

Norman Virus Control

for Terminal Services

Terminal servers reduce the total cost of ownership (TCO) in an organization. Companies using WTS solutions have a need for antivirus software that is specially designed for this environment, and that is somewhat different from traditional antivirus software for servers and workstations. Norman has taken this trend seriously and has developed a version of NVC v5 for Windows Terminal Services.

Key features

- On-access scanning of files
- Norman SandBox – revolutionary way to detect new and unknown malware
- Decompression library
- Automatic updates over the Internet – complete product and incremental updates of virus definition files

Complete list of topics and features

Why choose Norman Virus Control for Terminal Services?

Norman SandBox

On-access scanner

On-demand scanner

How does it work?

Automatic updates

Decompression library

Messaging

Messaging module for administrators

Why choose Norman Virus Control for Terminal Services?

In a Windows NT or Windows 2000 Terminal Services environment, users may be connected to the server via Terminal Services clients. Using this configuration, the Terminal Service clients do not run applications locally, but instead they depend on the server to run instances of the applications they use.

NVC is tailor-made to integrate with the Terminal Services, and applies the latest techniques to optimize the scanning performance that will occur on the server when multiple users access files simultaneously. In addition it gives administrators unique control functions of the various users utilizing the Terminal Server.

Norman SandBox

Norman's SandBox technology detects new and unknown computer viruses, including trojans and worms. Today, an email worm can infect tens of thousands of workstations in a matter of seconds. The antivirus vendors are expected to find the cure, update the virus definition files, and distribute these to its customers immediately. The need for speed is paramount. Norman's SandBox is a virtual world where everything is simulated. An emulator provides an environment where possible virus infected executables «run» just as they would do on a real system. When execution stops, the SandBox is analyzed for changes. The SandBox is particularly tuned to find new email-, network- and peer-to-peer worms.

On-access scanner

On-access scanning involves constant monitoring of the file system on servers and workstations. For an antivirus application, it is vital that viruses are detected and blocked before they are activated. Whenever a file is accessed in a read/write operation, or a program is executed, the On-access scanner is notified and scans the file before the virus can be activated.

Like the **On-demand scanner**, NVC's On-access scanner detects and repairs all types of malware. Whenever possible, an infected file is repaired before it is handed over to the application. If repair fails, NVC denies the user access to the infected file. There are a number of configuration options for the On-access scanner, and it is recommended that a strategy is established before this feature is configured. NVC provides guidelines in the program, help files, and documentation.

On-demand scanner

This scanner is used for manual scans of selected areas of a machine. Entire drive(s), or certain folders and subfolders - even specific files – can be selected for scanning. From Windows Explorer, for example, any object can be selected by clicking the right mouse button and select *Norman Virus Control* from the menu.



Peace of Mind

Norman is one of the world's leading companies within the field of data security. With products for virus control, spam control, email control, download control, personal firewall, encryption, data recovery, certified data erasure and computer forensics, the company plays an important role in the data industry.

NORMAN®

www.norman.com



- In networks, the system administrator can create scanning tasks to be executed on selected - or on all - workstations and servers in the organization. Tasks can be executed immediately, or scheduled for execution later, for example at fixed intervals. The On-demand scanner can use the Norman SandBox technology to further increase protection by detecting new unknown computer virus, worms, and trojans before they can cause harm to your systems.

How does it work?

- A Terminal Service session comprises a desktop view and an environment where the logged-on user can run applications. NVC is configured at the server and applies to all Terminal Service sessions. On-access scanning runs in «Services and remote users» mode, which means that if a virus is encountered, no virus alert will be displayed on the server. A modified alert dialog is displayed in the client's session. The default configuration for the «Services and remote users» On-access scanner is to scan only new or changed files, which reduces the impact of the scanner on the client session whilst maintaining solid antivirus protection.

Adding the name of the client session user, the name of the terminal client's machine, and the terminal server name modify the virus alert on the administrator's NVC Message console.

- Launching an On-demand scan in a Terminal Service session is no different from any other implementation of NVC.

Automatic updates

- Norman Internet Update (NIU) is an integrated part of NVC and can be configured to regularly check for new and updated files on Norman's product servers. NIU provides complete updating and upgrading of the application software and virus definition files to ensure that the latest version of the software is always installed.

NIU employs incremental updates of virus definition files to keep the size of the updates as small as possible, thereby reducing download time.

Decompression library

- A new advanced decompression module has been developed to scan files that have been compressed with different archive programs. With this module NVC can now scan more than 30 archive types and variants like ZIP, TAR, RAR, ARJ, UUENCODE, ARC etc. Files that contain other files of different archive formats will also be scanned to further increase security. In addition, if malware is found within an archived file, NVC will - if possible - clean the infection and repack the file (only valid for some formats).

Messaging

Messaging comprises two components: Message routing and Message handling.

- **Message routing** allows administrators to select what kind of messages will be routed to other PCs running NVC in the network.
- **Message handling** allows users as well as administrators to select what kind of messages are displayed or kept locally.

The messaging functionality is an effective way of keeping track of all activity related to Norman Virus Control components locally as well as in the network.

Messaging module for administrators

- Administrators can configure which incidents that should trigger messages to be sent by emails or SMS to selected receivers. In networks using SNMP you can also configure NVC to send messages to your preferred administration tool.

System requirements

- Windows NT 4 Terminal Server Edition
- Windows 2000 Advanced Server and 2003 Server with terminal services.
- Supports RDP (Microsoft) and ICA (Citrix)



22 x "100%" awards



Norman solutions for clients/workstations: Norman Virus Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP, OS/2, Linux (On-Demand scanning) | Norman Internet Control for Microsoft Windows 95, 98, Me, NT4.0, 2000, XP | Norman Personal Firewall | Norman Privacy

Norman solutions for servers: Norman Virus Control for Microsoft Windows NT4.0, 2000, 2003, XP | Norman Virus Control Firebreak for Novell Netware 4.11 and later | Norman Virus Control for Linux

Norman solutions for web, gateways and mailservers: Norman Spam Control | Norman Email Control | Norman Download Control | Norman Virus Control Net | Norman Virus Control for Lotus Domino (Win32, OS/2) | Norman Virus Control for Firewall-1 NG | Norman Virus Control for Microsoft Internet Information Server | Norman Virus Control for Microsoft Exchange | Norman Virus Control for MIMESweeper

NORMAN[®]

www.norman.com