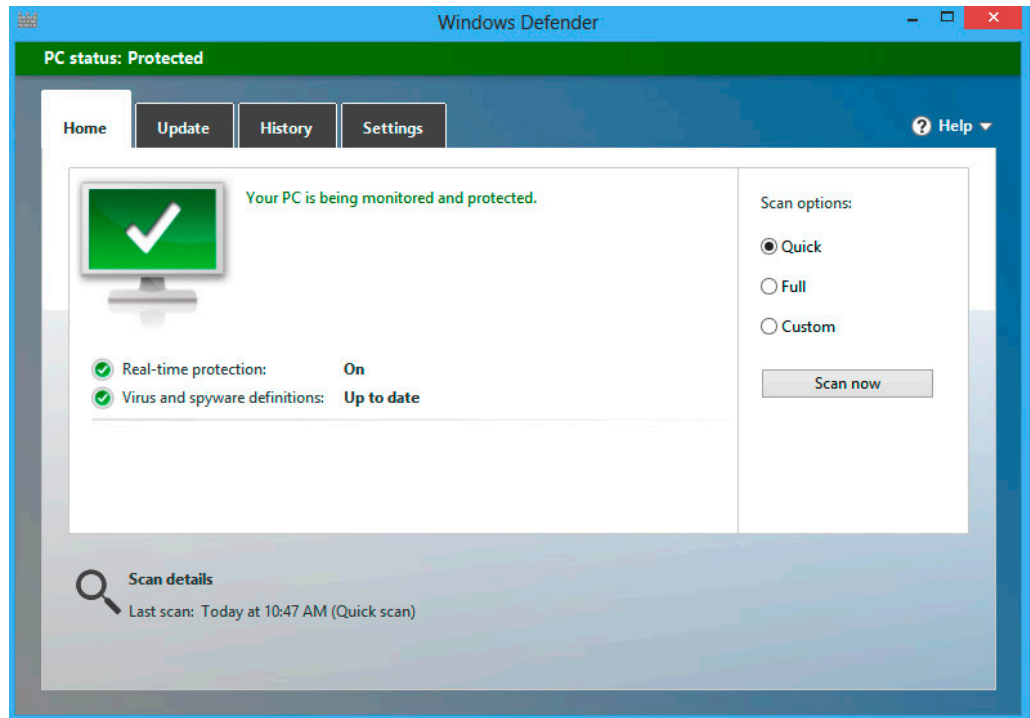
Windows Defender can be configured in the Settings tab. We recommend disabling real-time protection to prevent influence on the instrument's performance. Perform full scans on a regular basis instead.
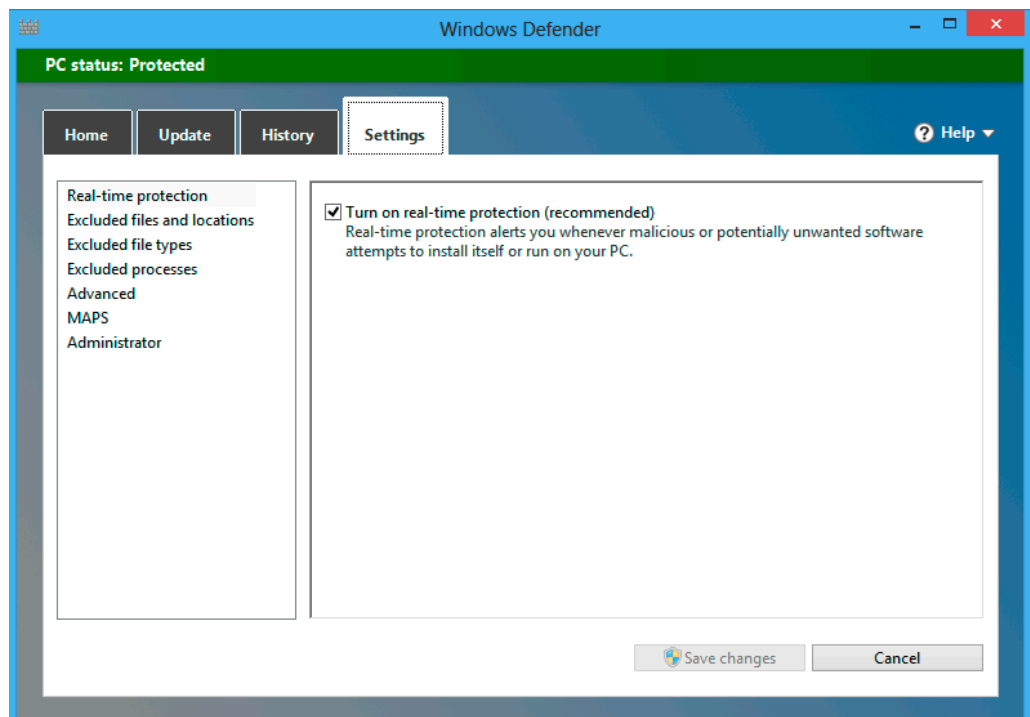
Please note that Windows Defender will be disabled if third-party anti-virus software is installed.

7.2 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.

7.3 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.

Different operating systems require slightly different steps to map the administrative share of your Rohde & Schwarz instrument. Therefore the procedure is described for PCs running Windows 10 and Windows 8.1.

7.3.1 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".

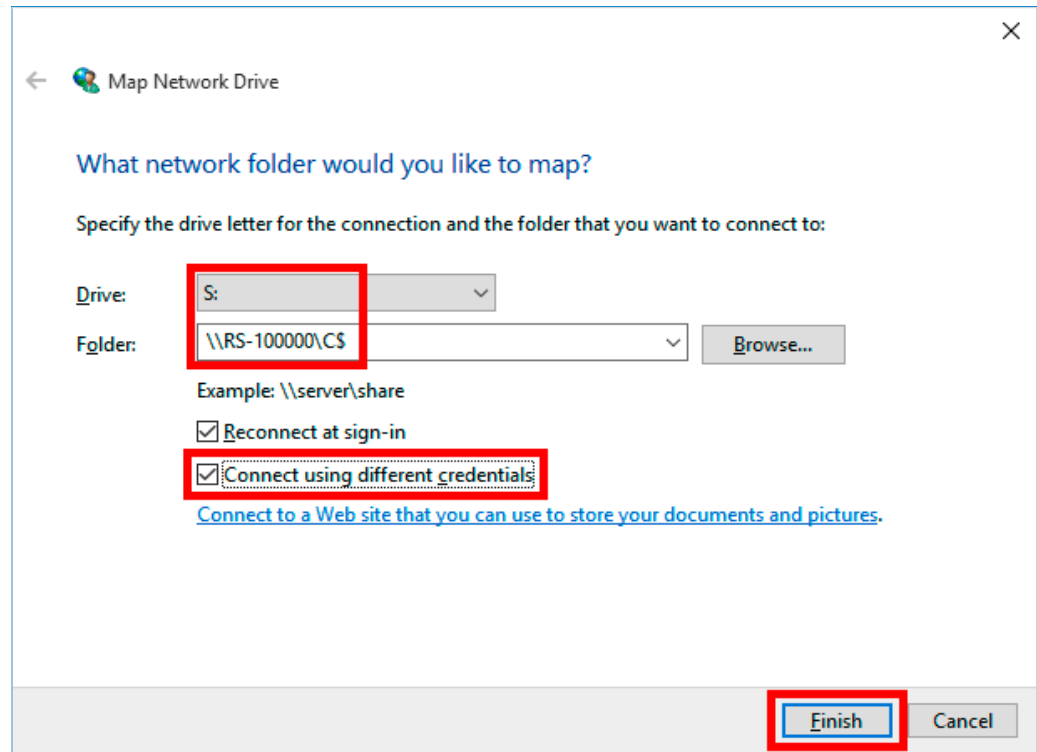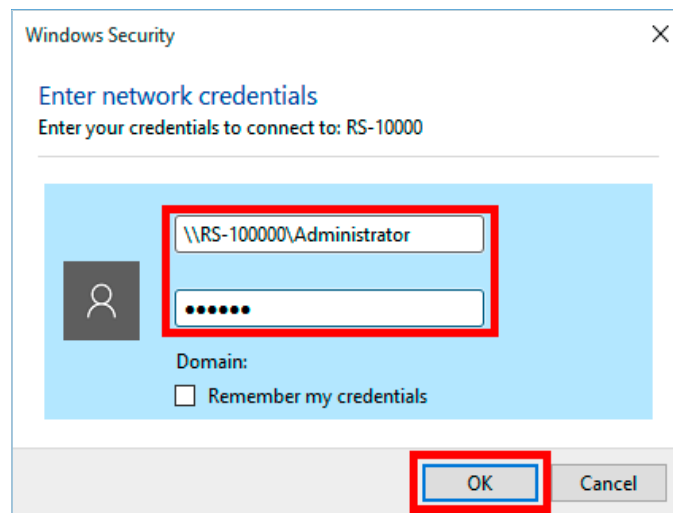Select the drive, folder and the option "Connect using different credentials" and confirm the dialog with the "Finish" button. We recommend using the administrative share "C$".

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.

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. Right-click the network share to open the context menu and select "Disconnect".

7.3.2 Mapping instrument drives on a computer with Windows 8.1
Open the File tab in Windows Explorer and right-click the folder "Computer" on the left side to open the context menu and select "Map network drive".

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$".
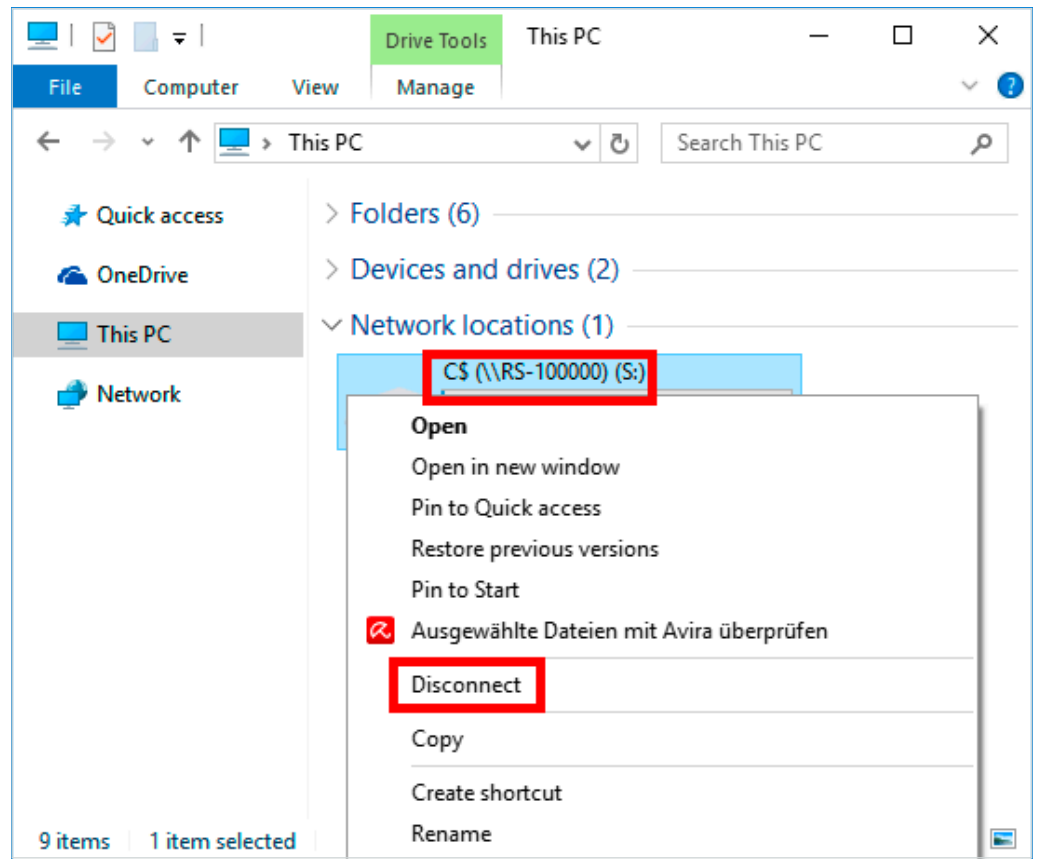

Enter the login information of your instrument's Administrator account. Please refer to the instrument's manual for details. It might be necessary to add the instrument's computer name in front of the name of the instrument's administrator account name.
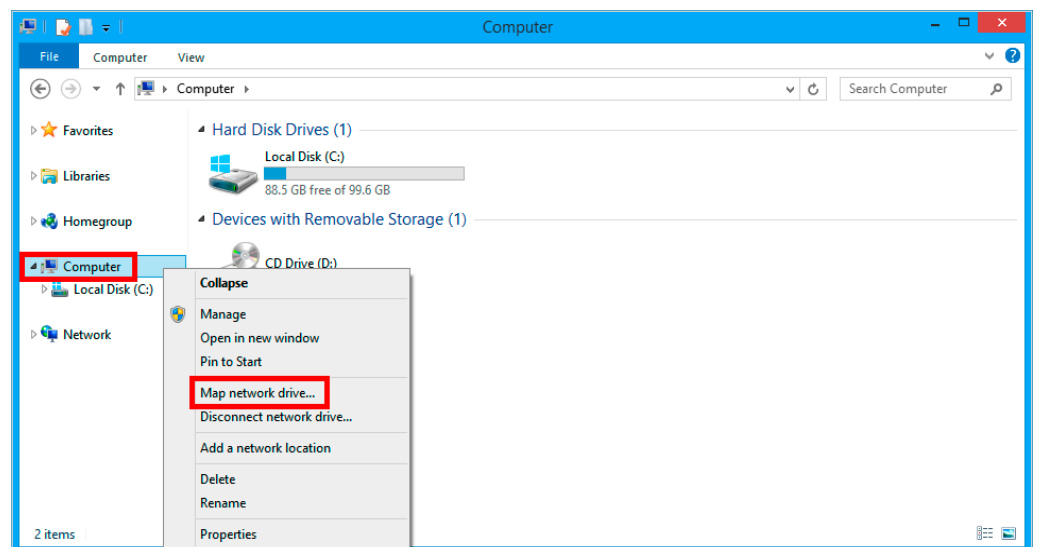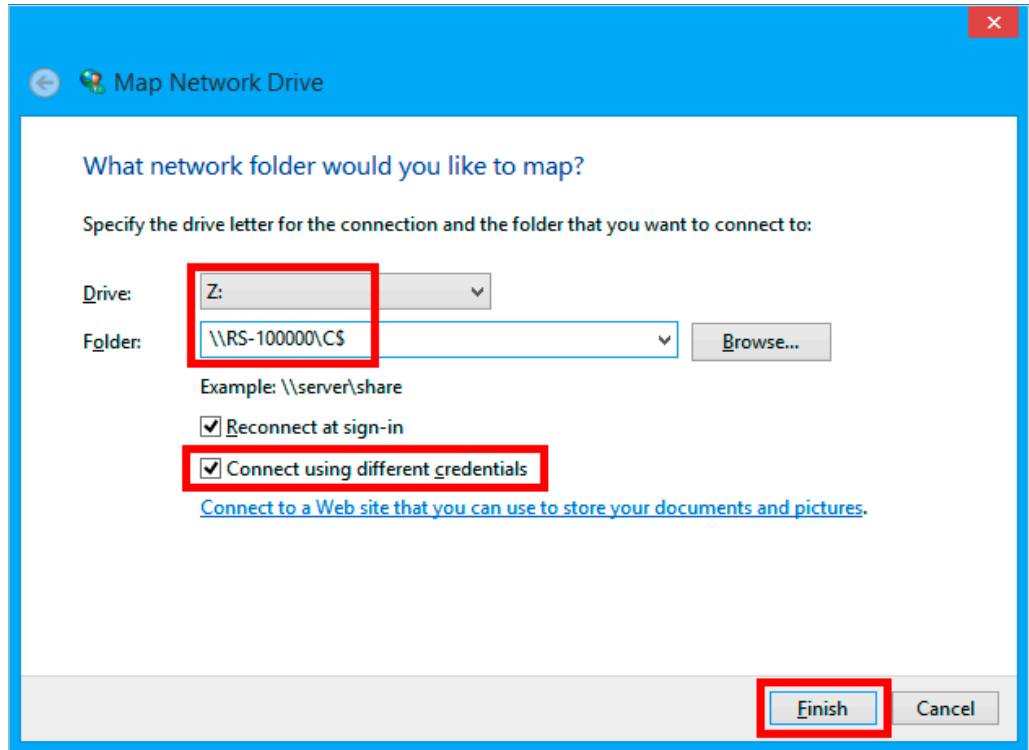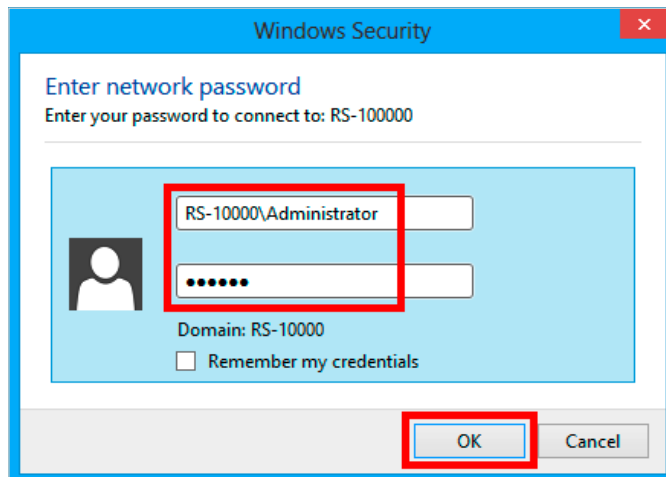

To scan the instrument's hard drive, start the anti-virus software on the control PC. Select one of the mapped drives of the instrument and run a virus scan. Please refer to the anti-virus software's user manual for how to scan a network drive.

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 folder "This PC" to see all drives. Right-click the network share to open the context menu and select "Disconnect".
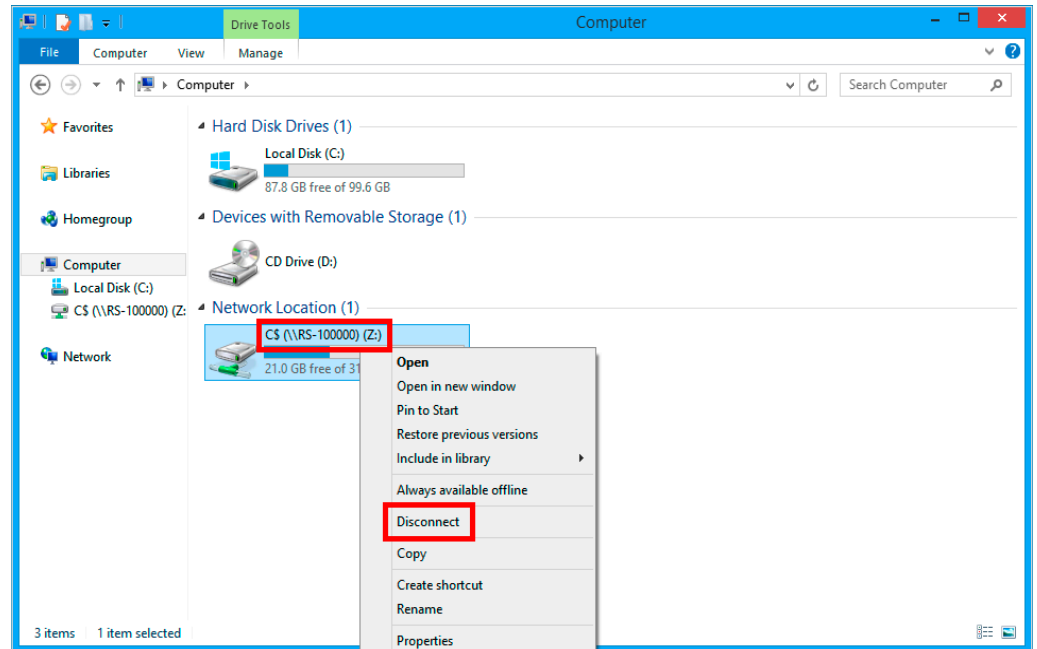
8 REFERENCES

[1]   Windows 8 Security Overview
         https://technet.microsoft.com/en-us/library/dn283963.aspx

[2]   What's Changed in Security Technologies in Windows 8
         https://technet.microsoft.com/en-us/library/dn169048.aspx

[3]   AppLocker Overview
         https://technet.microsoft.com/en-us/library/hh831409.aspx

[4]   Software Restriction Policies
         https://technet.microsoft.com/en-us/library/dn449105.aspx

[5]   Windows Firewall with Advanced Security Overview
         https://technet.microsoft.com/en-us/library/hh831365.aspx

[6]   Group Policy Settings Reference for Windows and Windows Server
         https://www.microsoft.com/en-us/download/details.aspx?id=25250

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