<table>
<thead>
<tr>
<th>Table of Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
</tr>
<tr>
<td>Copyright Notice</td>
</tr>
<tr>
<td>Limited Warranty</td>
</tr>
<tr>
<td>SonicWALL Network Anti-Virus</td>
</tr>
<tr>
<td>About this Guide</td>
</tr>
<tr>
<td>Guide Conventions</td>
</tr>
<tr>
<td>SonicWALL Technical Support</td>
</tr>
<tr>
<td>Activating SonicWALL Network Anti-Virus</td>
</tr>
<tr>
<td>mySonicWALL.com</td>
</tr>
<tr>
<td>Activating a Network Anti-Virus Subscription</td>
</tr>
<tr>
<td>Activating a Network Anti-Virus FREE TRIAL</td>
</tr>
<tr>
<td>Security Services&gt;Anti-Virus</td>
</tr>
<tr>
<td>Settings</td>
</tr>
<tr>
<td>Administration</td>
</tr>
<tr>
<td>Creating Reports</td>
</tr>
<tr>
<td>Adding, Editing, and Deleting a Group</td>
</tr>
<tr>
<td>Report Summary</td>
</tr>
<tr>
<td>System Detail Report</td>
</tr>
<tr>
<td>VirusScan ASaP Report Summary</td>
</tr>
<tr>
<td>System Search</td>
</tr>
<tr>
<td>Block Systems Search</td>
</tr>
<tr>
<td>Managing Licenses</td>
</tr>
<tr>
<td>Add/Renew Anti-Virus Subscription</td>
</tr>
<tr>
<td>Renewing the Current Subscription</td>
</tr>
<tr>
<td>Anti-Virus License Sharing</td>
</tr>
<tr>
<td>Configuring Anti-Virus Policies</td>
</tr>
<tr>
<td>Anti-Virus Enforcement</td>
</tr>
<tr>
<td>Enforcing Network Anti-Virus (SonicOS Enhanced)</td>
</tr>
<tr>
<td>Adding Network Anti-Virus Enforcement to a Zone</td>
</tr>
<tr>
<td>Network Anti-Virus E-Mail Filter</td>
</tr>
<tr>
<td>E-Mail Attachment Filtering</td>
</tr>
<tr>
<td>E-Mail Attachment Filtering Options</td>
</tr>
<tr>
<td>Warning Message Text</td>
</tr>
<tr>
<td>E-Mail Blocking</td>
</tr>
</tbody>
</table>
Security Services>Summary ................................................... 24
  Security Services Summary .................................................. 24
  Security Services Settings .................................................... 24
Installing the Network Anti-Virus Client .......................... 25
  System Requirements for SonicWALL Anti-Virus on Clients ...... 25
    Microsoft Windows Version Supported ................................. 25
    Supported Browsers .......................................................... 25
    Hard Disk Space ............................................................... 25
    System RAM ........................................................................ 25
    Network ................................................................................ 25
Installing on Windows 95/98/NT/XP/2000 computers .......... 26
Proxy Support ................................................................. 26
VirusScan ASaP Client User Information .......................... 27
  Testing VirusScan ASaP Client ............................................ 27
Advanced Menu for VirusScan ASaP Client ....................... 27
  Quarantine Viewer ............................................................. 27
  Enable/Disable VScan ........................................................ 28
  About VirusScan ASaP ....................................................... 28
Network Anti-Virus Tips and Troubleshooting ...................... 29
  Disabling Anti-Virus on Your Desktop ................................ 29
  Enabling Anti-Virus on Your Desktop ................................ 29
  Testing VirusScan ASaP ..................................................... 29
  Scheduling a Scan ............................................................. 29
  Quarantine Viewer Notes .................................................... 30
  Spool32 Error Message ...................................................... 30
    Problem ............................................................................. 30
    Solution ............................................................................... 30
  Missing or Disappearing System Tray Icon ......................... 31
  Cannot Listen on Port 6515 .................................................. 31
  Unable to Create Cabinet Installer Object ...................... 31
  Creating a Rescue Disk for Boot Sector Virus Repair .......... 32
  Online Reports are blank or missing charts .................... 32
  Can’t Find INX File to Execute ............................................ 33
  MyINX GPF Occurs When Installing VirusScan ASaP ....... 34
    Windows 98 and ME ...................................................... 34
  Cannot Connect to Update Server ....................................... 34
    Setting the Security Level ............................................... 35
    Restricted registry keys (Windows NT and 2000 only) ....... 35
  Cabinet Not Trusted Error .................................................. 36
Installation Declined .................................................................................. 36
  Windows NT or Windows 2000 ................................................................. 36
  Missing or Corrupt System File ................................................................. 37
  Outdated Version of myAgtInstall.exe ...................................................... 37
WebScan Service Running on the Proxy Server .............................. 38
  Missing or Corrupted REGSVR32.exe File .............................................. 38
  Unrestricted Windows NT 4.x, Windows 2000, All Windows9x, and ME ... 38
  REGEDIT Program Missing ...................................................................... 38
Computers Not Displayed on Reports ......................................... 39
  Windows NT 4.x or Windows 2000 .............................................................. 39
  Windows 9x or Windows ME ...................................................................... 39
  All operating systems ............................................................................... 40
VirusScan ASaP Installation Error: 0x80004005, myINX Script: .... 41
  INI file not found. .............................................................................. 41
  Solutions .................................................................................................. 41
  Removing McAfee VirusScan from Microsoft Plus! 98 ....................... 42
Excluding Files and Folders from Virus Scanning ....................... 42
Preface

Copyright Notice

© 2003 SonicWALL, Inc. All rights reserved.

Under the copyright laws, this manual or the software described within, can not be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

SonicWALL is a registered trademark of SonicWALL, Inc.

Other product and company names mentioned herein can be trademarks and/or registered trademarks of their respective companies.

Specifications and descriptions subject to change without notice.

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers’ entire liability and Customer’s sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL’s discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL’s obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL’s then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.
DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers’ liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.
SonicWALL Network Anti-Virus

SonicWALL Network Anti-Virus is a distributed, gateway-enforced solution that ensures always-on, always-updated anti-virus software for every client on your network. The SonicWALL constantly monitors the version of the virus definition file and automatically triggers download and installation of new virus definition files to each user’s computer. In addition, the SonicWALL restricts each user’s access to the Internet until they are protected, therefore acting as an automatic enforcer of the company’s virus protection policy. This new approach ensures the most current version of the virus definition file is installed and active on each PC on the network, preventing a rogue user from disabling the virus protection and potentially exposing the entire organization to an outbreak. And most importantly, SonicWALL Network Anti-Virus offloads the costly and time-consuming burden of maintaining and updating anti-virus software across the entire network. SonicWALL Network Anti-Virus also includes Network Anti-Virus E-Mail Filter to selectively manage inbound E-mail attachments as they pass through the SonicWALL to control the flow of executable files, scripts, and applications into your network.

⚠️ Alert! You must purchase an Anti-Virus subscription to enforce Anti-Virus through the SonicWALL. Log into your mySonicWALL.com account for more information or contact your reseller.
About this Guide

Welcome to the SonicWALL Network Anti-Virus Administrator’s Guide. This manual provides the information you need to successfully activate, configure, and administer SonicWALL Network Anti-Virus on SonicWALL Internet Security Appliances running SonicOS Enhanced 2.0.0.0 or higher. The audience for this guide is administrators who are concerned with enforcement of Anti-Virus policies to improve protection of their networks. You should be familiar with the features, functions, and operating characteristics of SonicWALL Internet Security Appliances.

Guide Conventions

Conventions used in this guide are as follows:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bold</td>
<td>Highlights items you can select on the SonicWALL Management Interface.</td>
</tr>
<tr>
<td><em>Italic</em></td>
<td>Highlights a value to enter into a field. For example, “type 192.168.168.168 in the <em>IP Address</em> field.”</td>
</tr>
<tr>
<td><em>Menu Item&gt;Menu Item</em></td>
<td>Indicates a multiple step Management Interface menu choice. For example, “<em>Security Services&gt;Content Filter</em> means select Security Services, then select Content Filter.</td>
</tr>
</tbody>
</table>

Icons Used in this Guide

These special messages refer to noteworthy information, and include a symbol for quick identification:

*Alert!* Important information that cautions about features affecting firewall performance, security features, or causing potential problems with your SonicWALL.

*Tip!* Useful information about security features and configurations on your SonicWALL.

*Note:* Important information on a feature that requires callout for special attention.
SonicWALL Technical Support

For timely resolution of technical support questions, visit SonicWALL on the Internet at <http://www.sonicwall.com/services/support.html>. Resources are available to help you resolve most technical issues or contact SonicWALL Technical Support.

Phone: (408) 745-9600
Fax: (408) 745-9300
Web: http://www.sonicwall.com
E-mail: sales@sonicwall.com
Activating SonicWALL Network Anti-Virus

If you don’t have SonicWALL Network Anti-Virus activated on your SonicWALL, you must purchase SonicWALL Network Anti-Virus from a SonicWALL reseller or your mySonicWALL.com account (limited to customers in the USA and Canada). If SonicWALL Network Anti-Virus isn’t activated on your SonicWALL, the Security Services>Anti-Virus page displays the Anti-Virus Upgrade page that provides links to activate the Network Anti-Virus subscription or get a free trial of Network Anti-Virus.

To activate SonicWALL Network Anti-Virus from your SonicWALL, you need the following:

- Your SonicWALL must be registered on mySonicWALL.com.
- You must have an Activation Key or purchased the Network Anti-Virus subscription on mySonicWALL.com.

If you have activated the Network Anti-Virus subscription, the Security Services>Anti-Virus page displays the settings for configuring the service.

mySonicWALL.com

mySonicWALL.com delivers a convenient, one-stop resource for registration, activation, and management of your SonicWALL products and services. Your mySonicWALL.com account provides a single profile to do the following:

- Register your SonicWALL Internet Security Appliances
- Purchase/Activate SonicWALL Security Services and Upgrades
- Receive SonicWALL firmware and security service updates and alerts
- Manage (change or delete) your SonicWALL security services
- Access SonicWALL Technical Support

Creating a mySonicWALL.com account is easy and free. Simply complete an online registration form. Once your account is created, you can register SonicWALL Internet Security Appliances and activate any SonicWALL Security Services associated with the SonicWALL.

Your mySonicWALL.com account is accessible from any Internet connection with a Web browser using the HTTPS (Hypertext Transfer Protocol Secure) protocol to protect your sensitive information. You can also access mySonicWALL.com license and registration services directly from the SonicWALL management interface for increased ease of use and simplified services activation.

If you activated SonicWALL Network Anti-Virus at mySonicWALL.com, the activation is automatically enabled on your SonicWALL within 24-hours or you can click the Synchronize button on the Security Services>Summary page to update your SonicWALL.
Activating a Network Anti-Virus Subscription

If you have an Activation Key for Network Anti-Virus, follow these steps to activate SonicWALL Network Anti-Virus:

1. Click the SonicWALL Network Anti-Virus Subscription link. The mySonicWALL.com Login page is displayed.

2. Enter your mySonicWALL.com account username and password in the User Name and Password fields, then click Submit. The System>Licenses page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the System>Licenses page appears after you click the Network Anti-Virus link.

3. Click Activate or Renew in the Manage Service column in the Manage Services Online table. Type in the Activation Key in the New License Key field and click Submit. Your SonicWALL Network Anti-Virus subscription is activated on your SonicWALL.

Activating a Network Anti-Virus FREE TRIAL

You can try a FREE TRIAL of SonicWALL Network Anti-Virus by following these steps:

1. Click the FREE TRIAL link. The mySonicWALL.com Login page is displayed.

2. Enter your mySonicWALL.com account username and password in the User Name and Password fields, then click Submit. The System>Licenses page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the System>Licenses page appears after you click the FREE TRIAL link.

3. Click FREE TRIAL in the Manage Service column in the Manage Services Online table. Your SonicWALL Network Anti-Virus trial subscription is activated on your SonicWALL.
Security Services>Anti-Virus

The Security Services>Anti-Virus page includes the settings for managing Network Anti-Virus on the SonicWALL.

**Alert!** If you are using SonicWALL Network Anti-Virus on a SonicWALL running SonicOS Enhanced, you must enable SonicWALL CFS Standard on each Zone in the Network>Zones page. See “Enforcing Network Anti-Virus (SonicOS Enhanced)” on page 21 for more information.

**Settings**

The Settings section of the Security Services>Anti-Virus page displays the following information:

- **Number of Anti-Virus Licenses** - Displays the number of anti-virus licenses that have been registered to the SonicWALL.
- **Expiration Date** - Displays the expiration date of the current subscription.

**Tip!** Each anti-virus license allows the use of SonicWALL Network Anti-Virus on one computer.

**Administration**

The Administration section provides links to Create Reports summarizing Anti-Virus activity on the network, Manage Licenses for managing your client licenses, and Configure for configuring your Network Anti-Virus policy.
Creating Reports

To view Network Anti-Virus statistics and reports, click the Create Report link. The Group Administration page is displayed with settings for adding and managing groups, as well as overview reports on the status of your groups, including the number of managed desktops, the number of outdated desktops, and the status of viruses cleaned, deleted or quarantined.

![Group Administration Page]

The default Unassigned and All Machines groups listed in the table cannot be edited or deleted. All Machines is the total of machines in any group and the Unassigned group. The Unassigned group contains any newly added machines or machine not added to a group.

Adding, Editing, and Deleting a Group

You add additional groups that don’t exist in your current profile by entering a group name in the Add New Group field and clicking Add Group. For example, you may want to define a new group for Engineering, Marketing, or Sales.

To delete a group, click Delete in the Delete Group column.

To edit the group name, click Edit Name in the Edit Group Name column.
Clicking the List link for a group displays the Report Summary page, which displays all the computers in the group.
System Detail Report

Clicking on a computer name link in the System Name column in the Report Summary page displays the System Detail Report, which displays virus information for the specific computer.
VirusScan ASaP Report Summary

Clicking the Chart link the VirusScan ASaP Report Summary page that displays charts for Viruses Found, Most Common Viruses, and Most Infected Computers. You can select a report period (Last 7 Days, Last 30 Days, Last 60 Days, or All) from the Select Report Period menu.

Clicking on a virus name link under Most Common Viruses displays information about the virus. Clicking on a machine link listed in Most Infected Computers displays a System Detail Report for the specific computer. You can select a report period (Last 7 Days, Last 30 Days, Last 60 Days, or All) from the Select Report Period menu.
System Search

Clicking on System Search in the Group Administration page displays the System Search page for locating a desktop or desktops within your managed environment. Enter one character or more, query by choosing System Name or Email Address from the Search systems where menu, and then click Search.
Block Systems Search

The Block System(s) link displays the System Block Search page to locate and block unidentified desktops from your managed service. Using the search function, enter one character or more and query via System Name or E-Mail Address. Alternatively, you can scroll through your All Machines Summary list and check the unidentified desktops to block.
Managing Licenses

To manage your Network Anti-Virus licenses, click the link labeled Manage Licenses on the Anti-Virus> Settings page. The mySonicWALL.com Login page is displayed. Type your mySonicWALL username and password in the User Name and Password, and then click Submit. The System>Licenses page is displayed.

Add/Renew Anti-Virus Subscription

The SonicWALL Network Anti-Virus subscription can be used to activate Network Anti-Virus, increase the number of Anti-Virus licenses, or renew the current subscription. Additional Network Anti-Virus activation keys are required to add or renew Network Anti-Virus licences.

1. Click Renew in the Anti-Virus line of the Licenses>Summary table.

2. Type the New License Key in the New License Key field. Multiple keys may be required. For example, if you have 30 computers on your network, and you purchased three 10-user subscription, then you enter three activation keys.

3. Click Submit. The operation takes a few seconds to complete. Once completed, the new number of Anti-Virus licenses appears in the Licenses>Summary table.

Alert! When adding licenses, a new subscription is granted with a single new number of licenses and a single expiration date. Multiple grants are not tracked. The time remaining on the previous subscription is combined with the new 12 or 24 month period of the additional grant to create a single subscription.
Renewing the Current Subscription

A Subscription Renewal is the process of renewing the existing Network Anti-Virus subscriptions and the number of Network Anti-Virus licenses does not increase. If the current subscription has 10 users, a 10-user renewal extends the subscription period by one year, but the total number of users remains the same. The purchase of a Network Anti-Virus activation keys is necessary to renew a current license.

Tip! When renewing a Network Anti-Virus subscription, the number of licenses for subscription renewal must be equal to or greater than the number of licenses in the current subscription.

To renew the current subscription, complete the following steps:

1. Click Renew in the Anti-Virus line of the Summary table.

2. Type the Activation Key in the New License Key field. Multiple keys can be required for activation. The number of licenses for renewal must equal the number of existing licenses to renew your subscription.

3. Click Submit. The operation takes a few seconds to complete. Once completed, the new expiration date appears in the Settings section of Security Services>Anti-Virus and the Security Services>Summary page.
Anti-Virus License Sharing

Network Anti-Virus License Sharing allows you to distribute Anti-Virus licenses among multiple firewalls. License sharing assigns a License Sharing Group (LSG) to a SonicWALL from which this feature is activated. You can then add other SonicWALLs to the LSG, by their serial numbers and assign them Network Anti-Virus licenses from the pool of remaining available licenses in the LSG.

To set up a License Sharing Group, follow the directions below:

1. In the Security Services>Anti-Virus page, click Manage Licenses. The mySonicWALL Login page is displayed.

2. Enter your mySonicWALL.com account username and password in the User Name and Password fields, then click Submit. The System>Licenses page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the System>Licenses page appears after you click the Network Anti-Virus link.

3. Click Share in the Manage Service column for Network Anti-Virus in the Manage Services Online table.

4. Click the Share button.

5. Type the serial number of the SonicWALL that you want to share Network Anti-Virus licenses from in the Please enter serial number of the appliance, you want to add to your License Sharing Group field.

6. Click Submit. The SonicWALL is added as the Group Creator to the License Sharing Group.
Tip! The SonicWALL appliance must be registered at <http://www.mysonicwall.com> before it can be added to the License Sharing Group.

7. To add a SonicWALL that you want to distribute Network Anti-Virus licenses, enter the SonicWALL serial number in the Appliance SN field and click Add. The SonicWALL is added to the License Sharing Group.

8. To distribute licenses between the SonicWALLs, type the number of licenses you want to share for the second SonicWALL into the Licenses field, and click Update. Repeat for each SonicWALL appliance. The distributed number of Network Anti-Virus licenses is displayed for each SonicWALL.

Alert! SonicWALLs with currently active Network Anti-Virus subscriptions cannot be added to the License Sharing Group. To share previously activated Network Anti-Virus licenses among multiple SonicWALLs, contact SonicWALL technical support.

You can also remove a SonicWALL appliance or redistribute the number of licenses between the SonicWALL appliances. To remove a SonicWALL appliance, click Remove next to the SonicWALL serial number. To redistribute licenses, type the new number of licenses into the License field and click Update. Repeat for each SonicWALL appliance. The License Availability information changes as you change the license distribution or add more SonicWALLs.
Configuring Anti-Virus Policies

To configure Anti-Virus Policies, click Configure in the Anti-Virus page.

The following features are available in the Anti-Virus Policies section:

- **Disable policing from Trusted to Public** - Unchecked, this option enforces anti-virus policies on computers located on Trusted Zones. Choosing this option allows computers on the LAN to access computers on the DMZ, even if anti-virus software is not installed on the LAN computers.

- **Days before forcing update** - This feature defines the maximum number of days may access the Internet before the SonicWALL requires the latest virus date files to be downloaded.

- **Force Update on alert** - SonicWALL, Inc. broadcasts virus alerts to all SonicWALL appliances with an Anti-Virus subscription. Three levels of alerts are available, and you may select more than one. When an alert is received with this option selected, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the Days before forcing update selection.

In addition, every virus alert is logged, and an alert message is sent to the administrator. Please refer to the Logging and Alerts section of the SonicWALL Administrator’s Guide for instructions on configuring log and E-mail alerts.

- **Low Risk** - A virus that is not reported in the field and is considered unlikely to be found in the field in the future has a low risk. Even if such a virus includes a very serious or unforeseeable damage payload, its risk is still low.

- **Medium Risk** - If a virus is found in the field, and if it uses a less common infection mechanism, it is considered to be medium risk. If its prevalence stays low and its payload is not serious, it can be downgraded to a low risk. Similarly it can be upgraded to high risk if the virus becomes more and more widespread.
- **High Risk** - To be assigned a high risk rating, it is necessary that a virus is reported frequently in the field. Additionally, the payload must have the ability to cause at least some serious damage. If it causes very serious or unforeseeable damage, high risk may be assigned even with a lower level of prevalence.

**Anti-Virus Enforcement**

SonicWALL Network Anti-Virus currently supports Windows 95, 98, NT, XP, and 2000 platforms. In order to access the Internet, computers with other operating systems must be exempt from Anti-Virus policies. To ensure full network protection from virus attacks, it is recommended that only servers and unsupported machines are excluded from protection, and that third party Anti-Virus software is installed on each machine before excluding that machine from Anti-Virus enforcement. There are three options for defining exempt computers:

- **Enforce Anti-Virus policies for all computers** - Selecting this option forces computers to install VirusScan ASaP in order to access the Internet or the DMZ. This is the default configuration.
- **Include specified address range in the Anti-Virus enforcement** - Choosing this option allows the administrator to define ranges of IP addresses to receive Anti-Virus enforcement. If you select this option, specify a range of IP addresses to be enforced. Any computer requiring enforcement needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered for enforcement.
- **Exclude specified address range in the Anti-Virus enforcement** - Selecting this option allows the administrator to define ranges of IP addresses that are exempt from Anti-Virus enforcement. If you select this option, specify the range of IP addresses are exempt. Any computer requiring unrestricted Internet access needs a static IP address within the specified range of IP addresses. Up to 64 IP address ranges can be entered.
Enforcing Network Anti-Virus (SonicOS Enhanced)

If your SonicWALL is running SonicOS Enhanced, you can enforce Network Anti-Virus by Zones. A Zone is a logical grouping of one or more interfaces designed to make management, such as the definition and application of Access Rules a simpler and more intuitive process than following strict physical interface scheme. There are four fixed Zone types: **Trusted**, **Untrusted**, **Public**, and **Encrypted**. You can choose to enforce or not enforce Network Anti-Virus on multiple interfaces in the same **Trusted** or **Public** Zones.

**Note:** See the *SonicOS Enhanced Administrator’s Guide* for more information on Zones and configuring Zones in SonicOS Enhanced.

Adding Network Anti-Virus Enforcement to a Zone

To enforce Network Anti-Virus to an existing or new Zone, follow these instructions:

1. Select the **Network>Zones** page.
2. For a new Zone, click the **Add** button. In the **Add Zone** dialog box, select **Enforce Anti-Virus Service** to enforce Network Anti-Virus on multiple interfaces in the same LAN or DMZ Zones.
3. For an existing Zone, click the **Notepad** icon. In the **Edit Zone** dialog box, select **Enforce Anti-Virus Service** to enforce Network Anti-Virus on multiple interfaces in the same LAN or DMZ Zones.

If Network Anti-Virus is enforced for a Zone, a green check mark is displayed in the **Anti-Virus** column of the **Zone Settings** table.
Network Anti-Virus E-Mail Filter

The Network Anti-Virus E-Mail Filter allows the administrator to selectively delete or disable inbound E-mail attachments as they pass through the SonicWALL. This feature provides control over executable files and scripts, and applications sent as E-mail attachments. This feature is available only with the purchase of an E-mail Filter subscription. Click Anti-Virus on the left side of the browser window, and then click E-Mail Filter.

E-Mail Attachment Filtering

The E-mail Attachment Filtering section configures the file extensions that are filtered by the SonicWALL.

- **Enable Rapid E-Mail Attachment Filtering** - Select this feature to automatically block the most prevalent e-mail viruses on the current Rapid E-mail Attachment Block List.

- **Enable E-Mail Attachment Filtering of Forbidden File Extensions** - Select this check box to filter E-mail attachments. Click Add. In the Add Forbidden File Extension, type the file extensions to be filtered in the File Extension field. Hackers commonly spread viruses through Visual Basic and Windows Executable files, therefore "vbs" and "exe" are provided as default extensions for this feature. To add a file extension to the list, type the file extension in the File Extension field and click OK. To delete a file extension, select the file extension from the list, and click Delete.
E-Mail Attachment Filtering Options

In this section, the administrator chooses the action that the SonicWALL performs when filtering E-mail attachments. The attached file can either be deleted or it can be disabled by altering the file extension. In either case, the original E-mail text is still sent to the intended recipient.

- **Disable Forbidden File by altering the file extension and attach warning text** - Select this option to disable forbidden attachment files as they pass through the SonicWALL and include a warning message created in the **Warning Message Text** field. The SonicWALL replaces the third character of file extensions with "_". If the E-mail attachment is a valid file, the E-mail recipient may return the attachment to its original file extension without damaging the file.

- **Delete Forbidden File and attach warning text** - Select this option to delete forbidden attachment files as they pass through the SonicWALL and include a warning message created in the **Warning Message Text** field.

**Warning Message Text**

This is a warning message that can be customized and added to E-mails filtered by the **Network Anti-Virus E-mail Filter**. Type the desired warning message in the **Warning Message Text** box. Up to 256 alphanumeric characters may be entered. When you have configured the **E-mail Filter** settings, click **Update**. Once the SonicWALL has been updated, a message confirming the update is displayed at the bottom of the browser window.

**E-Mail Blocking**

Select **Block SMTP E-Mail Fragments (Content-Type: message\partial)** to enable blocking of partial e-mail messages. E-mail fragments are e-mail messages with the MIME Content-Type: message/partial in the header. Partial e-mails can be a security threat by allowing viruses to escape undetected by virus scanners because they are fragmented. The virus becomes fully functional once reassembled on the client.
Security Services>Summary

The Security Services>Summary page provides a status listing of Security Services currently activated on your SonicWALL or available for activation.

Security Services Summary

A list of currently available services through mySonicWALL.com is displayed in the Security Services Summary table. Subscribed services are displayed with Licensed in the Status column. If the service is limited to a number of users, the number is displayed in the Count column. The service expiration date is displayed in the Expiration column.

Security Services Settings

- **Reduce Anti-Virus and E-mail Filter traffic for ISDN connections** - Selecting this feature enables the SonicWALL Anti-Virus to only check daily (every 24 hours) for updates and reduces the frequency of outbound traffic for users who do not have an “always on” Internet connection.
- **Synchronize** - Click Synchronize to update the licensing and subscription information on the SonicWALL.
Installing the Network Anti-Virus Client

After installing, configuring and enabling the SonicWALL Network Anti-Virus subscription, each computer designated for virus protection begins the automated installation of VirusScan ASaP. VirusScan ASaP is an Internet-based, managed anti-virus service. It is based on Network Associates’ myCIO.com VirusScan ASaP technology and provides continuous protection of the entire desktop environment against viruses.

In most cases, VirusScan ASaP automatically removes other anti-virus products and their components.

⚠️ **Alert!** Do not install the Anti-Virus Client software on a network server. Forcing the installation of Anti-Virus Client software on a network server may interfere with server processes and is not recommended or supported.

System Requirements for SonicWALL Anti-Virus on Clients

**Microsoft Windows Version Supported**

Windows 95, Windows 98, Windows 98 SE, Windows ME, Window NT 4.0 Workstation (SP 6 or later), Windows 2000 Professional (SP2 or later), Windows XP Home or Professional.

**Supported Browsers**

Microsoft Internet Explorer 5.5 with Service Pack 2 or later. Netscape Communicator 4.6 or later. Other browsers can be used on your computer but Internet Explorer is required for installation.

**Hard Disk Space**

VirusScan ASaP requires 7 MB of hard disk space over the requirements of Windows for a swap file. Windows generally needs twice as much free space as the amount of RAM for the swap file. A Windows 9x operating system with 32 MB of system RAM requires 64 MB free to operate properly and 7 additional MB for VirusScan ASaP.

**System RAM**

Minimum 32 MB for Windows 9x and Windows NT 4.x

64 MB or higher is recommended.

Minimum 64 MB for Windows 2000

128 MB or higher is recommended.

**Network**

SonicWALL Network Anti-Virus is designed to be a Web-based application and requires an Internet connection to install and update the software. Even though Rumor Technology shares updates, every computer using VirusScan ASaP must be able to connect to the Internet and access McAfee.com Web site to start the update process.

VirusScan ASaP only supports anonymous or Windows NT authentication proxies. Port 80 on your firewall must be open for outbound traffic to allow VirusScan ASaP updates.
Rumor technology functions entirely on the local area network (LAN). Port 6515 must be open on the proxy but can be closed on the firewall. Any network applications operating on the client computer that open port 6515 causes that node to malfunction as a Rumor server and also prevent other nodes from updating using Rumor. Also, any network applications running on the client server that open port 1967 causes the node to malfunction as a Rumor server or client.

Installing on Windows 95/98/NT/XP/2000 computers

When the Network Anti-Virus is enabled, all computers on the network are automatically redirected to an Upgrade Required page. The user clicks on the link to access the pages required for installation of the application. If Netscape is being used as the browser, the user is prompted to first install a plug-in that allows the VirusScan service to operate. After loading the plug-in, the following screen appears.

Type your e-mail address in the **E-mail Address** field and click **Continue** to begin the VirusScan ASaP installation. After restarting the computer, Internet access is allowed.

For some configurations of Windows NT and Windows 2000 workstations, the installation is slightly different, especially if the user does not have administrative or software installation privileges on the computer. Before the installation of VirusScan ASaP, an executable must be run on each workstation that allows VirusScan ASaP to be installed. This file can be downloaded from <ftp://ftp.sonicwall.com/pub/software/> and is called myCIOAgtInstall.exe. This allows users without administrative rights to install VirusScan ASaP.

This file can be installed either locally or with various distribution products, such as Microsoft SMS, or Tivoli. The myCIOAgtInstall.exe file can be launched from a logon script, but it must be executed by a user with local administrator privileges. Once this application has been executed, the user can proceed with the installation. The following is a summary of the actions required to load VirusScan ASaP on an NT or 2000 workstation where the user does not have local access:

1. Download the executable file called MyCIOAgtInstall.exe.
2. Run MyCIOAgtInstall.exe on the workstation.
3. Proceed with normal installation.

Alternatively, local administrator privileges can be granted to users, allowing full access to VirusScan ASaP downloads. Consult Microsoft documentation for the operating system in use for this procedure.

Proxy Support

Proxy authentication support is limited to anonymous and Windows NT challenge/response authentication. Basic authentication is not supported at this time. It is recommended that the HTTP proxy port be configured to port 80. Under some circumstances where Internet connection bandwidth is limited, the proxy server inactivity timeout should be configured for a longer period of time to avoid failed downloads.
VirusScan ASaP Client User Information

After the VirusScan ASaP Client is installed, there are a few options available to the user.

Testing VirusScan ASAP Client

To test the VirusScan ASAP client, you can download the EICAR Standard AntiVirus Test file which allows the client to detect a virus and display an alert. This file DOES NOT contain a virus, and cannot harm your system. To download the EICAR file, follow the steps below:

1. Press CTL + Shift, then with the cursor over the MyCIO icon, right mouse click.
2. A second menu appears that has more menu items than the standard menu. Click Help to view the Online Help menu.
3. Select Testing Virus Scan ASaP, and follow the instructions on the help page.
4. If the client is installed properly, the VirusScan ASaP client interrupts the download, and displays a virus alert dialog box.
5. If the client is installed incorrectly, the file is downloaded without interruption, and you should re-install the client software.

Advanced Menu for VirusScan ASaP Client

The Advanced Menu for VirusScan ASaP client is accessed by pressing Ctrl+ Shift, then right clicking the MyCIO icon in the system tray at the bottom right of the screen. Not only can you select a directory, file, or hard drive for virus scanning, but you can also display the Quarantine Viewer and Enable/Disable VShield.

Quarantine Viewer

Quarantine Viewer displays any virus information about the VirusScan ASaP client, and where they were located before cleaning from your computer. You can Delete the information files, Send them to your system administrator, Rescan the infected files, or Restore the cleaned file to your system.
If the infected file cannot be cleaned by VirusScan, the infected file is deleted from your system, and a window displaying an alert dialogue box counts down the seconds until the window is closed.

Enable/Disable VScan
You can disable the VScan to install software as anti-virus software can interfere with some software installations. Be sure to enable the VScan after any software installation as you are now vulnerable to viruses.

About VirusScan ASaP
Click the menu item, About VirusScan ASaP, to review the last time the client was updated, and the current virus engine used for scanning.
Network Anti-Virus Tips and Troubleshooting

Disabling Anti-Virus on Your Desktop
1. Press and hold the Ctrl and Shift keys and right-click on the VirusScan icon in the system tray.
2. Move the cursor until it is positioned over Scan Now.
3. Click Disable VShield.

Enabling Anti-Virus on Your Desktop
1. Press and hold the Ctrl and Shift keys and right-click on the VirusScan icon in the system tray.
2. Move the cursor until it is positioned over Scan Now.
3. Click Enable VShield.

Testing VirusScan ASaP
1. Disable On-Access Scanning following the Disabling Anti-Virus procedure above.
3. Select VirusScan ASaP.
4. Select Managing VirusScan ASaP.
5. Select Testing VirusScan ASaP.
6. Click downloading the test virus “eicar”.

Tip! This is not an actual virus. Eicar is an industry standard nonviral test file that is identified by many anti-virus programs as a test virus.

Scheduling a Scan
A virus scan can be scheduled using any Windows-compatible scheduler such as Windows NT AT scheduler or the Windows 98 Task Scheduler. To schedule a task, open your task scheduler program, locate the HtmlDlg.exe file in the windows\system\myCIO directory. To start VirusScan ASaP scanning, the HtmlDlg.exe program needs to know the location to begin scanning. To scan all local drives, type the following string after the HtmlDlg.exe filename:

-URL="myui://ScanNow.htm"-ResDll="myScnUi.Eng"-
Param="ScanObject,VT_BSTR,ALLFixed"-Caption="VirusScan ASaP"

To scan the C drive only, change the Param value to “ScanObject,VT_BSTR,C:”.
To scan a specific folder, change the Param value to “ScanObject,VT_BSTR,C:\( folder name)"
Quarantine Viewer Notes

Infected files that can be cleaned by the program are stored here. Files that cannot be cleaned are moved to the Quarantine folder. The message, Clean Failed, is not an error message, but an alert that the entire file is the virus and must be deleted. All files stored in the Quarantine folder are encrypted and cannot infect the system. Quarantined files can only be viewed using the Quarantine Viewer.

To open the Quarantine Viewer, follow these steps:
1. Press and hold the Ctrl and Shift keys.
2. Right-click on the VirusScan ASaP icon in the system tray.
3. Move the cursor to **Scan Now**.
4. Click on **Quarantine Viewer** to view any quarantined files.

Use the checkboxes on the left to select a file or files. The following buttons are available:
- **Select All** - selects all files
- **Reset** - unselects all files
- **Rescan** - rechecks the files for viruses
- **Restore** - puts the file back in its original location
- **Delete** - deletes the file
- **Send To** - sends the file to AVERT for analysis

Spool32 Error Message

**Problem**
Spool32.exe caused an invalid page fault error when printing on systems running VirusScan ASaP in a Windows 95 or 98 environment.

**Solution**
Update the SPOOLSS.dll file in the \windows\system directory.

For Windows 95, replace the original version, 4.00.950, with the updated version, 4.03.1212. The file is available from Microsoft and is also included with later releases of Windows 95. It is possible that another computer running Windows 95 has this file. Check the version of the file by right-clicking on the filename, then selecting **Properties**. Click the **Version** tab to see the file version number.

Microsoft has not released an updated DLL for Windows 98. However, the SPOOLSS.DLL file from Windows ME, version 4.90.0.3000, has been tested on Windows 98 and 98SE and works properly, solving the Spool32 error message.
Missing or Disappearing System Tray Icon

To restore the VirusScan icon to the system tray, use these steps:
1. Open the directory winNT\myCIO\agent.
2. Right-click and drag the MyAgtry.exe file to the desktop.
3. Release the right mouse button and select Create Shortcut Here.
4. Double-click on the new shortcut.

Cannot Listen on Port 6515

When the computer reboots, an error message, Cannot listen on port 6515, is displayed. There are two reasons that the error occurs:
- Another application is using port 6515 or 1967 required by Rumor Technology.
- The network card or network card driver is not functioning properly.
- A personal firewall is blocking traffic on port 6515 or 1967.

You can disable the application using the port, or configure the application to use a different port.

Rumor technology functions entirely on the local area network. Port 6515 must be open on the proxy, but it can be closed on the firewall. Any network applications operating on the client computer that open port 6515 cause that node to malfunction as a Rumor server and prevent other nodes from updating through Rumor. Also any network applications running on the client that open port 1967 cause the node to malfunction as a Rumor server or client.

If the network card or network card driver is failing, contact the vendor for troubleshooting information.

This error message is most likely to happen after VirusASaP is installed and the network adaptor card or driver has failed. Try browsing the local network as a short test. On a dial-up system, be sure that Dial-up networking has not been removed.

Unable to Create Cabinet Installer Object

When attempting to install VirusScan ASaP, the message, Unable to create Cabinet Installer Object, is displayed. These solutions are available.
- Read the following Microsoft Q177943 article located at <http://support.microsoft.com/support/kb/articles/Q177/9/43.ASP?LN=EN-US&SD=gn&FR=0.>
- Use this link to replace the missing or outdated file: <http://virusscanasap.mcafeearchas.com/vs2/bin/ComcatPatch.exe>.
- Reboot the system after running the patch and then install as usual. You may need to run the myciocleanup.exe utility to remove leftover files from the failed installation.
Creating a Rescue Disk for Boot Sector Virus Repair

A computer has a boot sector virus and needs to boot from a floppy disk in order to repair damage to the computer.

2. Click Create an Emergency Repair Disk.
3. Insert a known, clean floppy disk into your drive.
4. Click on the link Click here to create your Emergency Repair Disk.

**Note:** This is for Boot Sector viruses only. The DAT file for this disk is stripped down in order to fit onto a floppy disk, and it only contains definitions for boot sector viruses.

Online Reports are blank or missing charts

After logging into the customer area of the McAfee ASaP Web site, the reports are blank or the charts do not appear.

ChartFX, the plug-in required to view the charts, requires ActiveX in order to display the charts. Try one of the following solutions:

If you’re using a browser other than Microsoft Internet Explorer, open Internet Explorer first, and then use it to browse to http://www.mcafeeasap.com.

Check the version of Internet Explorer used to browse to the McAfee Web site. Version 4.02 or later is required to view the reports. Later versions of Internet Explorer are free and can be found at the Microsoft Web site at <http://www.microsoft.com>.

ActiveX Controls may be disabled on your Web browser. Use the following steps to enable ActiveX on Microsoft Internet Explorer:

1. Open your Web browser, and click **Tools** on the toolbar.
2. Select **Internet Options** from the menu.
3. Click the **Security** tab.
4. Click **Default Level**, and click **Apply**.
5. Click **Custom Level**, and enable all ActiveX controls.
Can’t Find INX File to Execute

Set up stalls and displays the message, “Installation Error 0x80070002 can’t find INX file to execute”.

The error is caused by one of the following situations: insufficient disk space to install the software, or a proxy server or firewall blocked cab files during installation but allows the initial installation to run.

Check free disk space. VirusScan ASaP requires 3 MB of hard disk space above Windows requirements for a swap file. Windows generally requires twice as much free space as the amount of RAM for the swap file. A Windows 9x system with 32 MB free needs 64 MB of free space to operate properly and then 3 MB more VirusScan ASaP.

If there is insufficient disk space on the computer, free up some space on the hard drive by deleting temporary files, and emptying the Internet cache files and cookies. If disk space is still insufficient, you can remove unused programs from the computer or decide if your next step is a larger hard drive.

To check for proxy validation errors, open the myagent.log file located in C:\windows\myagent.log or C:\WINNT\myagent.log. Scroll through the file looking for proxy validation errors.

If you have made more than one unsuccessful attempt to install, do the following:

1. Remove any VirusScan ASaP components that may have installed.

2. Delete the myagent.log file.

3. Re-install the software to generate a clean log file that displays where the installation failed.

All proxy server or firewall restrictions must be addressed by the network administrator. Once it is determined to be a firewall or proxy server problem, you should contact the vendor for configuration support. Also, VirusScan ASaP only supports anonymous or Windows NT authentication proxies. Port 80 on the firewall must allow inbound and outbound traffic, and port 6515 on the proxy must be open. Any listing on port 6515 can cause errors and prevent Rumor from working.
MyINX GPF Occurs When Installing VirusScan ASaP

Installation failure occurs with the message, “MyINX has performed an illegal operation”. This error is seen in approximately one out of 1000 installations. It is an issue that was escalated to Microsoft and through a joint debugging effort, it was determined that the issue is not SonicWALL’s or Microsoft’s fault.

A program called Encompass Monitor (EncMontr.exe) is causing the GPF (General Protection Fault) error. Another program that can be problematic is Remind.exe, but there may be additional programs causing this type of error.

To determine the program causing the error, use the following steps:
1. Run Dr. Watson. This program is included with Windows98, NT 4.0, Windows 2000, and ME, but not included with Windows95.
2. Reproduce the problem by installing the virus software again, and when the GPF error occurs, open the Dr. Watson log.
3. Determine which programs or device drivers are currently running.
4. Disable the suspected program and reboot the computer.
5. Try installing VirusScan again.

The Dr. Watson program on NT, 9x, and ME are completely different programs. For NT 4.x and Windows 2000, run Dr. Watson and all errors are written to the Drwatson.log file.

Windows 98 and ME
1. Run Dr.Watson.
2. Reproduce the error.
3. Right-click on the Dr. Watson system tray icon.
4. Select Dr. Watson.
5. Select View and then change the view to Advanced.

Windows ME has a tab called Hooks. Clicking the Hooks tab displays all of the files hooking into the operating system. Start eliminating applications from the list until the problem disappears. Also, check the 16-bit Modules tab and begin eliminating all non-Microsoft 16-bit modules. Checking the items running at start up is also useful to eliminating the problem.

With Windows 98 and ME, MSCONFIG.exe can be used to eliminate programs one at a time. Reboot the computer each time a program is eliminated.

Cannot Connect to Update Server

This issue can be caused by one of four known issues:
• Incorrect Internet Explorer settings
• Corrupt Internet cached files
• Incorrect proxy server or firewall settings
• Restricted registry keys

It is recommended to empty the Internet cache and restoring the settings for Internet Explorer.
To empty the cache, follow these steps:
1. Right-click on the Internet Explorer icon located on your desktop.
2. Click Properties.
3. Click Delete Files in the Temporary Internet Files section.
4. Enable Delete all offline content, and click OK.

Setting the Security Level
1. Right-click on the Internet Explorer icon located on your desktop.
2. Click Properties.
3. Click Security.
4. Adjust the Security level to Medium.
5. Click Custom Level and enable ActiveX settings.
6. Click OK, then OK again.

To check for proxy validation errors, open the myagent.log file located in C:\windows\myagent.log or C:\WINNT\myagent.log. Scroll through the file looking for proxy validation errors.

If you have made more than one unsuccessful attempt to install, do the following:
1. Remove any VirusScan ASaP components that may have installed.
2. Delete the myagent.log file.
3. Re-install the software to generate a clean log file that displays where the installation failed.

All proxy server or firewall restrictions must be addressed by the network administrator. Once it is determined to be a firewall or proxy server problem, you should contact the vendor for configuration support. Also, VirusScan ASaP only supports anonymous or Windows NT authentication proxies. Port 80 on the firewall must allow inbound and outbound traffic, and port 6515 on the proxy must be open. Any listing on port 6515 can cause errors and prevent Rumor from working.

Restricted registry keys (Windows NT and 2000 only)
This is caused when the network administrator, or someone with administrative rights, intentionally changed the default rights on the registry keys. The use of restricted registry keys is not supported by VirusScan ASaP, and the only known fix is to re-image the system.

VirusScan ASaP is designed to be a Web-based application and requires an Internet connection to install and update. The VirusScan ASaP Silent Installer does not require an Internet connection but does update over the Internet. Even though Rumor Technology shares updates, all computers using VirusScan ASaP must be able to connect to the McAfeeASaP.com site to start the update process.
Cabinet Not Trusted Error

There are two issues that can cause Cabinet Not Trusted: Error 0x800B0001:

- Internet Explorer is an old version. You must run Internet Explorer 5.0 or later.
- The proxy server is incompatible with VirusScan ASaP or is configured incorrectly preventing the update files from downloading.

To check for proxy validation errors, open the myagent.log file located in C:\windows\myagent.log or C:\WINNT\myagent.log. Scroll through the file looking for proxy validation errors.

If you have made more than one unsuccessful attempt to install, do the following:

1. Remove any VirusScan ASaP components that may have installed.
2. Delete the myagent.log file.
3. Re-install the software to generate a clean log file that displays where the installation failed.

All proxy server or firewall restrictions must be addressed by the network administrator. Once it is determined to be a firewall or proxy server problem, you should contact the vendor for configuration support. Also, VirusScan ASaP only supports anonymous or Windows NT authentication proxies. Port 80 on the firewall must allow inbound and outbound traffic, and port 6515 on the proxy must be open. Any listing on port 6515 can cause errors and prevent Rumor from working.

Installation Declined

While installing Anti-Virus, a message, “Installation declined, you failed to accept a vital component or you do not have admin rights”, is displayed.

Windows NT or Windows 2000

- The current user does not have administrative rights on the local computer. The user has to be added to the administrators group in User Manager, or the administrator has to install the MyAgtinstall.exe program from the MyCIO.com Web site while logged onto the computer with administrator rights.

More information is available at <http://www.mcafeeasap.com/content/virusscan_asap/managing_virusscan.asp#restricted>.


- The Temp folder was deleted. The Temp folder is created when installing the operating system. If it is missing, VirusScan ASaP displays the message “Installation declined, you failed to accept a vital component or you do not have admin rights.” To resolve this issue,
  1. Right-click on the My Computer icon on your desktop.
  2. Select Properties.
  3. Select the Environment Variable tab if running Windows NT. If you are running Windows 2000, select the Advanced tab, and then Environment Variables.
4. Look for the Temp variable and read the path to it. Typically, it is C:\Temp for Windows NT.
5. If the folder is missing, create a Temp directory on your C drive.
6. Run myciocleanup.exe.
7. Re-install VirusScan.

**Missing or Corrupt System File**

If the IMAGEHLP.dll file is missing or corrupted, the following messages can be displayed:
- An Internet Explorer message, “Your current security settings prohibit running ActiveX controls on this page”, is displayed.
- “Installation Declined” is displayed.

If you have deleted all of the temporary Internet files and cookies, restored all of the ActiveX settings, and still see this message on Windows 9x or Windows NT 4.x, follow the instructions below to download a patch to replace this file.

Check for the system file, imagehlp.dll, located in the \windows\system directory for Windows9x or \winnt\system32 directory for Windows NT. If the DLL does not exist, use the following steps to replace it.

2. Double-click on the file to execute it.
4. Double-click on the file to execute it and remove the remnants of the failed installation.
5. Restart the installation of VirusScan ASaP from the installation URL.

---

**Alert!** This patch is not for Windows 2000 or Windows ME.

**Outdated Version of myAgtInstall.exe**

This program is installed by an administrator on restricted workstations prior to installing VirusScan ASaP. If the program is a previous version, it displays the “Installation Declined” message.

To download the latest version of myAgtInstall.exe,

2. Select VirusScan ASaP.
3. Select Installing VirusScan.
4. Scroll down to Installation on Restricted Workstations.
5. Click on the link to begin downloading myAgtInstall.exe.
WebScan Service Running on the Proxy Server
Disable or remove WebScanX from the proxy server. WebScan is an obsolete product and cannot detect most new viruses.

Missing or Corrupted REGSVR32.exe File
To find out if the file is missing, perform a search for the file. If you determine that the file is missing, locate the file on the original Windows CD or copy it from another computer using the same version of Windows. The file should be copied to the directory listed, depending on your operating system:
- Windows 9x or ME - C:\Windows\System
- Windows NT or 2000 - C:\Winnt\SYSTEM32
- Windows XP - C:\Windows\SYSTEM32

Unrestricted Windows NT 4.x, Windows 2000, All Windows 9x, and ME
1. Right-click on your Internet Explorer icon on your desktop.
2. Select Properties.
3. Click Delete Files in the Temporary Internet files section.
4. Select Delete all offline content, and click Ok.
5. Click Delete Cookies. Click Ok to remove all cookies.
6. Click the Advanced tab.
7. Click Restore Defaults, then Apply.
8. Select the Security tab.
9. Click Default Level.
10. Click OK.

Clean up any leftover MyCIO program files and reinstall the application.

Tip! Some security setting changes require the system to be rebooted before they take effect on the computer. When in doubt, reboot the computer before reinstalling VirusScan ASaP.

REGEDIT Program Missing
The system file, REGEDIT.exe, is missing from the system. VirusScan ASaP is not able to write the necessary registry entries to the file. Copy the file from another computer and then copy it to the computer.
Computers Not Displayed on Reports

If you have installed VirusScan ASaP, and 24 to 48 hours later, the computers are not displayed on the report, it is possible that the recent installations are not reporting data.

Windows NT 4.x or Windows 2000

1. Double-click on My Computer, and locate the C:\winnt\Mycio\vscan\report. Leave the directory open.
2. Open Control Panel, and then Administrative Tools.
3. Open Services and stop the MyAgtSvc service.
4. When the XML file appears in the report directory, drag it to the desktop.
5. Restart the service.

Windows 9x or Windows ME

1. With Windows Explorer browse to the report folder c:\winnt\Mycio\vscan\report and leave it open.
2. Open DOS window change directory to the c:\windows\mycio\agent directory.
3. Type myagtsvc /stop (myagtsvc /start restarts the service.)
4. When the XML file appears, drag it to the desktop
Open the file and see if it's formatted properly. It should look something like this:

```xml
<?xml version="1.0" encoding="ISO-8859-1" ?>
- <Root>
  - <MachineID value="f28af801-baf3-11d4-b1ae-00b0d060bd13" time="11/17/2000 11:57:27">
    <MachineName value="John Doe" />
    <EmailAddress value="jdoe@yourcompany.com" />
    <IPAddress value="155.155.155.155" />
    <Software value="VirusScan ASaP" version="2,1,33,0" />
    <Entitlement value="your number goes here" />
  </MachineID>
</Root>
```

If the XML file is blank or garbled, there is a problem between Internet Explorer and VirusScan ASaP.
1. Uninstall VirusScan and Run the Myciocleanup utility if necessary (and check for left over parts of the installation.)
2. Reinstall VirusScan ASaP.

Check for a good XML file and if it looks good, wait 24 to 48 hours for the report to show up. If there are multiple XML files, delete all of them older than today's date. If the XML file still looks bad,
1. Change the Internet Explorer security settings to default.
2. Make sure the customer has the latest service pack for their current version of Internet Explorer.

If the XML file looks good, verify that the firewall or proxy server is not blocking the outgoing XML files. If this is a global problem (all systems on the LAN or a segment of the LAN are not reporting, then it is more likely a firewall issue. Most networks have a hub on the outgoing port of the firewall. If you can plug one of the affected systems and it to sends out a report, then the fire wall is the problem.

1. Plug in one system into the WAN side of the firewall.

2. Stop and restart the service as described above. (Repeat a few times if necessary.)

3. Check for a report. (Manually stopping and restarting the service usually boosts the reporting lag time to about 2 hours.)

All firewall or proxy server restrictions has to be addressed by the network administrator. Once the firewall or proxy server has been determined to be the problem, you need to contact the vendor for configuration support. Also VirusScan ASaP only supports anonymous or Windows NT authentication proxies. Port 80 on the firewall must be open (both inbound and outbound) and port 6515 on the proxy must be left open. Anything listing on port 6515 can cause errors and prevent Rumor from working.

**All operating systems**

Verify that all the systems were installed using the same URL. The company key is stored in the registry at; hkey_local_machine\software\myCIO\agent\szCompanyKey. Verify that this value on the non-reporting computer is the same as in their install URL
VirusScan ASaP Installation Error: 0x80004005, myINX Script: INI file not found.

A failure to install VirusScan ASaP occurs with the dialog box shown below and the message "myINX Script: INI file was not found. GetIniFileValue szUninstallPath=% % szProductPath % %\WcmdrSil.ini, Run unInstallShield, CmdProg"

If the system was rebooted, as required by Windows9x and ME, a VirusScan ASaP icon may appear in the system tray. Placing the cursor over the icon also displays the error message.

It appears that a partial installation VirusScan ASaP has occurred as evidenced by the additional files, directories, and registry changes to the system. VirusScan ASaP uses existing uninstall programs to uninstall current anti-virus programs, before it installs the VirusScan program. If existing uninstall program is missing, or moved, or damage, then the message, Installation Error:0x0004005, is displayed.

Alert! Windows 98 Plus pack includes McAfee VirusScan but uses a Microsoft uninstaller program rather than a McAfee uninstaller and always displays this error.

Solutions
- Remove the existing anti-virus using its uninstall program or Add/Remove Programs located in the Control Panel.
- If the uninstaller cannot be found, try re-installing the existing anti-virus program. Then uninstall it before re-installing VirusScan ASaP. On Windows 98 only, check for Microsoft Plus! 98 in the Start menu. If Microsoft Plus! 98 is present, skip to the Microsoft Plus! 98 uninstall instructions.
• With McAfee Anti-Virus 4.5, run the set up from the original media. The program displays the option of **Remove** or **Modify**. Select **Remove** and follow the prompts. Reboot and install VirusScan ASaP.

**Removing McAfee VirusScan from Microsoft Plus! 98**

1. Open the **Control Panel** from the **Start** menu.
2. Double-click **Add/Remove Programs**.
3. Select **Microsoft Plus! 98**.
4. Click **Add/Remove** and **Microsoft Plus! 98 Setup** launches.
5. Select **Add/Remove**, and click **Next**.
6. Select **VirusScan** from the list of programs.
7. Click **Next** again and then **Finish**.
8. Reboot the computer.

Install VirusScan on the computer.

---

**Tip!** *There is no reason to manually remove McAfee from the registry. The files are harmless if left in the registry.*

---

**Excluding Files and Folders from Virus Scanning**

**Problem**

Scanning certain files or folders in use by other programs can cause performance problems or software conflicts.

**Solution**

Exclude the files or folders using the VirusScan ASaP Exclusion Viewer. The Exclusion Viewer is a web-based tool, but the changes are written to the VirusScan ASaP section of the Windows registry.

2. Select **File** or **Folder**. If **Folder** is selected, you can enable **Exclude all subfolders also**.
3. Click **Browse** to locate the files or folder. After selecting the file or folder, click **OK**.
4. A message appears, “Changes were made to the list of excluded items. Would you like to save these changes?” Click **Yes** to save the changes.
5. As you add files and folders, a checkbox appears to the left of each item as it is added to the Exclusion Viewer. You can select and delete multiple items using the checkboxes.