SonicWALL Network Anti-Virus



Contents

Copyright Notice	2
Limited Warranty	2
Introduction	4
Managing Network Anti-Virus	5
Activating the Network Anti-Virus Subscription	6
The Network Anti-Virus Summary Tab	7
Anti-Virus Settings	7
Anti-Virus Administration	8
Reports	8
Add or Renew Licenses	9
Adding More Licenses	9
Renewing the Current Subscription	10
Configuring Anti-Virus Policies	11
Configuring Anti-Virus on the TELE3 TZ	13
Network Anti-Virus E-Mail Filter	16
E-Mail Attachment Filtering	16
Forbidden Attachment Options	17
Warning Message Text	17
Installing the Network Anti-Virus Client	18
Installing on Windows 95/98/NT/2000 computers	18
Proxy Support	19
VirusScan ASaP Client User Information	20
Advanced Menu for VirusScan ASaP Client	21
Quarantine Viewer	21
Enable/Disable VScan	21
About VirusScan ASaP	21
Anti-Virus License Sharing	22
Anti-Virus Activation Key	13

Copyright Notice

© 2002 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 SonicWALL Network Anti-Virus will perform in accordance to the accompanying written materials for a period of ninety (90) days from the date of receipt.

SonicWALL Inc.'s and its suppliers' entire liability and your exclusive remedy shall be, at SonicWALL's option, either a) return of the price paid, or b) repair or replacement of the PRODUCT that does not meet SonicWALL's Limited Warranty and which is returned to SonicWALL with a copy of your receipt. This Limited Warranty is void if failure of the PRODUCT has resulted from accident, abuse, or misapplication. Any replacement PRODUCT shall be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer.

In no event shall SonicWALL or its suppliers be liable for any damages whatsoever (including, without limitation, special, incidental, indirect, or consequential damages for loss of business profits, business interruption, loss of business information, or any other pecuniary loss) arising out of the use of or inability to use the PRODUCT.

Some states do not allow the exclusion or limitation of implied warranties or liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you. Where liability may not be limited under applicable law, SonicWALL's liability shall be limited to the amount you paid for the Product. This warranty gives you specific legal rights, and you may have other rights which vary from state to state. By using this Product, you agree to these limitations of liability.

THIS WARRANTY AND THE REMEDIES SET FORTH ABOVE ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESS OR IMPLIED.

No dealer, agent, or employee of SonicWALL is authorized to make any extension or addition to this warranty.

Introduction

By their nature, anti-virus products typically require regular, active maintenance on every PC. When a new virus is discovered, all anti-virus software deployed within an organization must be updated with the latest virus definition files. Failure to do so severely limits the effectiveness of anti-virus software and disrupts productive work time. With more than 50,000 known viruses and new virus outbreaks occurring regularly, the task of maintaining and updating virus protection can become unwieldy. Unfortunately, many small to medium businesses don't have adequate IT staff to maintain their anti-virus software. The resulting gaps in virus defenses may lead to data loss and decreased employee productivity.

The widespread outbreaks of viruses, such as "ILOVEYOU" and Melissa, illustrate the problematic nature of virus defense for small and medium businesses. Users without the most current virus definition files allow these viruses to multiply and infect many other users and networks. SonicWALL Network Anti-Virus prevents occurrences like these and offers a new approach to virus protection. The SonicWALL family of firewalls 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 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.

Managing Network Anti-Virus

This section contains detailed information on the activation, installation and configuration of the SonicWALL Network Anti-Virus subscription. Network Anti-Virus is configured from the SonicWALL Management Interface.

This section describes:

- Activating the Network Anti-Virus Subscription
- Configuring Network Anti-Virus
- Managing Network Anti-Virus Subscriptions and Reports

Configuring the Network Anti-Virus E-mail Filter

To access the Anti-Virus feature in the SonicWALL, click **General** on the left side of the browser window, and then click **Status** at the top of the window.



This window displays the current status of the SonicWALL. It contains an overview of the SonicWALL configuration as well as any other important messages. If a message stating, "This SonicWALL is not yet registered" is displayed, then it is necessary to complete the online registration before activating the Network Anti-Virus subscription. Click the link to http://www.mysonicwall.com and complete the online registration process.

To activate SonicWALL Network Anti-Virus, the SonicWALL must have firmware version 5.0.0 or greater. See the SonicWALL Internet Security Appliance User Guide for instructions on updating to the latest SonicWALL firmware.

The optional Network Anti-Virus subscription must be registered to activate Anti-Virus enforcement. The **Activation Key** is displayed on the back of this manual.

Activating the Network Anti-Virus Subscription

1. Click **Anti-Virus** on the left side of the browser window.

SonicWALL Administration - Microsoft Internet Explorer	
Ele Edit View Favorites Iools Help	16
← Back + → - ② ② ④ ④ ③Search ③Favorites ③Media ③ ③ - → = → > > 2 2	
Agdress 👜 http://192.168.168.1/management.html	
	€ Help
STATUS: Ready	
	imet //

- Click the Activate your <u>Network Anti-Virus Subscription</u> link. Enter the Activation Key located on the back of this manual in the Anti-Virus License Key field. Then enter a password in the Anti-Virus Password and Verify Password fields. The Anti-Virus password is used to add or renew licenses or to view network reports. The password must be between 6 to 12 alphanumeric characters in length.
- After entering the required information, click Submit. The operation takes several seconds to complete. Once the Network Anti-Virus activation is complete, a window appears confirming the activation and displaying the number of registered Network Anti-Virus Licenses.

The Network Anti-Virus Summary Tab

Click **Anti-Virus** on the left side of the browser window, and then click **Summary** at the top of the window.

🚳 SonicWALL Ad	Iministration - Microsoft Internet Explorer	= O X
_Eile <u>E</u> dit ⊻iew	w Egyontes Iools Help	15
⇔Back + ⇒ ·	- 🕼 🕼 🖄 Search 🝙 Favorites 🛞 Media 🎲 🖓 - 🌧 🖬 - 🖹 🖓 😿 🖁	
Address 🚳 http://	/192.168.168.1/management.html	
SONICWALL	ANTI-VIRUS Summary Configue E-Mail Hite	@ Help
General	Anti View Cattings	
Log	Anu-virus setungs	
Filter	Enable Anti-Virus	
Tools	Number of Anti-Virus	
Access	Licenses: 10	
Advanced	Expiration Date: 11/08/2002	
DHCP		
VPN	Anti-Virus Administration	
Anti-Virus) Genu Damark	
High Availability	view <u>Repuit</u>	
	Change Anti-Virus Password	
	Add or renew Anti-Virus Licenses	
		Update Reset
Logout	STATUS: Ready	
kttp://192.168.16	68.1/help_avsummary.html	internet

Anti-Virus Settings

The **Summary** tab displays the following information:

Enable Anti-Virus

After activating the Network Anti-Virus subscription, selecting the **Enable Anti-Virus** check box enables Anti-Virus enforcement on the network.

Number of Anti-Virus Licenses

The number of the current licenses that have been registered for the firewall.

Note: Each anti-virus license allows the use of SonicWALL Network Anti-Virus on one computer for a 12-month period.

Expiration Date

The expiration date of the current subscription is displayed.

Anti-Virus Administration

The **Anti-Virus Administration** section provides links to reports summarizing Anti-Virus activity on the network. Administrative activities such as changing passwords and renewing or adding licenses are also accessed here.

Reports

To view Network Anti-Virus statistics and reports, click the link labeled <u>View Report</u>. The Authentication window appears. Enter the Anti-Virus password in the **Anti-Virus Password** field and click **Submit**.



This window displays general information about Network Anti-Virus. Information about the number of desktops protected, and the number of updated and outdated desktops is shown at the top right corner of the window. The table offers information about the viruses found, the most common viruses and the most infected computers on the network.

Add or Renew Licenses

To manage Anti-Virus licenses, click the link labeled **Add or Renew Anti-Virus Licenses** in the **Anti-Virus Summary** tab.

SonicWALL Adm	sinistration - Microsoft Internet Explorer
Eile Edit View	Fgrontes Icols Help
de Back + ⇒ -	② ② △ ② Search ⓐ Favorites ③ Media ③ ▷ · 글 ☑ · 글 ♀ >/
Address @ http://1	92168.1681/management.html
SONICWALL	Add or Renew Anti-Virus Licenses
General	New Linner Ver
Log	New License Key:
Filter	Ivew License K.ey.
Tools	New Lacense K.ey.
Access	New License Key.
Advanced	New License Key
DHCP	Anti-Virus Password
VPN	Submit
Anti-Virus	
Hinh Availability	Please select Addition or Kenewal. Then enter the license key displayed in the back of your Network Anti-Virus Administrator's Guide, and the Sonic WALL Anti-Virus password. If you purchased more then one key, enter them all
	Addition: The total number of licenses for this SonicWALL will be increased. The expiration date will be pro-rated to
	rences ne remaining subscription period, as wen as me new 12 month subscription.
	Renewal: The existing licenses registered for this Sonic WALL will be renewed for an additional 12 month subscription
	Jperiod.
1	
Logout	STATUS: Ready
(E)	👋 💩 Internet

Adding More Licenses

The standard SonicWALL Network Anti-Virus subscription package can be used to activate Network Anti-Virus, to increase the number or Anti-Virus licenses or to renew the current subscription. Since a Network Anti-Virus Activation Key may not be reused, additional subscription packages are required to add or renew Anti-Virus licenses.

- 1. Select the **Add** option at the top of the **Add or Renew Licenses** window.
- 2. Enter the **Activation Key** displayed on the back of the Network Anti-Virus Administrator's Guide in the **New License Key** field.
- Create and enter an Anti-Virus password in the Anti-Virus Password field, and click Submit. The operation takes a few seconds to complete. Once completed, the new number of Anti-Virus licenses appears in the Anti-Virus Summary window.



Note: 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-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 Anti-Virus subscriptions and the number of 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.

Note: When renewing a Network Anti-Virus subscription, the number of licenses for subscription renewal must be equal to the number of licenses in the current subscription.

To renew the current subscription, complete the following steps:

- 1. Select the **Renewal** option at the top of the Add or Renew Licenses window.
- 2. Enter the Activation Key displayed on the back of the Network Anti-Virus Administrator's Guide in the **New License Key** field.
- Enter the Anti-Virus password in the Anti-Virus Password field, and click Submit. The operation takes a few seconds to complete. Once completed, the new expiration date appears in the Anti-Virus Summary window.

Configuring Anti-Virus Policies

To configure Anti-Virus Policies, click the **Configure** tab. The following features are available in the **Anti-Virus Policies** section of the **Configure** tab:

Note: If you have a TELE3 TZ, see page 13 for information on configuring Anti-Virus.

- Enable DMZ policing Selecting Enable DMZ policing enforces anti-virus policies on computers located on the DMZ.
- **Disable policing from LAN to DMZ** Choosing this option allows computers on the LAN to access computers on the DMZ, even if antivirus software is not installed on the LAN computers.
- Maximum number of days allowed 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.

- **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.

When an alert is received with this option enabled, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the **Maximum number of days allowed 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 Internet Security Appliance User Guide for instructions on configuring log and E-mail alerts.

• Reduce AV traffic for ISDN connections - Selecting this feature enables the SonicWALL Anti-Virus to only check daily for updates and reduces the frequency of outbound traffic for users who do not have an "always on" Internet connection.

SonicWALL Network Anti-Virus currently supports Windows 95, 98, NT, 2000, and XP 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 HomePort. This is the default configuration.

Include specified address range in the Anti-Virus enforcement

Choosing this option allows the administrator to define a range 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.

• Exclude specified address range in the Anti-Virus enforcement

Selecting this option allows the administrator to define a range 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.

Configuring Anti-Virus on the TELE3 TZ

To configure Anti-Virus Policies, click the **Configure** tab.

🗿 SonicWALL Adn	inistration - Microsoft Internet Explorer provided by SonicWALL, INC.
Elle Edit Yew	Fgrontes Iools Help
⇔Back • ⇒ •	2 2 2 2 QSearch LagFavorites (2) Meda (2) 2 - 2 2 - 2 2 - 2 2 3
Address 🔊 http://	92.168.1/management.html
SONICWALL	Anti-Vinius O'Help
General	
Log	Anti-Virus Policies
Filter	Tankla Tamo Data slaine
Tools	Dirable noticing from Wards Dart to
Access	HomePort:
Advanced	Maximum number of days allowed before forcing update: 5
DHCP	Force Update on Alert: Low Risk 🗖 Medium Risk 🔽 High Risk 🔽
VPN	Reduce AV traffic for ISDN connections
Anti-Virus	
High Availability	Exempt Computers
	Enter the IP addresses of comparer that will be allowed to access the Internet without Varus/Scan software. Enter enter single addresses or ranges of configious addresses.
Logout	STATUS: The configuration has been updated.
御	🔯 💼 Internet

The following features are available in the **Anti-Virus Policies** section of the **Configure** tab:

- Enable HomePort policing Selecting Enable HomePort policing enforces anti-virus policies on computers located on the HomePort.
- **Disable policing from WorkPort to HomePort** Choosing this option allows computers on the WorkPort to access computers on the HomePort, even if anti-virus software is not installed on the WorkPort computers.
- Maximum number of days allowed 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.

- **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.

When an alert is received with this option enabled, users are upgraded to the latest version of VirusScan ASaP before they can access the Internet. This option overrides the **Maximum number of days allowed 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 Internet Security Appliance User Guide for instructions on configuring log and E-mail alerts.

• Reduce AV traffic for ISDN connections - Selecting this feature enables the SonicWALL Anti-Virus to only check daily for updates and reduces the frequency of outbound traffic for users who do not have an "always on" Internet connection.

SonicWALL Network Anti-Virus currently supports Windows 95, 98, NT, 2000, and XP 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 on the WorkPort to install VirusScan ASaP in order to access the Internet or the HomePort. This is the default configuration.

Include specified address range in the Anti-Virus
 enforcement

Choosing this option allows the administrator to define a range 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. The address ranges can be on the WorkPort or the HomePort, or both.

• Exclude specified address range in the Anti-Virus enforcement

Selecting this option allows the administrator to define a range 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. The address ranges can be on the WorkPort or the HomePort, or both.

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.

Click **Anti-Virus** on the left side of the browser window, and then click the **E-Mail Filter** tab.

SonicWALL Admin	istration - Microsoft Internet Explorer	the second s		
File Edit View F	avantes Tools Help Send			
Back + () ·	💽 🔹 💭 Search 🔶 Favorites 👹 h	eda 😰 🔝 🖧 🏹 🛄 🛄		
Address A http://10.	0.2.132/management.html			
THE OWNER WHEN THE PARTY NAME				2 Hole
SOMEWAL	KA I PYTRUD			- neip
	Sector Contest			
General				
Log	E-mail Attachment Filtering			
Filter		Feshia E-mail Attachment Educing D		
Tools		Enable E-mail Attachment Filtering Alert Service	• 🗖	
Access				
Advanced		Forbidden File Extensions		
DHCP		oxe		
VPN		2		
Anti-Virus		vbs		
High Availability				
		Delete Extension		
	Politika Intelanta Ordera			
	Foroidden Attachment Options			
		@ Disable forbidden file by altering the file exte	nsion	
		C Delete forbidden file		
	Warning Message Text			
		This email contained a forbidden	2	
		attachment. Contact your network administrator for details.		
		A CONTRACTOR OF A CONTRACTOR OF A	<u></u>	
				Update Reset
Lesset 1	PTATIC BALL			
	STATUS: REAL			
		the most state and the second states in the second state		Contract and some set

E-Mail Attachment Filtering

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

Enable E-Mail Attachment Filtering

Select this check box to filter E-mail attachments. You must check this box to enable the **Forbidden File** options.

Forbidden File Extensions

Enter the file extensions to be filtered in the **Add 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.

Forbidden Attachment 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

Select this option to disable forbidden attachment files as they pass through the SonicWALL. 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

Select this option to delete forbidden attachment files as they pass through the SonicWALL.

Warning Message Text

This is a warning message that can be customized and added to Emails filtered by the **Network Anti-Virus E-mail Filter**. Enter 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.

Enable E-mail Attachment Filtering Alert Service

Selecting Enable E-mail Attachment Filtering Alert Service provides attachment blocking on inbound SMTP and POP3 e-mail protocols. Additionally, when this service is selected, the SonicWALL automatically block virus-specific attachments during rapid outbreaks, even before Anti-Virus signature (DAT) files are available. This feature also provides full filename blocking of virus files. The full filename attachment filtering allows SonicWALL to block only malicious attachments, while enabling all other attachments through. This is a significant improvement over blocking of productive files, such as Word documents (*.doc). In case of a virus outbreak with an attachment using the extension (*.doc), only the virus file is blocked and other Word attachments are allowed through the Anti-Virus protection.

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.

Installing on Windows 95/98/NT/2000 computers

When the Network Anti-Virus is enabled, all computers on the network are automatically re-directed to the page shown below:



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.

Warning! Do not allow the SonicWALL to install the Anti-Virus client to any Windows servers on your network. Installing the Anti-Virus client on a Windows server can cause a "blue screen of death", data loss, or other potentially serious problems.



Enter a unique username 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 functionalities 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 Control(CTL) and 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 diaglog 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 the Control (Ctrl) button and the Shift button, 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.

Anti-Virus License Sharing

Anti-Virus License Sharing allows you to distribute one or more Anti-Virus licenses among multiple firewalls. License sharing assigns a License Sharing Group (LSG) to a firewall from which this feature is activated. You may then add other firewalls to the LSG, by their serial numbers and assign them 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. Log into the Management station and click **Anti-Virus**.

SonicWALL Adr	ministration - Microsoft Internet Explorer	
File Edit Vies	w Pavorites Tools Help <u>Send</u>	
4+Back + →	- 🥥 👔 🖄 Search 🗃 Favorites 🤇 History 🔤 - 🌆 🖾 - 🗐	
Address @ http:	://10.0.2.132/management.html	- @60
SONICWALL	Arth vinus Summary Cooligues Elifal Filter	🕄 Help
Log	Anti-Virus Settings	
Filter		
Teole	Enable Anti-Virus	
	Number of Anti-Virus Licenses: 1	
Libraread	Expiration Date: 09/06/2003	
DUCD .		
Unur	Anti-Virus Administration	
Anti Vinus		
AND VIEWS	View Keport	
	Change Anti-Virus Password	
	Add or renew Anti-Virus Licenses	
		Update Reset
Logout	STATUS: Ready	
6)		internet

2. Click Add/Upgrade Licenses.

Add or Renew Anti-Virus Licenses Add or Benew ^ Add ^ Renew New License Key Mew License Key New License Key New License Key Mew License Key New License Key Mew License Key Me	License Shering ed in the back of your Network Atti-Vrou Administrator's nore then one key, enter them all
Add or former Add or former New License Key Anti-Vrue Parword Submit Please select Addition or Renewal Then enter the license key display Gade, and the SocieWALL And Veue pareword Types purchased Addition: The total number of licenses for the socie. NulL will be meaning independent periods and the socie Network of the new 12 month subception	License Shering ed in the back of your Network Am-Urue Administrator's more then one key, enter them all
New Leans Key : New Leans Key : Ani-Vrus Parword : Submit Please select Addition or Renewal Then enter the locase key display Gade, and the SocieWALL Ani-Vrus paraword 19 yos partnaed i Addition The total number of licenses for the Socie WALL will be in meaning indergraph operies as well are the res '12 moth subscript	Licence Shoring ed in the back of your Network Am-Vrus Administrator's nore then one key, enter them all
Preve License Koy New License Koy New License Koy Anit-Vrue Passwork Submit Pirase refect Addison or Renowal Then enter the license key display Guide, and the SocieWALL Atthe Verus password Socie WayLaw Addition The total number of licenses for this Socie WALL with the mean II month subcripts meaning indergraph operies and wall and new Fill Month subcripts	License Shoring ed in the back of your Henrock Asia-Vrau Administrator's more then one key, enter them all
Piere Locents Key New Locents Key New Locents Key Anti-Virus Panwork Submit Pierare select Addition or Renewal. Then exter the locents key display Gade, and the SocieWALL Arth. Venu parrowed Typoj parthaned Addition: The total number of licenses for this SocieWALL will be remaining noberpairon period, as well as the new 12 month subception	License Shering ed in the back of your Network Anti-Virue Administrator's nore then one key, enter them all
New Locans Key New Locans Key Anti-Virus Parsword Submit Please select Addition or Renewal Then enter the locans key daplay Gade, and the SocieWALL Acta Virus paraword Ty you purchased Addition. The total number of licenses for this Socie WALL will be im-	Licence Shering ed in the back of your Network Am-Unue Administrator's nore then one key, enter them all
Free Lacents Key Anii-Vine Fanword Sulam Flease refect Addition or Reserved Then enter the locents key diplay Guide, and the SocieWALL Ack Venu parrowed IF you perchased Addition: The total number of locents for this SocieWALL will be me	License Shoring ed in the back of your Hemorik Anti-Your Administrator's more then one key, enter them all
Ann-Virue Pasaword	License Sharing ed in the back of your Network Anti-Virue Administrator's nore then one key, enter them all
	License Shering ed in the back of your Network Anti-Virus Administrator's more then one key, enter them all.
Please select Addition or Renewal Then enter the locense key display Guide, and the SoneWALL Am. Virus parsword. If you parchared Addition: The total number of licenses for this SoneWALL will be in meaning nobecippion period, as well as the new 12 mech subscription	License Shering ed in the back of your Network Anti-Virus Administrator's more then one key, enter them al.
Piease relect Addition or Renewal Then enter the license key display Guide, and the SocieWALL Ark-Vuru paraword IF you parchased Addition (The total number of licenses for this SocieWALL will be in memaning molecular period, as well as the new 12 month subscripts	ed in the back of your Network Anti-Virus Administrator's more then one key, enter them all
Renewal. The existing licenses registered for this SonicWALL, will be	creased. The expiration date will be pro-rated to reflect the on. renewed for an additional 12 month subscription period.
	STATUS: Ready

3. Click **License Sharing** to configure license sharing between SonicWALLs.

Add or Renew Anti-Virus Licenses	
Add or Kenew C Add C Kenew	
New License Key:	
New License Key	
New License Key.	
Narr Licence Ver	
New License Key	
Ann-vitus Password	
Addition: The total number of licenses for this SosicWALL will be increased. The expirati remaining subscription period, as well as the new 12 month subscription	on date will be pro-rated to reflect the
Addition: The total number of licenses for this Socie WALL will be increased. The expirati remaining subscription period, as well as the new 12 month subscription. <i>Renewal:</i> The emitting licenses registered for this Socie WALL will be renewed for an additional states of the second	on date will be pro-rated to reflect the tional 12 month subscription period.
Addition: The total number of licenses for this Socie WALL will be accessed. The expirat remaining subscription period, as well as the new 12 month inductingtion. <i>Removal:</i> The emitting kienses registered for this Socie WALL will be renewed for an additional states of the second s	on date will be pro-rated to reflect the tional 12 month subscription period.
	Add er Renner Ansi-Virus Licenses Add er Renner Add er Renner New License Key New License Key New License Key New License Key Auti-Venu Paraword Submit

4. Click **OK** to configure the **License Sharing Group**.

5. Enter your Anti-Virus password to begin configuring the License Sharing Group, and click Submit.

SonicWALL Adm	vinistration - Microsoft Internet Explorer
File Edit View	Favorites Tools Help Send
↓Back + ⇒ -	🔘 🔄 🖞 QSearch 🔄 Pavortes Gristory 🖏 🚽 🖼 -
Address 2 http://	/10.0.2.132/management.html 👱 🖓 Go
SONICWALL General	Anti-Virus Licence Sharing Please enter your Anti-Virus password
Log	Submit
Filter	
Teols	
Access	
Advanced	Sonic WALL Anti-Virus License Sharing allows you to share your Anti-Virus license subscription among multiple firewalls. At this
DHCP	licenses among multiple frewalls, please contact SonicWALL tech support.
VPN	Gire this option CNR. F.F. you want to introduc some of your licenses to another forward
Anti-Virus	
Logout	STATUS: Ready
Done	Disternet

6. The License Sharing Group page appears and displays the number of available Anti-Virus licenses. Enter the serial number of the firewall to be added to your License Sharing Group, and click Submit.



Note: You can only add SonicWALL appliances to your group that do not have active Anti-Virus subscriptions. The SonicWALL appliance must also be registered at http://www.mysonicwall.com before it can be added to the group.

 To distribute licenses between the SonicWALL appliance, enter the number of licenses for the first SonicWALL appliance into the Licenses field, and click Update. Repeat for each SonicWALL appliance.

Firewall SN	Licenses		
0040100C0425	5	Update	Remove
0040100C19C7	50	Update	Remove
0040100c826b	20	Update	Remove
0040100F76F0	20	Update	Remove

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, enter 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 SonicWALL appliances. A typical **License Sharing Group** is displayed below:

ONICWALL	Anti-Virus License Sharing					
General	Total number of AntiVirus li	concor currently avail	able for th	aring is 1	10	
Log	Out of that number, 95 licen	ses are currently in use	by 4 fires	alls.		
Filler	15 licenses are available.					
Tools		Firewall SN	Licenses			
Access		0040100C8425	5	Update	Remove	
Advanced		0040100C19C7	50	Update	Remove	
DHCP		0040100c826b	20	Update	Remove	
VPN		0040100F76F0	20	Update	Remove	
Anti-Virus						
		Add a new Firewall to	the License	Sharing Gr	oup	
		Fraural SN			Add	
				_	10000	

If licenses are not available and you attempt to add more to the **License Sharing Group**, the following error message is displayed:

Filter	Anti-Virus Licenses Sharing Total number of AntiVirus licenses, currently available for sharing, is 100 Out of that number, 50 licenses are currently in use by 2 firewalls. 50 licenses are available.						
Tools		Firev	Firewall SN		ŧ		
Access		0040	100C1212	50	Update	Remove	
dvanced		0040	100F76F0	60	Update	Remove	
VPN		Add a new l	Firewall to t	he Licens	e Sharing Gro	мир	
nti-Virus		Firewall Sh	r [-		Add	
	Yes and The herb-thrackense court for 0001007740's entered accountify, You can exter reage han 1 to 50 For The The Court Force Courterpop One Data: You should change the number of Anti-First licenses per forwall one at a time. The total re automatically splated. To add freedul with Current Active Anti-First licenses per forwall one at a time. The total re automatically splated.						to 50 re a firewall from the Group, a new count and click tal remaining licenses count is

Anti-Virus Activation Key



SonicWALL, Inc. 1160 Bordeaux Drive Sunnyvale, CA 94089-1209 Phone: 408-745-9600 Fax: 408-745-9300 E-mail: sales@sonicwall.com Web: http://www.sonicwall.com

Part # 232-00068-04 Rev A. 03/02