MALWARE PROTECTION WINDOWS XP

White paper | Version 01.01

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 XP BASED INSTRUMENTS

1.1 Overview

Rohde & Schwarz is dedicated to ensuring that all Rohde & Schwarz products are shipped virus-free. Instruments that run Windows operating systems should be protected from malware just like any other PC. Users are 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 when connecting instruments to your company's network.

Note that no regular updates for Windows XP have been published since April 2014. Rohde & Schwarz provides commercially available upgrade kits from Windows XP to Windows 7 or even Windows 10 for many instruments, increasing instrument security and the availability of Windows updates and patches.

1.2 Computer virus control program

Rohde & Schwarz recognizes the potential risk potential of computer viruses for Windows based instruments connected to local area networks (LANs).

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

- All computers within Rohde & Schwarz 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. These include the use of isolated LANs, scanning of instruments and removable storage devices and/or reimaging hard drives, whenever appropriate for the 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 considerations

The steps described above help to ensure that instruments from Rohde & Schwarz are virus-free when delivered to the customer. The user is responsible for ensuring the security of the instruments from that point on.

Before connecting the instrument to your company's network, please consult with your IT department or system administrator to determine what specific policies apply. Remember that the instrument appears as a standard computer in 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 policies.

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

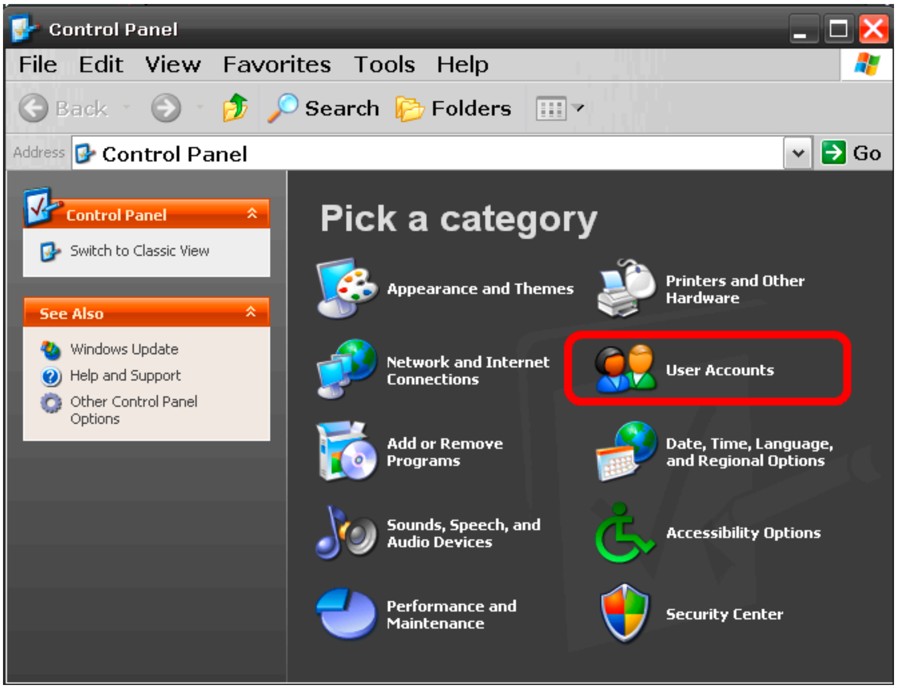
The virus definitions and operating system should be updated regularly. Rohde & Schwarz recommends checking both virus definitions and operating system updates in addition to scanning the instrument for any malware at least once a week. Be sure to always update the operating system and anti-virus definitions if advised to do so by your IT department or system administrator. Take the following steps to ensure the instrument's operating system is protected:

- Use the internet firewall on the instrument.
- Scan all removable storage devices (e.g. USB flash drives) regularly used with an instrument and deactivate the autorun/autoplay function to prevent inadvertent execution of malware from these devices.
- Install the latest Windows® patches and updates on the instrument. Note that no regular updates for Windows XP have been released since April 2014.
- Scan the instrument regularly with anti-virus software and update virus definition files. Running anti-virus software in the background ("on-access" mode) is NOT recommended as this will impact instrument performance significantly.

1.4 User accounts

Windows requires users to identify themselves by entering a user name and password in a login window. Rohde & Schwarz instruments usually have a factory-installed auto-login function, i.e. login is carried out automatically during instrument startup. The factory default for this auto-login function has administrator rights with unrestricted access, enabling printer installation and network configuration.

Two types of user accounts are available for many instruments, 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 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

A firewall can be used to protect a computer or instrument against attacks from the network with Windows XP SP2 and later versions. Rohde & Schwarz instruments are shipped with the Windows firewall enabled and preconfigured. Having the firewall activated on the instruments is helpful even when the instruments are used in your company's protected network. The number of worms, viruses and other malware circulating on the internet today make it 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 requirements for security and protection, please contact your IT department or system administrator to ensure conformity with your company's security policy.

2.1 Firewall port configuration

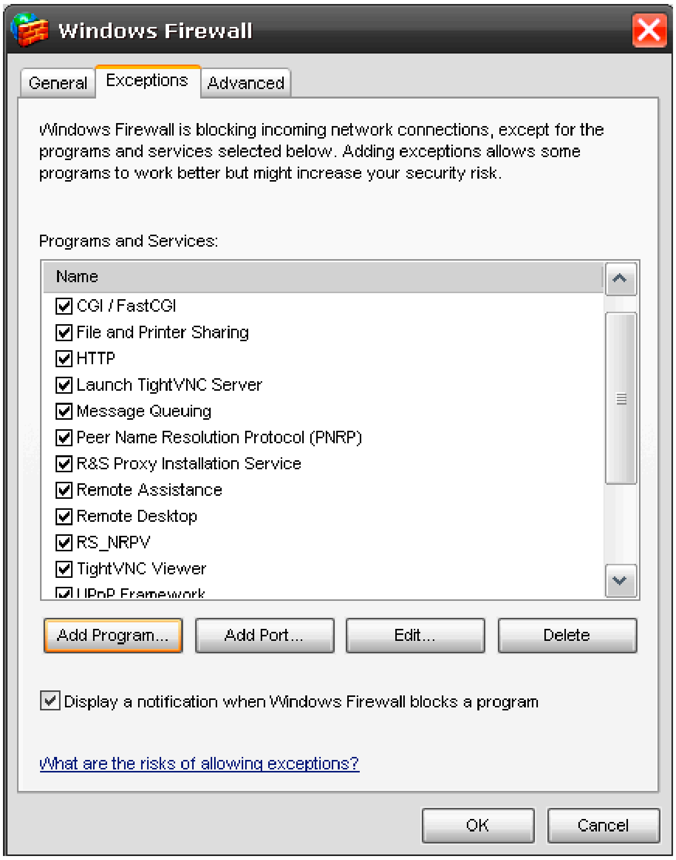
Rohde & Schwarz instruments are preconfigured so that all ports and connections for remote control are enabled. See the following table for details:

Ports	Service	Description
21 TCP	FTP	Instrument web server, FTP port
80 TCP (HTTP)	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	HiSLIP	High-speed LAN interface protocol
5025 TCP (data) 5125 TCP (abort)	TCP socket	'Raw SCPI' socket connection
5044 TCP and UDP	LXI class B	LXI LAN messages and events, multicast address UDP: 224.0.23.159
5800 TCP, 5900 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.

Note that changing firewall settings requires administrator rights. You can manage the firewall settings at “Windows Start” ▷ “Control Panel” ▷ “Windows Firewall”:



Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.

Programs and Services:

Name
- ☑ CGI / FastCGI
- ☑ File and Printer Sharing
- ☑ HTTP
- ☑ Launch TightVNC Server
- ☑ Message Queuing
- ☑ Peer Name Resolution Protocol (PNRP)
- ☑ R&S Proxy Installation Service
- ☑ Remote Assistance
- ☑ Remote Desktop
- ☑ RS_NRPV
- ☑ TightVNC Viewer
- ☑ UPnP Framework

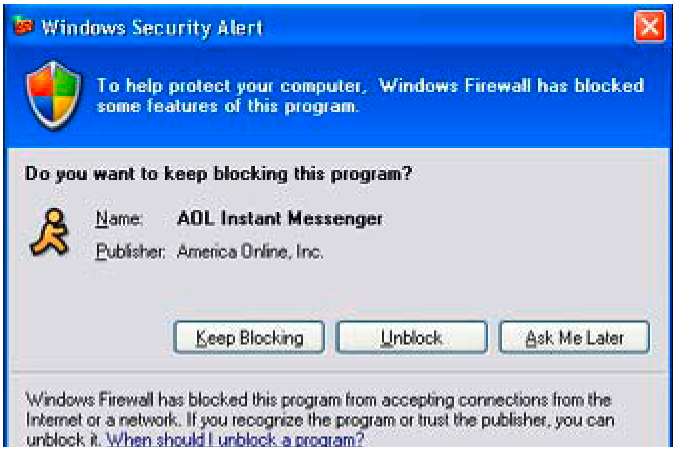
☑ Display a notification when Windows Firewall blocks a program

What are the risks of allowing exceptions?

Default firewall configuration problems come in two forms:

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

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



To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: AOL Instant Messenger

Publisher: America Online, Inc.

Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

To unblock the program, click “Unblock” in the “Security Alert” dialog box. You can find a detailed description for firewall setup and configuration at: http://support.microsoft.com/kb/875357/en-us

3 USB DEVICES

USB flash drives and removable hard drives are common in the work-place, as they have considerable storage capacity and can be used to conveniently store instrument settings, measurement results, hardcopies etc. However, they also create many problems, such as a large number of viruses, trojans and other malware that can infect computers via USB storage devices. Once an infected USB drive is plugged into an instrument, the malware on it can spread through the entire network.

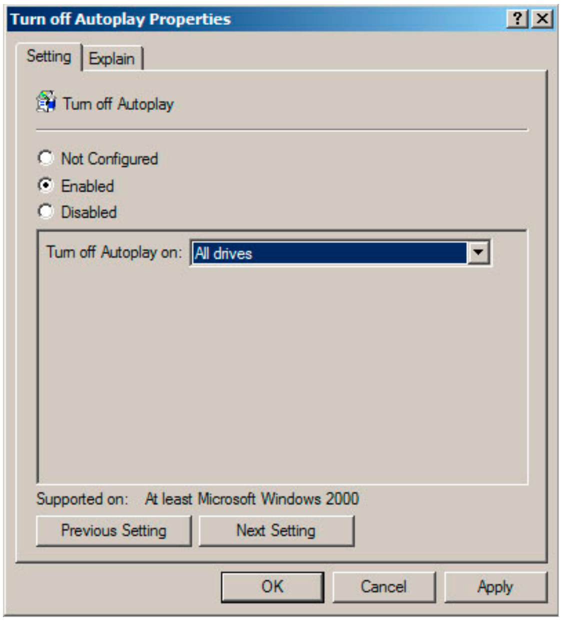
3.1 Disable USB autorun function

Generally, viruses that propagate via USB drives use the Windows "autorun" function as it does not require any user confirmation and runs silently in the background. Rohde & Schwarz instruments have the autorun/autoplay function disabled. This prevents any malware from automatically executing itself from a USB drive.

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

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

- ▶ Click "Windows Start" ▷ "Run" and then enter gpedit.msc to open the group policy settings.
- ▶ Go to "Computer Configuration" ▷ "Administrative Templates" ▷ "System", scroll down and double-click "Turn off Autoplay" to start the settings dialog.



Turn off Autoplay Properties

Turn off Autoplay

○ Not Configured
● Enabled
○ Disabled

Turn off Autoplay on: All drives

Supported on: At least Microsoft Windows 2000

- ▶ Click the "Enabled" radio button, then from the "Turn off Autoplay on" drop down list select "All drives" to prevent any program from automatically executing from any USB drive or other removable media.
- ▶ Note: If "System" is not listed, a settings template needs to be added. Right-click "Administrative Templates" and choose "Add/Remove Templates". In the dialog, click "Add", and select "system.adm". Click "Open" and "Close" to return to the main window.
- ▶ You can find a detailed description of the autorun function, if required, at: http://support.microsoft.com/kb/967715/en-us

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 from malware.

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

4 ANTI-VIRUS SOFTWARE

As with personal and business computers, users must take appropriate steps to protect their instruments from infection. Besides the use of strong firewall settings and regularly scanning any removable storage device used with a Rohde & Schwarz instrument, anti-virus software should also be installed on the instrument. Rohde & Schwarz does not recommend running anti-virus software in the background ("on-access" mode) on Windows based instruments, as it may compromise instrument performance but does recommend running it during non-critical hours at least once a week.

Today's anti-virus software requires a significant amount of system resources (both hard drive and memory). Therefore, 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 these 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 can update regularly over the internet or via offline installation. Please contact your IT department to find the right solution for your anti-virus software. Keep in mind that any anti-virus software update will compromise instrument performance.

5 WINDOWS PATCHES AND UPDATES

Until April 2014, Microsoft had regular security updates and other patches to protect Windows XP based operating systems. The updates were released on the Microsoft® Update website and associated update server. Instruments using Windows XP, especially those that connect to a network, should install all available updates.

Note: Microsoft® Update supersedes Windows Update, which was only for Windows based products.

The following section describes the installation and configuration of the Windows Update Agent. This enables the instrument to download and install all available Windows patches and updates.

Make sure that at least Windows XP SP2 is installed on your Rohde & Schwarz instrument. Refer to the instrument's manual for how to check the current operating system version. If it uses an older version, contact your Rohde & Schwarz representative for update possibilities. Rohde & Schwarz provides an instrument recovery DVD from Windows XP SP2 to Windows XP SP3 to reimage the instrument's hard drive.

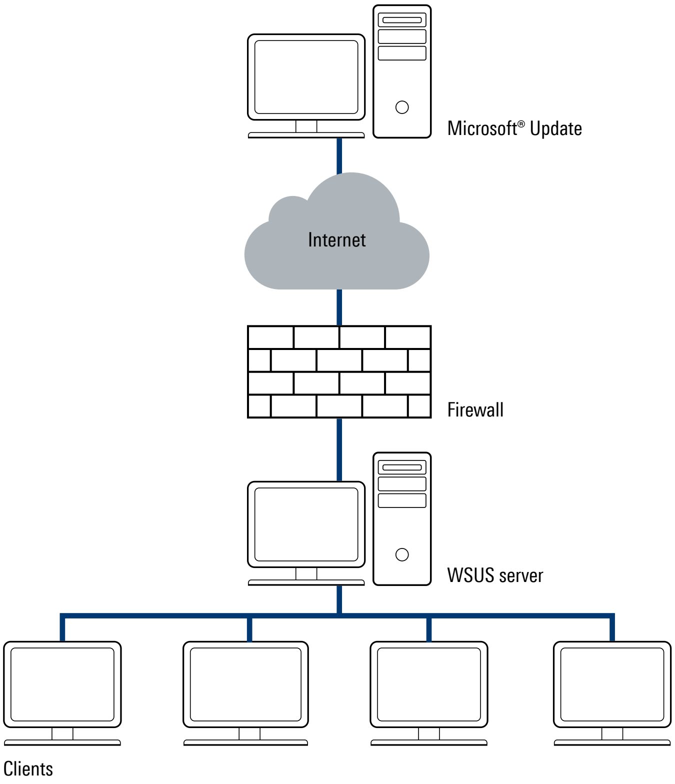
Note: Upgrading an instrument from SP2 to SP3 with the Microsoft® Update service, or by manual installation of an executable standalone service pack is not recommended.

Note: Rohde & Schwarz also provides upgrade kits from Windows XP to Windows 7 or even Windows 10 for many instruments, which increases instrument security and availability of Windows updates and patches.

In general, there are two scenarios for instruments using the Microsoft® Update service:

- The instruments have access to the internet, and download updates directly from the Microsoft® Update server.
- The instruments download updates from an update server in your company.

Update scenario via WSUS server



In the second scenario, system administrators set up a server that runs Windows server update services (WSUS) inside the corporate firewall, which synchronizes content directly with Microsoft® Update and distributes updates to client computers and instruments.

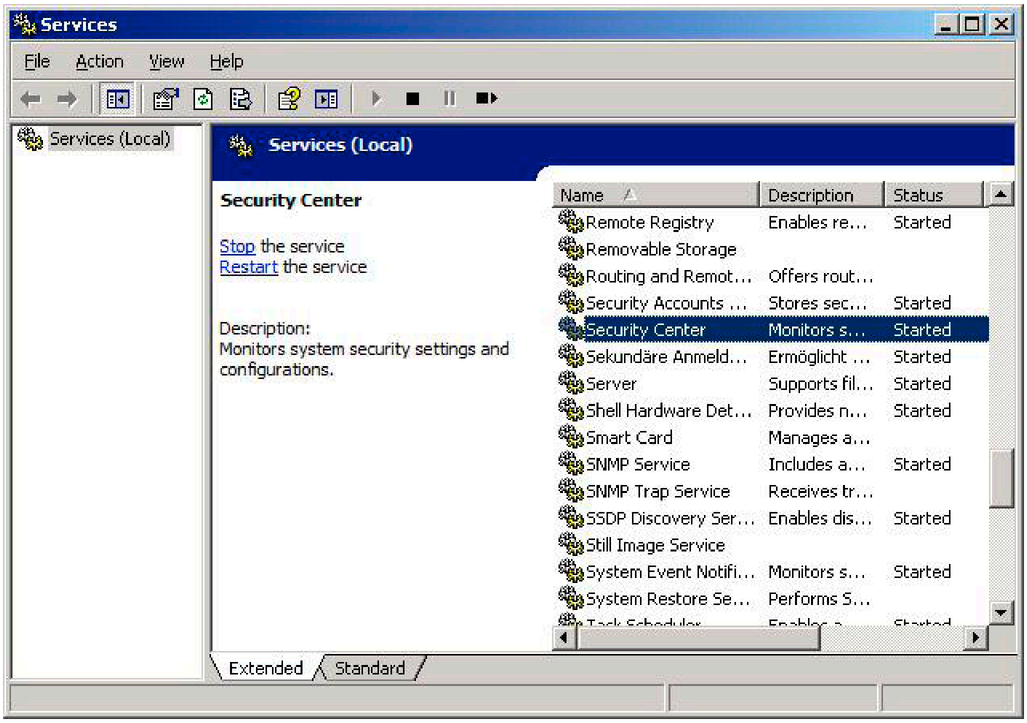
5.1 Installation and configuration of Windows Update Agent

Most Rohde & Schwarz instruments use Windows XP Embedded, a customizable version of Windows XP Professional. The operating system is scaled and optimized to the specific instrument requirements. In many cases, the Windows update service has to be separately installed on the instruments.
Download the Windows Update Agent installer WindowsUpdateAgent30-x86.exe from the Microsoft website http://go.microsoft.com/fwlink/?LinkID=100334 and copy it onto a USB flash drive. The installation is straightforward and does not present critical installation options.

The Windows Update Agent installation steps are listed below:

- ▶ Press Ctrl + Esc or click "Start" to bring up the Windows start menu and then run Windows Explorer.
- ▶ Select the directory on the USB flash drive where the Windows Update Agent installer is located.
- ▶ Start the installation by double-clicking the .exe file.
- ▶ Read and accept the license agreement by clicking the "Next" button.
- ▶ Follow the installation wizard to finish the installation.

To configure the Windows Update Agent settings, select "Windows Start" ▷ "Control Panel" and then "Administrative Tools" ▷ "Services" and double-click on "Security Center" to open the settings dialog:



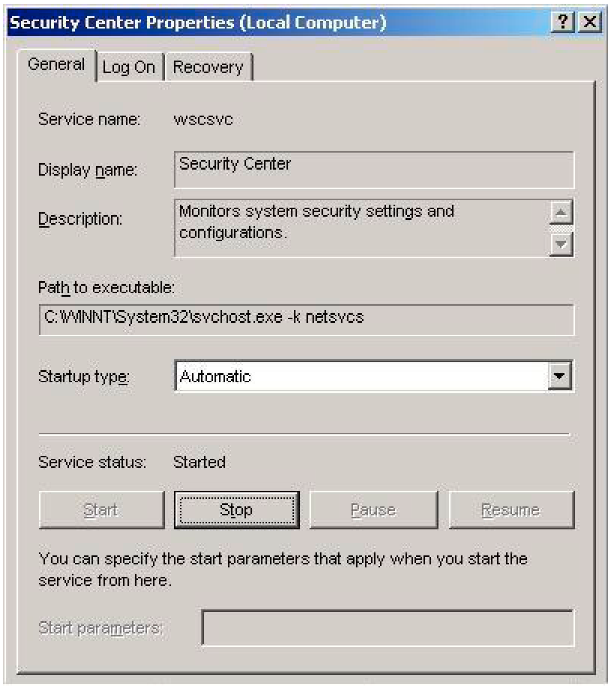
Security Center

Stop the service
Restart the service

Description:
Monitors system security settings and configurations.

Name	Description	Status
Remote Registry	Enables re...	Started
Removable Storage		
Routing and Remot...	Offers rout...	
Security Accounts ...	Stores sec...	Started
Security Center	Monitors s...	Started
Sekundäre Anmeld...	Ermöglicht ...	Started
Server	Supports fil...	Started
Shell Hardware Det...	Provides n...	Started
Smart Card	Manages a...	
SNMP Service	Includes a...	Started
SNMP Trap Service	Receives tr...	
SSDP Discovery Ser...	Enables dis...	Started
Still Image Service		
System Event Notifi...	Monitors s...	Started
System Restore Se...	Performs S...	
Task Scheduler	Enables a...	Started

Select "Automatic" as the startup type and press "Start" to run the service:



Security Center Properties (Local Computer)

Service name: wscsvc

Display name: Security Center

Description: Monitors system security settings and configurations.

Path to executable:
C:\WINNT\System32\svchost.exe -k netsvcs

Startup type: Automatic

Service status: Started

You can specify the start parameters that apply when you start the service from here.

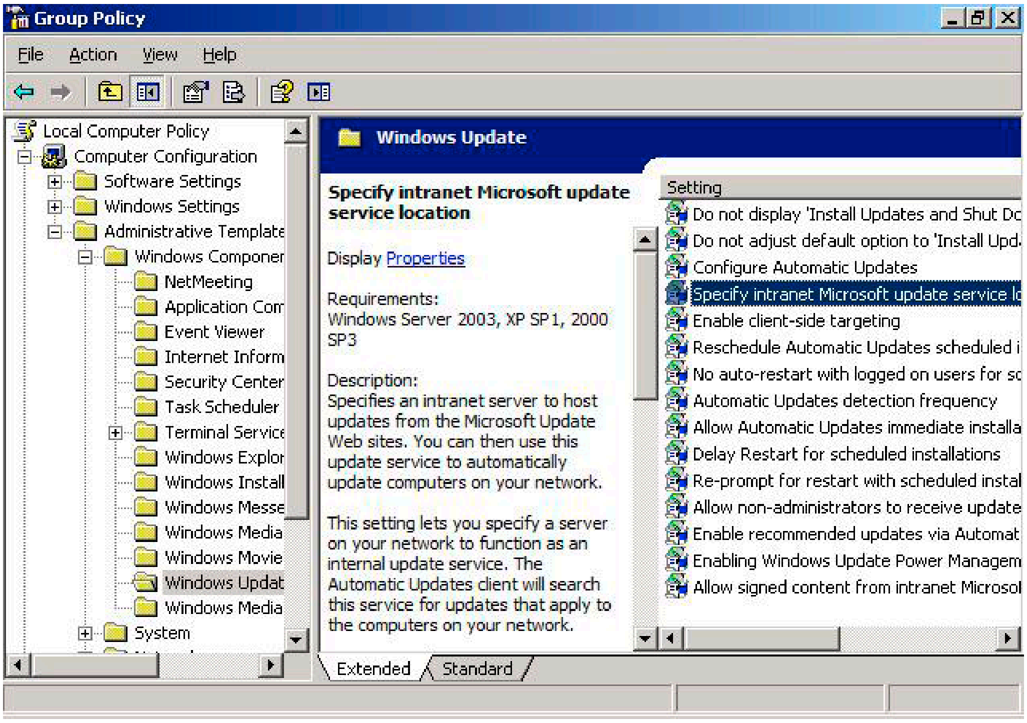
Start parameters:

Press "OK" to finish the configuration.

5.2 Instruments connected to a Windows update server

Many companies have a Windows update (WSUS) server running on the network. If an instrument is connected to the network, it can be configured to use the WSUS server for Windows updates. Please contact your IT department or system administrator to make sure the instrument configuration complies with your company's policy and make sure that Windows XP updates are distributed via your company's WSUS server.

You can control or change the WSUS client settings on the instrument via “Windows Start” ▷ “Run” and then enter gpedit.msc to start the group policy settings. Navigate in the window to “Computer Configuration” ▷ “Administrative Templates” ▷ “Windows Components” ▷ “Windows Updates”. Scroll to and double-click “Specify intranet Microsoft update service location” to start the settings dialog:



Specify intranet Microsoft update service location

Display Properties

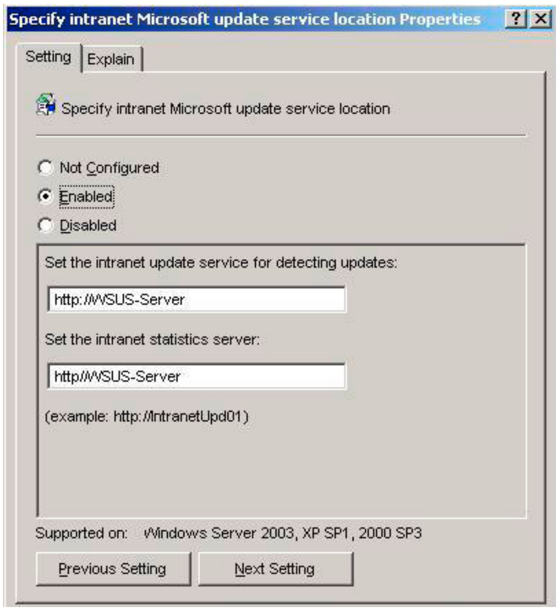
Requirements:
Windows Server 2003, XP SP1, 2000 SP3

Description:
Specifies an intranet server to host updates from the Microsoft Update Web sites. 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 your network.

Setting
- Do not display 'Install Updates and Shut Do
- Do not adjust default option to 'Install Upd.
- Configure Automatic Updates
- Specify intranet Microsoft update service lo
- Enable client-side targeting
- Reschedule Automatic Updates scheduled i
- No auto-restart with logged on users for sc
- Automatic Updates detection frequency
- Allow Automatic Updates immediate installa
- Delay Restart for scheduled installations
- Re-prompt for restart with scheduled instal
- Allow non-administrators to receive update
- Enable recommended updates via Automat
- Enabling Windows Update Power Managem
- Allow signed content from intranet Microsol

First click “Enabled”, then specify the server name within the company’s network to be used for detecting updates:


Specify intranet Microsoft update service location Properties
?
Setting
Explain
Previous Setting
Next Setting

Specify intranet Microsoft update service location

○ Not Configured
● Enabled
○ Disabled

Set the intranet update service for detecting updates:

http://WSUS-Server

Set the intranet statistics server:

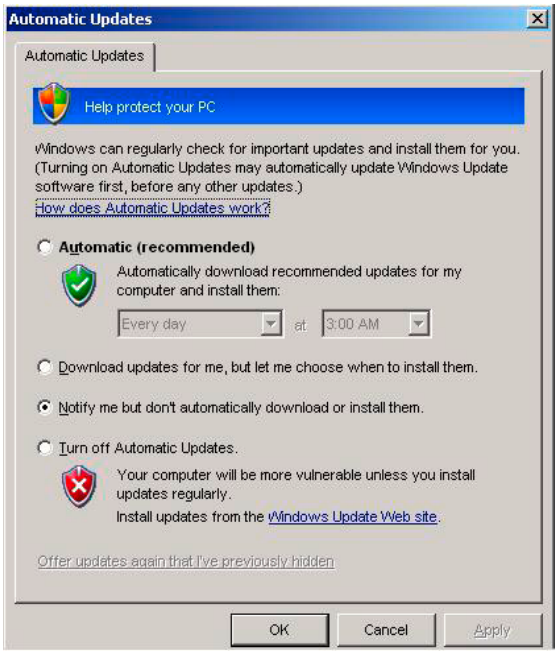
http//WSUS-Server

(example: http://IntranetUpd01)

Supported on: Windows Server 2003, XP SP1, 2000 SP3

5.3 Configuring automatic updates

The automatic update settings can be managed via “Windows Start” ▷ “Control Panel” ▷ “Automatic Updates”:



Windows can regularly check for important updates and install them for you. (Turning on Automatic Updates may automatically update Windows Update software first, before any other updates.)

How does Automatic Updates work?

○ **Automatic (recommended)**

Automatically download recommended updates for my computer and install them:

Every day at 3:00 AM

○ Download updates for me, but let me choose when to install them.

● Notify me but don't automatically download or install them.

○ Turn off Automatic Updates.

Your computer will be more vulnerable unless you install updates regularly.

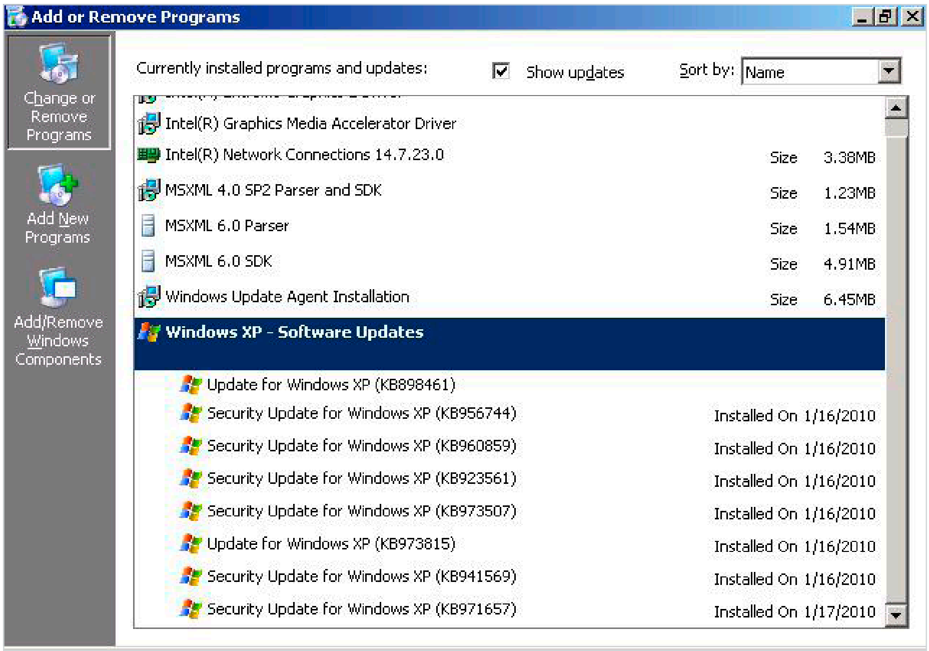
Install updates from the Windows Update Web site.

Offer updates again that I've previously hidden

Rohde & Schwarz instruments should use the “Notify me…” configuration, where user confirmation is required before download and installation. Download of updates and installation can temporarily impair instrument performance and may require a reboot. The user should schedule the update process so that it does not occur when the instrument is in use.

5.4 Viewing installed updates

Installed updates can be viewed via “Windows Start” ▷ “Control Panel” ▷ “Add or Remove Programs”:



Currently installed programs and updates: ☑ Show updates Sort by: Name

Intel(R) Graphics Media Accelerator Driver		
Intel(R) Network Connections 14.7.23.0	Size	3.38MB
MSXML 4.0 SP2 Parser and SDK	Size	1.23MB
MSXML 6.0 Parser	Size	1.54MB
MSXML 6.0 SDK	Size	4.91MB
Windows Update Agent Installation	Size	6.45MB
Windows XP - Software Updates		
Update for Windows XP (KB898461)		
Security Update for Windows XP (KB956744)	Installed On	1/16/2010
Security Update for Windows XP (KB960859)	Installed On	1/16/2010
Security Update for Windows XP (KB923561)	Installed On	1/16/2010
Security Update for Windows XP (KB973507)	Installed On	1/16/2010
Update for Windows XP (KB973815)	Installed On	1/16/2010
Security Update for Windows XP (KB941569)	Installed On	1/16/2010
Security Update for Windows XP (KB971657)	Installed On	1/17/2010

Make sure that the property “Show updates” is selected in the dialog box.

6 REFERENCES

[1] NSA security papers
http://www.nsa.gov/ia/guidance/security_configuration_guides/

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

[3] Microsoft Windows Update Agent, download link
http://go.microsoft.com/fwlink/?LinkID=100334

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

[5] Microsoft support: Troubleshooting Windows firewall settings in Windows XP Service Pack 2 for advanced users
http://support.microsoft.com/kb/875357/en-us

Trademarks
Microsoft, Windows and Windows XP are U.S. registered trademarks of the 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

R&S® is a registered trademark of Rohde & Schwarz GmbH & Co. KG
Trade names are trademarks of the owners
PD 3608.6483.52 | Version 01.01 | October 2020 (jr)
White paper | Malware Protection Windows XP
Data without tolerance limits is not binding | Subject to change

3608648352
3608.6483.52 01.01 PDP 1 en