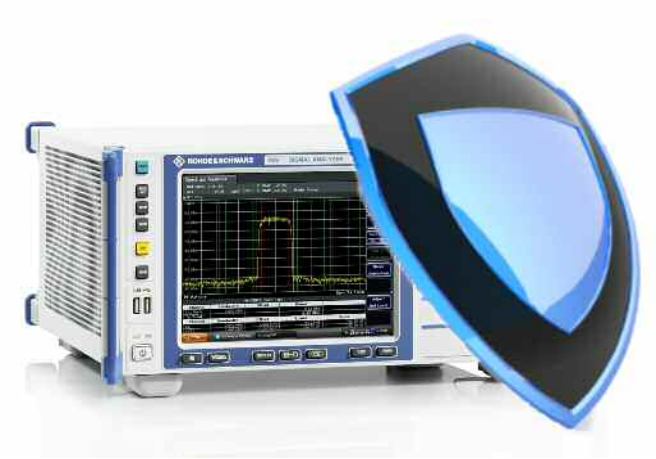
Malware Protection
White Paper



Rohde & Schwarz recognizes the potential risk of computer virus infection when connecting Windows®-based test instrumentation to other computers via local area networks (LANs), 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 paper discusses the use of anti-virus software, with recommended configuration settings. It also outlines how to keep the Windows® XP operating system properly updated through regular installation of OS patches.

Malware Protection
White Paper
Jochen Wolle
06.2010-1EF73_0e

ROHDE&SCHWARZ

Table of Contents

1 Windows®-Based Instruments

1.1 Overview

Rohde & Schwarz is dedicated to ensuring that all R&S products are shipped virus-free. Instruments that run Windows operating systems should be protected from malware just like any other PC. Users are strongly advised to take measures to protect their instruments such as using anti-virus software and installing OS patches and updates on a regular basis. It is highly recommended that you work closely with your IT department or system administrator to ensure compliance with your company policies when connecting instruments to your company's network.

1.2 Computer Virus Control Program

Rohde & Schwarz recognizes the potential risk of computer virus infections on Windows-based instrumentation which are 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 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, as appropriate depending upon 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.

1.3 Preventative Maintenance 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. Remember that the instrument appears to be a standard computer to the network. Follow your company's policies with regards to computer security and virus protection.

It is also important to update both the virus definitions and operating system regularly. 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 OS and anti-virus definitions if advised to do so by your IT department or system administrator. The following steps should be taken to ensure the instrument's operating system is protected:

- Use the Internet firewall on the instrument.
- Scan all removable storage devices (e.g. USB thumb drives) that are used with an instrument regularly 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.
- Scan the instrument regularly with anti-virus software, and keep virus definition files updated. It is NOT recommended to run anti-virus software in the background ("on-access" mode) as this will impact instrument performance significantly.

1.4 User / Admin Account

Windows requires that users identify themselves by entering a user name and password in a login window. In general, R&S instruments provide a factory-installed auto-login function, i.e. login is carried out automatically during the startup of the instrument. The factory default for this auto-login function has administrator rights with unrestricted access, so that printer installation and network configuration are possible.

For many instruments you can set up two types of user account, either an administrator account with unrestricted access to the instrument OS 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

With Windows XP SP2 and later versions, a firewall can be used to protect a computer or instrument against attacks from the network. R&S instruments are shipped with the Windows firewall enabled and preconfigured. Having the firewall activated on the instruments is helpful even when you use the instruments within your company's protected 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 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

R&S instruments are preconfigured in such a way 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, 111 udp	Portmapper	Portmapper service for VXI-11 / LXI
161 udp 162 udp 705 tcp (AgentX)	SNMP	Standard ports for SNMP agent
319 tcp udp 320 tcp udp	1588 PTP	LXI Class B/A – IEEE1588 PTP (Precision Time Protocol)
2525 tcp	RSIB	R&S SCPI socket connection
4880 tcp	HiSLIP	High Speed LAN Interface Protocol
5025 (data) 5125 (abort)	TCP Socket	'Raw SCPI' socket connection
5044 tcp 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 udp	RS Installer	R&S Software distributor service
14142 - 16383 tcp udp (dynamic assignment)	ONC-RPC	Sun ONC-RPC protocol – VXI-11

2.2 Changing Firewall Settings

Rohde & Schwarz highly recommends the use of the firewall on your instrument.

Note that changing firewall settings requires administrator rights. You can manage the firewall settings via **Windows Start ⇨ Control Panel ⇨ Windows Firewall**:

Problems that are related to the default firewall configuration appear in two ways:

- 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, 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:

http://support.microsoft.com/kb/875357/en-us

3 USB Devices

USB thumb drives and removable hard drives are now common throughout the workplace, as they have considerable storage capacity and can be used to store instrument settings, measurement results, hardcopies etc. in a very convenient way. However, they also introduce new problems; a large number of viruses, trojans and other malware infect computers via USB storage devices. Once an infected USB drive is plugged into an instrument, the malware on it can spread through the whole network.

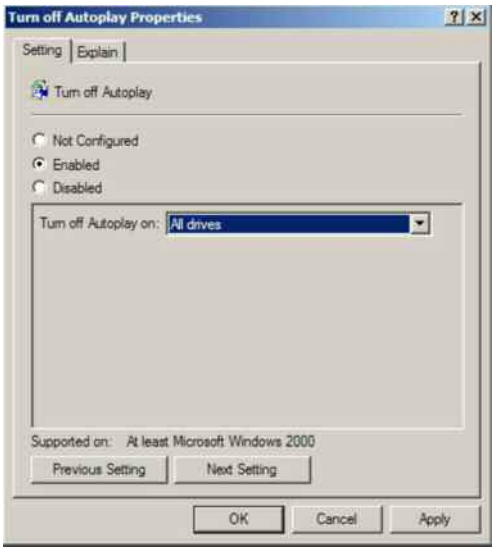
3.1 Disable USB Autorun Function

Generally, viruses that propagate via USB drives use the “autorun” function of Windows, as it does not require any user confirmation and runs silently in the background. R&S instruments are preconfigured with 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 used 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 on **Turn off Autoplay** to start the settings dialog:



- Click on 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 thumb 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 a R&S instrument.

4 Anti-Virus Software

As with personal and business computers, users must take appropriate steps to protect their instruments from infection. Beside the use of strong firewall settings and regularly scanning any removable storage device used with a R&S instrument, it is also recommended that anti-virus software be 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 consumption). Therefore some instruments may not be capable of installing or running anti-virus software due to limited resources. Other options in that case are to scan these instruments with software run from a USB thumb drive, or to mount these instruments as a drive on the network and scan them from another computer with anti-virus software. These options will be detailed later.

Note: The following sections are intended to highlight recommendations for anti-virus software, using as examples a few commonly used programs. It is recognized that there are other capable programs; the ones used in the following sections serve as general examples and the principles apply to other programs which may be used by your IT department or system administrator.

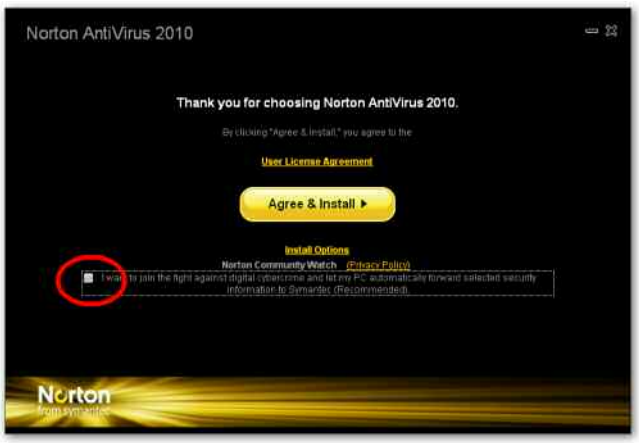
Installing, configuring and using anti-virus software requires administrator rights.

4.1 Norton™ AntiVirus 2010

This section describes the installation, configuration and use of the anti-virus software Norton AntiVirus 2010 on R&S instruments.

4.1.1 Installation

Install the Norton AntiVirus 2010 software on the instrument as described in the vendor's manual. Deactivate the control check box **I want to join the fight...** on the installation welcome page and start the installation with **Agree & Install**:



After installation completes, Norton AntiVirus 2010 tries to connect to the Symantec server to get the latest virus signatures and program updates (a process called LiveUpdate).

4.1.2 Requirements

Norton AntiVirus 2010 has the following requirements:

- 200 MB Free space on the instrument's hard drive
- 256 MB Memory
- Windows XP SP2 or later

Make sure that as a minimum Windows XP SP2 is installed on your R&S instrument. Refer to the instrument's user manual for how to check the current OS version. If it's based on an older version, contact your R&S representative for update possibilities. For many instruments R&S provides an instrument recovery DVD with the latest OS version for re-imaging the instrument's hard drive.

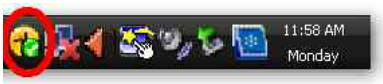
During LiveUpdate or a virus scan, two processes (both named **ccSvcHst.exe)** run on the instrument and occupy **up to 270 MB** of memory.

Therefore, Rohde & Schwarz recommends that the firmware on the instrument be stopped before starting LiveUpdate or a virus scan. Refer to the instrument's manual for how to stop execution of the instrument's firmware.

4.1.3 Deactivate Automatic Updates and Virus Scans

Symantec LiveUpdate needs an Internet connection and administrator rights in order to be executed. The updates are downloaded from the Symantec server or from a proxy server in your company. Contact your IT department or system administrator for details on your company's policy.

Configure "LiveUpdate" and "Scans to be executed on demand" to avoid degradation of the instrument's performance. Double-click on the Norton AntiVirus icon in the system tray to bring up the main dialog:



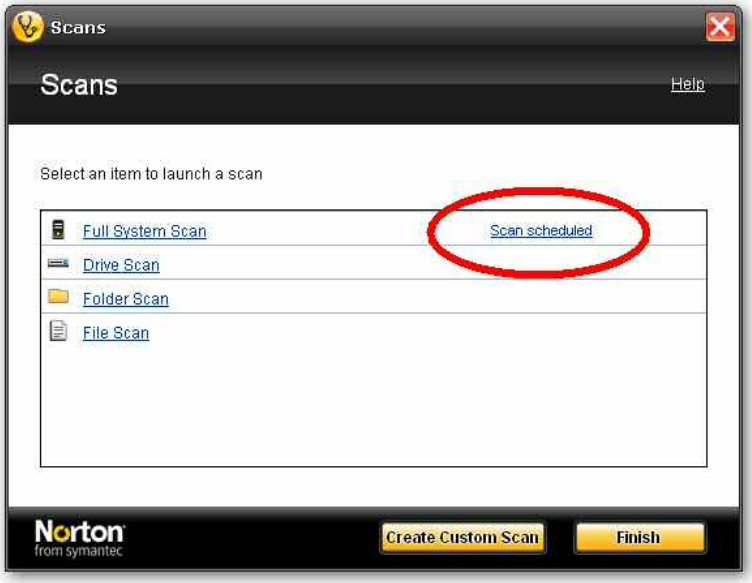
Click on **Settings** to configure LiveUpdate and scans:

Deactivate both **Automatic LiveUpdate** and **Pulse Updates** in the **Computer Settings** dialog:

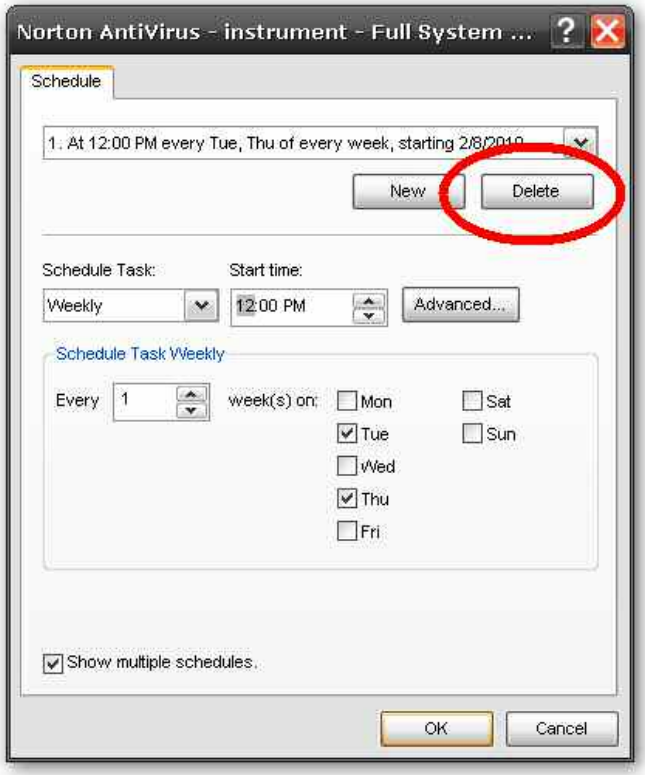
Save the settings with **OK**.

The final step of the configuration is to deactivate automatic virus scans. Bring up the main dialog as in the steps above and select **Run Custom Scan**.

Select **Scan scheduled** to modify the list of scheduled virus scans:

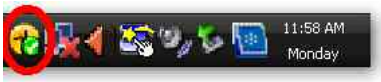


Delete entries in the schedule dialog until the drop down box is empty. This deactivates any automatic virus scans:



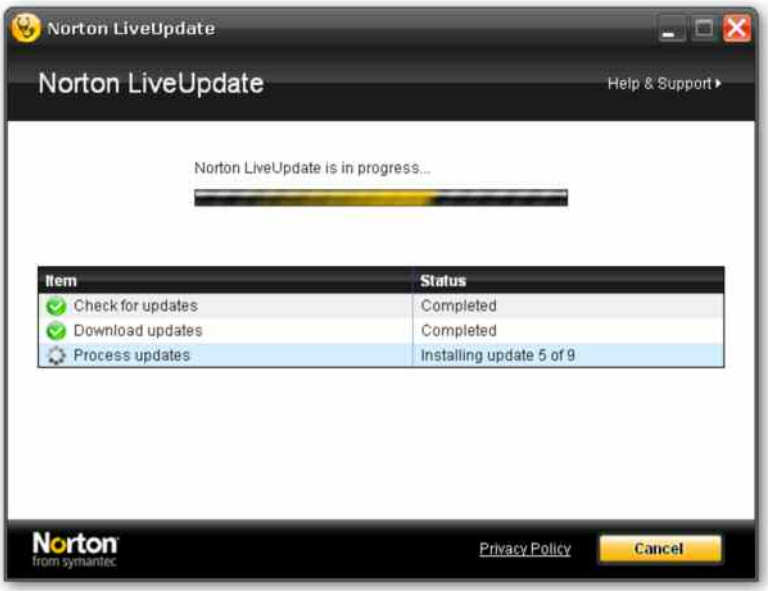
4.1.4 Update Virus Signatures and Scan for Viruses on Demand

To start LiveUpdate for the virus signature database and the anti-virus software on the instrument, you need an Internet connection. Double-click on the Norton Antivirus icon in the system tray to bring up the main dialog:



Start the update process with **Run LiveUpdate**:

When LiveUpdate is finished, press the **OK** button.



Once the virus signature database is updated you can start the virus scan process.

To start the virus scan process press **Scan Now** in the main dialog:

In the following dialog you can choose between the three scan options:

You can either scan commonly infected areas (**Quick Scan**), scan your entire instrument (**Full System Scan**), or run a custom scan of drives, folders and files (**Custom Scan**).

When the scan process is complete click on **Finish** to close the dialog.

4.2 Kaspersky® Anti-Virus 2010

This section describes the installation, configuration and use of the anti-virus software Kaspersky Anti-Virus 2010 on R&S instruments.

4.2.1 Installation

Install the Kaspersky Anti-Virus 2010 software on the instrument as described in the vendor's manual.

After installation completes, you should start Kaspersky Anti-Virus 2010 to connect to the Kaspersky server to get the latest virus signatures and program updates.

4.2.2 Requirements

Kaspersky Anti-Virus 2010 has the following requirements:

- 300 MB Free space on the instrument's hard drive
- 256 MB Memory
- Windows XP SP2 or later

Make sure that as a minimum Windows XP SP2 is installed on your R&S instrument. Refer to the instrument's manual for how to check the current OS version. If it's based on an older version contact your R&S representative for update possibilities. For many instruments R&S provides an instrument recovery DVD with the latest OS version to re-image the instrument's hard drive.

During a virus signature / program update or a virus scan, two processes (both named **avp.exe)** run on the instrument and occupy **up to 320 MB** of memory.

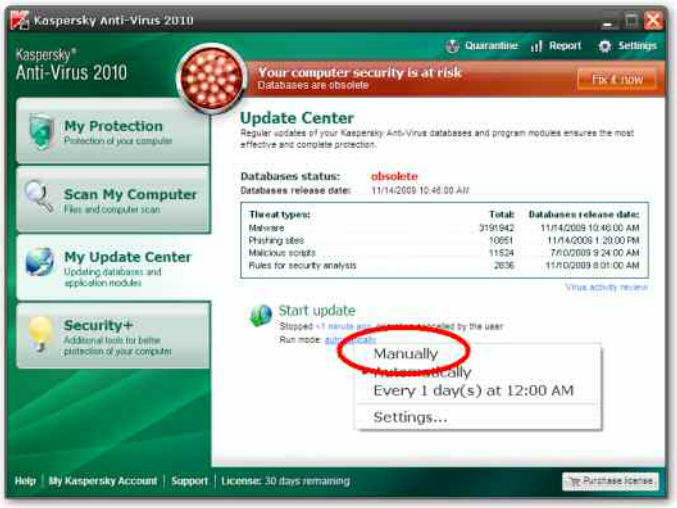
Therefore, Rohde & Schwarz recommends that the firmware on the instrument be stopped before starting updates or a virus scan. Refer to the instrument's manual for how to stop execution of the instrument's firmware.

4.2.3 Deactivate Automatic Updates and Virus Scans

Kaspersky Anti-Virus 2010 needs an Internet connection and administrator rights in order to be executed. The updates are downloaded from the Kaspersky server or from a proxy server in your company. Contact your IT department or system administrator for details on your company's policy.

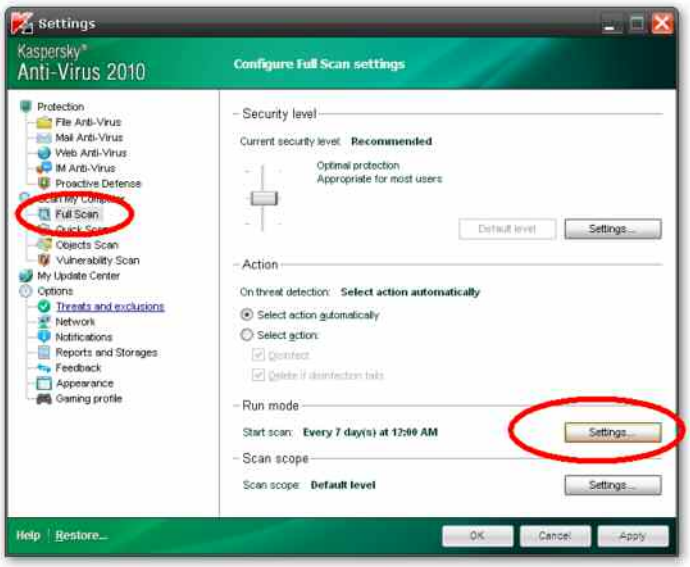
Configure virus definition updates and virus scans to be executed on demand to avoid degradation of the instrument's performance. Double-click on the Kaspersky Anti-Virus icon in the system tray to bring up the main dialog:

Click on **My Update Center**. To deactivate automatic virus / program updates select **Manually** under **Start update ⇨ Run mode**:

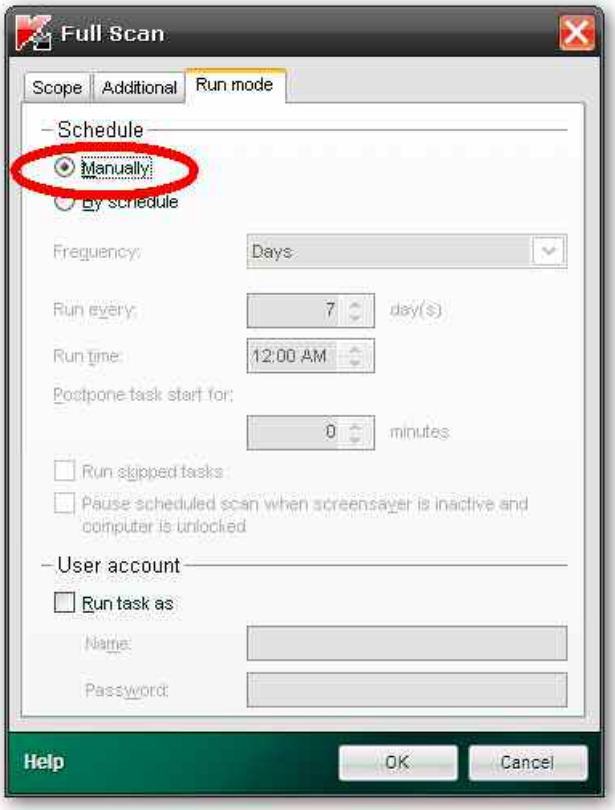


To configure automatic virus scans select **Settings** in the upper right of the main dialog:

Select **Full Scan** in the left hand navigation pane and then **Settings** to configure the Run Mode:



Select **Manually** under **Schedule** and confirm with **OK** to deactivate automatic virus scans:



4.2.4 Update Virus Signatures and Scan for Viruses on Demand

To start updates for the virus signature database and the anti-virus software on the instrument, you need an Internet connection. Double-click on the Kaspersky Anti-Virus icon in the system tray to bring up the main dialog:

To start the update process select **My Update Center** on the left hand tabs in the main dialog and then **Start Update**:

To start a virus scan select **Scan My Computer** on the left hand tabs in the main dialog and then **Start Full Scan**:

Other options for virus scanning are **Quick Scan** or **Objects Scan**.

4.3 Microsoft® Security Essentials

This section describes the installation, configuration and usage of the anti-virus software Microsoft Security Essentials on R&S instruments.

4.3.1 Installation

Install the Microsoft Security Essentials anti-virus software on the instrument as described in the vendor's manual. No Internet connection is necessary to complete the installation.

After installation completes, Microsoft Security Essentials tries to connect to the Microsoft server to get the latest virus signatures and program updates. To prevent this, deactivate the control box **Scan my computer for potential threats** and select **Finish** to complete the installation.

4.3.2 Requirements

Microsoft Security Essentials has the following requirements:

- 300 MB Free space on the instrument's hard drive
- 256 MB Memory
- Windows XP SP2 or later

Make sure that as a minimum Windows XP SP2 is installed on your R&S instrument. Refer to the instrument's manual for how to check the current OS version. If it's based on an older version contact your R&S representative for update possibilities. For many instruments R&S provides an instrument recovery DVD with the latest OS version to re-image the hard drive of the instrument.

During a virus signature / program update or a virus scan, two processes (named **MsMpEng.exe** and **msseces.exe**) run on the instrument and occupy **up to 110 MB** of memory.

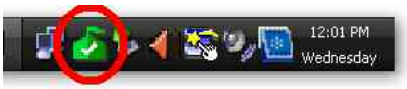
Therefore, Rohde & Schwarz recommends that the firmware on the instrument be stopped before starting a virus scan. Refer to the instrument's manual for how to stop execution of the instrument's firmware.

4.3.3 Deactivate Automatic Virus Scans

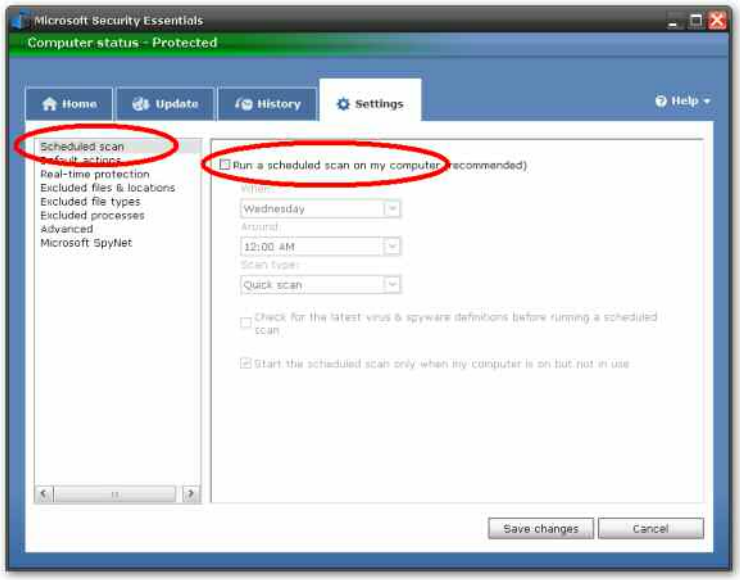
Microsoft Security Essentials needs an Internet connection and administrator rights to be executed.

Note: *The virus signature updates are downloaded from the Microsoft server automatically if the virus signature database is older than 24h. There is no configuration to disable this automatic update process. Also, Microsoft Security Essentials can not be configured to use a proxy server in your company.*

Configure virus scans to be executed on demand to avoid degradation of the instrument's performance. Double-click on the Microsoft Security Essentials icon in the system tray to bring up the main dialog:



Select the **Settings** tab and **Scheduled scan** on the left hand navigation pane. Deselect **Run a scheduled scan…** to deactivate automatic virus scans.

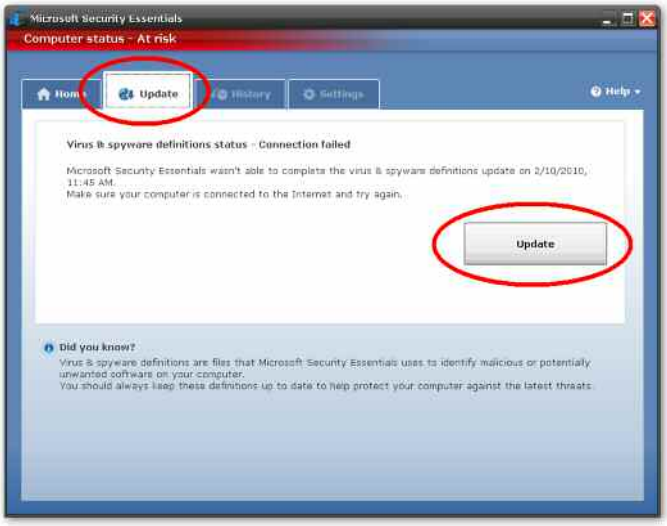


Store the configuration with **Save changes**.

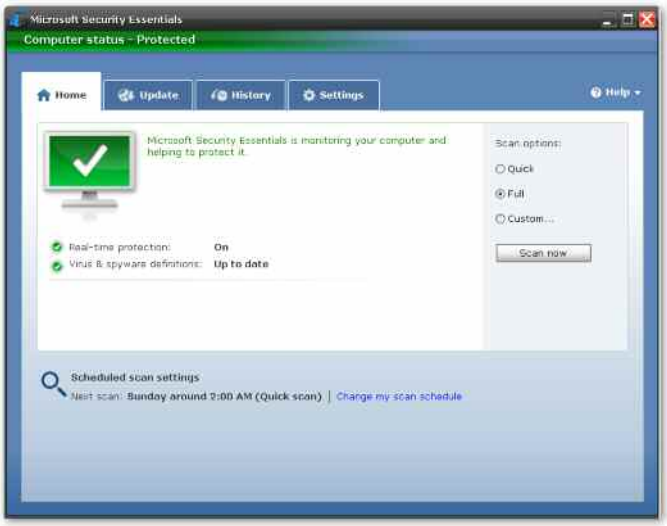
4.3.4 Update Virus Signatures and Scan for Viruses on Demand

To start updates for the virus signature database and the anti-virus software on the instrument you need an Internet connection. Double-click on the Microsoft Security Essentials icon in the system tray to bring up the main dialog:

Select the **Update** tab in the main dialog and then press **Update** to start the update process:



To start a virus scan select **Full Scan** in the main dialog and then **Scan now**:



Other options for virus scanning are **Quick Scan** or **Objects Scan**.

4.4 Scanning from a USB thumb drive

There may be instruments that do not have the resources to have anti-virus software installed. For these instruments, scanning can be done from a USB thumb drive.

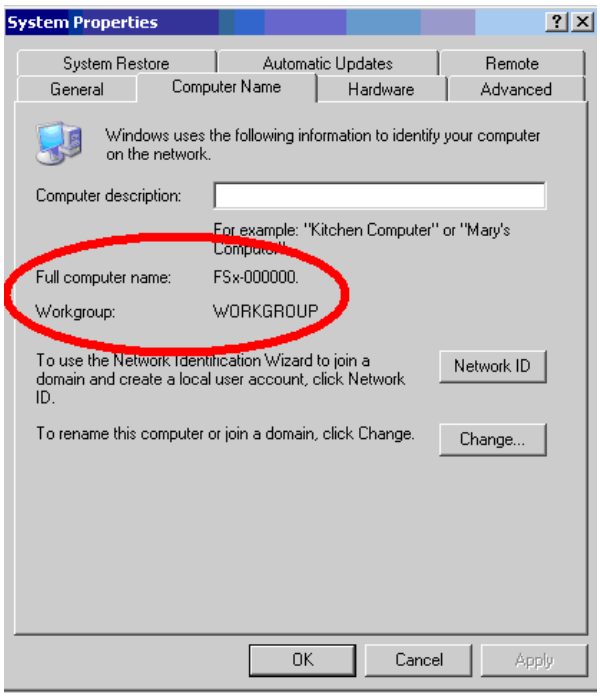
4.5 Scanning Instruments from another PC

Before scanning with anti-virus software from another computer the instrument has to be mounted as a drive on the network.

Note: Scanning instrument hard drives remotely has some limitations and should only be used if the other options are not available: only visible files can be scanned, memory and processes will not be scanned, and a rootkit can completely hide itself.

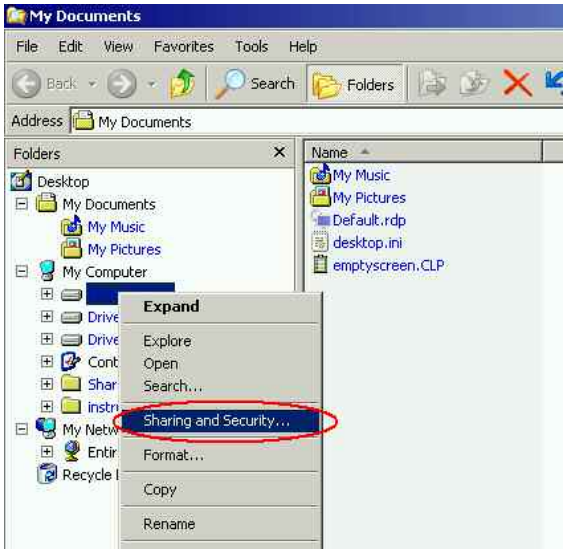
4.5.1 Share Drives of the Instrument

Connect the instrument to the network. Check for the instrument's computer name and Workgroup. (This information is needed later on to scan this specific instrument from your PC). To view these settings use **Windows Start ⇨ Control Panel ⇨ System** and select the **Computer Name** tab in the dialog:

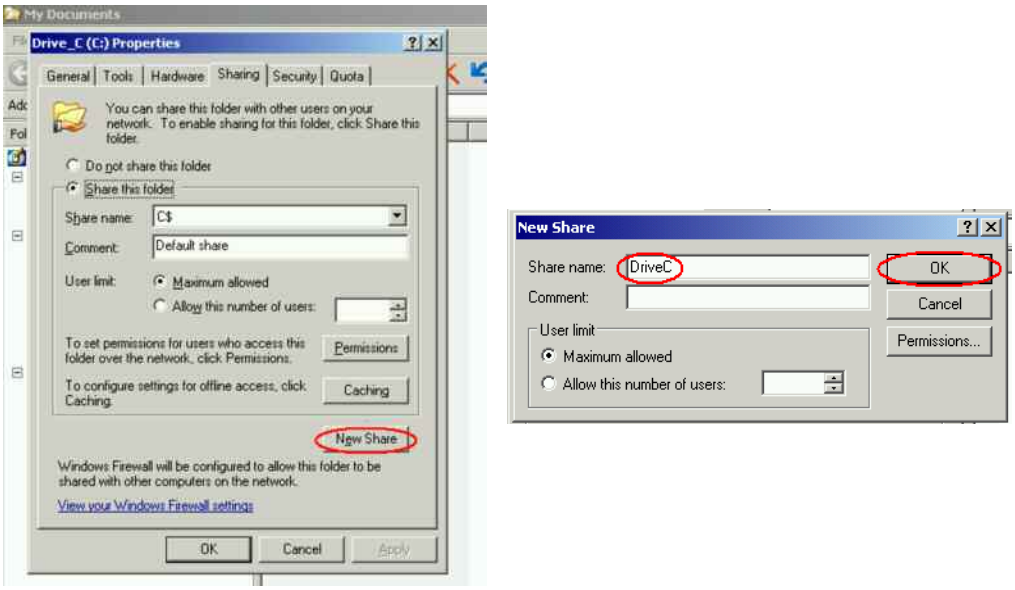


In this case the instrument's computer name is FSx-000000 and is part of the workgroup WORKGROUP.

Start the Windows Explorer on the instrument and expand the folder **My Computer** to see all the drives. Right-click on Drive C: to open the context menu and select **Sharing and Security**:



In the dialog which opens up select **New Share** to enter a name e.g. "DriveC", and confirm with OK.



The symbol for Drive C: should now have changed to the symbol for a shared drive:

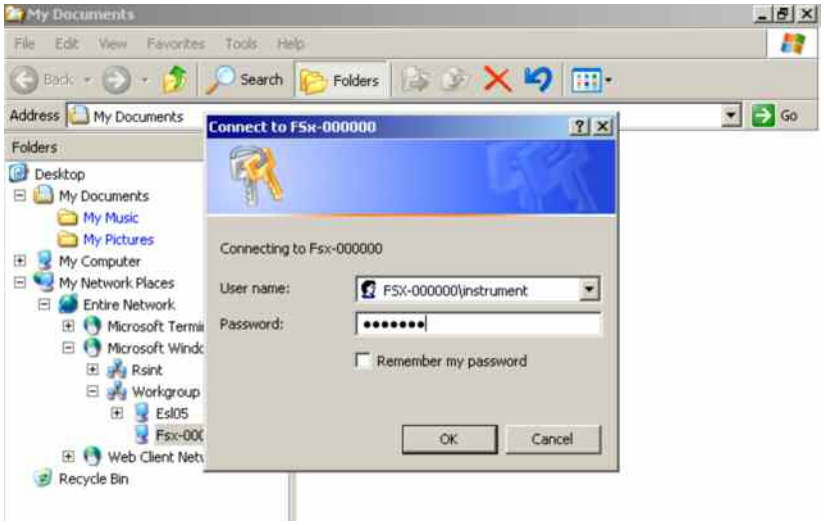
Repeat the procedure for any other drives (e.g. drive D: and E: of your instrument). This enables a remote virus scan to access all drives of the instrument.

4.5.2 Mapping Drives and Scanning for Viruses

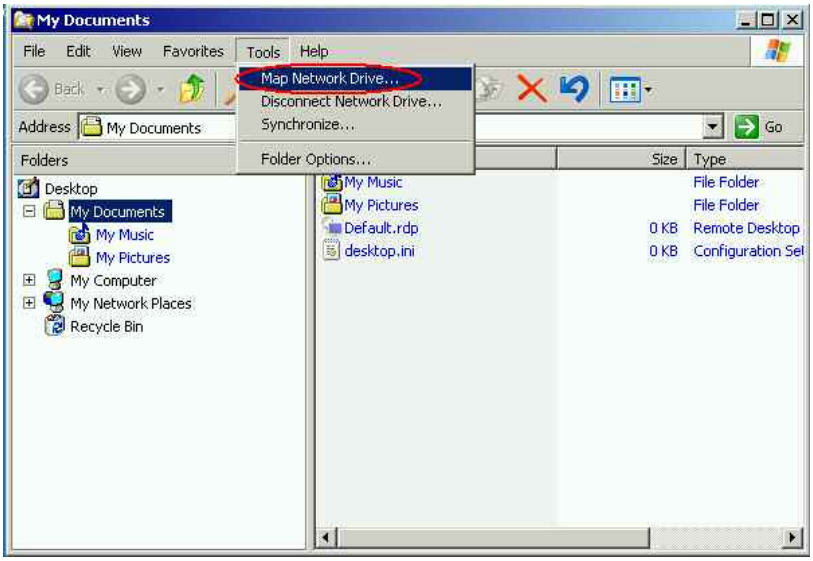
Open the Windows Explorer on your PC and expand the folders **My Network Places ⇨ Entire Network ⇨ Microsoft Windows Network ⇨ Workgroup.**

Note that **Workgroup** might be a different name if you used a different name in the workgroup configuration.

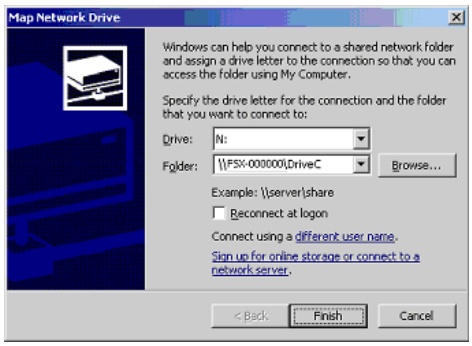
Click on the computer name of the instrument you want to scan, e.g. Fsx-000000 in this example. You will be prompted for a user name and password. Enter **User Name** and **Password** - see the instrument's manual for these settings.



The folders of the instrument will appear in the right hand window. Select **Tools** in the menu bar and then **Map Network Drive…**



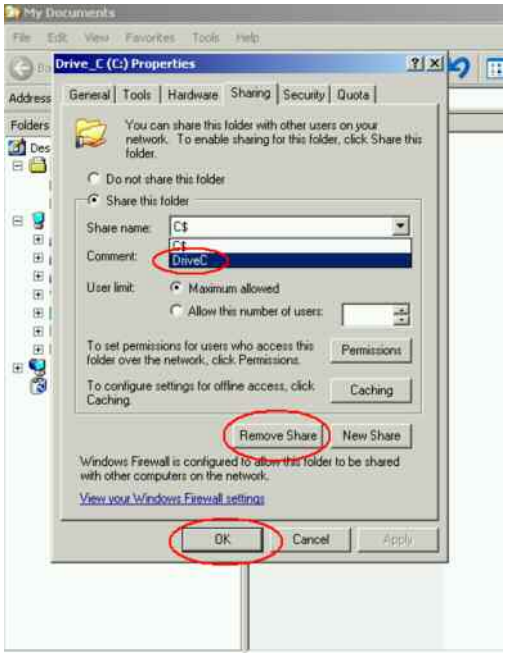
In the **Map Network Drive** dialog, map the first shared drive (e.g. 'DriveC' of the instrument) as a network drive (e.g. 'N:' on the control PC). You can use **Browse** to find the complete network name of the shared drive (e.g. '\\FSX-000000\DriveC') in the network tree. Click **Finish** to complete the network drive mapping. In this example the instrument drive C: is now mapped to drive N: on the control PC.



Repeat these steps for any other instrument hard drives and map them to free drives on the control PC.

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 instrument to its original state, the drive sharing on the instrument has to be removed: Start the Windows Explorer and expand folder **My Computer** to see all drives. Right-click on Drive C: to open the context menu. Select **Sharing** in the properties dialog.



Expand the **Share name** list and select 'DriveC' then click on **Remove Share** or on the radio button **Do not share this folder**. Finally click **OK** to remove the drive sharing. Repeat these steps for any other shared drives, if applicable.

5 Windows Patches and Updates

Microsoft regularly creates security updates and other patches to protect Windows-based operating systems. These are released through the Microsoft Update website and associated update server. Instruments using Windows, especially those that connect to a network, should be updated regularly.

Note that Microsoft Update supersedes Windows Update, which was for Windows-based products only.

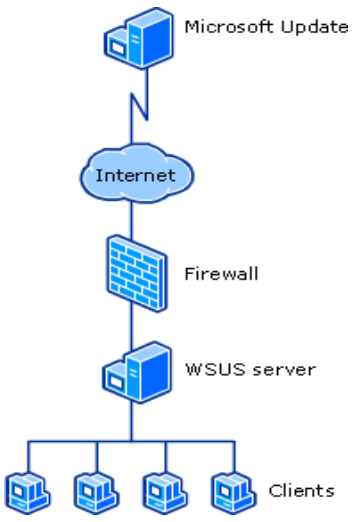
The following sections describe the installation of the Windows Update Agent and its configuration. This enables the instrument to download and install the latest Windows patches and updates.

Make sure that as a minimum Windows XP SP2 is installed on your R&S instrument. Refer to the instrument's manual for how to check the current OS version. If it's based on an older version contact your R&S representative for update possibilities. For many instruments R&S provides an instrument recovery DVD with the latest OS version to re-image the hard drive of the instrument.

Note: It's **NOT** recommended to upgrade an instrument from SP2 to SP3 with the Microsoft Update service, or by manual installation of a standalone service pack executable. For most instruments re-imaging of the OS is necessary.

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

- The instruments are permitted access to the Internet, and download updates directly from the Microsoft Update server.
- The instruments download updates from an update server in your company.



In the second scenario, system administrators 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.

5.1 Installation and Configuration of Windows Update Agent

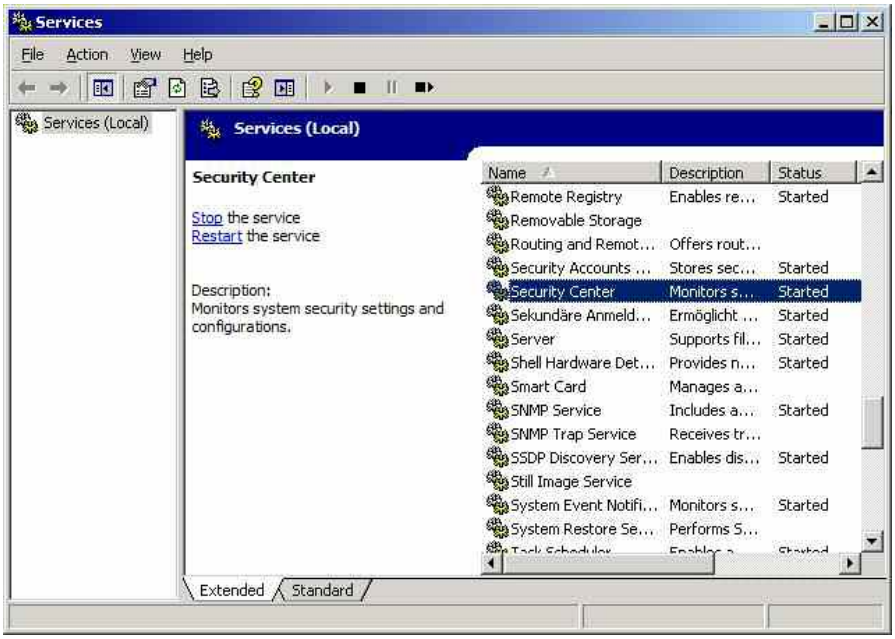
Most R&S instruments are based on Windows XP Embedded which is a customizable version of Windows XP Professional. The OS is scaled and optimized to the requirements of the specific instruments. Therefore, in many cases, the Windows update service has to be separately installed on the instruments.

Download the Windows Update Agent installer **WindowsUpdateAgent30-x86.exe** from the Microsoft web site http://go.microsoft.com/fwlink/?LinkID=100334 and copy it onto a USB thumb drive. The installation is straightforward and does not present critical installation options.

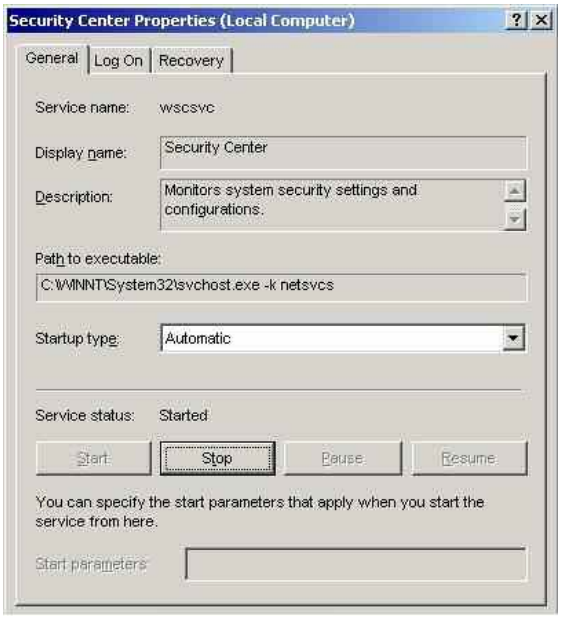
The Windows Update Agent installation steps are listed below:

- Press CTRL + ESC or click **Start** to bring up the **Windows Start** menu and then start the Windows Explorer.
- Select the directory on the USB thumb drive where the Windows Update Agent installer is located.
- Start the installation by double-clicking on the EXE file.
- Read and accept the license agreement by pressing 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 bring up the settings dialog:



Select **Automatic** as the Startup Type and press **Start** to start the service:



Press **OK** to finish the configuration.

5.2 Configuring Automatic Updates

Windows can be configured to install important updates as they become available by enabling automatic updating. Optional updates are not downloaded or installed automatically.

To start the automatic updates go to **Windows Start ⇨ Control Panel ⇨ Security Center**. Open the dialog and select **Turn on Automatic Updates**.

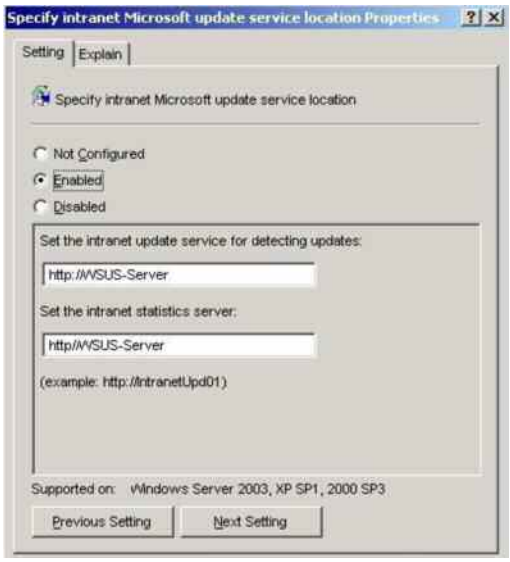
Automatic updates are now activated on the instrument.

5.3 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, you can configure it to use the WSUS server for Windows updates. Please contact your IT department or system administrator to set up the update configuration of the instrument in compliance with your company policy.

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 pane to **Computer Configuration ⇨ Administrative Templates ⇨ Windows Components ⇨ Windows Updates**.Scroll to and double-click on **Specify intranet Microsoft update service location** to start the settings dialog:

First click on **Enabled**, then specify the server name within the company's network to be used for detecting updates:



Note: Make sure that automatic updates are enabled as described in section 5.1.

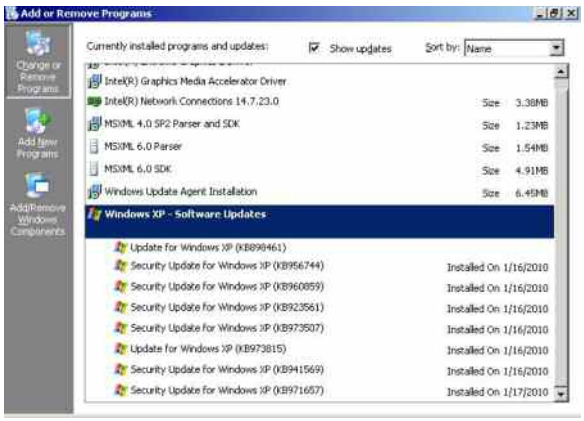
5.4 Configuring Automatic Updates

Configuration of automatic updates is very flexible. For example, updates can be scheduled to a specific day and time, notification to the user can be activated, etc. The automatic update settings can be managed via **Windows Start ⇨ Control Panel ⇨ Automatic Updates:**

For R&S instruments, Rohde & Schwarz highly recommends the use of the “Notify me…” configuration, where confirmation from the user is required before download and installation. Download of updates and installation can cause performance degradation on the instrument during that time and may require a reboot. Therefore the user should control when the update process runs, so that it does not occur when the instrument is in use.

5.5 Viewing installed Updates

Installed updates can be viewed via **Windows Start ⇨ Control Panel ⇨ Add or Remove Programs**:



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

6 Related Documents and Links

- NSA Security papers
  http://www.nsa.gov/ia/guidance/security_configuration_guides/
- News about Security threats
  http://www.securityfocus.com/
- Microsoft Windows Update Agent – Download Link
  http://go.microsoft.com/fwlink/?LinkID=100334
- Microsoft Support: How to disable the Autorun functionality in Windows
  http://support.microsoft.com/kb/967715/en-us
- Microsoft Support: Troubleshooting Windows Firewall settings in Windows XP Service Pack 2 for advanced users
  http://support.microsoft.com/kb/875357/en-us

About Rohde & Schwarz

Rohde & Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established 75 years ago, Rohde & Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability
- ISO 14001-certified environmental management system

Regional contact

USA & Canada

USA: 1-888-TEST-RSA (1-888-837-8772)
from outside USA: +1 410 910 7800
CustomerSupport@rohde-schwarz.com

East Asia

+65 65 13 04 88

CustomerSupport@rohde-schwarz.com

Rest of the World

+49 89 4129 137 74

CustomerSupport@rohde-schwarz.com

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

www.rohde-schwarz.com