MALWARE PROTECTION WINDOWS 7

White paper | Version 01.00

ROHDE&SCHWARZ

Make ideas real

CONTENTS

Rohde&Schwarz recognizes the potential computer virus risk when Windows based test instruments are connected to other computers with local area networks (LAN) or when removable storage devices are inserted.

This white paper introduces measures to minimize malware threats and discusses how to minimize risk while maintaining instrument performance.

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

1 WINDOWS 7 BASED INSTRUMENTS

1.1 Overview

Instruments that run Windows 7 operating systems should be protected from malware just like any other PC. Users are strongly advised to protect their instruments with anti-virus software and by installing all available operating system patches and updates. You should work closely with your IT department or system administrator to ensure compliance with your company policies for connecting instruments to your company's network. This document does not differentiate between Windows 7 32-bit and Windows 7 64-bit. If you are using any anti-virus software make sure it is designed for your operating system.

Note that since January 2020 regular updates for Windows 7 are no longer published. For many instruments, Rohde&Schwarz provides commercially available upgrade kits from Windows 7 to Windows 10, increasing instrument security and availability of Windows updates and patches.

1.2 Computer virus control program

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

Rohde&Schwarz has established processes within the company that take all reasonable precautions to prevent the spread of viruses from instruments to customer 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 into contact with customer instruments to reinforce anti-virus security protocols. This includes all personnel from manufacturing, service, support, sales and distribution.

1.3 Preventative maintenance

After instrument delivery, the user is responsible for its security.

Before connecting the instrument to your company's network, please consult with your IT department or system administrator to determine which specific policies apply. Remember that the instrument appears as a standard computer to the network. If applicable, consider connecting the instrument to a network separated from your company's network (e.g. using VLANs). Follow your company's computer security and virus protection policy.

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

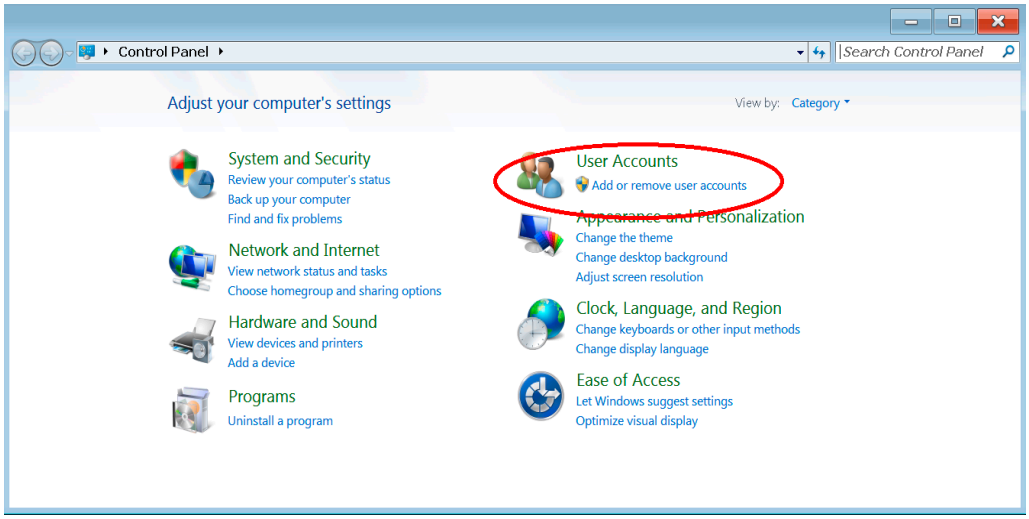
It is also important to regularly update both the virus definitions and operating system. Rohde&Schwarz recommends checking both virus definitions and operating system updates, in addition to scanning the instrument for any malware, at least once per week. Be sure to always update the operating system and anti-virus definitions if recommended by your IT department or system administrator. The following steps should be taken to ensure the instrument's operating system is better protected:

- Do not disable the firewall on the instrument, keep it always running
- Regularly scan all removable storage devices (e.g. USB flash drives) that are used with an instrument and deactivate the autorun/autoplay function to prevent inadvertent execution of malicious code from these devices
- Install the latest Windows patches and updates on the instrument. Note that since January 2020 regular updates are no longer provided for Windows 7.
- Scan the instrument regularly with anti-virus software, and keep virus definition files updated. We do not recommend running anti-virus software in the background ("on-access" mode) as this will significantly impact instrument performance.

1.4 User accounts

Windows requires users to identify themselves by entering a user name and password in a login window. In general, Rohde&Schwarz instruments come with a factory-installed auto-login function, i.e. login is carried out automatically during the startup of the instrument. For most instruments the factory default for this auto-login function has administrator rights with unrestricted access, making possible printer installation and network configuration.

For many instruments you can set up two types of user accounts, either an administrator account with unrestricted access to the instrument operating system or a standard user account with limited access. You can manage the accounts via "Windows Start" ▷ "Control Panel" ▷ "User Accounts". Refer to the instrument´s user manuals for more information on how to change or add new users and on how to de-activate the automatic login.



Note: Changing firewall settings, installing and configuring anti-virus software and Windows updates require unrestricted administrator rights.

2 FIREWALL SETTINGS

With Windows 7 a firewall can help protect a computer or instrument against attacks from the network. Rohde&Schwarz instruments come with the Windows firewall enabled and preconfigured. Activating the instrument firewall is helpful even when using the instruments within a protected company network. With the number of worms, viruses and other malware circulating on the internet today, it is inevitable that something will penetrate the enterprise firewall. Instrument firewalls not only help protect against threats inside the perimeter, but they can also prevent the spread of many viruses and worms.

If you have additional security and protection requirements, please contact your IT department or system administrator to ensure conformity with your company's security policy.

The Windows 7 firewall has three different profiles for the independent configuration of the firewall settings. The following profiles are defined:

Private profile
Used when a network adapter is connected to a network that the user or administrator has identified as a private network. A private network is one that is not connected directly to the internet, but is behind some kind of security device, such as a network address translation (NAT) router or hardware firewall.

Domain profile
The domain profile applies to network adapters where the host system can authenticate a domain controller.

Public profile
Used when a network adapter is connected to a public network. When the profile is not set to the private or domain profile, the default profile is public. The public profile settings should be the most restrictive because the computer is connected to a public network where security cannot be controlled.

Rohde&Schwarz instruments come with preconfigured firewalls, which enables all necessary ports for the Rohde&Schwarz software on all profiles.

2.1 Firewall port configuration

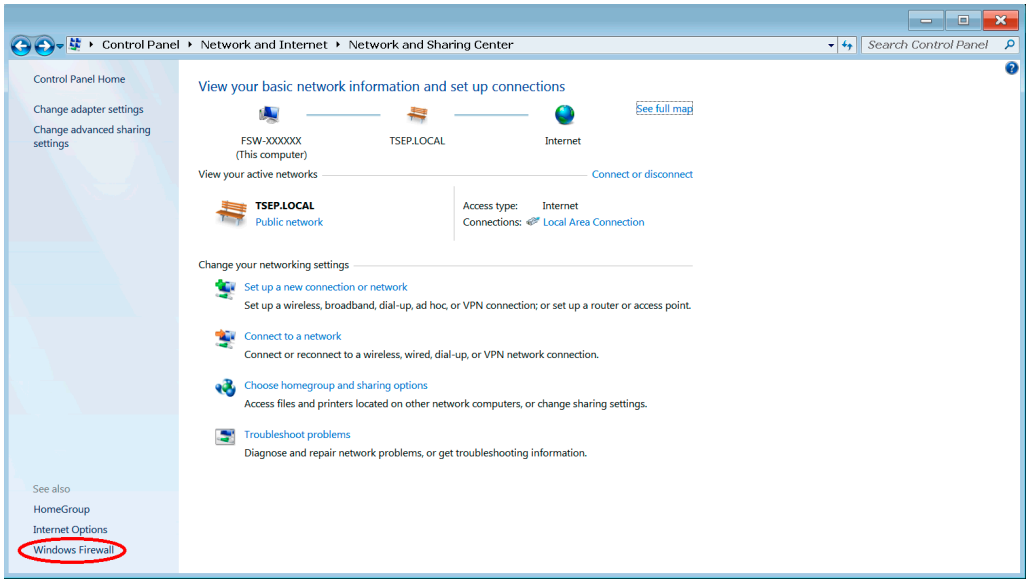
Rohde&Schwarz instruments are preconfigured in such a way that all ports and connections for remote control are enabled. See the following table for details on open ports for remote control. Some instruments do not have all ports open by default. Please refer to the instrument documentation.

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 (AgentX)	SNMP	Standard ports for SNMP agent
319, 320 TCP and UDP	1588 PTP	LXI Class B/A, 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 class B	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

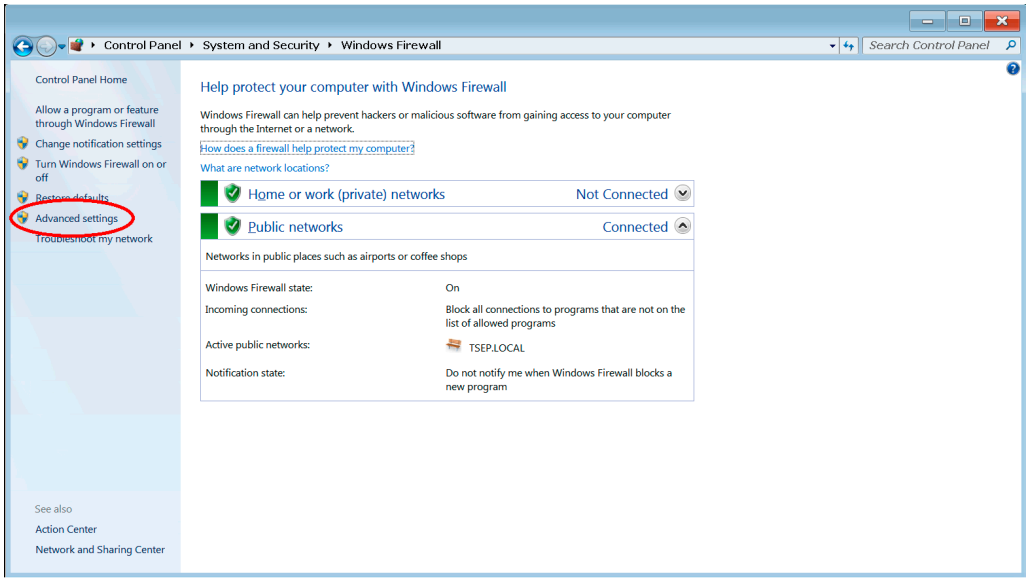
2.2 Changing firewall settings

Rohde&Schwarz recommends using the firewall on your instrument. Please do not disable the firewall and confirm any change with your IT department.

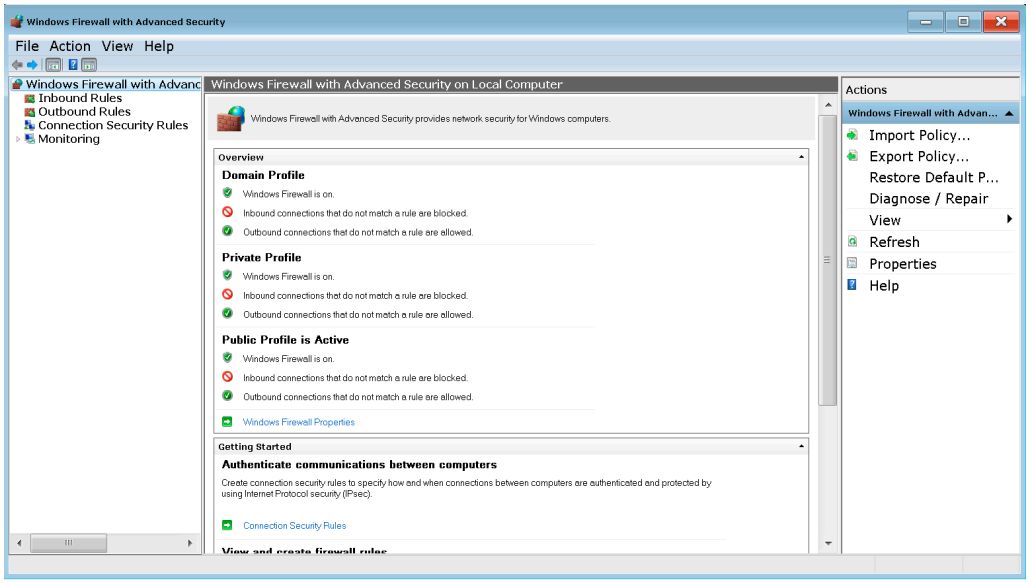
Note that changing firewall settings requires administrator rights. You can manage the firewall settings via "Windows Start" ▷ "Control Panel" ▷ "Network and Internet" ▷ "Network and Sharing Center":



Click the “Windows Firewall” entry:



Click the “Advanced settings” entry and the firewall configuration windows will appear:



The Windows firewall defines three general rules:

Inbound rules

Inbound rules explicitly allow or explicitly block traffic attempting to access the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly allow traffic secured by IPsec for remote desktop through the firewall but block the same traffic if it is not secured by IPsec. When Windows is first installed, inbound traffic is blocked; to allow traffic, you must create an inbound rule.

Outbound rules

Outbound rules explicitly allow or explicitly block traffic originating from the computer that matches the criteria in the rule. For example, you can configure a rule to explicitly block outbound traffic to a specific computer through the firewall but allow the same traffic to other computers. Outbound traffic is allowed by default, so you must create an outbound rule to block traffic.

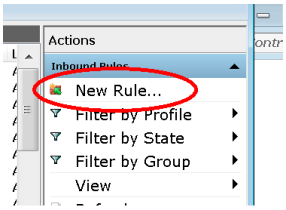
Connection security rules

Connection security involves the authentication of two computers before they begin communications and the securing of information sent between two computers. Windows firewall with advanced security uses internet protocol security (IPsec) for connection security through key exchange, authentication, data integrity and optionally data encryption. Connection security rules use IPsec to secure traffic while it crosses the network. You can use connection security rules to specify that connections between two computers must be authenticated or encrypted. You might still have to create a firewall rule to allow network traffic protected by a connection security rule.

Normally there is no need to change the configuration of the firewall. In rare circumstances it might be necessary to create a new firewall rule. Please note that this configuration influences your computer security, so do not change the firewall configuration unless you are familiar with firewall concepts.

To create a new rule, select the appropriate category of rules on the left side:

After you have selected the appropriate category of rules (inbound, outbound, connection security) you can create a new rule by clicking "New Rule…" on the right side of the screen:

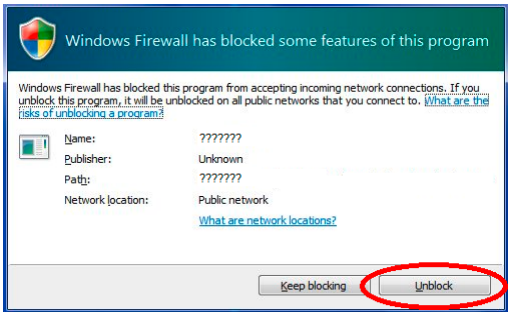


The “New Rule” wizard will start. This wizard guides you through the steps. The different steps are described in detail on the Microsoft TechNet.

Problems related to the default firewall configuration take two forms:

- Client programs may not receive data from the instrument
- Server programs that are running on the instrument may not respond to client requests

If a program is being blocked by the firewall, you may receive the following Windows firewall security alert:



To unblock the program, click “Unblock” in the security alert dialog box. You can find a detailed description for firewall setup and configuration at the Microsoft MSDN website: https://docs.microsoft.com/en-us/dotnet/framework/wcf/samples/firewall-instructions

3 USB DEVICES

USB drives and removable hard drives are convenient and common in the workplace. They have considerable storage capacity for instrument settings, measurement results, hardcopies etc. However, they also create new problems; a large number of viruses, trojans and other malware have infected computers via USB storage devices. Once an infected USB drive is plugged into an instrument, the malware on it can spread throughout the whole network.

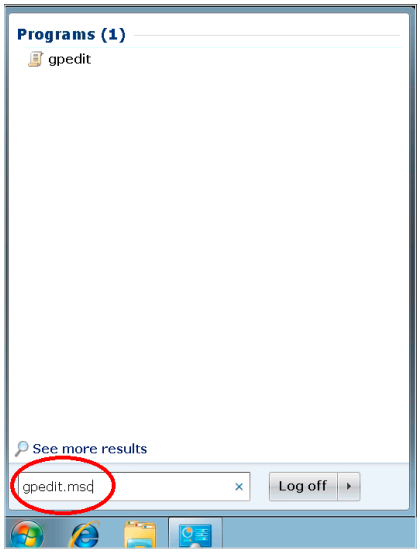
3.1 USB autorun function

Generally viruses that propagate via USB drives use the Windows “autorun” function, since it does not require any user confirmation and runs in the background. Rohde&Schwarz instruments are preconfigured with the autorun/autoplay function disabled, preventing malware from automatically running from a USB drive.

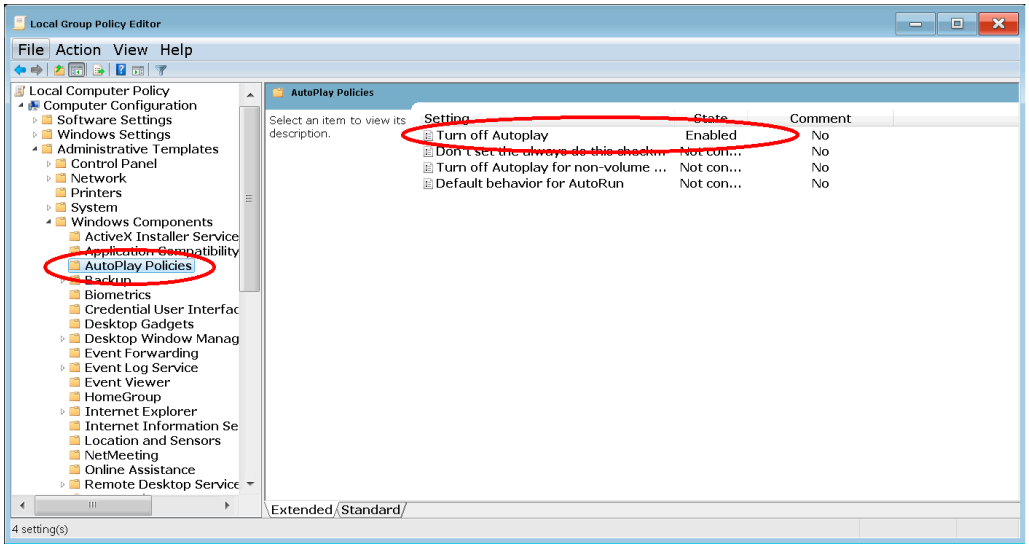
You can control or change the settings in the group policy editor.

If the instrument is used on a corporate network, and is a member of the network domain, your IT department or system administrator can centrally configure the group policy settings.

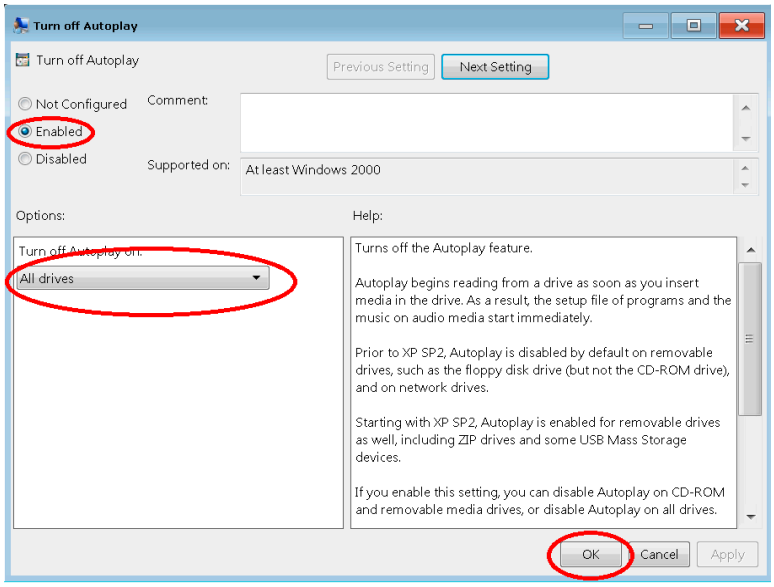
Click “Windows Start” and enter gpedit.msc to open the group policy settings.



Go to “Computer Configuration” ▷ “Administrative Templates” ▷ “Windows Components” ▷ “Autoplay Policies”:



Open the “Turn off Autoplay” entry with a double-click. Check the “Enabled” checkbox and the “All drives” option and confirm with OK.



If required, you can find a detailed description of the autorun function at the Microsoft support website.

3.2 Scan USB devices

Rohde&Schwarz recommends scanning USB flash drives and removable hard drives with anti-virus software on a regular basis to keep them free of malware.

Use your computer and anti-virus software to scan the USB storage devices before plugging them into an Rohde&Schwarz instrument.

4 ANTI-VIRUS SOFTWARE

As with personal and business computers, users must take steps to protect their instruments from infection. Besides strong firewall settings and regular scans of any removable storage device used with an Rohde&Schwarz instrument, it is also recommended that anti-virus software is installed on the instrument. While Rohde&Schwarz does not recommend running anti-virus software in the background ("on-access" mode) on Windows based instruments, due to potentially degrading instrument performance, it does recommend running it during non-critical hours at least once per week.

Today's anti-virus software requires a significant amount of system resources (both hard drive space and memory). Some instruments may not be capable of installing or running anti-virus software due to limited resources. Other options here are to scan these instruments with software run from a USB flash drive, or mounting the instruments as a drive on the network and scanning them from another computer with anti-virus software.

If anti-virus software is not regularly updated, it will not help protect your system, because it will be out of date. Any modern anti-virus software is regularly updated over the internet or with offline installation. Please contact your IT department to find the best solution for your anti-virus software. Keep in mind that any anti-virus software update will influence instrument performance.

5 MICROSOFT® PATCHES AND UPDATES

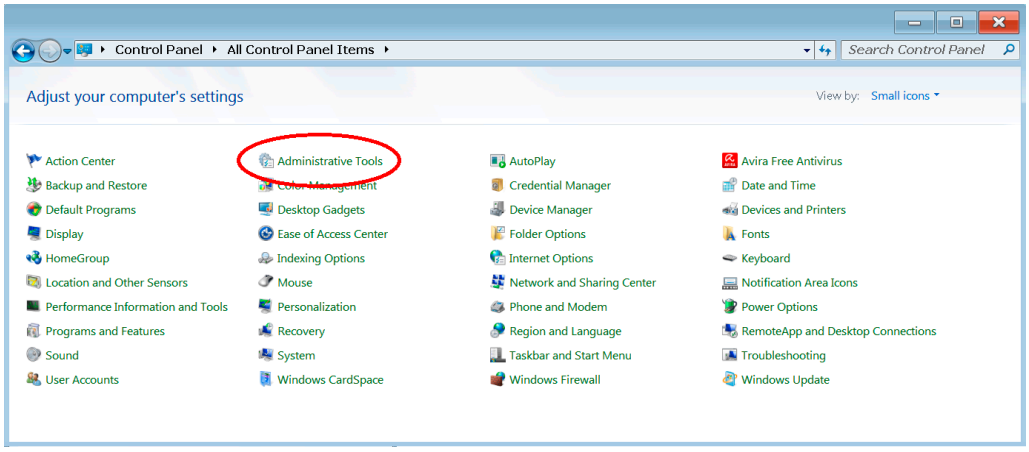
Until January 2020, Microsoft® regularly made security updates and other patches to Windows 7 based operating systems. Instruments that are connected to a network and run Windows 7 should have all available updates installed.

Note: For many instruments, Rohde&Schwarz provides kits to upgrade from Windows 7 to Windows 10 to increase instrument security and availability of Windows updates and patches.

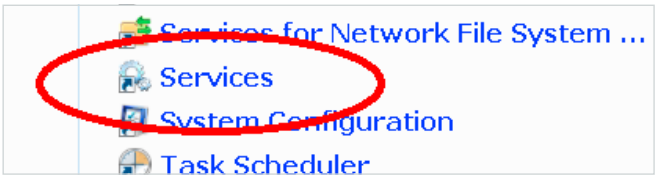
5.1 Enabling Windows Update service

On some Rohde&Schwarz instruments the Windows Update service is by default deactivated. The customer has to independently activate the service. Start the service management console to verify whether the service is activated.

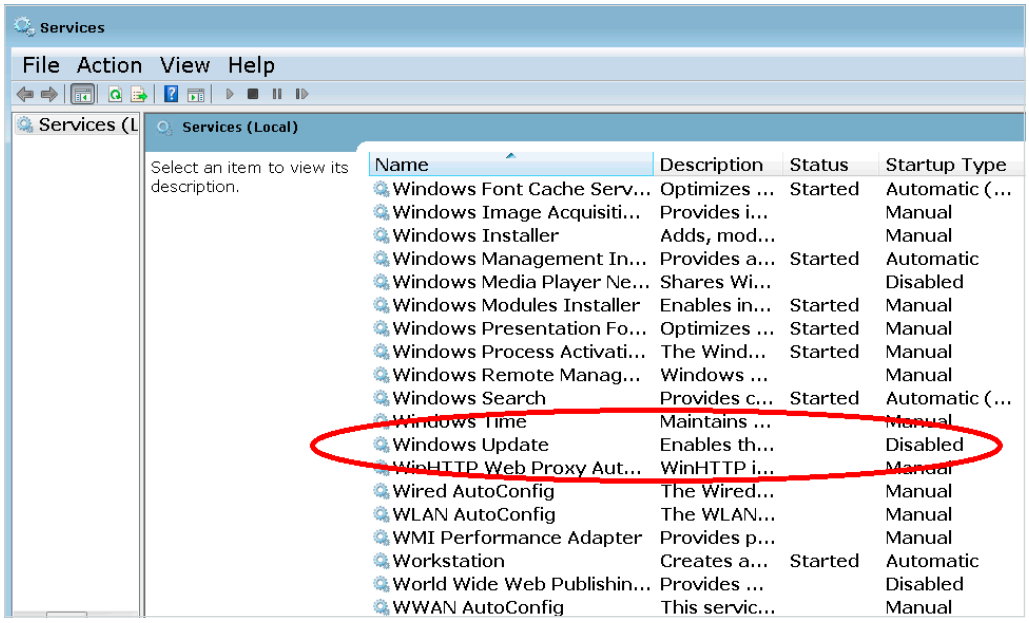
Navigate to “Control Panel” ▷ “Administrative Tools”. Note that this item is only visible if the “View by:” category is set to “Small icons”.



Afterwards select the “Services” management console:

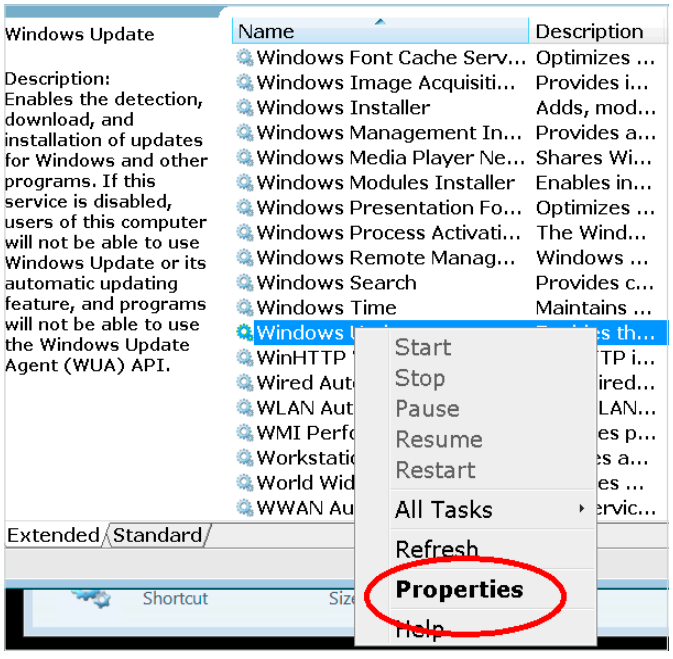


Once the “Services” console is displayed, search for the “Windows Update” service:

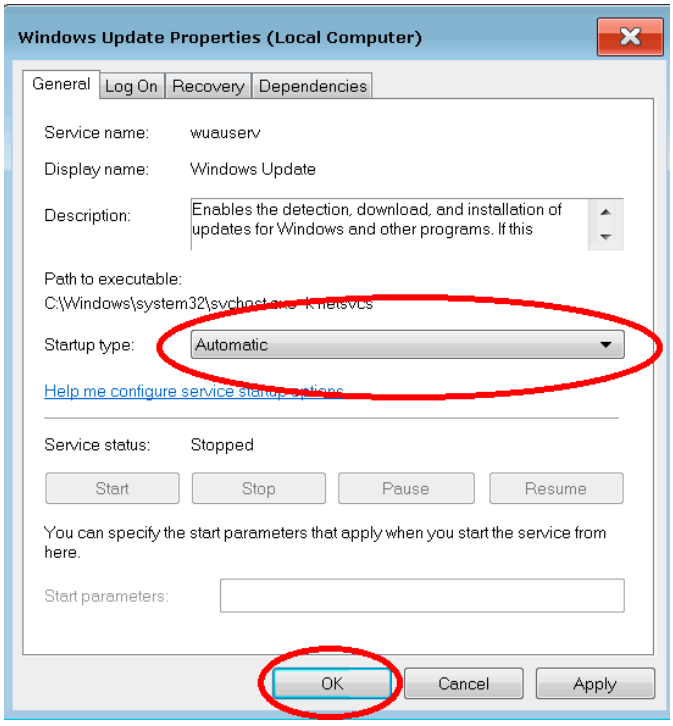


If the service is disabled (as shown in the screenshot above), proceed with the following steps to activate the service. If the service is enabled, you can proceed with the “Windows Update” as described in the next chapter.

To enable the service, select the “Windows Update” service and open the context menu and select “Properties”.



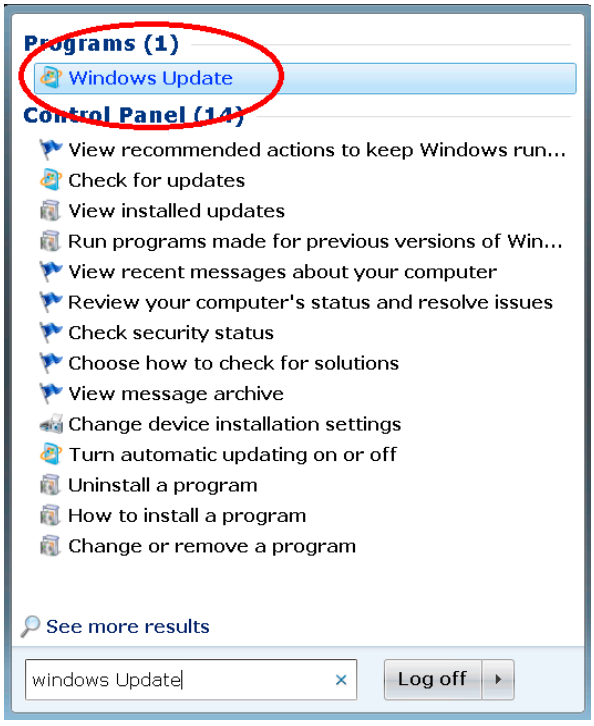
After “Windows Update Properties” dialog is displayed, select "Automatic" to the right of “Startup type” and confirm the dialog with “OK”.



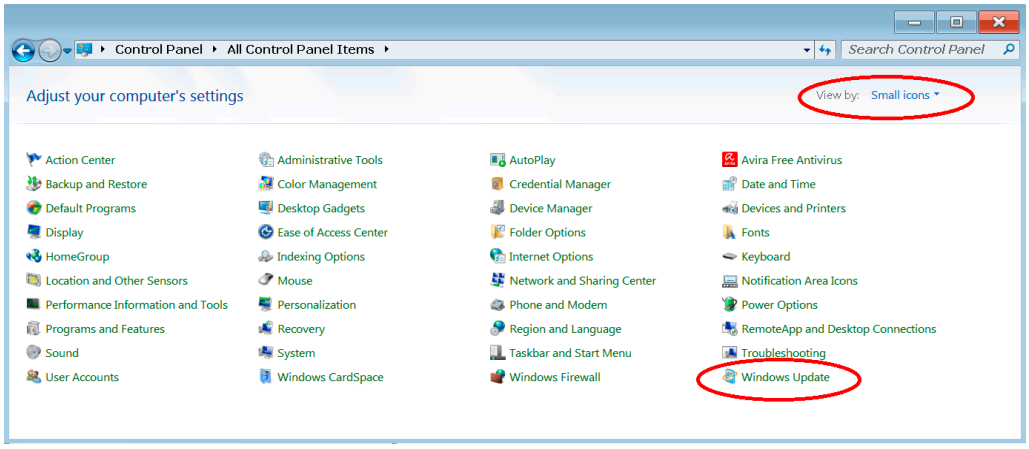
Now the service will be started and all available Windows updates can the installed.

5.2 Starting Windows Update manually

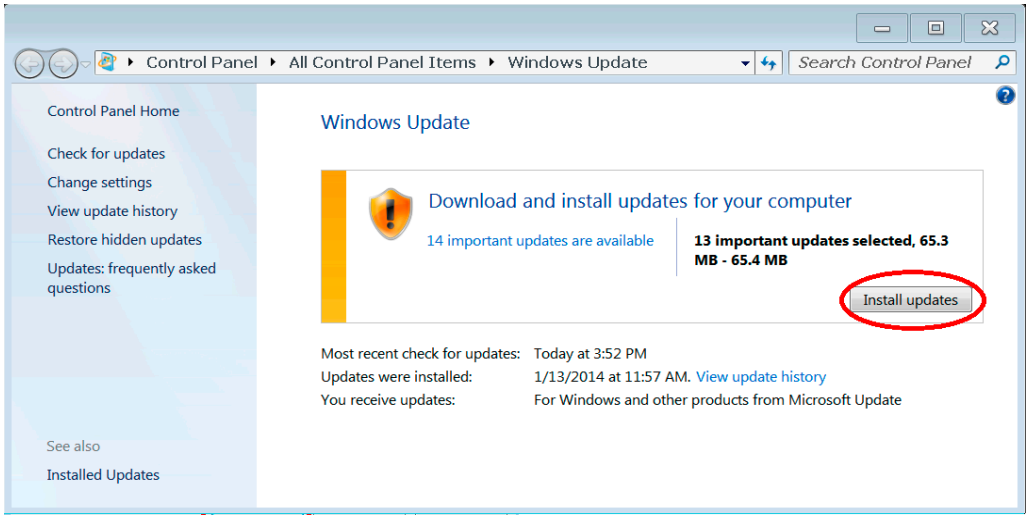
The following steps describe how to control the Windows update process. To access the “Windows Update” enter “windows update” into the start input field.



Or alternatively navigate via “Control Panel” ▷ “Windows Update”. Note that this item is only visible if the “View by:” category is set to “Small icons”.



After the Windows Update is selected, the software will check if any update is available for your instrument.

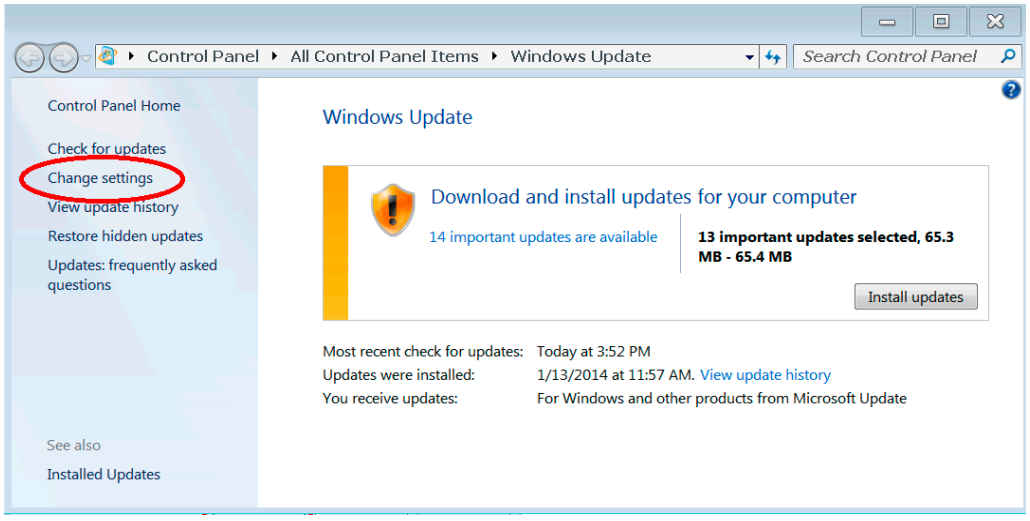


To install the update, click “Install updates”. Note that more than one iteration might be necessary to install all available updates. Please shut down the firmware when updating.

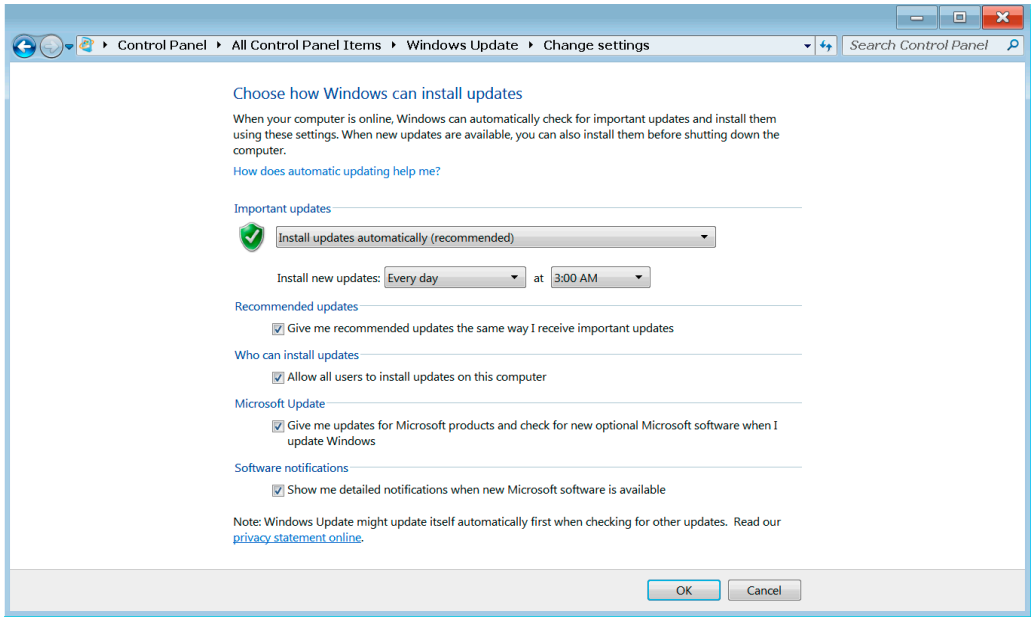
5.3 Starting Windows Update automatically

Windows Update can also automatically start the updating process, but Rohde&Schwarz does not recommend it. During installation system performance will decrease and some of the updates may cause a system reboot, cancelling any ongoing measurement procedures.

If customers choose this way to update using this method, they should schedule when no measurements are being made. To configure the Windows update you have to start the Windows Update as described above. To open the configuration dialog, select “Change settings”.



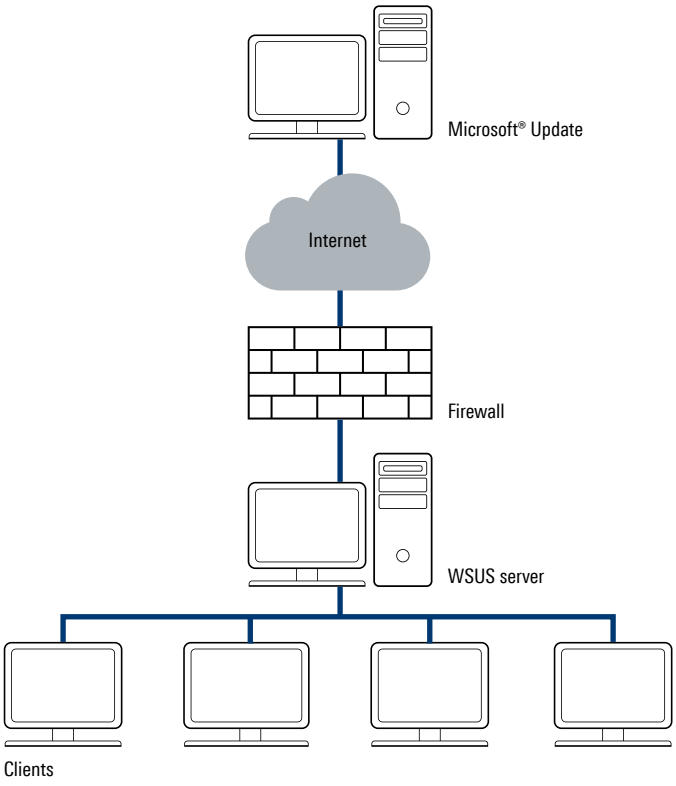
In the “Change settings” dialog the customer can choose how to install Windows updates.



5.4 Windows updates over WSUS server

Windows also enables system administrators to set up a server running Windows Server Update Services (WSUS) inside the corporate firewall, which synchronizes content directly with Microsoft® Update and distributes updates to client computers and instruments.

Update scenario via WSUS server



If this is how you receive Windows updates, please contact your IT department for further instructions and make sure that Windows 7 updates are distributed via your company's WSUS server.

6 REFERENCES

[1] News about security threats
http://www.securityfocus.com/

[2] Microsoft support: How to disable the autorun functionality in Windows
http://support.microsoft.com/kb/967715/en-us

[3] Microsoft support: Troubleshooting Windows firewall settings in Windows 7 SP 1
http://support.microsoft.com/kb/875357/en-us

[4] Advanced firewall settings for Windows 7, allowing certain programs through the firewall
http://windows.microsoft.com/en-us/windows/communicate-through-windows-firewall#1TC=windows-7

[5] Firewall "New Rule" wizard guides you through the creation steps
http://technet.microsoft.com/en-us/library/cc771477(v=ws.10).aspx

[6] The detailed description to unblock programs, can be find in the description for firewall setup and configuration
http://msdn.microsoft.com/en-us/library/ms751530(v=vs.110).aspx

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

PD 3608.6477.52 | Version 01.00 | October 2020 (jr)
White paper | Malware Protection Windows 7
Data without tolerance limits is not binding | Subject to change

3608647752
3608.6477.52 01.00 PDP 1 en