

# **V3Net for Windows Server 6.0 User Guide**

---

## Table of Contents

|                                                                  |           |
|------------------------------------------------------------------|-----------|
| <b>TABLE OF CONTENTS .....</b>                                   | <b>2</b>  |
| <b>TABLE OF FIGURES .....</b>                                    | <b>5</b>  |
| <b>PREFACE .....</b>                                             | <b>7</b>  |
| <b>MAIN FEATURES .....</b>                                       | <b>8</b>  |
| <b>INSTALLATION.....</b>                                         | <b>9</b>  |
| SYSTEM REQUIREMENTS .....                                        | 9         |
| INSTALLATION PROCEDURE .....                                     | 10        |
| UNINSTALLATION .....                                             | 17        |
| <b>UPDATING TO THE LATEST ENGINE.....</b>                        | <b>18</b> |
| SMART UPDATE UTILITY.....                                        | 18        |
| UPDATE CONFIGURATION .....                                       | 19        |
| <b>VIRUS SCAN AND REPAIR.....</b>                                | <b>22</b> |
| SYSTEM SCAN .....                                                | 22        |
| <i>Customized List to Scan</i> .....                             | 23        |
| QUICK SCAN .....                                                 | 23        |
| EXPLORE SCAN .....                                               | 24        |
| REAL TIME MONITORING .....                                       | 24        |
| <i>Starting and Stopping Monitoring Viruses</i> .....            | 25        |
| HOW TO REPAIR VIRUSES.....                                       | 26        |
| <i>Repair Viruses Detected during the Scan</i> .....             | 26        |
| <i>Repair Viruses Detected during Real Time Monitoring</i> ..... | 27        |
| <b>MENUS .....</b>                                               | <b>29</b> |
| HOME.....                                                        | 30        |
| SYSTEM SCAN .....                                                | 32        |

|                                            |           |
|--------------------------------------------|-----------|
| EVENT LOG .....                            | 33        |
| SCAN LOG .....                             | 34        |
| QUARANTINE STATION .....                   | 35        |
| SECURITY WARNING REPORTS .....             | 37        |
| MENU BAR .....                             | 38        |
| <i>File(F)</i> .....                       | 38        |
| <i>View(V)</i> .....                       | 38        |
| <i>Tools(T)</i> .....                      | 38        |
| <i>Help(H)</i> .....                       | 39        |
| TOOLBAR .....                              | 39        |
| <i>Quick Scan Line</i> .....               | 39        |
| <i>Web Link</i> .....                      | 39        |
| <i>Explorer Toolbar</i> .....              | 39        |
| <i>Alert Icon Toolbar</i> .....            | 40        |
| <b>SCAN AND REPAIR SETTINGS .....</b>      | <b>41</b> |
| HOW TO OPEN THE CONFIGURATION WINDOW ..... | 41        |
| EASY CONFIGURATION .....                   | 42        |
| SYSTEM SCAN/MONITORING .....               | 43        |
| <i>System Scan</i> .....                   | 45        |
| <i>Screen Saver Scan</i> .....             | 47        |
| <i>Scheduled Scan</i> .....                | 49        |
| <i>System Monitoring</i> .....             | 52        |
| <i>Internet Monitoring</i> .....           | 54        |
| <i>Startup Program Monitoring</i> .....    | 56        |
| <i>Items Not To Scan</i> .....             | 58        |

|                                            |    |
|--------------------------------------------|----|
| ADVANCED SCAN SETTING .....                | 59 |
| <i>File Types to Scan</i> .....            | 59 |
| <i>Compressed files</i> .....              | 60 |
| <i>Scan Method</i> .....                   | 60 |
| <i>Possible Harmful Programs</i> .....     | 61 |
| SETTING THE ADVANCED SCAN .....            | 61 |
| <i>Macro Policy</i> .....                  | 62 |
| <i>System Scan/Monitoring Policy</i> ..... | 62 |
| <i>Self Protect</i> .....                  | 63 |
| BLOCK NETWORK .....                        | 64 |
| <i>Ports Blocking</i> .....                | 65 |
| <i>Port Registering</i> .....              | 66 |
| <i>Ports not to block</i> .....            | 67 |
| ALARM E-MAIL .....                         | 68 |
| <i>E-mail Account Setting</i> .....        | 69 |
| SECURITY SETTING .....                     | 71 |
| <i>Use security functions</i> .....        | 71 |
| <i>Items to be protected</i> .....         | 72 |
| <i>Password Setting</i> .....              | 72 |
| OTHER CONFIGURATIONS .....                 | 73 |
| <i>Alert Setting</i> .....                 | 73 |
| <i>Disk Space Designation</i> .....        | 74 |

## Table of Figures

|                                                                     |    |
|---------------------------------------------------------------------|----|
| Figure 1 V3Net for Windows Server 6.0 Setup Wizard .....            | 10 |
| Figure 2 License Agreement .....                                    | 11 |
| Figure 3 Verification of other product installation .....           | 12 |
| Figure 4 Choose Install Location .....                              | 13 |
| Figure 5 Start Copying Files .....                                  | 14 |
| Figure 6 Smart Update Utility .....                                 | 15 |
| Figure 7 Configuration Wizard.....                                  | 16 |
| Figure 8 Smart Update .....                                         | 19 |
| Figure 9 Environment Setup.....                                     | 19 |
| Figure 10 System Scan .....                                         | 22 |
| Figure 11 Home Menu.....                                            | 25 |
| Figure 12 Repair Viruses Detected during the Scan .....             | 26 |
| Figure 13 Repair Viruses Detected during Real Time Monitoring ..... | 27 |
| Figure 14 Home Menu.....                                            | 30 |
| Figure 15 System Scan Menu .....                                    | 32 |
| Figure 16 Event Log .....                                           | 33 |
| Figure 17 Scan Log .....                                            | 34 |
| Figure 18 Quarantine Station .....                                  | 35 |
| Figure 19 Security Warning Reports .....                            | 37 |
| Figure 20 Easy Configuration .....                                  | 42 |
| Figure 21 System Scan/Monitoring .....                              | 43 |
| Figure 22 System Scan .....                                         | 45 |
| Figure 23 Screen Saver Scan .....                                   | 47 |
| Figure 24 Scheduled Scan .....                                      | 49 |

|                                            |    |
|--------------------------------------------|----|
| Figure 25 System Monitoring.....           | 52 |
| Figure 26 Internet Monitoring .....        | 54 |
| Figure 27 Startup Program Monitoring ..... | 56 |
| Figure 28 Items Not To Scan.....           | 58 |
| Figure 29 Advanced Scan Setting .....      | 59 |
| Figure 30 Setting the advanced scan .....  | 62 |
| Figure 31 Block Network .....              | 64 |
| Figure 32 Ports Blocking .....             | 65 |
| Figure 33 Port Registering.....            | 66 |
| Figure 34 Alarm E-mail.....                | 68 |
| Figure 35 E-mail Account Setting .....     | 69 |
| Figure 36 Edit Alarm E-mail.....           | 70 |
| Figure 37 Security Setting .....           | 71 |
| Figure 38 Other Configurations .....       | 73 |

## Preface

### Copyright AhnLab, Inc. 1988-2004, All rights reserved.

The contents of this User's Guide and AhnLab V3Net for Windows Server 6.0 are protected under all relevant copyright, computer protection, and intellectual property laws.

### Product Registration

On-line (product) registration is required for all users that have installed V3Net for Windows Server 6.0. If the user is not registered, access to the latest engines and a variety of other customer support services will not be available.

### Registration Renewal (Contract Extension)

After the customer guaranteed period of protection (1 year), it is required to renew your registration. If the registration renewal (contract extension) is not completed, access to the latest engine updates and other customer support services will not be available, and the installed product will cease to function properly. Go to the AhnLab Inc. website (<http://www.ahnlab.com>) Customer Support > Registered Product to view the customer guaranteed period of the currently installed product.

### AhnLab Inc. Customer Satisfaction Center

Registration renewal (contract extension) for all products is available at the AhnLab Inc. Internet shopping mall, at <http://www.ahnlab.com>. Contact the Customer Satisfaction Center for questions about registration renewal.

- Home Page <http://info.ahnlab.com/english/>
- E-Mail us at [customer@ahnlab.com](mailto:customer@ahnlab.com)
- Registration Renewal (Contract Extension) guide 02-2186-3090
- Customer Satisfaction Center: 02-2186-3000

#### Caution

After the customer guarantee period has ended (1 year), this product must be removed from the user's system. If not, it is considered an illegal use of the software and may be subject to punishment by a civil and/or criminal law.

### Customer Support Service

On-line customer registration is required for all users that have installed V3Net for Windows Server 6.0. Without registration, the customer guarantee period is not granted. Registered customers are eligible for a variety of customer support services during the guarantee period (1 year) as follows:

- Product counseling via phone, fax and on-line
- Weekly engine updates on Wednesdays
- Engine updates and new virus news sent via E-mail
- Digital virus calendar (screen saver)
- Free invitation to security seminars and training programs

#### Caution

If a copy is installed without a serial number, the evaluation version will install. There is a 30 day use limit on the evaluation version. After that period, the software should be removed from the system. If it is not removed, it is considered an act of illegal use of the software and may be subject to punishment by civil and/or criminal law.

## Main Features

---

The following are brief descriptions of the major V3Net for Windows Server 6.0 functions.

### Auto update to the latest engine

AhnLab Inc.'s unique anti-virus engine is updated weekly to control new viruses effectively. You can easily update to the latest engine by using the Smart Update utility. For more information, refer to **Updating to the Latest Engine**.

#### Note

AhnLab Inc. also provides exclusive anti-virus engines for scan/repair of particular viruses. Such exclusive engines scan and repair certain viruses that are spreading fast and causing serious damages. Exclusive engines are provided on your system without charge on the AhnLab Inc. Visit web-site: <http://www.ahnlab.com/english>.

### Backup data before repairing

When an infected file is detected on your computer, V3Net for Windows Server 6.0 will first create a backup copy of the file and store it in a different location before beginning the virus repair process. After the repair process you can restore the backup file to the original file location if the original file is damaged. For more information, refer to **Quarantine Station**

### Reporting use's System Weaknesses

Monitors your computer in real-time for security weaknesses and vulnerabilities to viruses. If it finds any, it will give a Security Warning Report that will inform you of the weakness, and then offers a solution to better protect your computer from infection. For more information, refer to **Security Warning Reports**

### Easy Configuration

You can select the desired security level (high, medium, low). If the security level is set to one of the pre-sets, you do not have to configure the settings of individual virus scan/repair functions.

### Block Network

When a new virus spreads rapidly via a network, the ports suspected as the possible origin of the infection can be temporarily blocked. It is recommended that such ports are blocked to protect the system until a new version of engine is available.

### Alarm E-mail

When the number of viruses found reaches a user-specified level established in the pre-set period, an Alarm E-mail is sent to the user immediately. Alarm E-mails are also sent when the engine update has either completed, failed, or the system monitoring restart has failed.

## Installation

---

### System Requirements

To install V3Net for Windows Server 6.0, your computer should meet the following specifications. Please check your system specification before you start installation.

| Item       | Recommended                                                                                                                          | Minimum                               |
|------------|--------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| CPU        | Pentium III IA 64 / AMD64 or above                                                                                                   | Pentium 150MHz IA 64 / AMD64 or above |
| RAM        | 256MB                                                                                                                                | 32MB or above                         |
| HDD        | 200MB                                                                                                                                | 30MB or above                         |
| CD-ROM     | 24X or above                                                                                                                         | 4X or above                           |
| Resolution | 1024 * 768                                                                                                                           | 800 * 600 or more                     |
| OS         | Windows NT Server 4.0(SP6 and more), Windows 2000 Server/Advanced Server/DataCenter Server, Windows 2003 Server Standard/ Enterprise |                                       |

**Caution**

To install this program, you must log in to the computer with Administrator authority. You cannot install or remove this program without Administrator authority.

## Installation Procedure

1. Insert the V3Net for Windows Server 6.0 CD-ROM into the CD-ROM drive.  
→ The InstallShield Wizard window will be displayed.

### ✓ Notes

If the InstallShield Wizard window does not display:

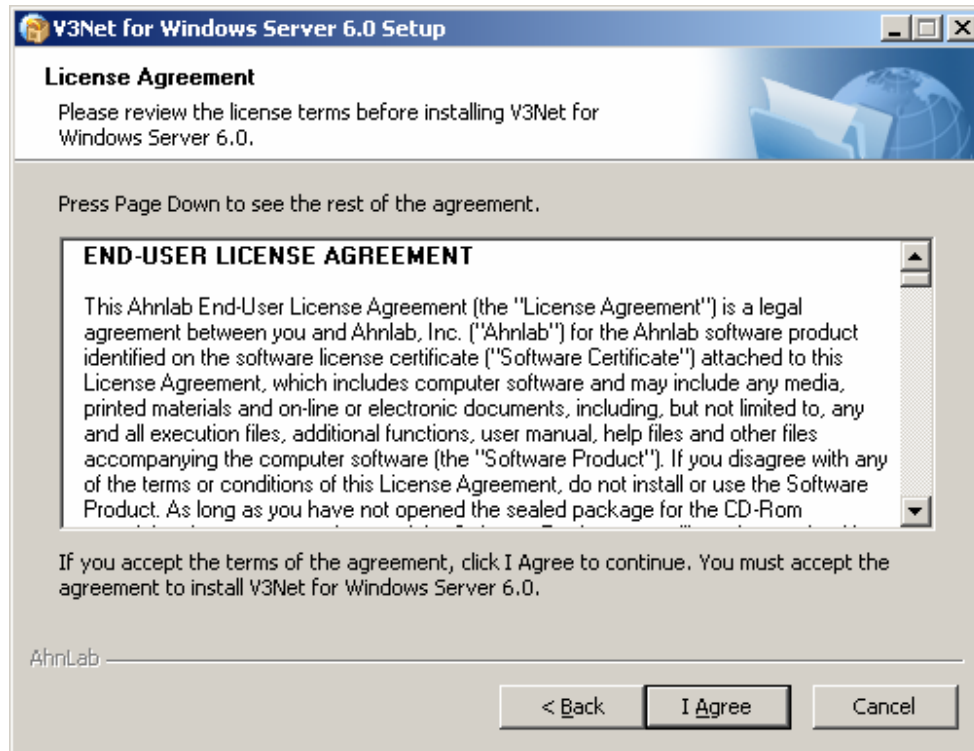
1. Click on the Start menu, then select Run.
2. When the Run window displays, enter the correct path of the V3Net for Windows Server 6.0 installation executable file (install.exe) in the Open field, including the CD-ROM drive name in which the V3Net for Windows Server 6.0 CD is inserted, and then press OK. (Ex: 'D:\install.exe')

2. After you complete these pre-installation steps, the V3Net for Windows Server 6.0 InstallShield Wizard will start. Press **Next** to begin the installation of V3Net for Windows Server 6.0.



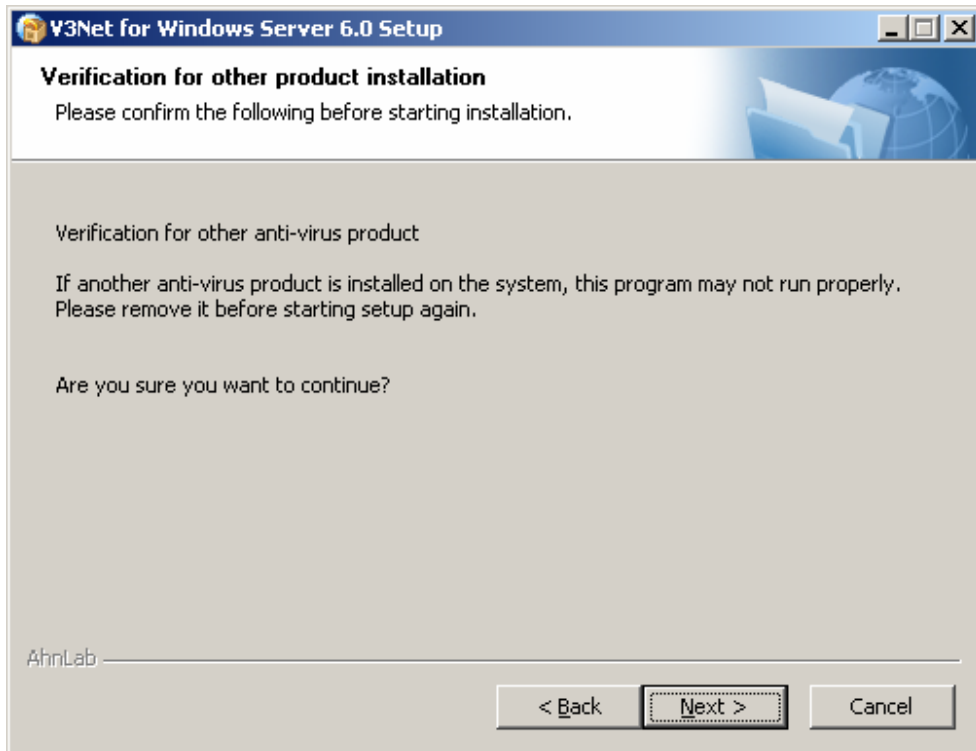
Figure 1 V3Net for Windows Server 6.0 Setup Wizard

3. The **License Agreement** will be displayed. Read the license agreement and select **I Agree** to signify your agreement and acceptance of the license agreement.



**Figure 2 License Agreement**

4. **Verification of other product installation** will be displayed. Check whether another version of the V3Net for Windows Server 6.0 or any other anti-virus product is presently installed prior to installing V3Net for Windows Server 6.0. If another anti-virus product is not presently installed, press **Yes** to proceed with the installation of V3Net for Windows Server 6.0.



**Figure 3 Verification of other product installation**

**Caution**

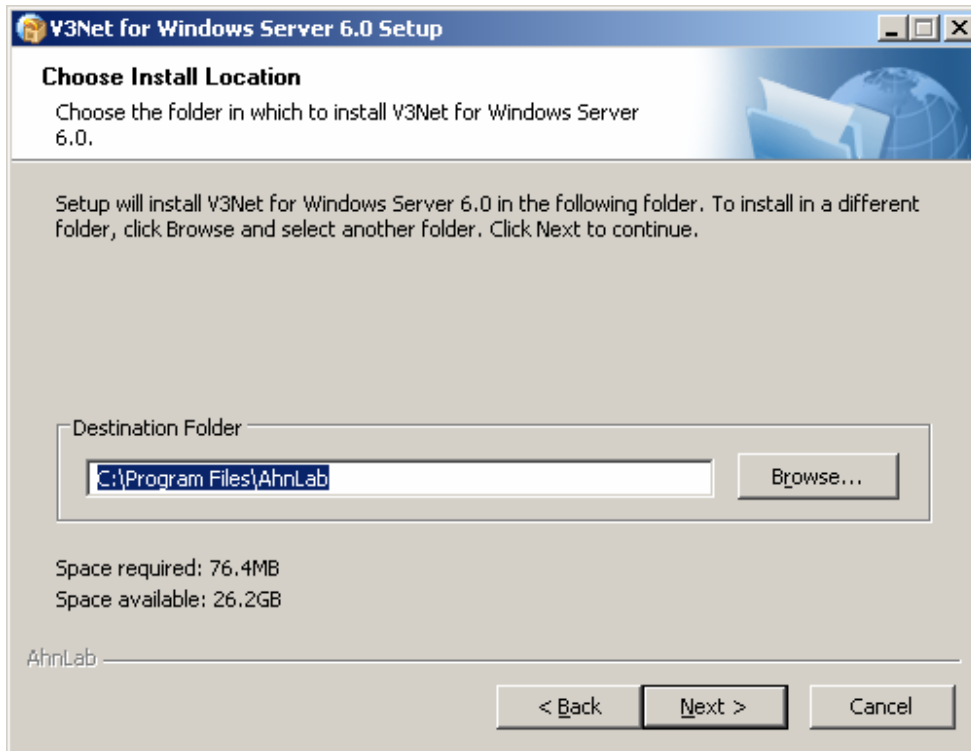
If another anti-virus product is installed on the system, press **No** to stop the InstallShield Wizard, and remove it. Then begin the V3Net for Windows Server 6.0 installation again. If there is a previous version of V3Net for Windows Server 6.0 already installed on a user's system, the **Remove Previous Version** window will display. Click **Yes** to remove it and restart the system. When the system restarts, the V3Net for Windows Server 6.0 InstallShield Wizard will automatically run.

5. The **User Information** window will appear. Enter the name, company name and product number and click **Next >**.

**Caution**

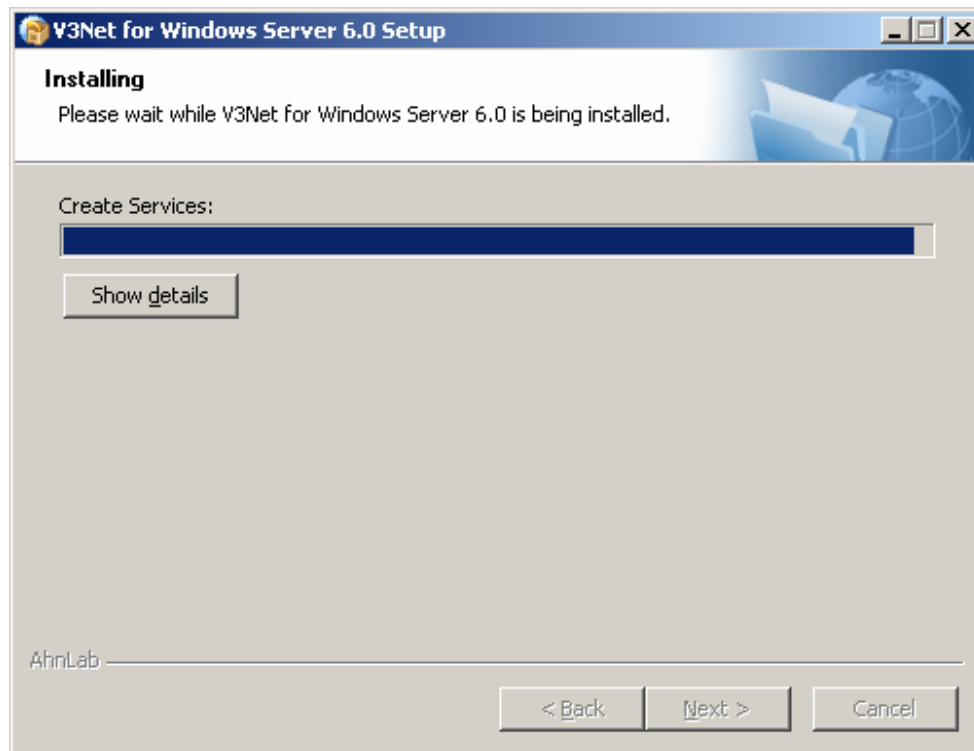
If the correct product number is not entered, the 30-day evaluation version will be installed and not the full version. With the evaluation version, you can neither update to the latest engine after the 30-day period, nor use most of the functions of the V3Net for Windows Server 6.0.

6. The **Choose Install location** window will be displayed. Specify the default path of the folder where V3Net for Windows Server 6.0 program files will be copied and press **Next**. To specify folders other than the default path, 'C:\Program Files\AhnLab', press **Browse...**



**Figure 4 Choose Install Location**

7. The **Start Copying Files** window will be displayed. Press **Next** to copy the V3Net for Windows Server 6.0 program files to the specified path. The window displays the status of the installation, and finally displays the **InstallShield Wizard Complete** screen. After installation, the **Online Registration** window will appear and ask if you want to register the V3Net for Windows Server 6.0 software online. If you select "Yes, I'd like to register the customer information now." and press **Next**, the registration web page will launch and display. To complete the product registration, fill in the customer information form and submit.



**Figure 5 Start Copying Files**

**Caution**

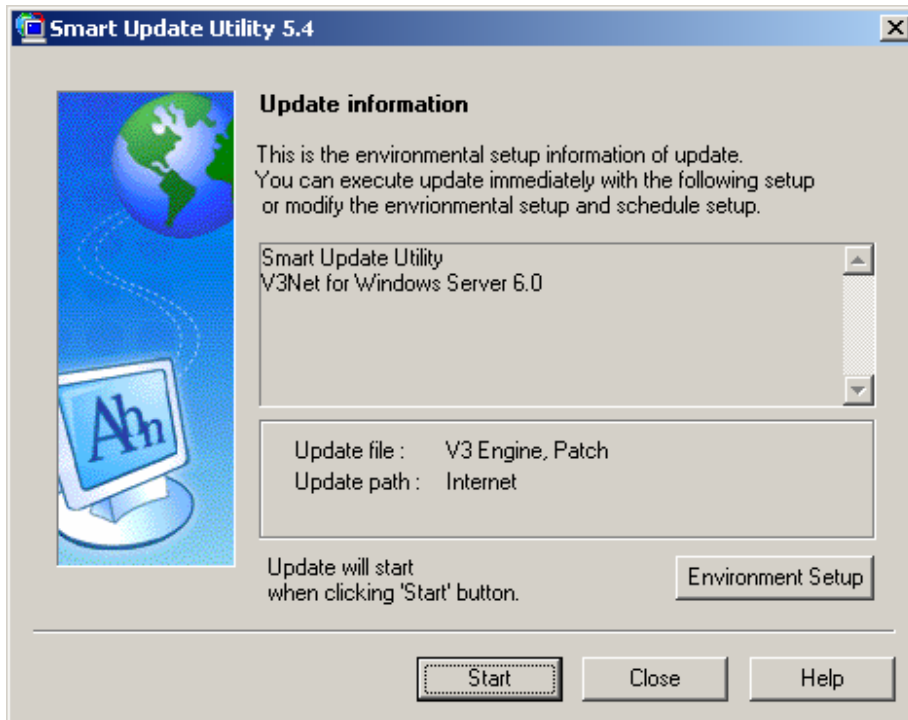
If the correct product number is not entered, the 30-day evaluation version will be installed and not the full version. With the evaluation version, you can neither register online, nor update to the latest engine after the 30-day period.

8. After installation, select items to be executed immediately, and press **Finish**. The selected items will be executed right after the installation is completed.
  - Execute Update Utility: The Smart Update Utility supports the automatic download of the latest scanning/repairing engine. If you press Start, you will begin the update to the latest anti-virus engine.
  - Execute Virus Scanning: The Virus Scan window locates, isolates, and diagnoses infected files, and displays the information.

### Smart Update Utility

If you select "Execute Update Utility," the Smart Update Utility 5.4 window will be displayed.

9. The utility analyzes the user's system to determine which of the latest engine files are needed before downloading and installing.



**Figure 6 Smart Update Utility**

**✓ Notes**

It may take several minutes for the system analysis operation to complete in some cases. Please wait for all operations to complete.

10. The update information file, 'readme.txt' will be displayed automatically when the latest engine file is successfully installed on the user's system. Close the 'readme.txt' file after confirming that the latest downloaded engine update is complete.

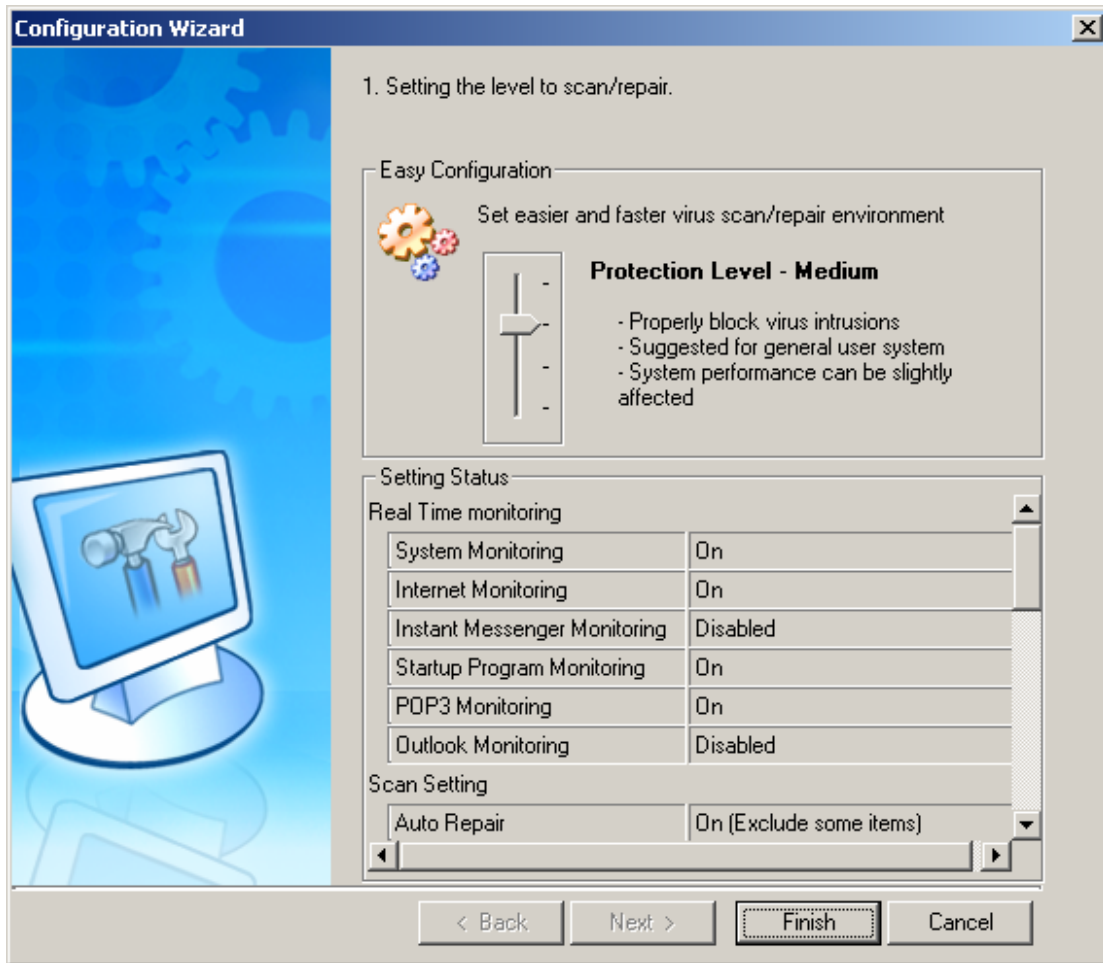
**✓ Notes**

If you click the Configuration icon in the Smart Update Utility window, you can configure the update. For more information, refer to

Update Configuration.

### Configuration Wizard

11. After installation and Smart Update, Configuration Wizard will be displayed.



**Figure 7 Configuration Wizard**

12. Select the virus scan/repair and protection level of the system in the Easy Configuration frame of the Configuration Wizard.

### Easy Configuration

- **High:** Blocks all viruses. (Recommended for systems with high risk of virus infection)
- **Medium:** Blocks most virus infection. (Recommended for typical user systems)
- **Low:** Minimal Blocking of virus infections. (Recommended for systems with low risk of virus infection)
- **Customized:** Blocks viruses based on customized scan/repair settings. (Recommended for systems with special needs)

#### **Caution**

If you are new to V3Net for Windows Server 6.0, it is recommended that you select from among "High, Medium, Low" levels of security. If you select High, system performance may be affected.

13. Finish all configurations, and press **Finish**. The InstallShield Wizard Complete window will be displayed and the installation is therefore complete.

## Virus Scanning

14. If you select "Execute Virus Scanning", the System Scan window will be displayed. If you click the icon at the bottom of the System Scan window, the following message will appear.
  - View settings...: Displays the configuration of a virus scan or repair
  - View reports...: Displays the results of the virus scan
15. If viruses are not detected in the selected sectors, close the system by clicking the Close.

## Uninstallation

1. You can start the V3Net for Windows Server 6.0 Remove Utility by following these steps:
2. Click on the Start menu and select Programs>AhnLab> V3Net for Windows Server 6.0 > V3Net for Windows Server 6.0 Uninstall.
3. V3Net for Windows Server 6.0 will display and show the progress of the uninstall.

### Caution

To uninstall the V3Net for Windows Server 6.0, you must log on to the computer with Administrator authority.

## Updating to the Latest Engine

This section describes how to download the latest anti-virus engine using the Smart Update Utility and how to configure the update settings.

**Note**

If your anti-virus engine is outdated, the Engine Update Information window will automatically display when V3Net for Windows Server 6.0 starts. Select **Update Now** and update your engine to the latest version.

## Smart Update Utility

Download the latest anti-virus engine using the Smart Update Utility:

1. Start the Smart Update Utility.
  - Select **Smart Update** in the File menu on the menu bar.
  - Select **Update** from the toolbar.
  - Select **Smart Update** from the alert icon menu on the Task tray.
  - Select **Smart Update** from the toolbar in Explorer or MS Internet Explorer 5.0 or higher programs.

**Note**

If your anti-virus engine is outdated, the Engine Update Information window will automatically display when the V3Net for Windows Server 6.0 program starts. Select **Update Now** and update your engine to the latest version.

2. Click **Start** on the Smart Update Utility 5.4 window. The utility analyzes the user's system to determine which of the latest engine files are needed before downloading and installing the latest engine.



**Figure 8 Smart Update**

**Note**

It may take several minutes for the system analysis operation to be completed in some cases. Please wait until the analysis is complete.

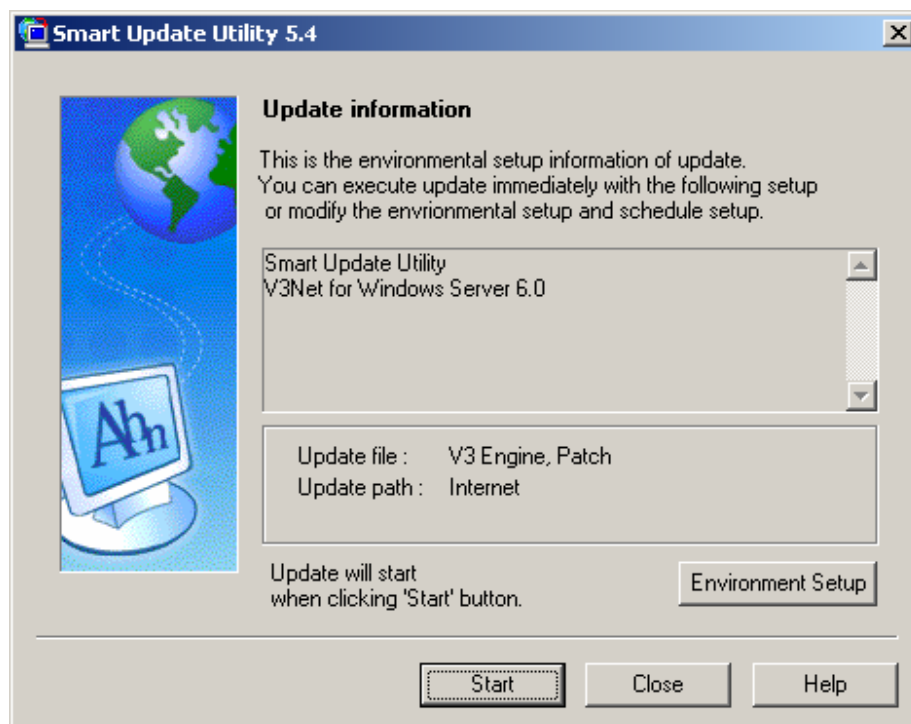
3. The update information file, readme.txt, will be displayed automatically when the latest engine file is successfully installed on the user's system. Close the readme.txt file after confirming that the latest downloaded engine update is complete.

**Caution**

When you update files that are currently running, you must restart the system to complete the update.

## Update Configuration

1. Click **Environment Setup** in the Smart Update Utility window. The Select the product to update window appears.



**Figure 9 Environment Setup**

2. Select the product and utility to update to the latest engine and click **Next >**. It is recommended that you select **Patch file** to update the patch files as well.
  - Use this system as a server for updates: If you select this option, other computers connected to your computer can also obtain the updated engine service.

- Smart Update Utility: Downloads the latest version of the Smart Update Utility.
- V3Net for Windows Server 6.0: Downloads the latest update files of the V3Net for Windows Server 6.0 application.
- Engine File: Updates new engine files

3. Select the method to update and click **Next >**.

- Updating through the Internet: Update the latest engine file through AhnLab's Internet server. (Recommended for personal users)
- Updating through the shared folder on the network drive: Set a time to update the system's server on the user's local network, and share the folder with the latest engine file, so that other computers on the network can share the update. (Recommended for corporate network users)

4. Enter the required information according to selected method to update, and click **Next >**.

### Updating through the Internet

- Server Information Setting:
  - Location: Designates the server location for Internet updates
  - Retrial Number: The number of server connection after a failure to connect to the web server (Default: 15)
- Use proxy server
  - Connect to web site via proxy server
  - Address: Proxy server address
  - Port: Port used on proxy server

### Updating through the shared folder on the network drive

- Account to execute the scheduled Auto Update: Enter the user name and password to execute engine updates automatically based on prescribed schedules.
  - User Name
  - Password
- Share Folder Information: Network shared folder information for the latest engine update
  - UNC Path: Shared folder path by network drive
  - User Name: User's name with permission that allows connection to the shared folders
  - Password: User's password that allows connection to the shared folders

5. Set the general option for smart update.

- Use automatic update: Automatically confirms the engine version at a set time interval and updates to the latest engine.
- Update period (time): Auto engine update period
- Open message automatically after update: Displays the readme.txt file that logs all additions and changes when the system is updated to the latest engine.

- Use integrity scan: Scans for system integrity before downloading and installing the latest engine update.

 **Note**

If you click the **Schedule Setup** on this screen, you can save the engine update schedule previously set.

6. Click **Finish** in the Smart Update Utility 5.4 window to complete the installation.

## Virus Scan and Repair

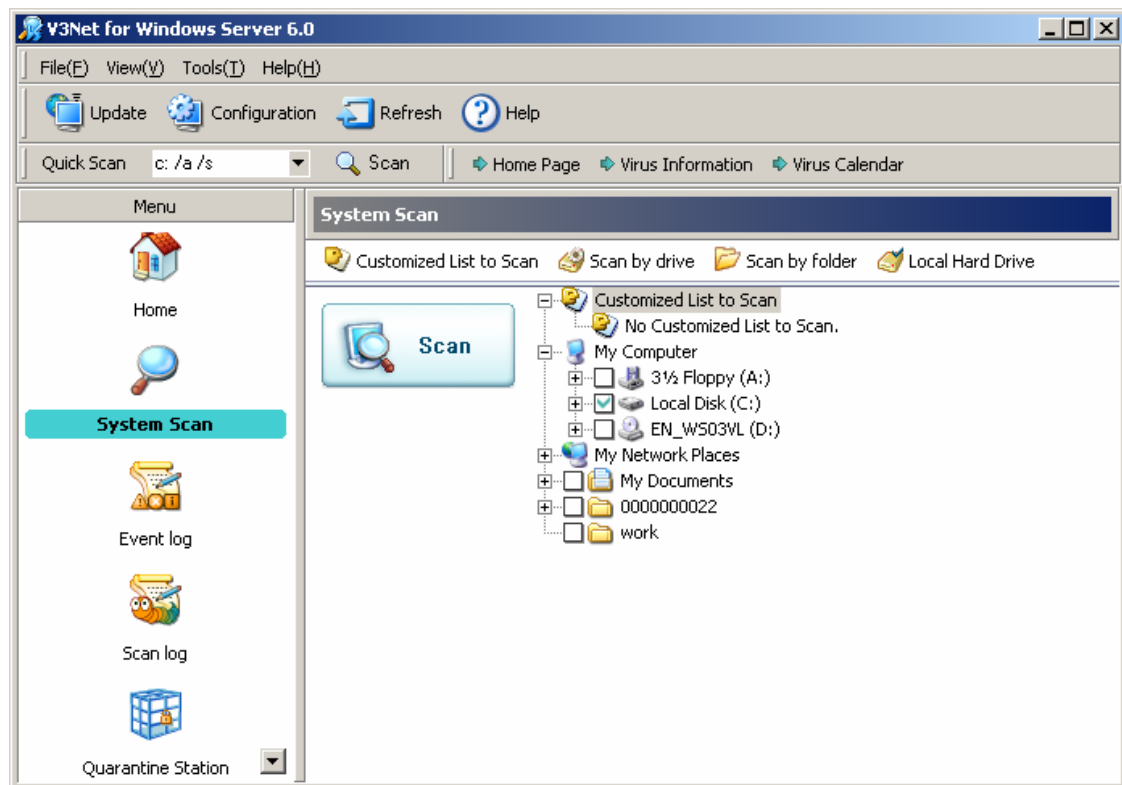
V3Net for Windows Server 6.0 scans and repairs viruses detected on the user's computer, and monitors all virus intrusion.

1. **Real Time Monitoring** for blocking virus intrusion and prevent infection.
2. **System Scan** or **Quick Scan** for scanning for any virus infection on the user's system.
3. Set **Scheduled Scan** for regular system scan.

### System Scan

If there are suspicious sectors that may be infected by viruses, this function immediately checks whether they are infected or not. This function scans sectors with a high risk for virus infection.

1. Select **System Scan** from the V3Net for Windows Server 6.0 Home menu in the left frame.



**Figure 10 System Scan**

2. Select the following menus located in the right frame of the main window to select drives, folders, or files to scan.
  - Customized List to Scan: Allows the user to set specific scan sectors repeatedly
  - Scan by Drive: Allows the user to select specific drives to scan. This feature does not allow you to select specific folders on the drives.

- Scan by Folder: Allows the selection of specific scan sectors by folder that are stored on each drive.
  - Local Hard Drive: Click this icon to display the contents of the local hard drive as sectors to scan.
3. Click the **Scan** in the right frame of the window. The **System Scan** window is displayed to show the scan results of the selected sectors.

 **Note**

Select the **Close the system automatically after scan if viruses are not detected** option in the System Scan window and the system will automatically close if no viruses are detected.

4. If viruses are not detected in the selected sectors, close the system by clicking the **Close**.

## Customized List to Scan

1. Sectors you wish to scan repeatedly can be set in the Customized List to Scan. Clicking the **Customized List to Scan** at the top. The Customized List to Scan window will be displayed.
2. Select items to scan in your system and click **Add (A)>>** The selected items will be displayed in the right frame. To delete items from the list, select the item then click **<<Delete (D)**.
3. Click **Ok** to close the Customized List to Scan window.
4. Click **Scan** at the right frame of the window to scan the customized list. The **System Scan** window is displayed to show the scan results of the selected sectors.

## Quick Scan

1. Enter the paths for folders, files, and drives to be scanned by the Quick Scan command line located at the top of the V3Net for Windows Server 6.0 main window. The options you can enter for the Quick scan line are as follows.

### [Drive] [Folder Name] [File Name] [Option]

- Scan by drive; C:
  - Scan by folder; C:\winnt
  - Scan by file; D:\data\homework.txt
  - Scan including sub folders; C:\winnt /s
  - Scan multiple folders; C:\winnt C:\temp D: /s
  - Scan all files; C: /a
  - Scan compressed files; D:\data /c /s
  - Scan network shared folders; \\ABC\\t
2. If viruses are not detected in the selected sectors, click **Close** to close the Quick Scan.

## Explore Scan

1. Right-click the drives, folders or files to scan using Windows Explorer. Using a simple toolbar or shortcut menus for the Internet or Windows Explorer provided by V3Net for Windows Server 6.0, you can immediately scan specific drives, folders or files.

### Note

Click **View>Toolbars>V3** in the menu bar on the upper area of Windows Explorer to display the V3 toolbar. If the Windows Explorer toolbar does not display, then, select **System Scan/Monitoring>Explorer Scan>Shortcut Menu and Toolbar** from the menu bar on left inside the Configuration window.

2. Select **Virus Scan** in the pop-up menu.
3. **Explorer Scan** window will be displayed to scan the selected drives, folders, and files, and then show the results. The Explorer Scan function automatically repairs viruses upon detection, or exits the scanning process if no viruses are detected. It scans all files, including compressed files. The scan method will be applied to System Scan in the exact same way. Refer to **System Scan** for more detailed information on virus scans and repair configurations.

## Real Time Monitoring

You can protect your system with the Real Time Monitoring features. The following describes the Real Time Monitoring features and how to Start and Stop Monitoring of viruses.

### System Monitoring

Runs real-time scanning of all files and data from all application programs on the user's system. The System Monitoring function is essential to block viruses from their entries. It is strongly recommended that you keep V3Net on at all times. If system monitoring is off, the V3 icon in your Task tray will be displayed as a mark. Real-time Monitoring functions will run as long as your system is on, even after you have terminated the V3Net for Windows Server 6.0.

### Internet Monitoring

Scans all data and files downloaded via web browsers in real time.

### Startup Program Monitoring

Runs real-time monitoring of all startup programs registered in the registry, the startup program folder, and all system configuration files that are launched on Windows startup.

### Caution

Startup Program Monitoring function does not monitor files added to the startup program folder or registry while a new user accounts log in. If you want to monitor newly added files of a new user account as well, reset the function.

## Starting and Stopping Monitoring Viruses

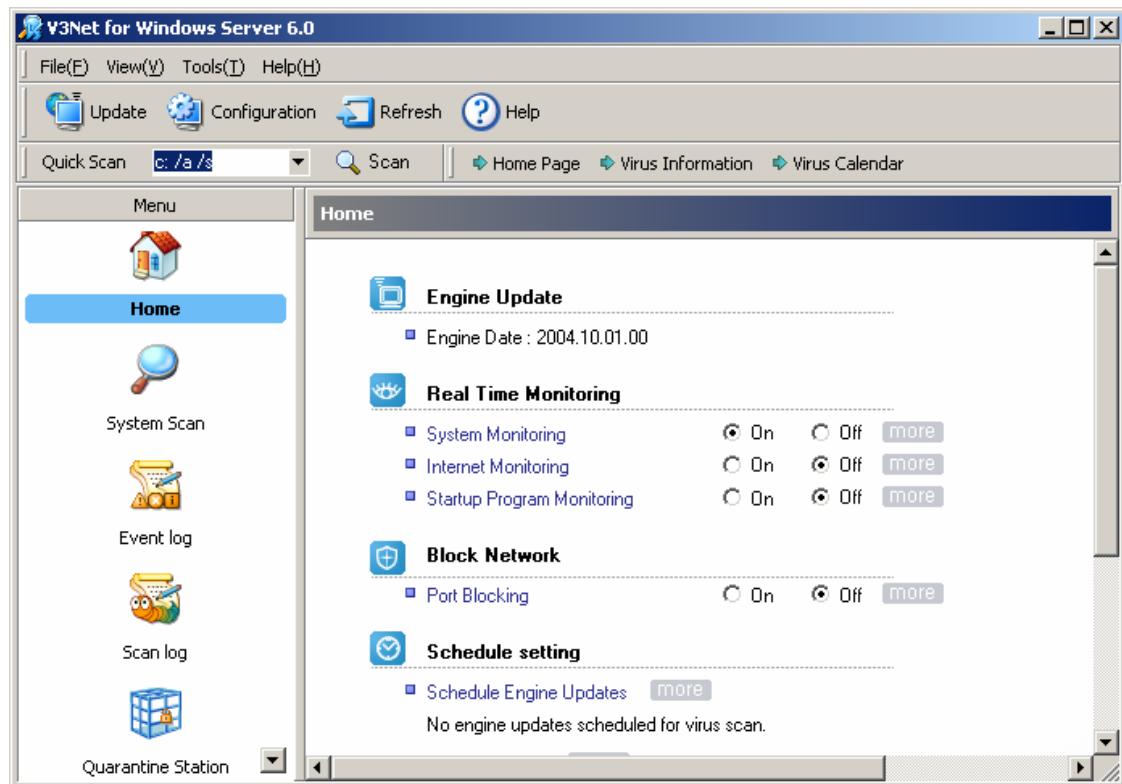


Figure 11 Home Menu

### Home menu

- Click Home on the left frame of the main window, and the **Real Time Monitoring** function menu displays in main window. Click On to activate Real Time Monitoring function, click Off to deactivate.
- Click Real Time Monitoring in the Tools menu on the top menu bar to start the Real Time Monitoring function. Choose Disable to stop Real Time Monitoring.

### Alert icon menu on the system tray

Right-click the Alert icon on the system tray. Select Real Time Monitoring on the menu to select the monitoring function to be executed. To stop its execution, de-select Real Time Monitoring.

### Configuration

Select Configuration on the toolbar or the Configuration of Tools on the menu bar. The Configuration window appears. Select System Scan/Monitoring, displayed in the left frame of the Configuration window. Select the items to scan or monitor in the system scan/monitor window.

## How to Repair Viruses

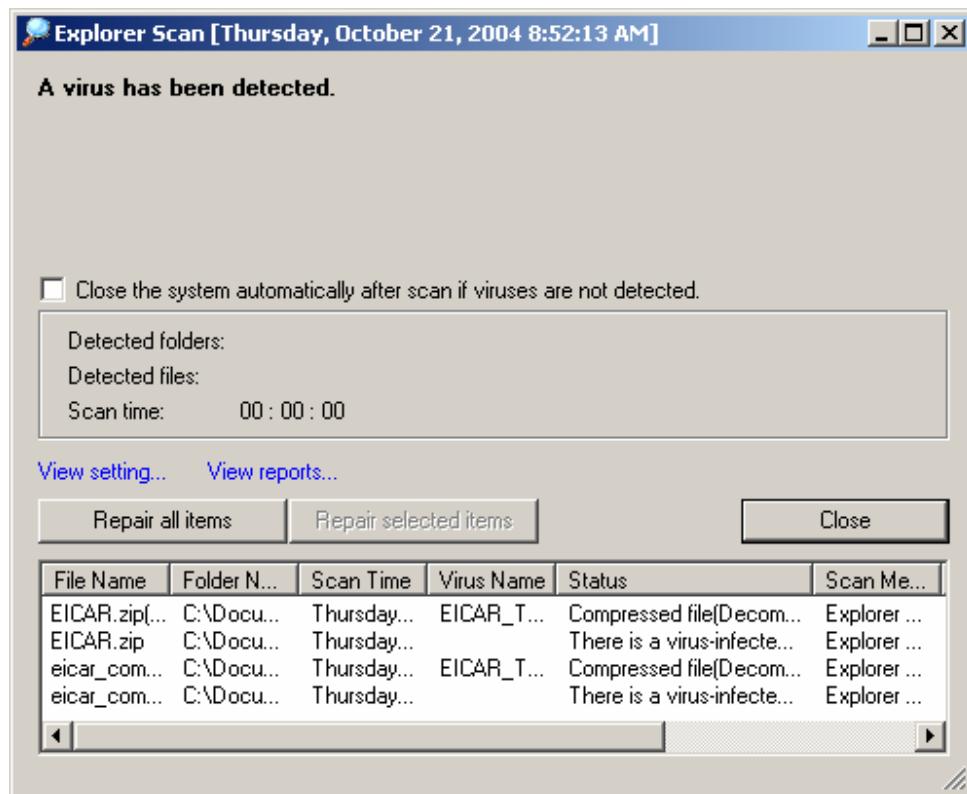
Since files with the **Failed to repair** messages cannot be repaired, please send them to the Report Center of AhnLab, Inc. Please refer to the **Quarantine Station** section to learn how to submit files to the Center.

### Note

You can configure specific virus repair processes for each function in the **Configuration** window. Refer to **Scan And Repair Settings** for more detailed information on configuration items and methods. If you do not select a specific option for Configuration, any infected file will be either deleted, repaired or left as it is, reflecting the default virus repair settings of V3Net for Windows Server 6.0 .

## Repair Viruses Detected during the Scan

If virus infected files are detected during the scanning process, the following window will appear: It shows the name and directory of the infected file and the time of virus detection as shown below.



**Figure 12 Repair Viruses Detected during the Scan**

- Close the system automatically after scan if viruses are not detected.: If viruses are not detected after scan, the system will automatically close after the monitoring window has closed.
- Repair all items: Click Repair All Items in the Scan Result window to repair all infected files at once.
- View setting...: Displays the configuration for virus scan/repair.
- View Reports...: Displays the results of the virus scan.

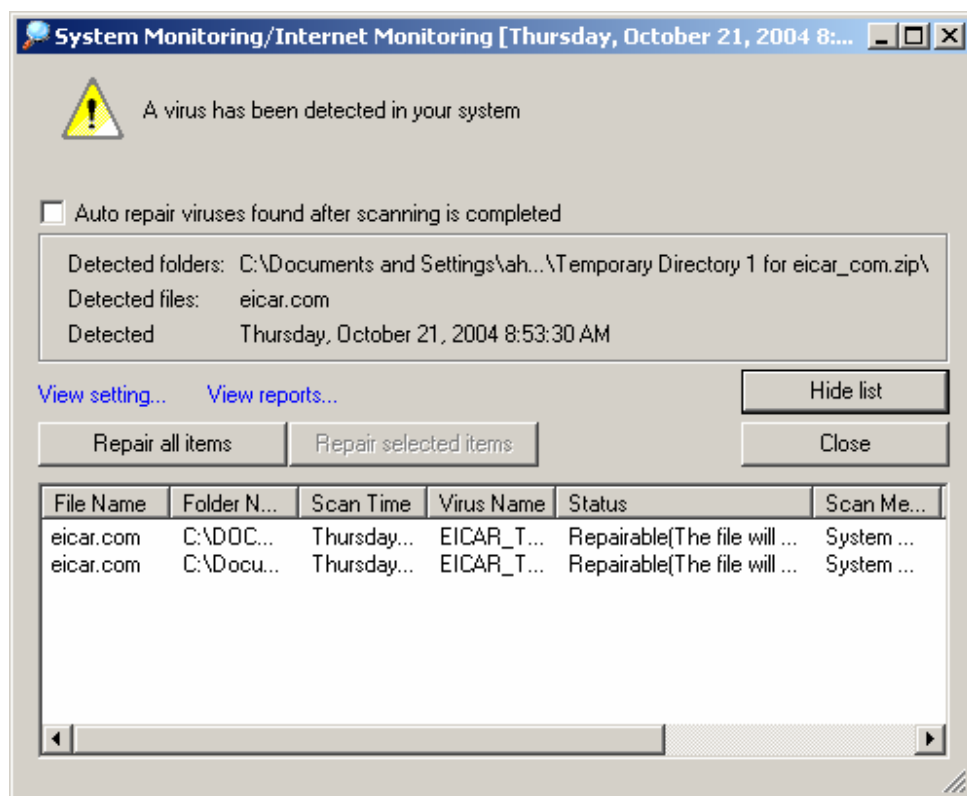
- View the list details: Click this icon, and you will be able to see the detailed list of viruses detected after the repair. Select all viruses to repair from the list of infected files, and click Repair selected items to repair these viruses. To close the list of details, click Hide list.
- Repair selected items: You can select and repair each infected file displayed in View List. You can select multiple items by dragging the mouse or by pressing the Ctrl key while selecting multiple items.

**Note**

To verify if virus infected files were repaired or deleted, click **Scan log** in the left menu of the V3Net for Windows Server 6.0 main page.

## Repair Viruses Detected during Real Time Monitoring

If viruses are detected during system monitoring, the following window will appear. It shows the virus name, file name, and the time of virus detection, as shown below.



**Figure 13 Repair Viruses Detected during Real Time Monitoring**

- Auto repair viruses found after scanning is completed: Viruses detected after repair and after the monitoring window has closed are automatically repaired without notice to the user.
- Repair all items: All virus-infected files displayed by the View the list details will be automatically repaired.
- View setting...: Displays the configuration for virus scan/repair.
- View Reports...: Displays the results of the virus scan.

- View the list details: Click this icon, and you will be able to see the detailed list of viruses detected after the repair. Select all viruses to repair from the list of infected files, and click Repair selected items to repair these viruses. To close the list of details, click Hide list.
- Repair selected items: You can select and repair each infected file displayed in View List. You can select multiple items by dragging the mouse or by pressing the Ctrl key while selecting multiple items.

 **Note**

To verify if virus infected files were repaired or deleted, click **Scan log** in the left menu of the V3Net for Windows Server 6.0 main page.

## Menus

---

You can start V3Net for Windows Server 6.0 by:

- Double-clicking the V3Net for Windows Server 6.0 program icon on the desktop.
- Double-clicking, or right-clicking and selecting **Open** the V3Net for Windows Server 6.0 notification icon on the system tray.
- Clicking on the Start menu and selecting Program>AhnLab-> V3Net for Windows Server 6.0

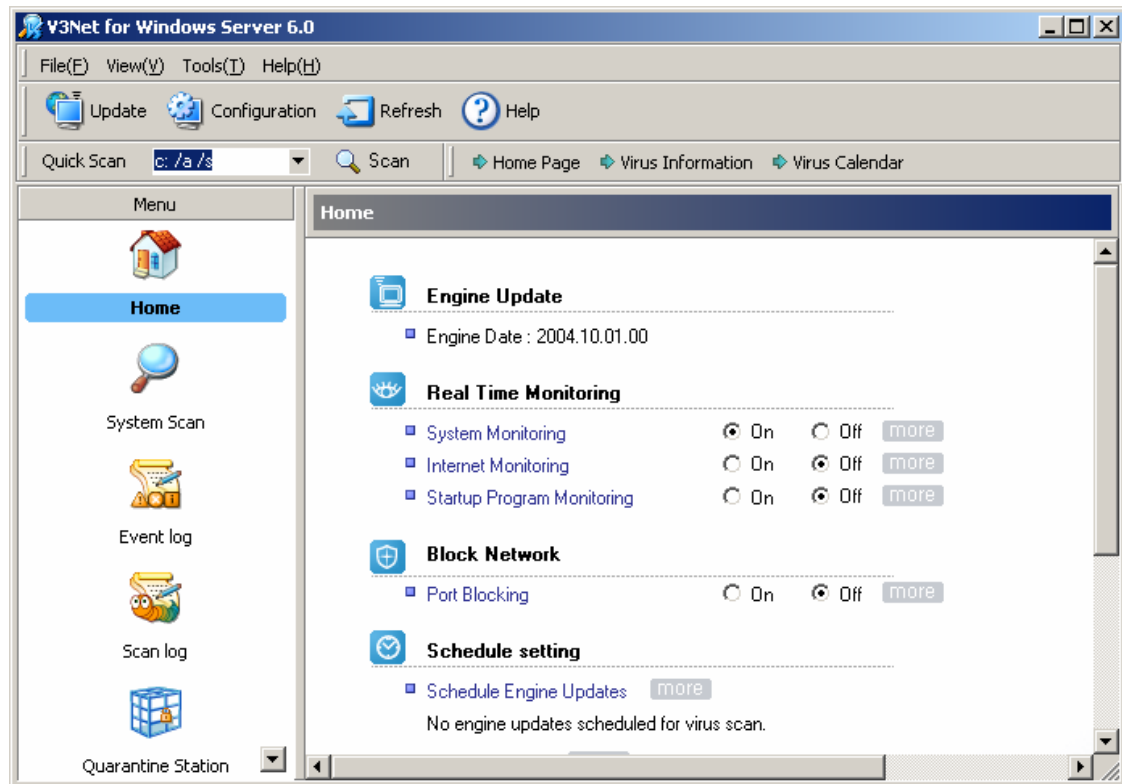
The V3Net for Windows Server 6.0 main screen will display. If you select the standard menu in the left frame, sub-menus will display.

The Home screen is your central page for accessing and configuring all V3Net for Windows Server 6.0 features and settings.

- **System Scan:** Scans for viruses on the user's system.
- **Event Log:** Displays V3Net for Windows Server 6.0 event log sorted by date.
- **Scan Log:** Displays the virus scan results by V3Net for Windows Server 6.0
- **Quarantine Station:** Displays the virus repair results.
- **Security Warning Report:** Displays the security vulnerabilities on the user's system.

## Home

When you select Home from the V3Net for Windows Server 6.0 menu in the left frame, the menu and operation status will be displayed in the right frame.



**Figure 14 Home Menu**

On the upper left part of the V3Net for Windows Server 6.0 Home screen, you can see the names of the latest viruses that are currently spreading. Click the virus name to find information about the virus on the AhnLab web-site.

### **Note**

Click the **x** on the upper right corner of the Urgent Virus Warning window to close. To open it again, click **Configuration>Other Settings**, and then select **Show Urgent Warning**.

### Engine Update

Displays the most recent date that the engine was updated. Click **more** to open the readme.txt file. You can view the date and version information of the latest engine update.

### Real Time Monitoring

Sets each sector's real time functions to On or Off. If you click the **more** icon next to each function item, the Configuration window displays additional information on that program function.

- System Monitoring
- Internet Monitoring
- Startup Program Monitoring

 **Notes**

Refer to the Virus Scan and Repair and learn how to set custom configurations for each function in the Configuration window.

### Block Network

When a new virus spreads rapidly via a network, the ports suspected as the possible origin of the infection can be temporarily blocked. It is recommended that such ports are blocked to protect the system until a new version of engine is available.

### Schedule Setting

- **Update Configuration:** Displays the schedule for the saved virus scan/engine update. If you click the **more** icon next to each function item, you can add, modify or delete the schedule.
- **Scheduled Scan:** Displays the system scan schedule (Year/Month/Day/Time) and the items that will be scanned. Click **more** to display the Scheduled Scan window in which you can add, modify or remove the scan schedule.

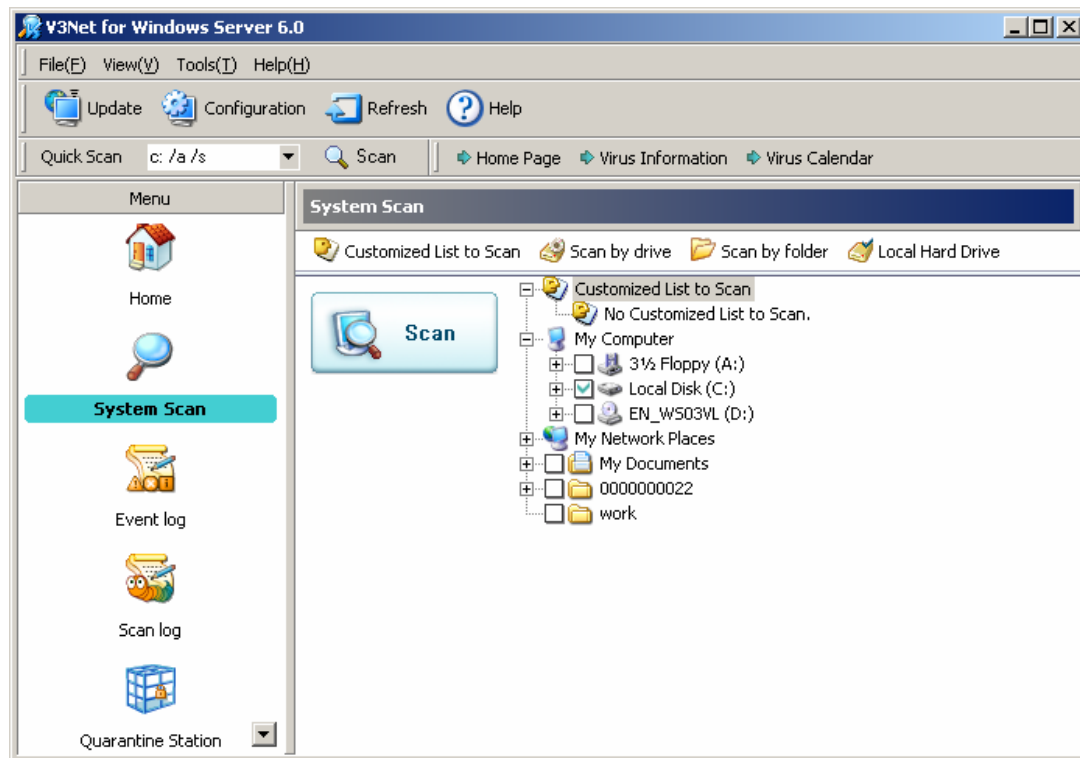
### Last Scan Activities

Displays the time, sector and results (number of files scanned/ number of files infected/ number of files repaired) of the most recent scan performed.

## System Scan

If there are suspicious sectors that may be infected by viruses, this function immediately checks whether they are infected or not. This function scans sectors with a high risk for virus infection.

1. Select **System Scan** from the V3Net for Windows Server 6.0 Home menu in the left frame.



**Figure 15 System Scan Menu**

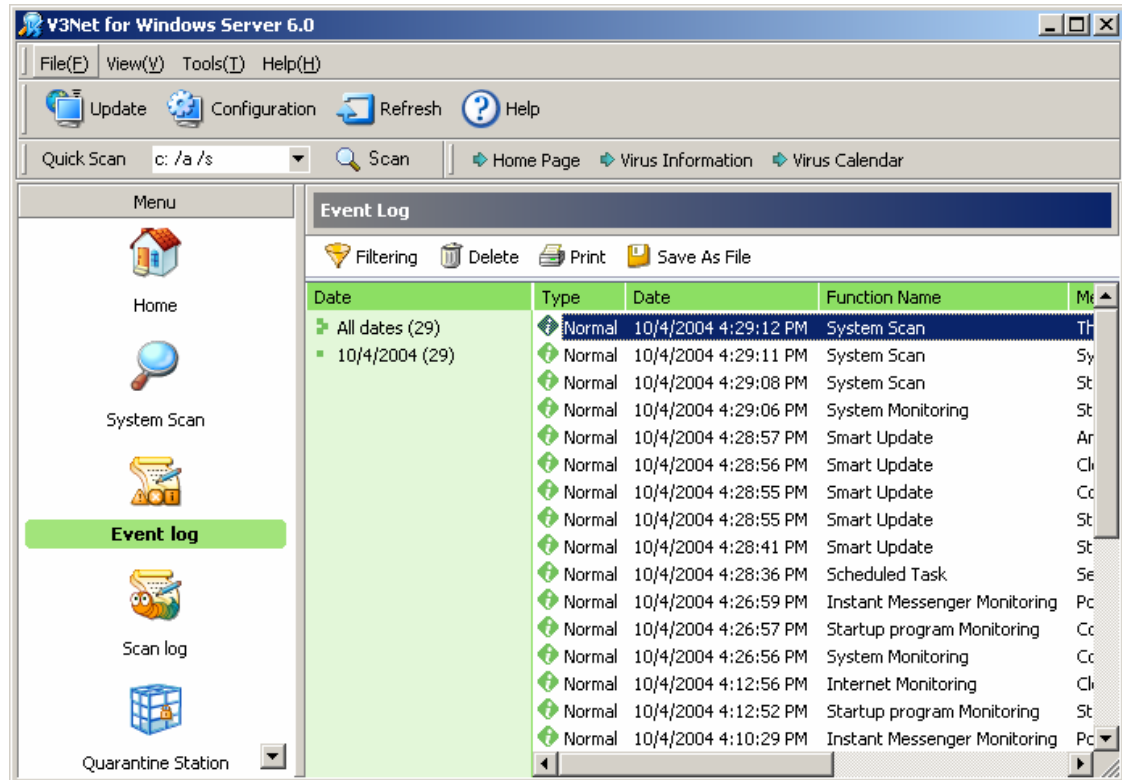
2. Select the following menus located in the right frame of the main window to select drives, folders, or files to scan.
  - Customized List to Scan: Allows the user to set specific scan sectors repeatedly
  - Scan by Drive: Allows the user to select specific drives to scan. This feature does not allow you to select specific folders on the drives.
  - Scan by Folder: Allows the selection of specific scan sectors by folder that are stored on each drive.
  - Local Hard Drive: Click this icon to display the contents of the local hard drive as sectors to scan.
3. Click the **Scan** in the right frame of the window. The **System Scan** window is displayed to show the scan results of the selected sectors. If viruses are not detected in the selected sectors, close the system by clicking the **Close**.

### Note

Select the Close the system automatically after scan if viruses are not detected option in the System Scan window and the system will automatically close if no viruses are detected.

## Event Log

Select **Event Log** from the V3Net for Windows Server 6.0 Home menu in the left frame.



**Figure 16 Event Log**

### Filtering

Filters log records of specified dates and types (normal, error, and warning) from the whole log.

### Delete

Deletes all registered event records on the selected dates in one action.

### Print

Prints all registered event records at once, organized by the dates that appear on the Event Log window.

### Save As File

Saves all event records that appear on the Event Log window as one text file, all at once

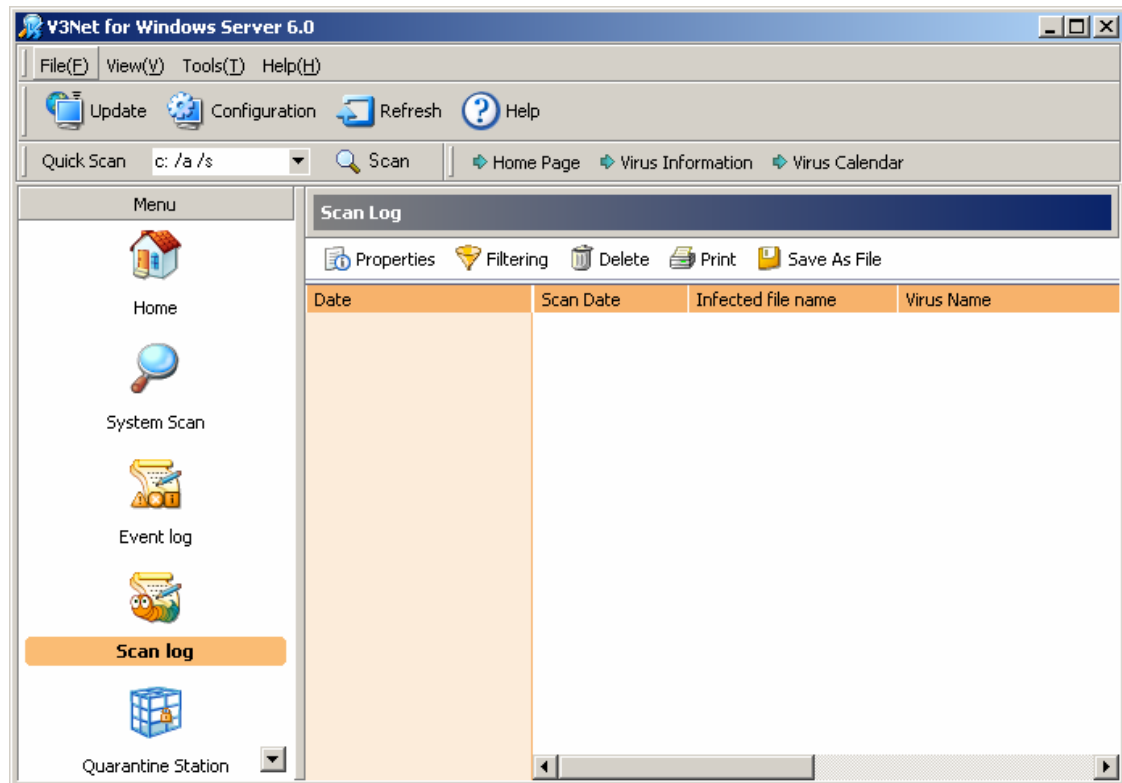
#### **Note**

If event records from a specific date are not displayed, remove the event records file and create a new one in the following manner:

1. Move to the V3Net for Windows Server 6.0 folder. (Default: C:\Program Files\AhnLab\V3Net for Windows Server 6.0)
2. Remove the Log folder under the V3Net for Windows Server 6.0 folder and create and name a new file to store the log.

## Scan Log

Select **Scan Log** from the V3Net for Windows Server 6.0 Home menu in the left frame.



**Figure 17 Scan Log**

### Properties

Displays the properties in the virus Scan Log, including the scan date, infected file name, virus name, status, scan method, and owner.

### Filtering

Filters log record of specific dates and types from the whole log. It includes the process status before and after repair.

### Delete

Deletes all scan records registered on specific and selected dates, all at once.

### Print

Prints all scan records that appear in the Scan Log window, all at once.

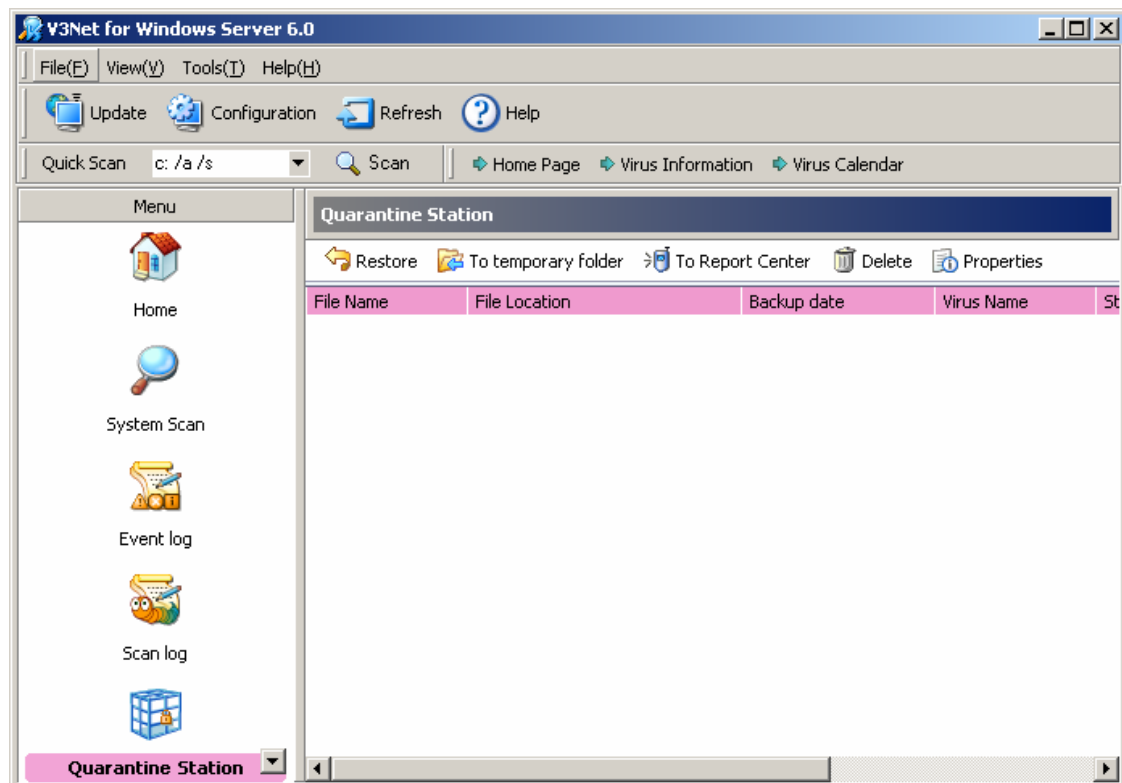
### Save As File

Saves all scan records that appear on the Scan Log window as one text file, all at once.

## Quarantine Station

Managing Backup Files by using Quarantine Station

1. Click **Quarantine Station** in the left menu or click **Quarantine Station** from **View** on the menu bar to verify the location of backups of infected files. V3Net for Windows Server 6.0 backs up files to a separate memory location that prevents the occurrence of possible damage before the repair of infected files.



**Figure 18 Quarantine Station**

2. The Quarantine Station lets you send infected files to the Report Center, or you can choose to restore the files to their original location or to a temporary folder.

### Back Up Properties

Double-click backup files, or right-click one of the files and select **Properties** at the top of the menu. Detailed information about the infected file, including the location, name, size, created date and backup date of the infected file, as well as the name and status of the virus, will appear.

### Submit to the Report Center

If you try to repair failed-to-repair files, their data can be damaged in process of repair. Please send those files to the Report Center of AhnLab, Inc as follows.

1. Select Failed to repair files from the backup files in the right frame of the main window.
2. Click **To Report Center** at the top of the right frame.

 **Caution**

Only files with a Failed to repair status can be sent to the Report Center. If you choose files tagged with a Repairable status, and click **To Report Center**, a warning message will appear, indicating that this is not an appropriate file for the Report Center.

3. Enter the sender's information (name, telephone number, address, email address) and the effects and symptom descriptions of the infection submitted in the **To Report Center** window.
4. Click **Submit** to send the selected backup files to AhnLab, Inc.'s Report Center.

### Delete Backup Files

Backup files displayed as Repair Completed should be deleted from the system since they are infected by viruses. We strongly recommended this action.

1. Select file to be repaired normally from the backup files in the right frame of the main window.
2. Select **Delete** from the top of the right dialogue box.

### Restore backup files

If files containing important information have been damaged, and have the Failed to repair status designation, or the Repair Completed status designation, and files that have a high risk of damage, they may be restored into a temporary folder or to the original location, as explained below:

 **Caution**

If files are restored to the original location, or a temporary folder other than the Quarantine Station, damaging virus activities may resume and your system could suffer serious damage, because it was backed up before it was repaired.

1. Select a specific backup file to restore on the backup file list.
2. Click **Restore** or **To Temporary Folder** at the top of the right frame to restore the selected backup files to a temporary folder of the user's designation.
3. If you click **To Temporary Folder**, specify a folder to which you want to restore the backup files.

 **Caution**

Before restoring backup files, set the **System Monitoring** function to off. If the function is on and the Scan setting of System Monitoring is set to Auto repair, the backup files may not be restored. Files infected by malicious viruses cannot be restored normally or may be damaged while they are being restored. Therefore, it is strongly recommended to backup all suspected files in a place that is safe from virus threats.

## Security Warning Reports

AhnLab provides a solution for system vulnerabilities based on information that has been analyzed and studied. If the security weakness creates possibilities of intrusion of viruses or malicious code, V3Net for Windows Server 6.0 will detect them on the user's system. The Security Warning Report window will keep showing on the System Tray until you click the link on the window and check the detailed information. Select the Security Warning Report window, check the information, and take necessary measures.

### Note

If you want to hide the security alert message on the system tray, de-select the Display an alert icon at the task in **Configuration > Other Configurations > Alert Setting**.

If you select the **Security Warning Report** from the **Home** menu in the left frame, a menu will be displayed in the right frame. You can check more detailed information on causes and solutions of security weakness, etc.

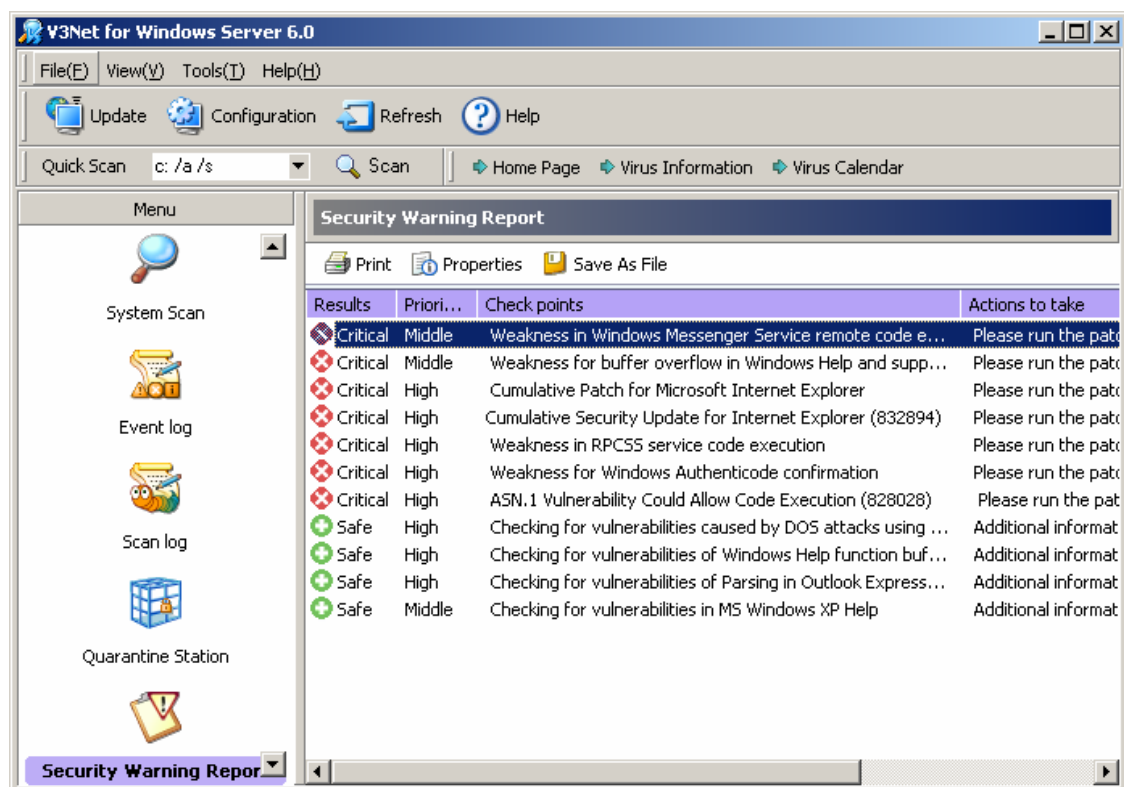


Figure 19 Security Warning Reports

### Print

Prints all security warning reports that have been received to date.

### Properties

Displays detailed properties of registered security warning reports, organized by importance, priority ranks, results and solutions.

## Save As File

Saves the security warning reports that have been received to date as a text file, in a location of the user's choice

### Caution

The items displayed as Critical in the Result column in the Security Warning Report, mean that appropriate measures should be taken. Refer to our solutions and related links on our web site. Your system may be damaged by virus infections if security warning reports are ignored and appropriate measures are not taken.

## Menu Bar

The menu bar on the upper area of the V3Net for Windows Server 6.0 execution frame contains menu items such as **File (F)**, **View (V)**, **Tool (T)**, and **Help (H)**.

### File(F)

- Smart Update (U): Opens the Smart Update Utility Window.
- Exit (X)

### View(V)

- Toolbar (T): Displays the Toolbar in the upper screen.
- Web Link (W): Displays the Web Link in the upper screen.
- Quick Scan Line (Q): Displays the Quick Scan Line in the upper screen.
- Home (H): Displays the Home screen.
- System Scan (M): Displays the System Scan screen.
- Event Log (E): Displays the Event Log screen.
- Scan Log (L): Displays the Scan Log screen.
- Quarantine Station(R): Displays the Quarantine Station screen.
- Security Warning Reports (S): Displays the Security Warning Reports screen.

### Tools(T)

- Screen Saver Scan (S): Runs Screen Saver Scan.
- Explore Scan (E): Runs Explore Scan.
- Real Time Monitoring (A): Runs real time monitoring of selected functions from the submenu.
  - System Monitoring
  - Internet Monitoring
  - Instant Messenger Monitoring
  - Startup Program Monitoring
  - POP3 Monitoring
  - Outlook Monitoring
- Scheduled Scan (C): Displays the Set Scheduled Scan screen.
- Configuration (P): Displays the Configuration screen.

## Help(H)

- Help Topics(H): Displays the Help contents.
- Virus Information(I): Displays the web page that enables detailed searches for, and about, viruses.
- Virus Calendar(C): Displays the web page that enables you to verify information on viruses by past dates and other highly specific virus profile information.
- Homepage(W): Displays the AhnLab homepage.
- Online Registration(R): Launches the online product registration web page for AhnLab, Inc. Customer Support Center.
- V3Net for Windows Server 6.0 Information(A): Displays the version information of the product.

## Toolbar

There is a toolbar on the upper screen of the V3Net execution frame. You can run each function by selecting specific items from the toolbar.

- Update: Allows updating of V3Net with the latest engine when the Smart Update Utility window is executed.
- Configuration: Allows setting the scan/repair configuration functions in the Configuration window.
- Refresh: Displays the selected screen information after updating.
- Help: Displays the contents of the Help menu.

### Note

If the toolbar does not appear on the upper screen, select **View(V)>Tools(T)** from the menu bar on the top screen.

## Quick Scan Line

Executes a Virus Scan after designating specific sectors. Refer to **Quick Scan** for more detailed information.

## Web Link

The Web Link launches the linked web page immediately on the upper work screen and provides direct links to the AhnLab.Inc. related pages.

- Homepage: Displays the AhnLab Inc. homepage.
- Virus Information: Launches the web page that explains the analysis results for common viruses on the AhnLab homepage.
- Virus Calendar: Moves from the AhnLab homepage to the web page. Gives information on viruses with a high probability of activity, and their most likely active dates.

### Caution

You must first connect to the Internet to launch linked web pages when you click web links.

## Explorer Toolbar

If Windows Explorer and MS Internet Explorer 5.0 or higher programs are executed, the toolbar will be displayed as follows:

- Execute: Displays the Execute screen of V3Net.
- Configuration: Allows for setting the scan/repair configuration items by function in the Configuration window.
- Smart Update: Allows updating to the latest anti-virus engine in the Smart Update Utility window.
- Homepage: Displays the AhnLab homepage.
- Virus Scan: Executes a virus scan for selected drives, folders or files.

 **Note**

If the V3Net for Windows Server 6.0 Toolbar does not appear in Windows Explorer or MS Internet Explorer 5.0 or higher programs, then select **View(V)>Toolbar(T)>V3** from the web browser's menu bar.

## Alert Icon Toolbar

If you right-click the V3Net for Windows Server 6.0 notification icon on the system tray, the toolbar will display as follows:

Open: Displays the Execute window of V3Net.

- Real Time Monitoring: Runs real time monitoring of selected functions from the submenu.
  - System Monitoring
  - Internet Monitoring
  - Startup Program Monitoring
- Configuration...: Allows for setting the scan/repair configuration items by function in the Configuration window.
- Smart Update: Executes the Smart Update Utility to download and install the latest anti-virus engine.
- Close: Closes the Alert Icon menu.

 **Note**

If the V3Net Alert Icon does not appear on the system tray, then select **Configuration>Other Configurations>Show Alert Icon on the System Tray**.

## Scan and Repair Settings

---

This chapter describes how to configure V3Net for Windows Server 6.0 virus scan and repair settings, using the **Configuration** window.

### How To Open the Configuration Window

You can open the **Configuration** window in any of the following ways:

- Select **Configuration** of Tools from the menu bar.
- Select **Configuration** from the toolbar.
- Select **Configuration...** from the alert icon menu on the system tray.
- Select **Configuration** from the V3Net for Windows Server 6.0 shortcut tools and menu in Windows Explorer or MS Internet Explorer 5.0 or higher programs.

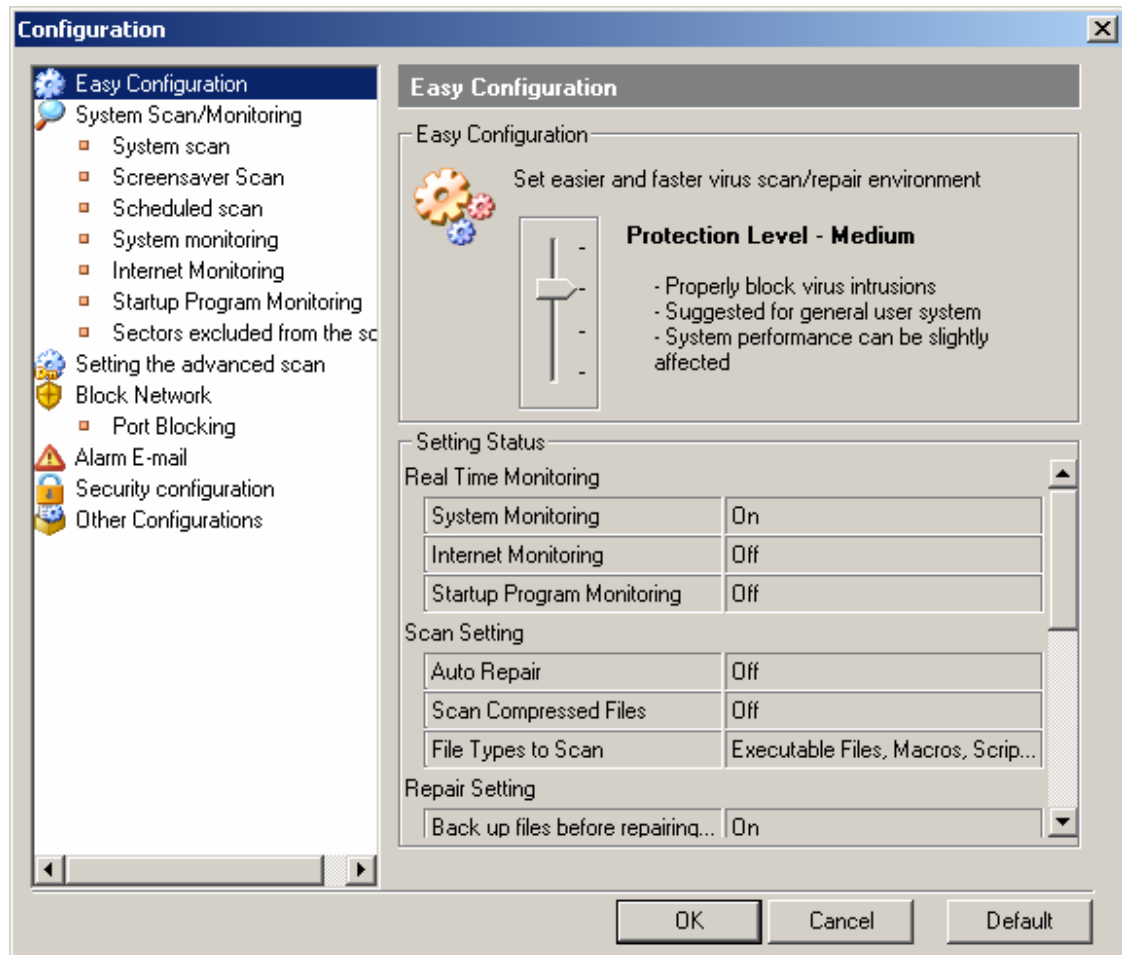
 **Note**

The configuration settings for each scan/repair function in the **Configuration** window are set as defaults. You can apply the default values instantly by clicking the **Set as Defaults** button on lower right screen of each function's menu window.

## Easy Configuration

This function enables you to quickly and easily configure your system to scan/repair viruses.

1. Open the **Configuration** window by selecting **Configuration** from the toolbar or from **Tools** on the menu bar.
2. Select **Easy Configuration** from the left frame of the **Configuration** window.



**Figure 20 Easy Configuration**

3. Select the desired security level in the frame on the right. Whenever you change the security level, detailed status information for each level will appear at the bottom of the right frame.
  - High: Blocks all viruses (Recommended for systems with a high risk of virus infection) If you select **High**, system performance may be affected.
  - Medium: Blocks most virus infections. (Recommended for typical users.)
  - Low: Minimal Blocking of virus infections. (Recommended for systems with low risk of virus infection)
  - Customized: Blocks viruses based on customized scan/repair settings. (Recommended for the system in special environments.)

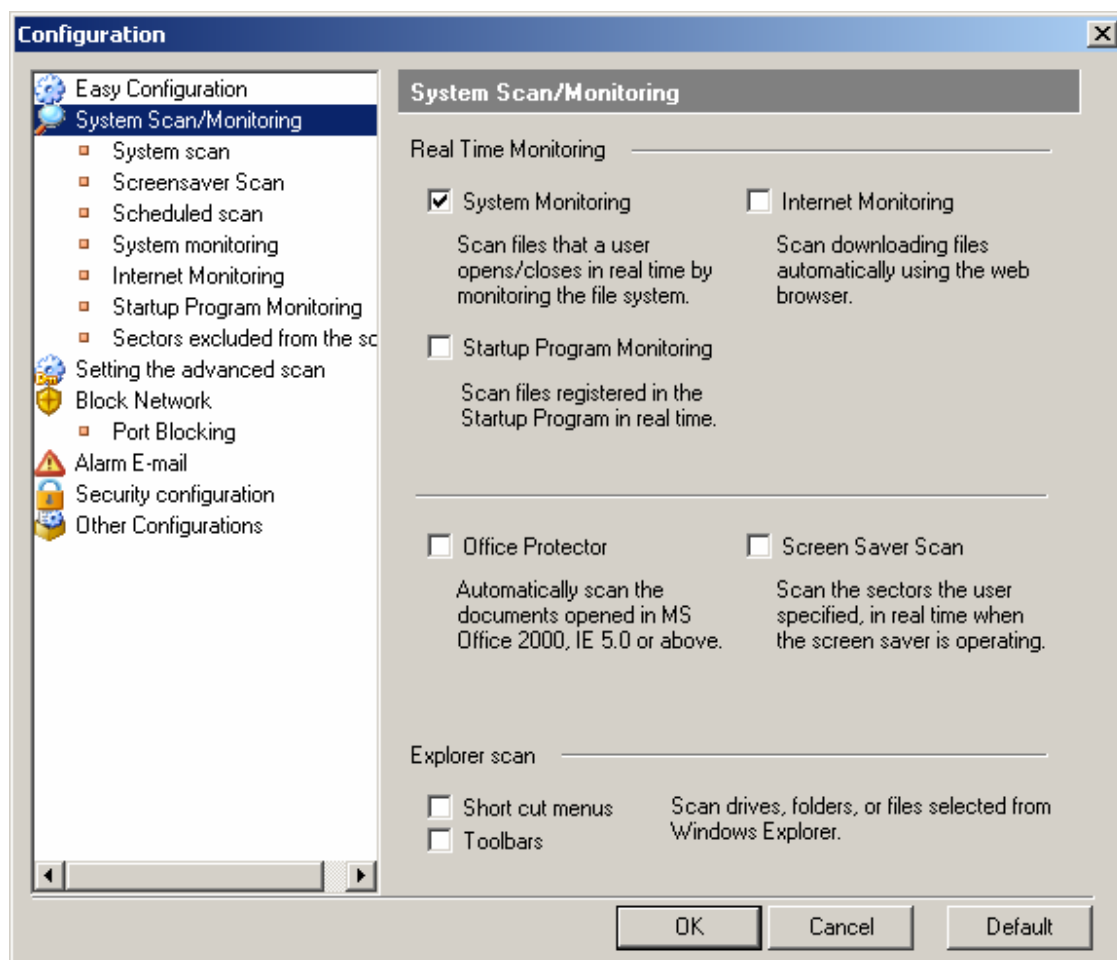
**Note**

If you select the Customized setting for your system security level, you may set each scan/repair function from the left frame of the Configuration window. If you click each menu item in the left frame of the Configuration window after selecting the desired security level in Easy Configuration, the Information window appears: (But, if you select Customized, the Information window will not appear.) If you click **OK**, all values entered in the Function Setting window for each menu will be saved as Customized. And if you change the setting without selecting the Customized setting, the security level will automatically change to Customized.

- Click **OK** to apply the selected security level.

## System Scan/Monitoring

- Open the **Configuration** window by selecting **Configuration** from the toolbar or from **Tools** on the menu bar. The **Configuration** window appears.



**Figure 21 System Scan/Monitoring**

- Select **System Scan/Monitoring**, displayed in the left frame of the **Configuration** window.
- Select the items to scan or monitor in the system scan/monitor window.

### **System Monitoring**

Runs real-time scanning of all files and data from all application programs on the user's system. The System Monitoring function is essential to block viruses from their entries. It is strongly recommended that you keep V3Net on at all times. If system monitoring is off, the V3 icon in your Task tray will be displayed as a mark. Real-time Monitoring functions will run as long as your system is on, even after you have terminated the V3Net for Windows Server 6.0.

### **Internet Monitoring**

Scans all data and files downloaded via web browsers in real time.

### **Startup Program Monitoring**

Runs real-time monitoring of all startup programs registered in the registry, the startup program folder, and all system configuration files that are launched on Windows startup.

#### **Caution**

Startup Program Monitoring function does not monitor files added to the startup program folder or registry while a new user accounts log in. If you want to monitor newly added files of a new user account as well, reset the function.

### **Office Protector**

If you open OLE files using MS Office 2000 or MS Internet Explorer 5.0 or higher programs, the relevant files are automatically scanned.

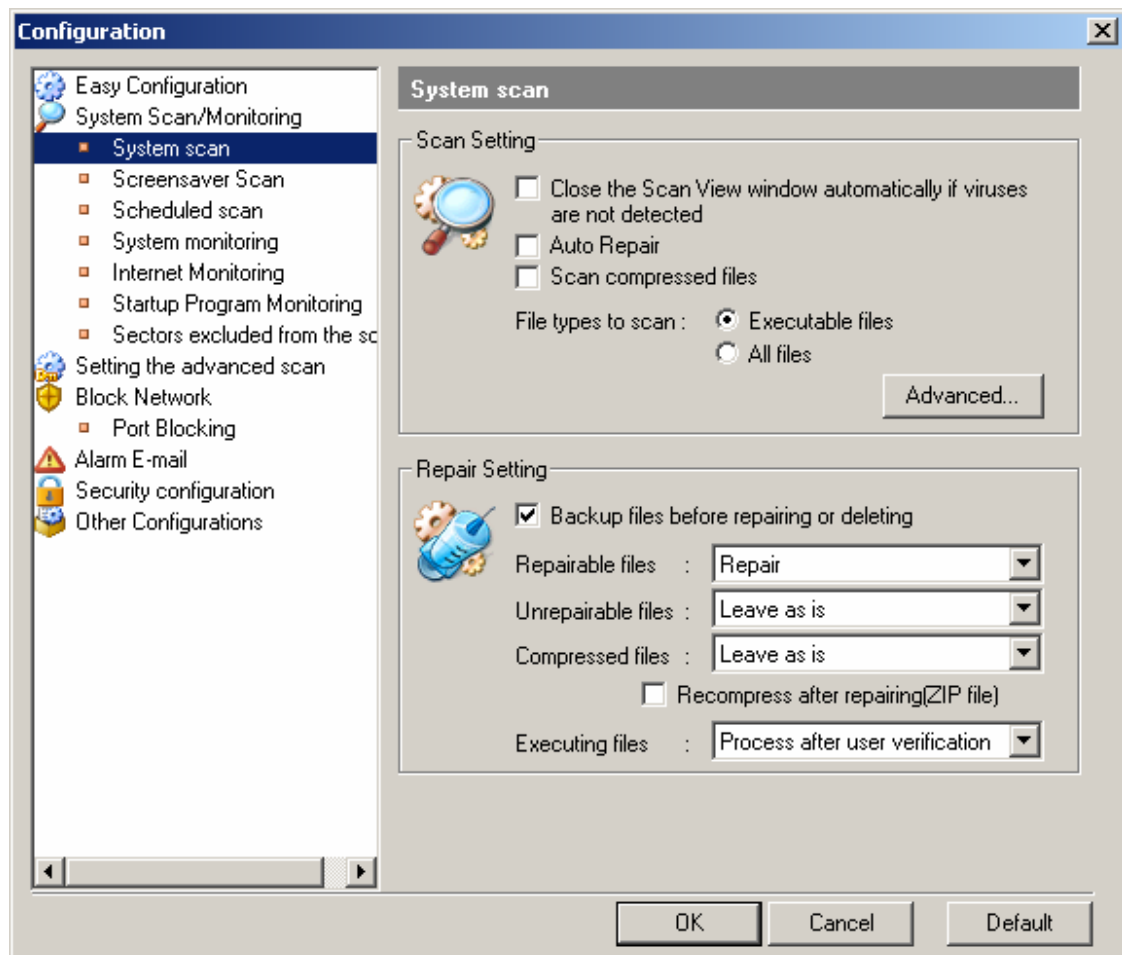
### **Screen Saver Scan**

When the screen saver is on, V3Net will automatically scan the areas set in Customized List to Scan.

## System Scan

Configure the virus scan/repair settings for System Scan.

1. Open the **Configuration** window by selecting **Configuration** from the toolbar or from **Tools** on the menu bar. The **Configuration** window appears.
2. Select **System Scan**, displayed in the left frame of the **Configuration** window.



**Figure 22 System Scan**

3. Configure the virus scan/repair settings for **System Scan** by referring to the below and clicking **Confirm**.

## Scan Setting

- Close the Scan View window automatically if viruses are not detected: If scanning is completed without detecting any viruses, the Scan window will automatically close.
- Auto Repair: If a virus is detected, it is automatically repaired without alerting the user.
- Scan compressed files: Scans compressed files.
- File types to scan:

- Executable files: Scans all execution files with a risk of virus infection including program files, macros and scripts.
- All files: Scans all files, regardless of file types.

## Advanced

### Repair Setting

- Backup files before repairing or deleting: Backup the original files before repairing or deleting infected files.
- Repairable files: How to manage repairable files. Select one of the following:
  - Leave as is
  - Repair
  - Delete
- Un-repairable files: How to manage files that are un repairable. Select one of the following:
  - Leave as is
  - Delete
- Compressed files: How to manage compressed files. Select one of the following:
  - Leave as is
  - Delete
  - Re-compress after repairing (ZIP file): Unzips the zip files, scans/repairs the viruses, and re-compresses files as zip files.
- Executing files: How to manage virus infected files that are currently running. Select one of the following:
  - Process after user verification
  - Leave as is
  - Restart the system after the repair
  - Repair after forced termination

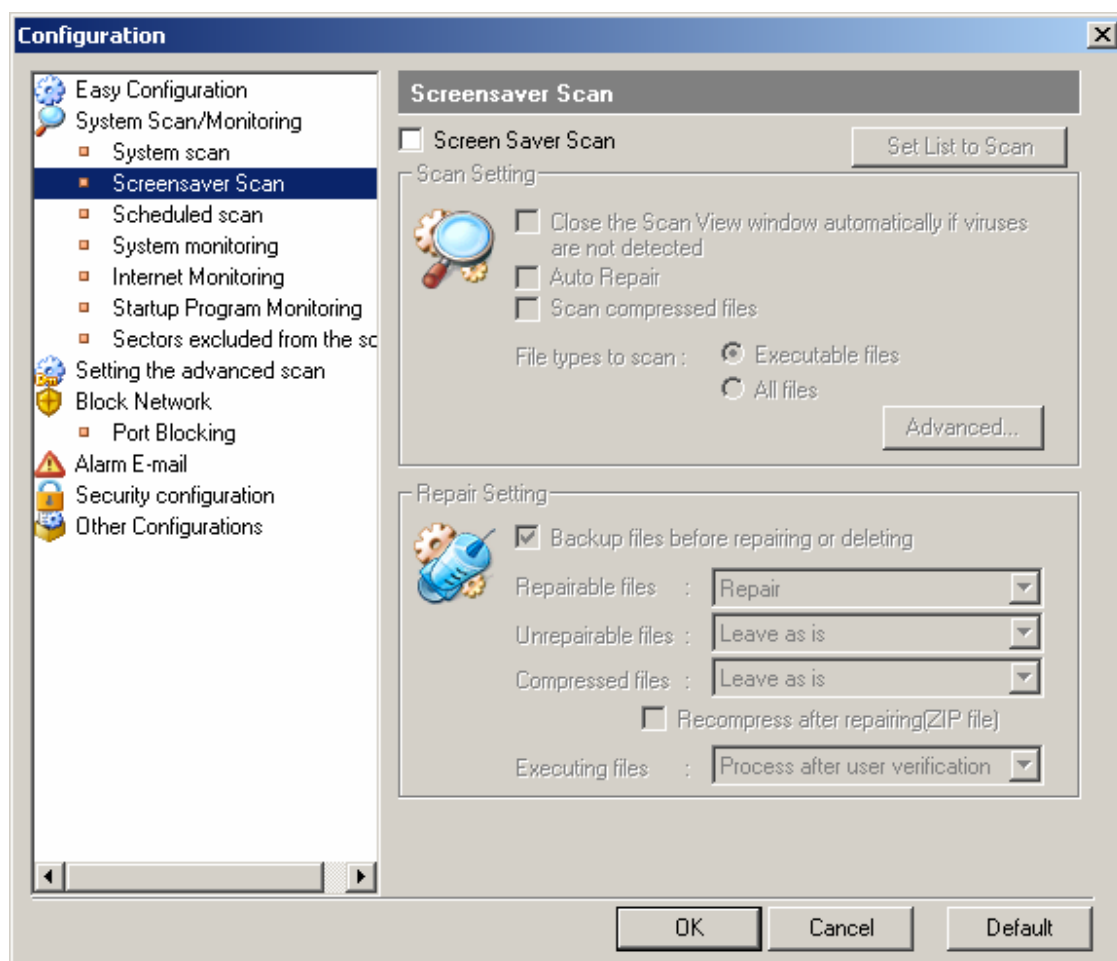
#### Caution

If you select the **Delete** option for **Un-repairable files**, those files will be completely removed from your system and can never be restored from the **Recycle Bin** or the **Quarantine Station**. Files that are currently running or encoded will appear in the folder but the file size will be changed to 0 bytes.

## Screen Saver Scan

When the screen saver is on, V3Net will automatically scan the areas set in Customized List to Scan.

1. Select **Configuration** menu in V3Net and select **Screen Saver Scan** in the left pane of Configuration window
  - Select **Screen Saver Scan** and click **Set List to Scan** at the upper right side. The Set List to Scan window appears.
  - Select the items to be scanned while the screen saver is on and click **Add >>** to add them to the customized list.



**Figure 23 Screen Saver Scan**

### Note

If a List to Scan is not specified, V3Net for Windows Server 6.0 scans the entire local hard drive of the user's system.

2. Configure the virus scan/repair settings referring to the below.

## Scan Setting

- Close the Scan View window automatically if viruses are not detected: If scanning is completed without detecting any viruses, the Scan window will automatically close.
- Auto Repair: If a virus is detected, it is automatically repaired without alerting the user.
- Scan compressed files: Scans compressed files.
- File types to scan:
  - Executable files: Scans all execution files with a risk of virus infection including program files, macros and scripts.
  - All files: Scans all files, regardless of file types.

## Advanced

### Repair Setting

- Backup files before repairing or deleting: Backup the original files before repairing or deleting infected files.
- Repairable files: How to manage repairable files. Select one of the following:
  - Leave as is
  - Repair
  - Delete
- Un-repairable files: How to manage files that are un repairable. Select one of the following:
  - Leave as is
  - Delete
- Compressed files: How to manage compressed files. Select one of the following:
  - Leave as is
  - Delete
  - Re-compress after repairing (ZIP file): Unzips the zip files, scans/repairs the viruses, and re-compresses files as zip files.
- Executing files: How to manage virus infected files that are currently running. Select one of the following:
  - Process after user verification
  - Leave as is
  - Restart the system after the repair
  - Repair after forced termination

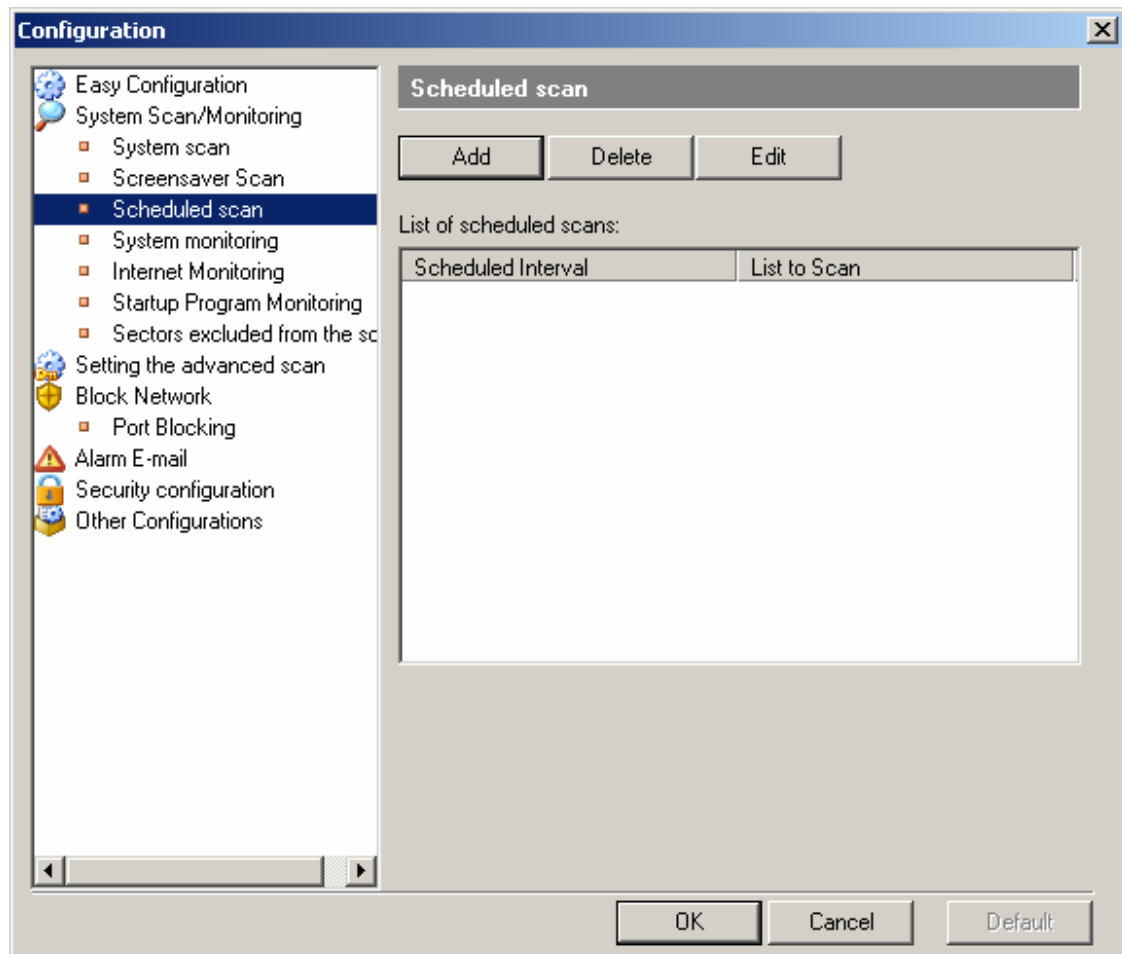
#### Caution

If you select the **Delete** option for **Un-repairable files**, those files will be completely removed from your system and can never be restored from the **Recycle Bin** or the **Quarantine Station**. Files that are currently running or encoded will appear in the folder but the file size will be changed to 0 bytes.

## Scheduled Scan

This function enables you to scan items at scheduled times. The frequently scanned sectors are automatically scanned at user-specified intervals and times.

1. Open the Scheduled Scan window.
  - Click Scheduled Scan on the V3Net for Windows Server 6.0 Home screen.
  - Select the Scheduled Scan menu in the Configuration window.



**Figure 24 Scheduled Scan**

2. Click **Add** to open the Schedule Scan Wizard.
3. Add drives, folders or files to scan to the List to Scan and click **Next >**. Select the scan interval to set the items to scan, and to be added to the List to Scan.

### Interval Choices:

- On every system start-up.
- Once a month, at a specified time and date.
- Once a week, at a specified time and date.

- Once a day, at a specified time.
- Once, at a specified time and date.

 **Note**

Windows NT users, who add network paths that are only available to the users registered in the List to Scan, should specify the names and passwords, so that the scheduled scan can run automatically. Click **Authorization Setting** to open the Authorization Setting window. Input the necessary user name and password to authorize a Scheduled Scan in the Authorization Setting window and click **OK**.

4. Click **Next >** and set the configuration for scan and repair.

### Scan Setting

- Close the Scan View window automatically if viruses are not detected: If scanning is completed without detecting any viruses, the Scan window will automatically close.
- Auto Repair: If a virus is detected, it is automatically repaired without alerting the user.
- Scan compressed files: Scans compressed files.
- File types to scan:
  - Executable files: Scans all execution files with a risk of virus infection including program files, macros and scripts.
  - All files: Scans all files, regardless of file types.

## Advanced

### Repair Setting

- Backup files before repairing or deleting: Backup the original files before repairing or deleting infected files.
- Repairable files: How to manage repairable files. Select one of the following:
  - Leave as is
  - Repair
  - Delete
- Un-repairable files: How to manage files that are un-repairable. Select one of the following:
  - Leave as is
  - Delete
- Compressed files: How to manage compressed files. Select one of the following:
  - Leave as is
  - Delete
  - Re-compress after repairing (ZIP file): Unzips the zip files, scans/repairs the viruses, and re-compresses files as zip files.
- Executing files: How to manage virus infected files that are currently running. Select one of the following:

- Leave as is
- Restart the system after the repair
- Repair after forced termination

 **Note**

If you select the Delete option for Un-repairable files, those files will be completely removed from your system and can never be restored from the Recycle Bin or the Quarantine Station. Files that are currently running or encoded will appear in the folder but the file size will be changed to 0 bytes.

5. Click **Finish**, then you will see the newly configured scan schedule displayed.

 **Note**

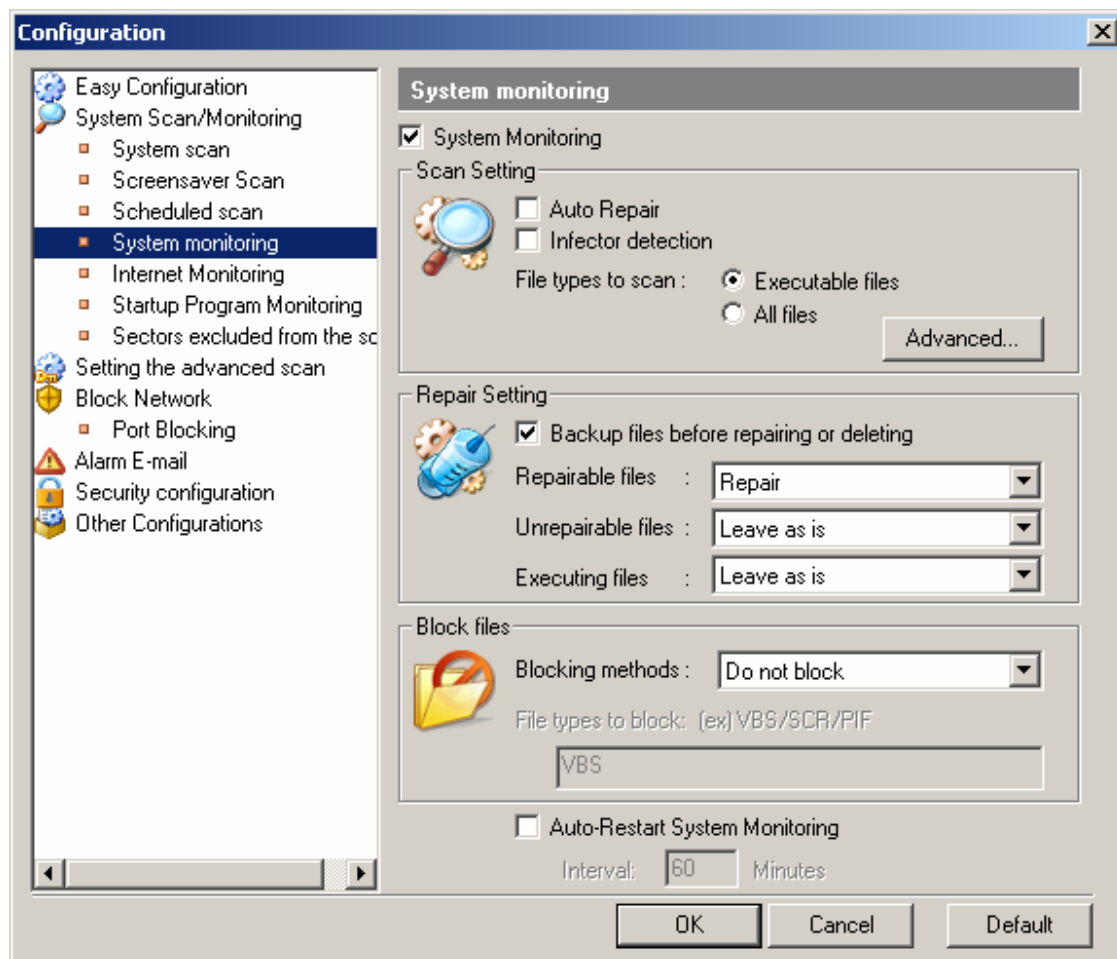
To modify or delete scheduled scan items, click **Edit** or **Delete**.

The items registered in the Customized List to Scan are automatically scanned based on the specified schedule.

## System Monitoring

Configure the virus scan/repair settings for system monitoring.

1. Open the **System Monitoring** menu window..
  - Select System Monitoring>More in the Home menu window.
  - Select System Monitoring from the left menu in the Configuration window.



**Figure 25 System Monitoring**

2. Select **System Monitoring** to execute the system monitoring function.
3. Configure the virus scan/repair settings for system monitoring referring to the below.

### Scan Setting

- Auto Repair: If a virus is detected, it is automatically repaired without alerting the user.
- Infector detection: Traces the originating computer name and IP address of the virus spreading through network shared folders.
- File types to monitor:

- Executable files: Scans all execution files with a risk of virus infection including program files, macros and scripts.
- All files: Scans all files, regardless of file types.

## Advanced

### Repair Setting

- Backup files before repairing or deleting: Backup the original files before repairing or deleting infected files.
- Repairable files: How to manage repairable files. Select one of the following:
  - Leave as is
  - Repair
  - Delete
- Un-repairable files: How to manage files that are un repairable. Select one of the following:
  - Leave as is
  - Delete
- Executing files: How to manage virus infected files that are currently running. Select one of the following:
  - Leave as is
  - Restart the system after the repair
  - Repair after forced termination

#### Caution

If you select the **Delete** option for **Un-repairable files**, those files will be completely removed from your system and can never be restored from the **Recycle Bin** or the **Quarantine Station**. Files that are currently running or encoded will appear in the folder but the file size will be changed to 0 bytes.

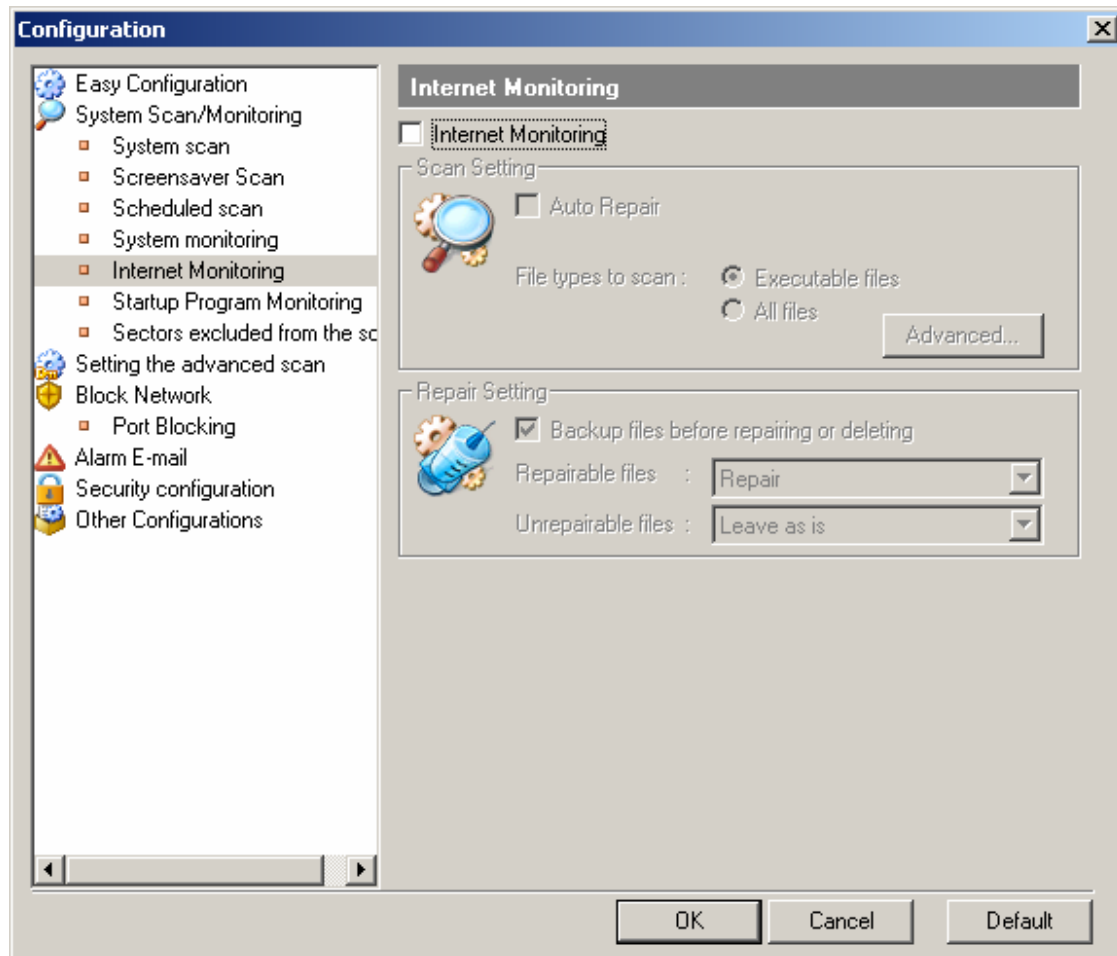
### Block files

- Blocking methods
  - Do not block: Does not block specific file types.
  - Rename as \*.V3F: Enter the file type that will be changed to V3F, which effectively blocks viruses.
  - Delete: Enters file types to be deleted.
  - Block: Enters file types to block.
- File types to block: If there is a high risk for virus infection, enter the file extensions to block. Use the / character to add multiple file types.
- Auto-Restart System Monitoring: If this check box is enabled, system monitoring will automatically resume after a specified time (minutes) entered as an Interval. For instance, if you enter 60 under Interval after selecting the Auto-Restart System Monitoring, monitoring resumes after 60 minutes from the time when the monitoring stops.

## Internet Monitoring

Configure the virus scan/repair settings for Internet monitoring.

1. Open the **Internet Monitoring** menu window.
  - Select Internet Monitoring>More in the Home menu window.
  - Select Internet Monitoring from the left menu in the Configuration window.



**Figure 26 Internet Monitoring**

2. Select **Internet Monitoring** to execute the Internet monitoring function.
3. Configure the virus scan/repair settings referring to the below.

### Scan Setting

- Auto Repair: If a virus is detected, it is automatically repaired without alerting the user.
- File types to monitor:
  - Executable files: Scans all execution files with a risk of virus infection including program files, macros and scripts.

- All files: Scans all files, regardless of file types.

## Advanced

### Repair Setting

- Backup files before repairing or deleting: Backup the original files before repairing or deleting infected files.
- Repairable files: How to manage repairable files. Select one of the following:
  - Leave as is
  - Repair
  - Delete
- Un-repairable files: How to manage files that are un repairable. Select one of the following:
  - Leave as is
  - Delete

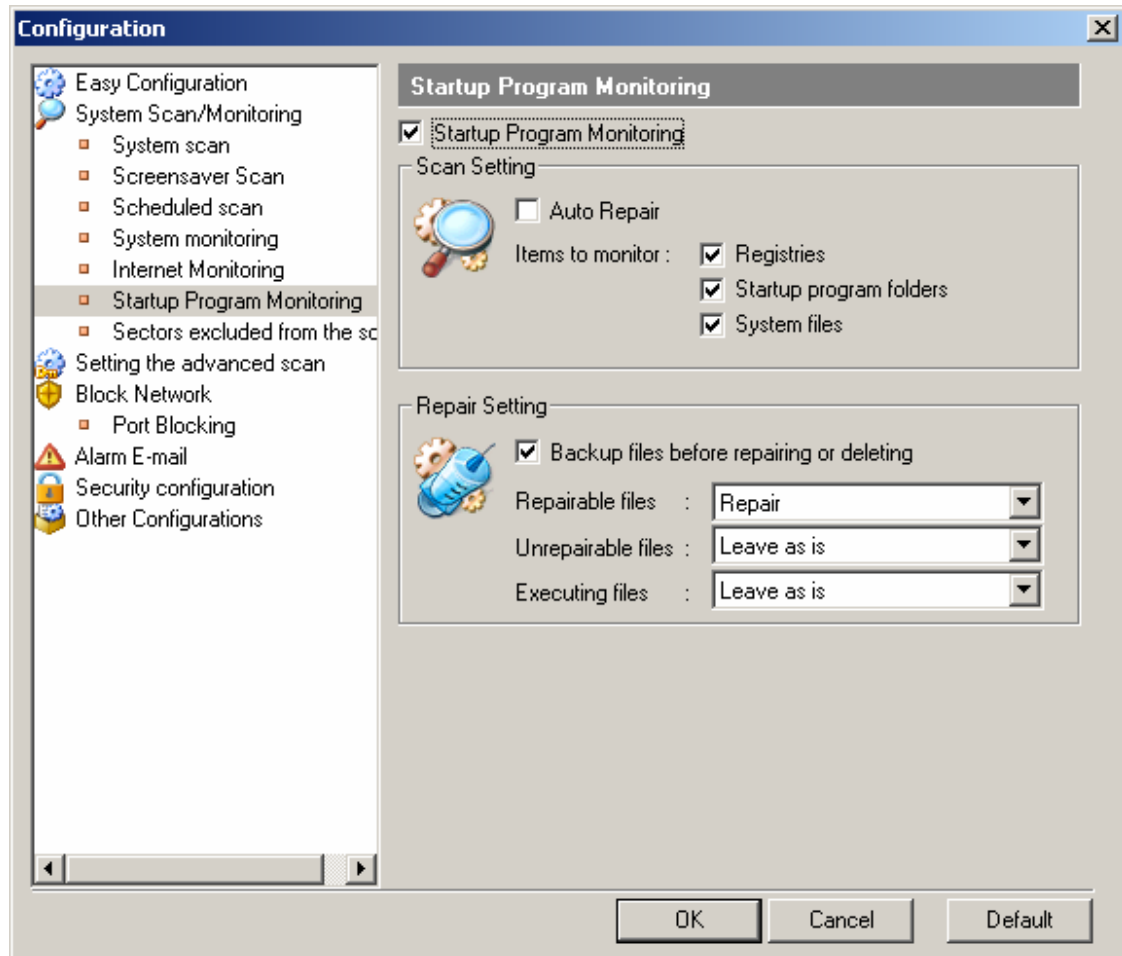
#### Caution

If you select the **Delete** option for **Un-repairable files**, those files will be completely removed from your system and can never be restored from the **Recycle Bin** or the **Quarantine Station**. Files that are currently running or encoded will appear in the folder but the file size will be changed to 0 bytes.

## Startup Program Monitoring

Configure the virus scan/repair settings for Startup Program Monitoring.

1. Open the Startup Program Monitoring menu window.
  - Select Startup Program Monitoring>More in the Home menu window.
  - Select Startup Program Monitoring from the left menu in the Configuration window.



**Figure 27 Startup Program Monitoring**

2. Select **Startup Program Monitoring** to monitor all startup programs.
3. Configure the virus scan/repair settings for Startup Program Monitoring referring to the below.

### Scan Setting

- Auto Repair: If a virus is detected, it is automatically repaired without alerting the user.
- File types to monitor:
  - Registries: Scans files registered in the registry.
  - Startup program folder: Scans files in the startup program folder.

- System files: Scans files registered in system configuration files.

## Advanced

### Repair Setting

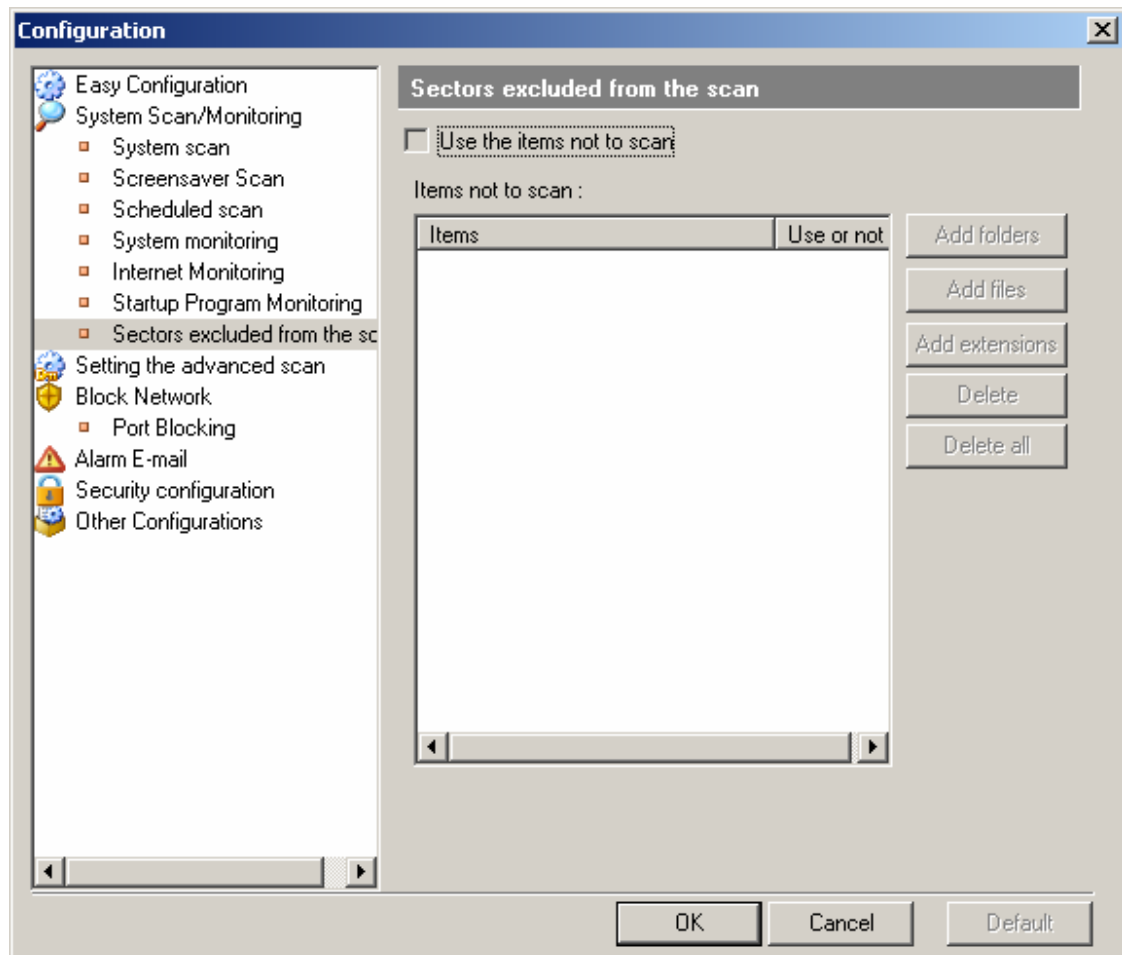
- Backup files before repairing or deleting: Backup the original files before repairing or deleting infected files.
- Repairable files: How to manage repairable files. Select one of the following:
  - Leave as is
  - Repair
  - Delete
- Un-repairable files: How to manage files that are un repairable. Select one of the following:
  - Leave as is
  - Delete
- Executing files: How to manage virus infected files that are currently running. Select one of the following:
  - Leave as is
  - Restart the system after the repair
  - Repair after forced termination

#### Caution

If you select the **Delete** option for **Un-repairable files**, those files will be completely removed from your system and can never be restored from the **Recycle Bin** or the **Quarantine Station**. Files that are currently running or encoded will appear in the folder but the file size will be changed to 0 bytes.

## Items Not To Scan

1. Open the Configuration window.
  - Select Configuration in the toolbar.
  - Select Configuration from the left menu in the Configuration window.



**Figure 28 Items Not To Scan**

2. Select **Items Not To Scan** from the left menu in the **Configuration** window.
3. Select **Use the Items not to scan** to register sectors of your system that are safe from virus intrusions, and exclude these sectors from virus scans.

### **Caution**

You should be cautious when choosing an item not to scan, since these sectors will be excluded from any scan/monitoring.

- Add folders: Add folders to register the items not to scan
- Add files: Add files to register the items not to scan
- Add extensions: Add extensions to register the items not to scan
- Delete: Exclude selected folders or files that are registered as areas not to scan.

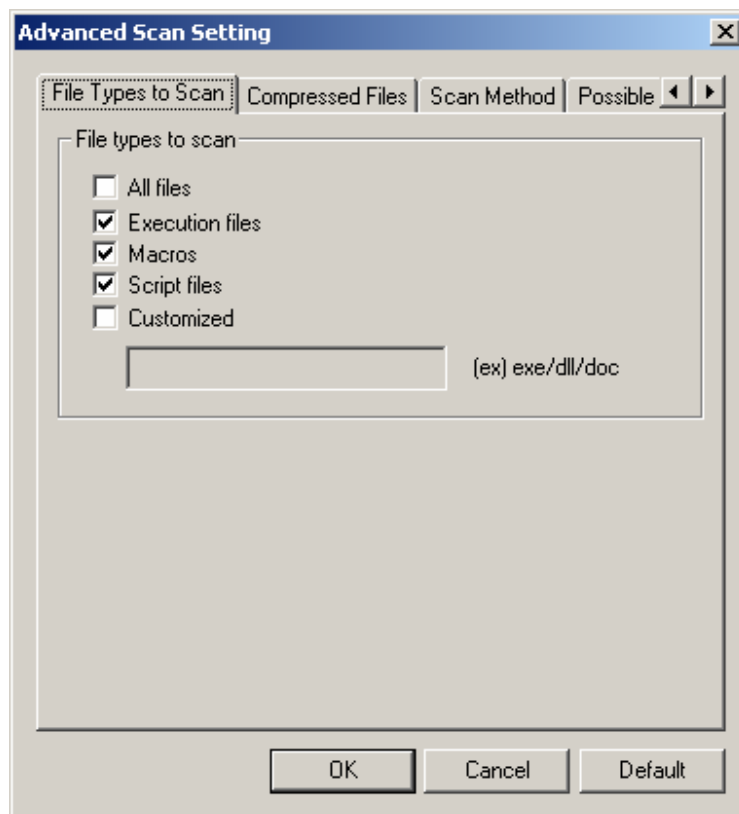
- Delete all: Exclude all folders or files that are registered as areas not to scan

### **Caution**

The V3Net for Windows Server 6.0 excludes sectors specified as items not to scan in any scan type. If you think there is a slight chance of exposure to risks, do not specify those areas as excluded items that are not to be scanned.

## Advanced Scan Setting

If you click **Advanced...** in the **Scan Setting** frame, you can select the Scan compressed files and File types to scan in the following Advanced Scan Setting window.



**Figure 29 Advanced Scan Setting**

### File Types to Scan

- All files: Scans all files regardless of file types.
- Execution files: Scans execution files.
- Macros: Scans macros.
- Script files: Scans script files.
- Customized: Specifies file extensions to scan. Use / for multiple extensions. Ex) exe/dll/doc

## Compressed files

- Scan compressed files: Scans compressed files.
- Multi-compressed files: Decompress all multi-compressed files and scans them. You can specify the compression level of the compressed files to be scanned.
- Executable compressed files: Scans executable compressed files created by such programs as PKLITE, LZEXE, or DIET.
- Incremental Scan: Does not scan previously scanned compressed file. All modified or newly created files are scanned only once.
- All compressed file types:
  - Scans all types of compressed files.
  - Specifies the type (extension) of compressed files to scan. Extensions ace, arj, lzh, rar, and zip are specified as defaults.

## Scan Method

### System Scan

- Scan after disabling shared files/folders: Disables all shared folders of the system and starts scanning for viruses. The disabled shared folders will not be recovered after the system scan is complete.
- Scan after closing shells: Closes the shell process (normally refers to Explorer.exe) and starts the System Scan. This feature is not normally used because the Active Desktop and the taskbar icons may not be restored. [Caution] If you select this option, all icons on the taskbar will disappear and all tasks involved in the Explorer.exe process will be terminated.

### System Monitoring

- Scan Floppy Disc
  - Scans floppy disc boot sector
  - Scans floppy disc when closing the Windows.
- Scan Range
  - Scans local drive reading
  - Scans local drive writing
  - Scans network drive reading
  - Scans network drive writing
- Warning Messages: Displays warning messages when a virus is found. (Windows NT series only)

#### Caution

You must select **Scan Local Drive Writing** to use the infection tracking function.

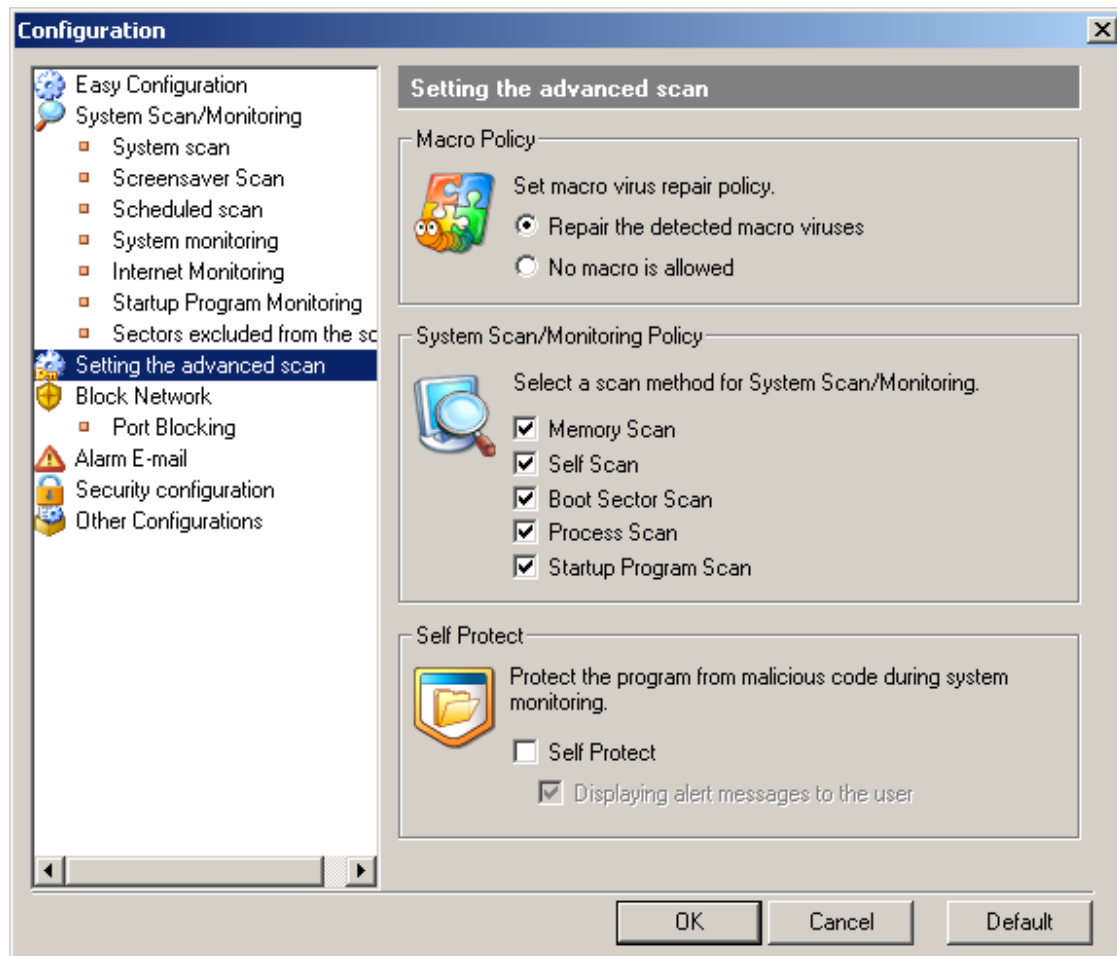
## Possible Harmful Programs

### System Scan

- Scan possible harmful programs : This feature runs a scan for possibly harmful programs which may not be actual viruses, but are programs that can potentially disclose the user's private information or can be interpreted and managed as actual viruses and thereby interfere with the user's tasks.
- Joke: A scan for programs that can be interpreted and managed as actual viruses and thereby interfere with the user's tasks.
- Key Logger: A scan for harmful programs that can disclose the user's private information, like social security or credit card numbers, by remote monitoring of keyboard strokes.
- Other: Scan for other possibly harmful programs.

## Setting the advanced scan

1. Open the **Configuration** window by selecting **Configuration** from the toolbar or from **Tools** on the menu bar. The Configuration window appears.



**Figure 30 Setting the advanced scan**

2. Select **Setting the advanced scan** from the left menu in the **Configuration** window.

### Macro Policy

Set the Macro Policy to prevent macro viruses from being applied to Office Protector Monitoring and System Scan.

- Repair the detected macro viruses: Repair the detected macro viruses in documents during operating Office Protector or System Scan.
- No macro is allowed: Blocks the use of macros when macro viruses are detected in documents during Office Protector or System Scan operation.

### System Scan/Monitoring Policy

Select sectors to scan every time the system is scanned.

- Memory Scan: Scans virus infected files and other malicious programs residing in the memory sectors.

- Self Scan; Scans the V3Net for Windows Server 6.0 program files before executing it.
- Boot Sector Scan: Scans Boot Sector
- Process Scan: Scans the currently running programs and back orifice programs.
- Startup Program Scan: Scans programs registered in the Startup program.

**Caution**

Infected files and malicious programs detected during a Memory Scan will be automatically repaired regardless of the scan settings in System Scan. That is, a malicious program which can cause virus infection in the memory sector is automatically terminated upon detection. Values set in System Scan/Monitoring will not be applied to **Explore Scan** or **Office Protector**.

## Self Protect

When System Monitoring is on, this feature monitors executable files consisting the V3Net for Windows Server 6.0 program and protects them from malicious programs.

**Caution**

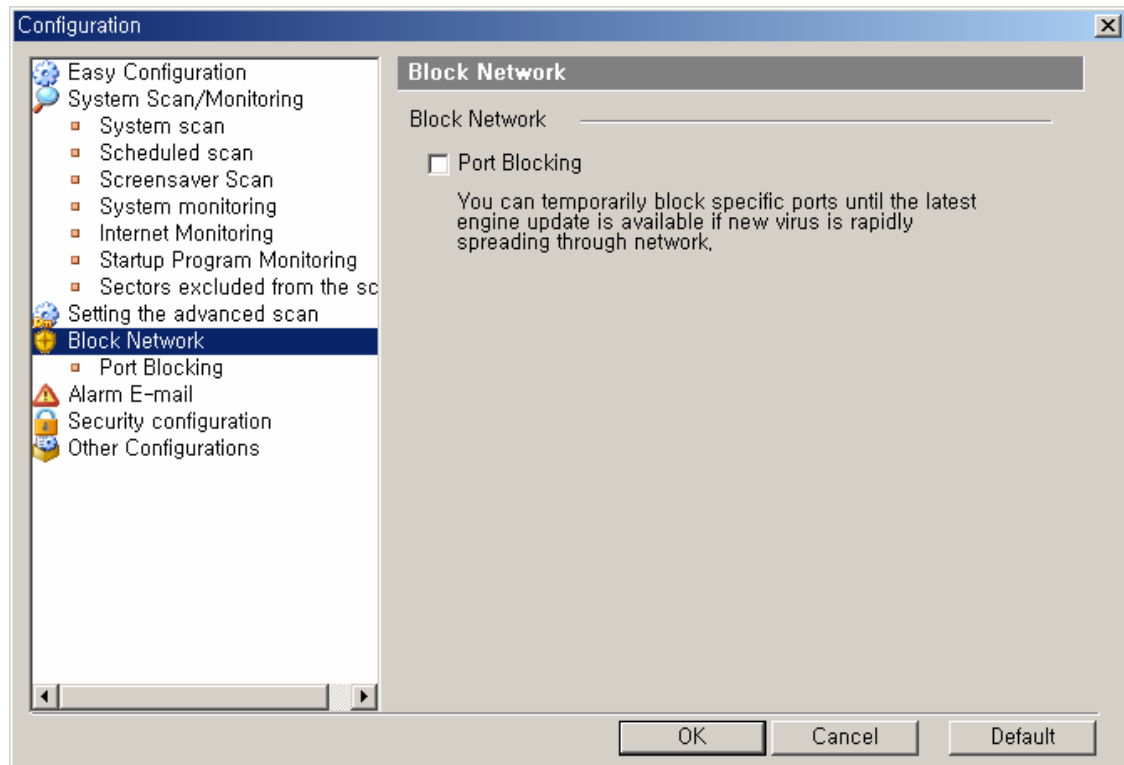
This function only operates when System Monitoring function is on.

### Displaying alert messages to the user

If suspicious processes access the V3Net for Windows Server 6.0 program files, an alert message will appear. For example, if someone attempts to view the file properties of a V3Net for Windows Server 6.0 configuration file, the Self Protect Function alert message will display.

## Block Network

1. Select Block Network from the left menu in the Configuration window.



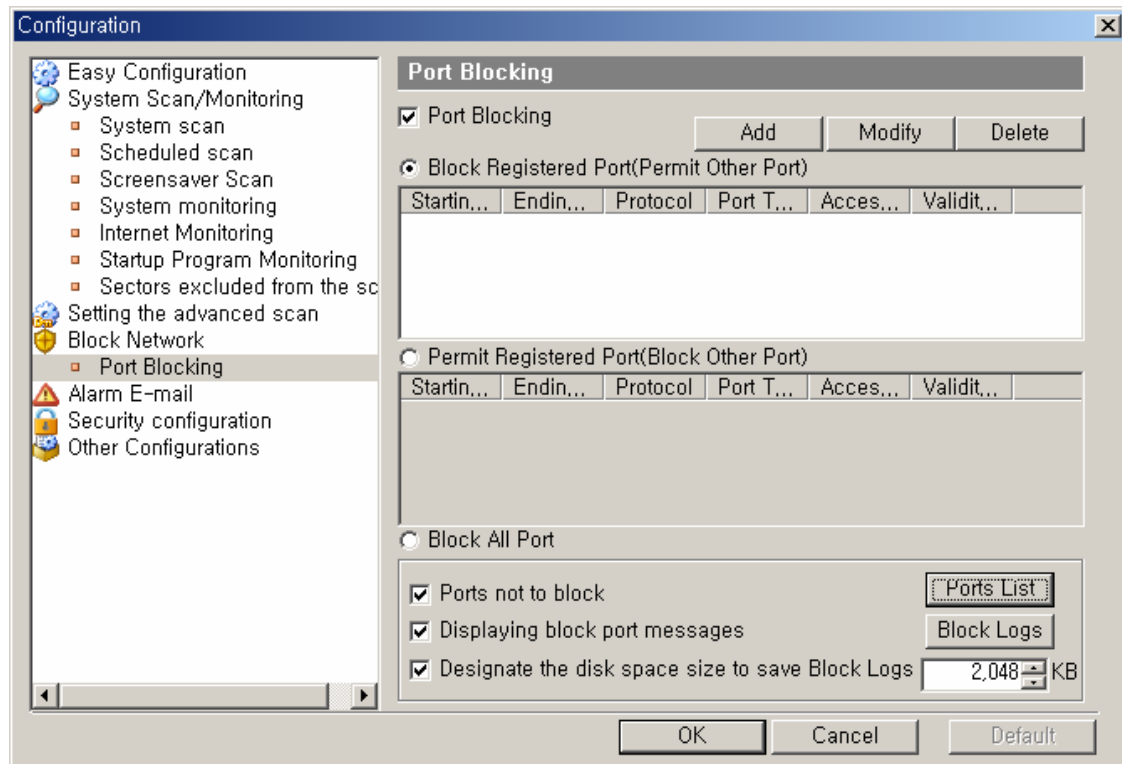
**Figure 31 Block Network**

2. Click Port **B**locking to begin the blocking of the selected ports. Ports cannot be blocked if this checkbox is not selected. Ports currently in use are also subject to the Port Blocking function. Therefore, this function should be used only when there is an imminent threat of network penetration by a new rapidly spreading virus.
3. Click **OK** after selecting Port Blocking. If you click **Default** to recover the initial settings.

## Ports Blocking

You can block registered ports and permit all others, or the other way round. When a virus is spreading rapidly, all networks can be block temporarily.

1. Select Block **Network > Port Blocking** from the left menu in the Configuration window.



**Figure 32 Ports Blocking**

2. Click **Port Blocking** on the top right screen to start the function. Ports cannot be blocked if this checkbox is not selected.

### Port Permission / Block settings

Only one of the following three options can be applied.

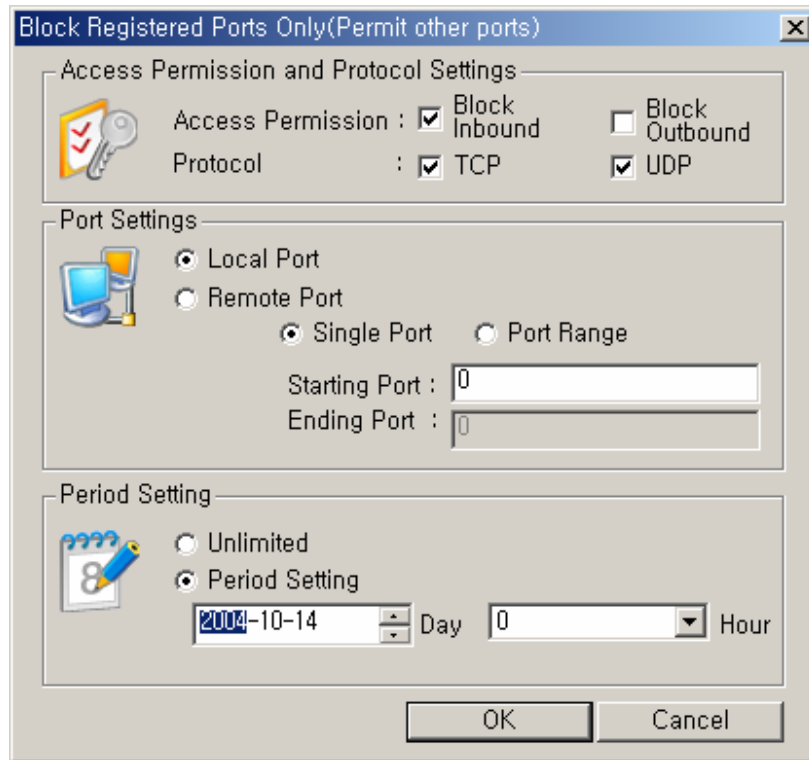
- Block registered port (Permit other port): Click Add on the top, to register ports to block. All other ports are permitted.
- Permit registered port (Block other port): Click Add on the top, to register ports to permit. All other ports are blocked.
- Block all port: All ports including the ones currently in use, are blocked. This can cause system errors. Therefore, select this option only when network traffic increases rapidly or a new virus is spreading rapidly.

#### **Caution**

When Block all port is selected, a warning window appears. All network connections are blocked, including the ones currently in use. It can cause system errors if the ports currently being used are blocked.

## Port Registering

1. Click **Add** on the top right and the Port **Blocking Configuration** window will display. Enter the proper information for the selected item to be blocked or permitted, then click **OK**.



**Figure 33 Port Registering**

### Access Permission and Protocol

One of the two options must be selected. Both can be selected at the same time.

- Process
  - Inbound
  - Outbound
- Protocol
  - TCP
  - UDP

### Port Settings

Either one of the two can be selected.

- Remote port
- Local Port

- Single Port
- Port Range
  - Starting Port
  - Ending Port

### Period Setting

- Unlimited: Registered ports are maintained as blocked or permitted.
  - Period Setting: Registered ports are blocked or selected only for set periods.
2. Click **OK** to confirm the port block settings. To modify the registered port information, double click the port or click Modify on the top. Click Delete to remove the registered port information. Use Ctrl or Shift keys to select multiple ports.

### Ports not to block

If Use the **Ports not to block** is selected and click **Ports List**, the following Ports list is activated, and the selected ports are always permitted. Ports on the list are those that should always be permitted for the normal operation of V3NET for Windows Server 6.0. If **Ports not to block** is not selected, the following list is not applied.

| Port Number | Protocol | Port Setting | Access permission | Description                                                                                                                                                                                                         |
|-------------|----------|--------------|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 80 ~ 83     | TCP      | Remote       | Outbound          | These ports should always be permitted for Windows Update and Smart Update to keep the engine updated to the latest version.                                                                                        |
| 443         | TCP      | Remote       | Outbound          |                                                                                                                                                                                                                     |
| 1080        | TCP      | Remote       | Outbound          |                                                                                                                                                                                                                     |
| 8080        | TCP      | Remote       | Outbound          |                                                                                                                                                                                                                     |
| 8088        | TCP      | Remote       | Outbound          |                                                                                                                                                                                                                     |
| 11523       | TCP      | Remote       | Outbound          |                                                                                                                                                                                                                     |
| 2869        | UDP      | Remote       | Outbound          | These ports should always be permitted for frequent Windows updates.                                                                                                                                                |
| 25          | TCP      | Remote       | Outbound          | These ports should always be permitted for sending Alarm E-mails to selected pre-set administrator accounts.                                                                                                        |
| 2186        | TCP      | Remote       | Outbound          | These ports should always be permitted for the AhnLab Policy Center, a centralized management security solution by AhnLab Inc.                                                                                      |
| 5465        | TCP      | Remote       | Outbound          |                                                                                                                                                                                                                     |
| 6063        | TCP      | Remote/Local | Inbound           |                                                                                                                                                                                                                     |
| 8951        | TCP      | Remote       | Outbound          | When computers with V3NET for Windows Server 6.0 installed are controlled by the AhnLab Policy Center, a centralized management security solution by AhnLab Inc., relevant ports must be set as items not to block. |
| 2191        | UDP      | Remote       | Outbound          |                                                                                                                                                                                                                     |
| 53          | TCP/UDP  | Remote       | Inbound           | These ports should always be permitted for DNS Server to get the IP Address.                                                                                                                                        |

## Block Logs

When this button on the right is clicked, a text file is displayed. The file list blocks ports by a time series.

## Displaying block port messages

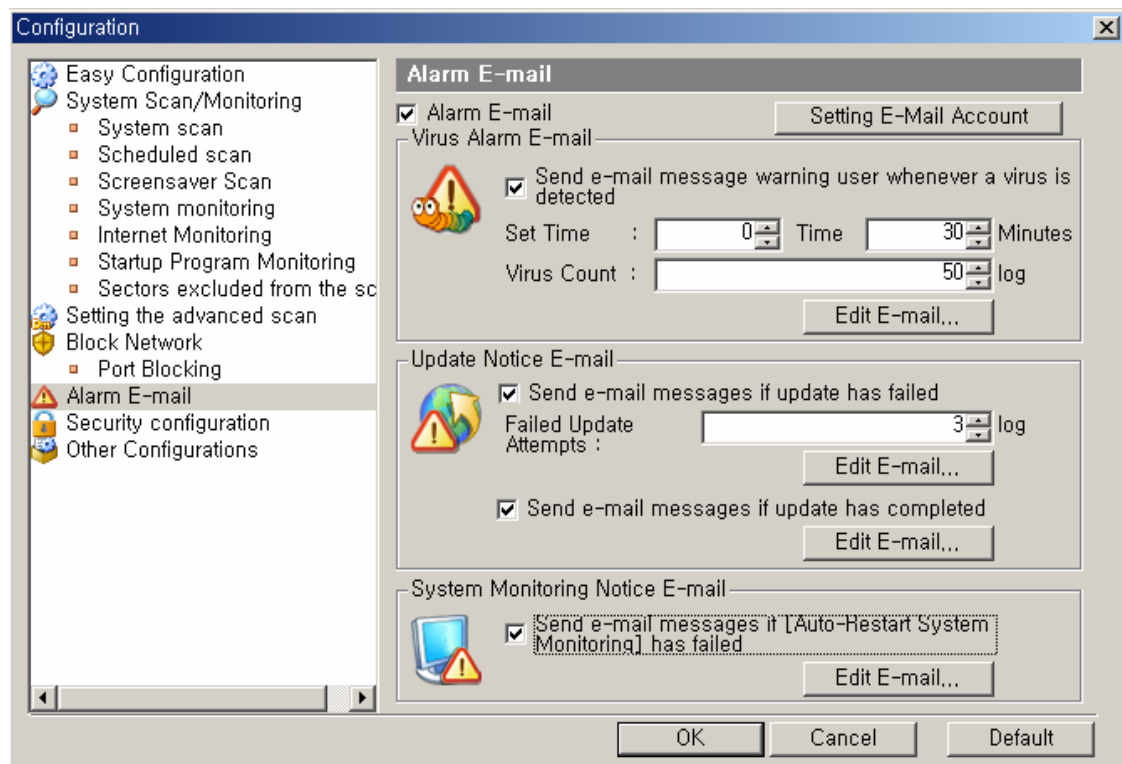
Every time a port is blocked, an event message appears on the task-bar.

## Designate the disk space size to save Port Block Logs

Up to 2048KB of port log can be saved. If the limit is exceeded, logs are deleted from the first to the last records.

## Alarm E-mail

1. Select **Alarm E-mail** from the left menu in the Configuration window.



**Figure 34 Alarm E-mail**

2. Click **Alarm E-mail** and **Creating an e-mail account** on the top right. The Creating an e-mail account window displays.

## E-mail Account Setting

3. Enter account information for the e-mail address that is used for alerts. Click **Setting Test** after entering the information, to check if the Alarm E-mail is correctly sent. Click **OK** to close the window.

**Creating an e-mail account**

Creating an e-mail account

Specify e-mail account information of administrator to receive notice messages.

**E-mail**

Recipient :

Sender :

**Server**

SMTP Server Address :

Mail Server Port :

Authentication Method :

**Login**

User Name :

Password :

Setting Test

OK Cancel

**Figure 35 E-mail Account Setting**

### E-mail

- Recipient: Enter the e-mail account of the administrator that will receive the Alarm E-mails.
- Sender: Enter the sender e-mail information.

### Server Information

- SMTP Server: Enter the SMTP mail server address to be used for sending Alarm E-mails.
- Mail server port: Enter the mail server port number to be used for sending Alarm E-mails. (Default is 25)
- Authentication method: Select the mail server authentication method to be used for sending Alarm E-mails.
- AUTH LOGIN: Login information activated.
  - User Name
  - Password

- LOGIN PLAIN: Login information activated.
  - User Name
  - Password

4. Select Alarm E-mail option and click **OK**.

### Virus Alarm E-mail

When the number of viruses found in a pre-set period exceeds the user-specified limit, an Alarm E-mail is sent to the registered administrator account.

- Send e-mail message to warn whenever a virus is detected.
- Set time: Default 30 minutes
- Virus found: Default 50

### Update Alarm E-mail

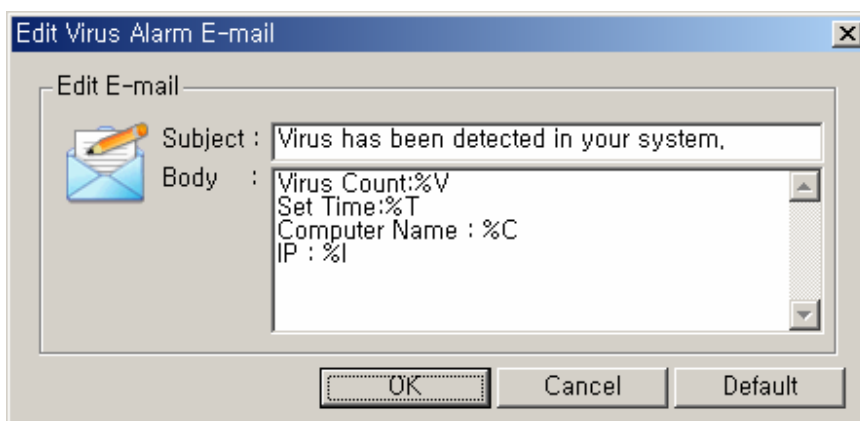
Alarm E-mail is sent to the registered administrator's account whenever an update is completed or has failed.

- Sending Alarm E-mail on an update failure
- Number of fails: Default 3
- Sending Alarm E-mail on update complete

### System Monitoring Alarm E-mail

Alarm E-mail is sent to the registered administrator's account whenever [Auto-Restart System Monitoring] has failed.

- Sends Alarm E-mail when [Auto-Restart System Monitoring] fails
5. Click **Edit Mail...** to open the mail editing window. The user can directly enter the mail subject and body.
- Subject line / Body / Computer Name / IP Address



**Figure 36 Edit Alarm E-mail**

## Security Setting

1. Open the **Configuration** window by selecting **Configuration** from the toolbar or from **Tools** on the menu bar. The Configuration window appears
2. Select **Security Setting** from the left menu in the **Configuration** window.

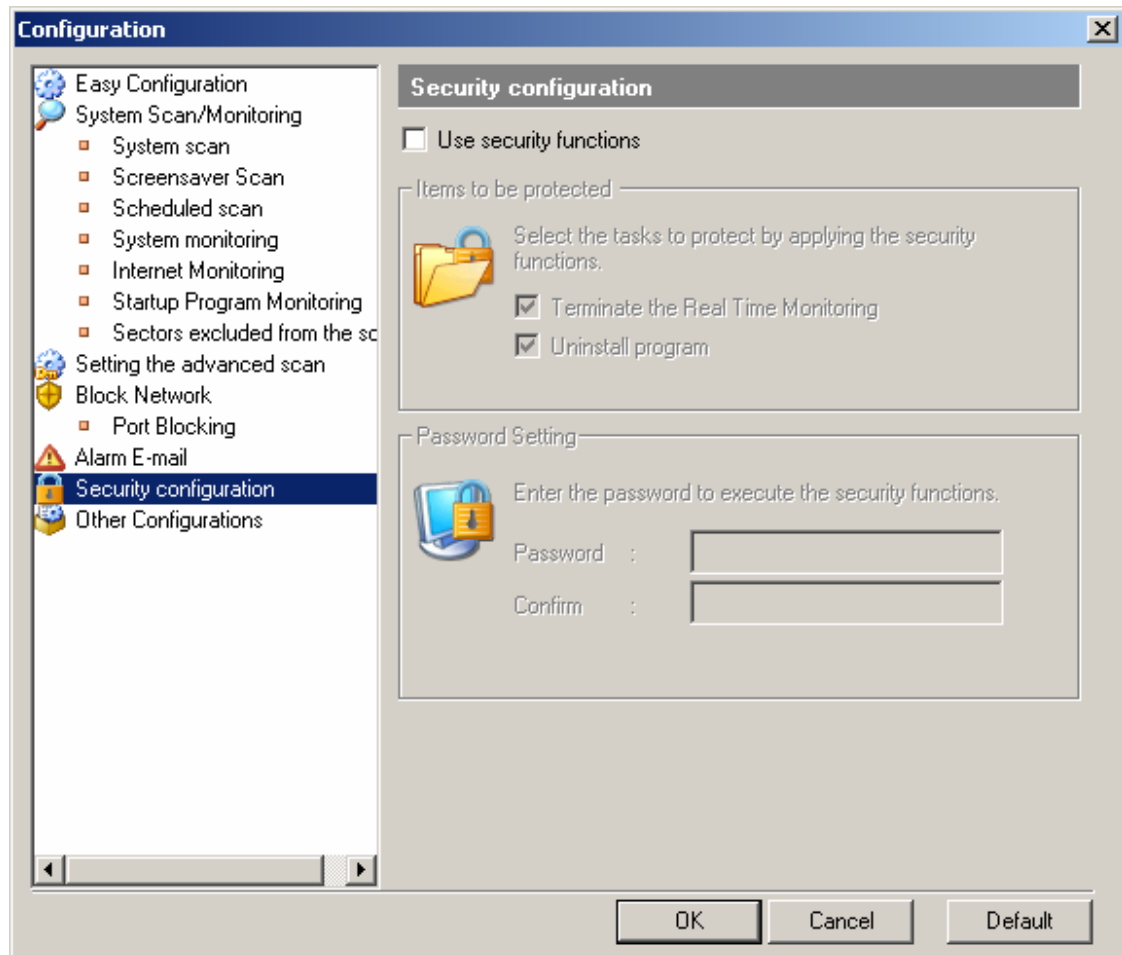


Figure 37 Security Setting

### Use security functions

If this function is enabled, only the authorized users with specified passwords can perform important tasks such as deleting the V3Net for Windows Server 6.0, system monitoring, or closing the system.

#### **Caution**

If you enter wrong password or do not enter password, you will not be allowed to perform the protected tasks.

## Items to be protected

Select the tasks to be protected by allowing only authorized users.

- Terminate the Real Time Monitoring: Closes Real Time Monitoring (Off).
- Uninstall program: Uninstalls the V3Net for Windows Server 6.0.

### Caution

Items protected and set in the program's configuration is applied regardless of the security levels (high, medium, low) set in the **Easy Configuration** feature. That is, even if you set the security level as **low**, the protection feature has priority over security levels.

## Password Setting

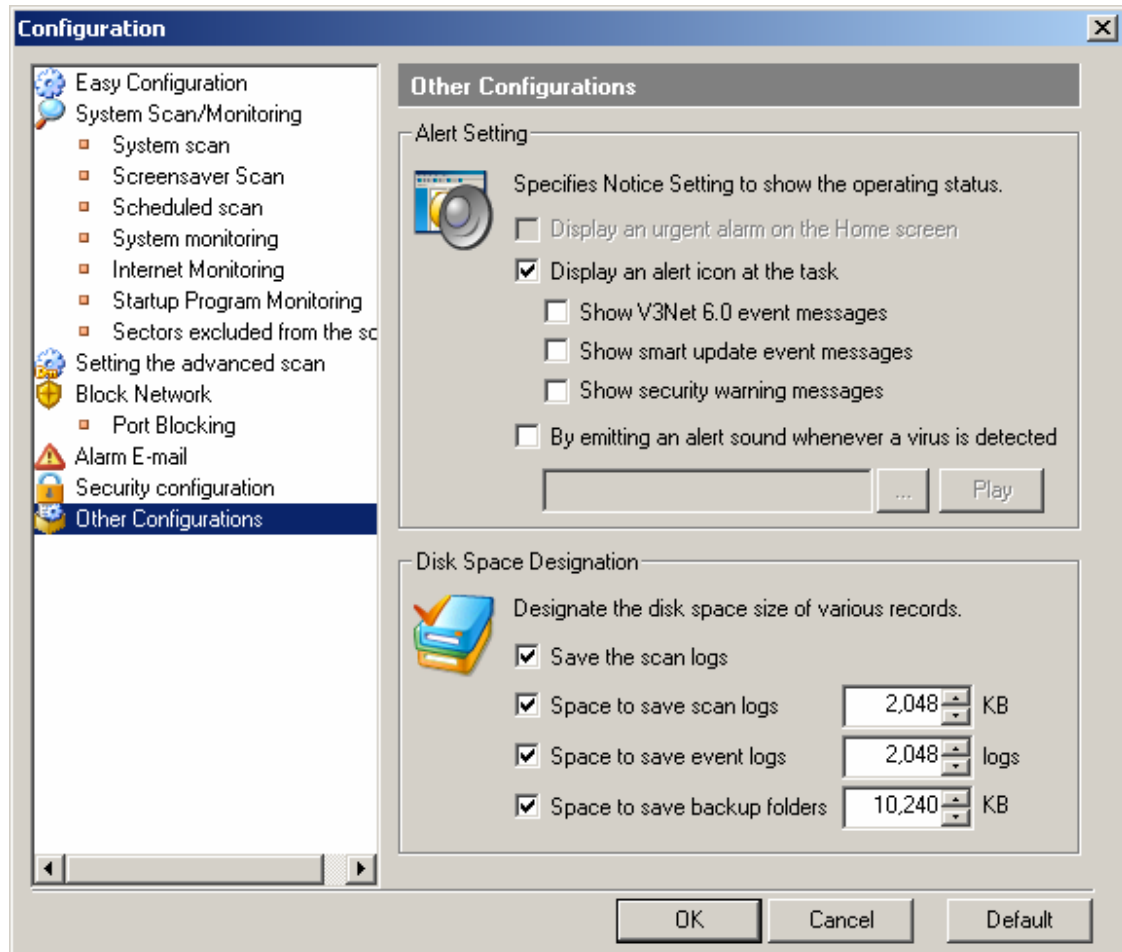
Enter passwords of users that can perform tasks classified as protected. Users without passwords cannot perform protected tasks.

### Caution

An error message will appear if you select the **Use Security Functions** icon and don't set a password. You must set a password to use the Security Function. If you forget your password, please contact the AhnLab Customer Support Center. The items set as **Items to be protected** will be protected, even if the system protection level (High, Medium and Low) in the **Configuration > Easy Configuration** is modified.

## Other Configurations

1. Open the **Configuration** window by selecting **Configuration** from the toolbar or from **Tools** on the menu bar. The Configuration window appears.
2. Select **Other Setting** from the left menu in the **Configuration** window.



**Figure 38 Other Configurations**

### Alert Setting

- Display an urgent alarm on the Home screen: Urgent Viruses Alert frame appears on the Home screen. It will disappear when this item is unselected.
- Display an alert icon at the task: Displays V3Net for Windows Server 6.0 alert icon in the system tray and keeps showing an error message like below until the user selects it.
  - Show V3Net for Windows Server 6.0 event messages: If important events occur such as engine update errors or virus detection, event messages are sent to alert the user.
  - Show smart update event messages: If a smart update error occurs, an event message is sent to alert the user.

- Show security warning messages: If a vulnerability is found on the user's system, a security alert message is sent to alert the user.
- By emitting an alert sound whenever a virus is detected.: Select an alert sound notifies the user that a virus is detected by clicking button and Click **Play** to listen specify a WAV file.

## Disk Space Designation

Save the scan logs: Saves virus scan/monitoring log by each date. Click **Scan Log** in the left menu to display.

- Space to save scan logs: Maximum size of scan log 512~4,194,303KB
- Space to save event logs : Maximum size of event log 512~4,194,303
- Space to save backup folders: Maximum size of file backup 512~4,194,303KB

## Index

### A

|                                          |    |
|------------------------------------------|----|
| Access Permission and Protocol.....      | 67 |
| Alarm E-mail.....                        | 8  |
| Alert icon menu on the system tray ..... | 26 |
| Alert Icon Toolbar .....                 | 41 |

### B

|                     |       |
|---------------------|-------|
| Block files .....   | 54    |
| Block Logs .....    | 69    |
| Block Network ..... | 8, 32 |

### C

|                                    |    |
|------------------------------------|----|
| Compressed files .....             | 61 |
| Customer Satisfaction Center ..... | 7  |
| Customer Support Service.....      | 7  |
| Customized List to Scan.....       | 24 |

### D

|                                                            |    |
|------------------------------------------------------------|----|
| Designate the disk space size to save Port Block Logs..... | 69 |
| Displaying block port messages .....                       | 69 |

### E

|                         |   |
|-------------------------|---|
| Easy Configuration..... | 8 |
|-------------------------|---|

|                        |    |
|------------------------|----|
| <b>Edit Mail</b> ..... | 71 |
|------------------------|----|

|                        |    |
|------------------------|----|
| Explorer Toolbar ..... | 40 |
|------------------------|----|

### F

|                          |    |
|--------------------------|----|
| File Types to Scan ..... | 60 |
|--------------------------|----|

### H

|            |    |
|------------|----|
| Home ..... | 26 |
|------------|----|

### I

|                          |        |
|--------------------------|--------|
| Internet Monitoring..... | 25, 45 |
|--------------------------|--------|

### M

|                    |    |
|--------------------|----|
| Macro Policy ..... | 63 |
|--------------------|----|

### O

|                        |    |
|------------------------|----|
| Office Protector ..... | 45 |
|------------------------|----|

### P

|                                        |    |
|----------------------------------------|----|
| Period Setting .....                   | 68 |
| Port Permission / Block settings ..... | 66 |
| Port Settings.....                     | 67 |
| Ports Blocking .....                   | 66 |
| Possible Harmful Programs .....        | 62 |
| Product Registration .....             | 7  |

### R

|                           |    |
|---------------------------|----|
| Registration Renewal..... | 7  |
| Restore backup files..... | 37 |

### S

|                                 |        |
|---------------------------------|--------|
| Scan Method.....                | 61     |
| <b>Scheduled Scan</b> .....     | 32     |
| Screen Saver Scan .....         | 45     |
| Server Information.....         | 70     |
| Startup Program Monitoring..... | 25, 45 |
| System Monitoring .....         | 25, 45 |

System Monitoring Alarm E-mail .....71

System Scan/Monitoring Policy .....63

## **U**

Update Alarm E-mail .....71

Updating through the shared folder on the  
network drive.....21

Updating through the Internet.....21

## **V**

Virus Alarm E-mail .....71