Installation Guide
and User Manual

www.gwava.com
(866) GO-GWAVA • fax (646) 304-6250 • info@gwava.com
100 Alexis Nihon • Suite 500 • St-Laurent • QC • Canada • H4M 2P1

Table of Contents

Getting Started with WASP 1.x 4
Introduction 5
What is New in WASP 5
Which Server? 6
Unzip 6
File Locations 6
Known issues 7
Web Access Set-Up 10
Virus Scanning 12
Oversized Messages 14
Fingerprinting 15
Quarantine Options 18
Log-In 19
Licensing 20
Advanced 22
About 24
30-day demo 24
Removing WASP 25
The Wasp Program Interface 26
Appendix: AV Engine Configuration 31

Getting Started with WASP 1.x

Intended Audience

This manual is intended for IT administrators in their use of WASP or anyone wanting to learn more about WASP. It includes installation instructions and feature descriptions.

Technical Support

If you have a technical support question, please consult the GWAVA Technical Support section of our website at www.gwava.com. The technical support number for WASP is (801) 437-5678.

Sales

To contact a Beginfinite sales team member, please e-mail info@gwava.com or call Tel: 866-GO-GWAVA (866-464-9282) in North America or +1 514 639 4850.

Corporate Headquarters

100 Alexis Nihon Blvd., Suite 500
Montreal, Quebec, H4M 2P1, Canada

About WASP

WASP is a powerful anti-virus defense designed for use with Novell GroupWise WebAccess.

Copyright Notices

The content of this manual is for informational use only, and may change without notice. Beginfinite Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation. GroupWise and WebAccess are registered trademarks of Novell, and copyrighted by Novell.

V-1.03i

Introduction

WASP is virus defense software for the WebAccess portion of your GroupWise Messaging System. WASP connects directly with the WebAccess Agent's Web Server, scanning attachments as they are uploaded via the browser. WASP lets you give your users the convenience of WebAccess with the security you've come to expect from the GWAVA suite of security products.

What is New in WASP

WASP now adds support in Advanced for Short Filename Access. For a complete list of the latest information about WASP, changes, consult C:\PROGRAM FILES\BEGINFINITE\WASP\README.TXT or visit www.gwava.com.

System Requirements

- NetWare 4.11 (SP9 or greater), 4.2, 5.0, 5.1, 6.0 or 6.5.
- GroupWise 5.5EP and above are required
- Disk space usage is:
  - 6 MB on the workstation
  - 1 MB on the server
  - This does NOT include quarantine and log files
- Memory usage on the server is about 2 MB
- A third-party anti-virus NLM
- For upload protection, WASP must be installed on the same server as your WebAccess Servlet.
- TCP/IP must be installed and configured on the servers running WASP
- Long filename support must be enabled on the server with the WASP directories.

We STRONGLY recommend the latest GroupWise patches are applied to your system. At release time these were:

- GroupWise 5.5 (EP) - SP5
- GroupWise 6.0 - SP4
- GroupWise 6.5 - SP1

Licensing

WASP is licensed per user. You must purchase a license for the appropriate number of users on your system. For information about this, contact us at info@gwava.com.

Installation

To begin installing WASP, run the executable file: waspXX.exe (where "XX" is the version number). Install it to a local workstation that has mapped drive access to the server(s) on which you will install the WASP program files.

Which Server?

WASP needs to be installed on the same server running the WebAccess servlet. The WebAccess servlet (i.e. web server) must be running on NetWare. The WebAccess **Agent** does not have to be running on the same server as WASP. In fact, the WebAccess **Agent** can be running on NetWare, Windows or Linux, as long as WASP and the servlet (Web Server) are running on NetWare. A Linux-based version of WASP is currently under development.

Unzip

Unzipping the download from GWAVA.Com unpacks the installer executable. Run the installer after the unzipping is complete.

File Locations

WASP installs the following files in locations specified by the user:

- WASP.NLM
- GWAVASOA.NLM: If GWAVA is installed on same server, care must be taken to keep the versions of GWAVAOSA in sync, as only one can be in memory.

Configuration

When you run WASP for the first time after installation, you must manually enter your network configuration and anti-virus engine and then activate WASP.

- WASP does not auto-configure and does **NOT** scan attachments by default.
- **Note**: Configuration changes will not affect the WASP program until WASP is unloaded and reloaded or you press CTRL-S at the console.

Known issues

Traditional Volumes

If using traditional volumes with the following Netware versions:

- NW 5.1 SP5,NW 5.1 SP6,NW 5.1 SP7
- NW 6.0 SP3,NW 6.0 SP4,NW 6.0 SP5
- NW 6.5 SP1,NW 6.5 SP2

There is a known bug in Novell's filehooking API that manifests itself by WASP not detecting any files being uploaded. This can be addressed in any of the following ways (choose just one):

- Upgrade to NW 5.1 SP8 or NW 6.5 SP3 (or higher)

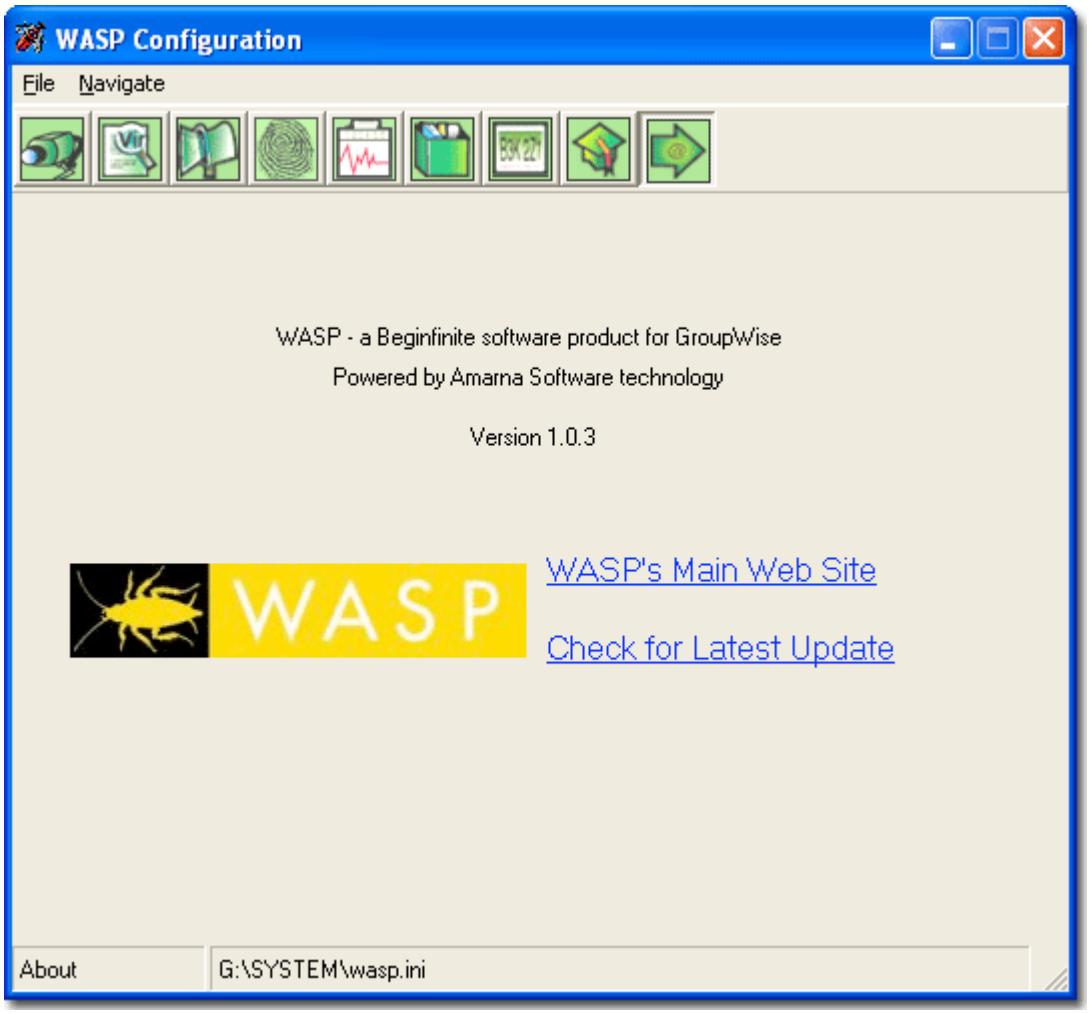
Use an NSS volume for the location of the WebAccess Upload Directory (the location is specified in WEBACC.CFG in SYS:\NOVELL\WEBACCESS)

Apply a special FILESYS.NLM patch from Novell which is available for NW 5.1 SP7, NW 6.0 SP5, or NW 6.5 SP2. The file is named flsysft11.exe and can be found on Novell's support website, http://support.novell.com. Installation instructions are included with the file. As of December 2004, the URL is http://support.novell.com/cgi-bin/search/searchtid.cgi?/2970382.htm.

Namespace

A namespace issue can cause difficulty with filenames. If files are still not being detected, hit CTRL-T at the GWAVA console. If the last line shows only the volume name (e.g. SYS:) and not the full path, turn on the Short Filename access option in the **Advanced** section of WASP's configuration program. Exit and restart WASP.

The WASP Interface



The WASP Interface

This interface gives you access to all of WASP's features, even when in 30-day demo mode.

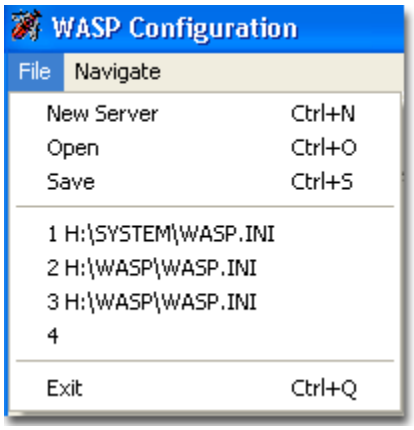
Launching WASP

Launch the executable WASP executable from the Start menu after running the installer. WASP will have to be configured with your network settings and enabled before it protects your GroupWise Web Access installation.

Navigation

Two menus are present at the top of all screens in the Configuration Program—**File** and **Navigation**. File allows you to load and save configuration files while the Navigation menu mirrors the icons at the top of the WASP manager.

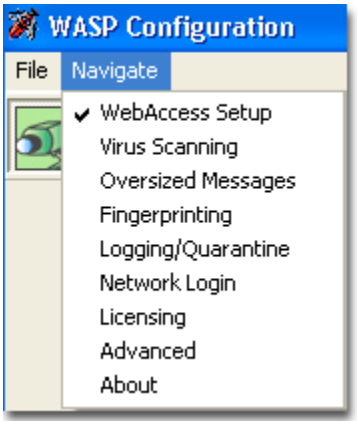
Menus



The File menu allows administrators to create a **New Server** file (Ctrl-N), **Open** (Ctrl-O) or **Save** (Ctrl-S) changes made to WASP settings. One can also shift between configuration recent configuration files.

- To install a new WASP server, simply choose File/New
- To load an existing WASP server, select **Open** from the File menu or select a previously used WASP server path from the menu.
- To save choose **Save** from the **File** menu. You'll be prompted to force WASP to restart automatically with the new settings.
- Exit will exit the WASP program. You'll be given a chance to save any changes.

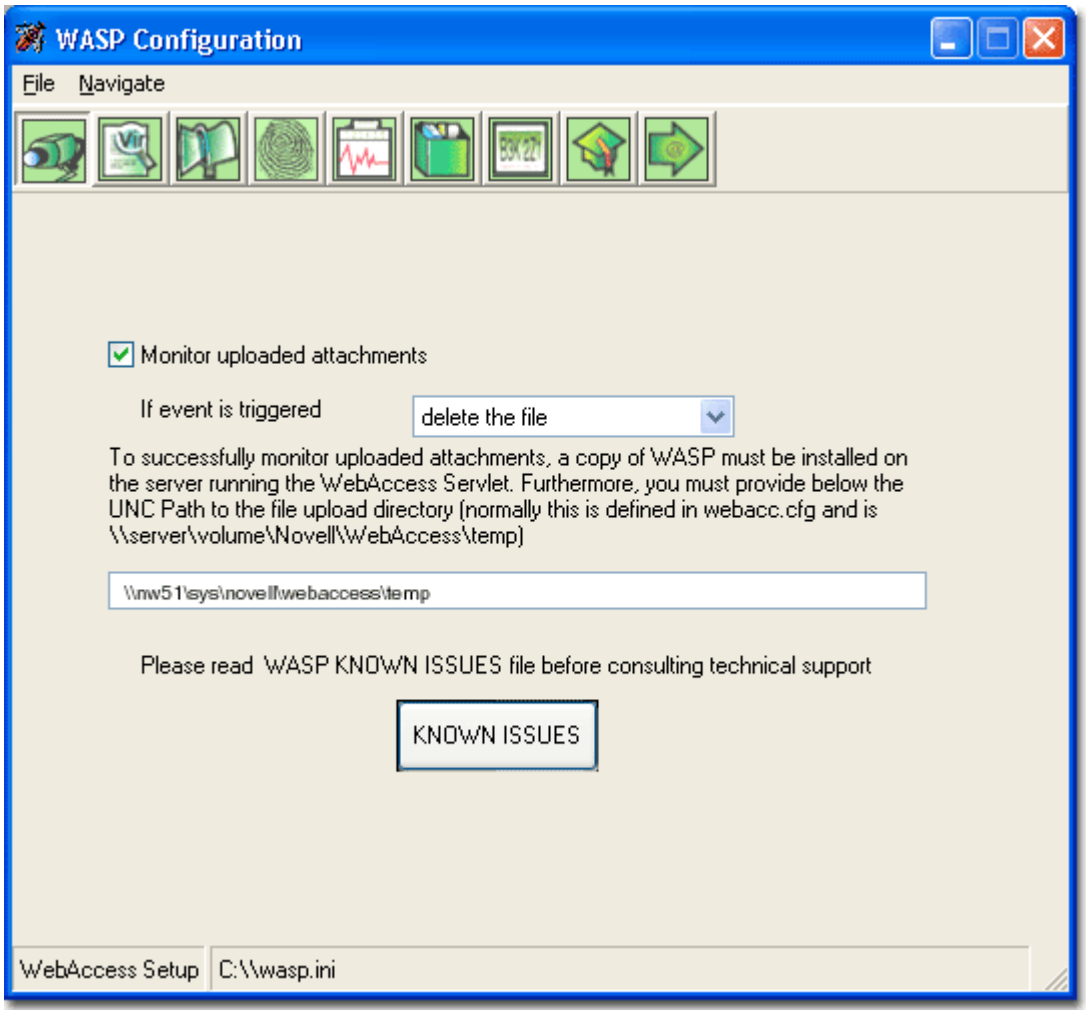
What are the navigation screens in WASP?



- **Web Access Set-Up** - specifies the directories to be scanned.
- **Virus Scanning**: Control and configure which third party AV engines are used by WASP to protect your network. **Note**: WASP has no anti-virus engine of its own.
- **Oversized Messages**: Toggle oversized message filtering, limit the maximum size or maximum aggregate size of messages that can be sent by users.
- **Fingerprinting**: Configuration options for attachment fingerprint scanning to identify what file types are being uploaded irrespective of their extensions.
- **Logging/Quarantine**: Configure the creation of logs, event logs, schedule output at particular times, generate reports, as well as turn on and off quarantine.
- **Licensing**: Enter **BOTH** your WASP **license code and license key.**
- **Advanced**: only adjust these settings under the guidance of GWAVA Technical Support; do not change these settings without contacting Beginfinite Technical Support.
- **About**: informational screen about WASP. Your version number is found here.

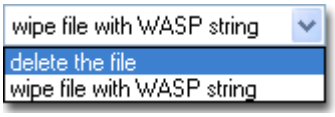
Web Access Set-Up

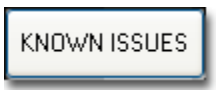
Configure WASP's primary functions



This screen is the most fundamental screen in WASP. From here, WASP can be enabled or disabled. To allow WASP to protect your GroupWise WebAccess, enable the Monitor uploaded attachments checkbox.

WASP's scope of action is fairly straightforward. When an offending attachment is detected by WASP, you may either **Delete the file** or **Wipe the file with a WASP string**. The first option obviously trashes the file. Wipe the file replaces the attachment with a WASP generated 'placeholder' file of exactly equal size which informs the recipient that an attachment was infected. The placeholder contains the virus name (if the AV engine supports this), the size, the fingerprint type, or any other relevant information.





The **Known Issues** button will present a browser window with a file installed in the Wasp Programs directory. The text will contain late breaking information about configuring WASP.

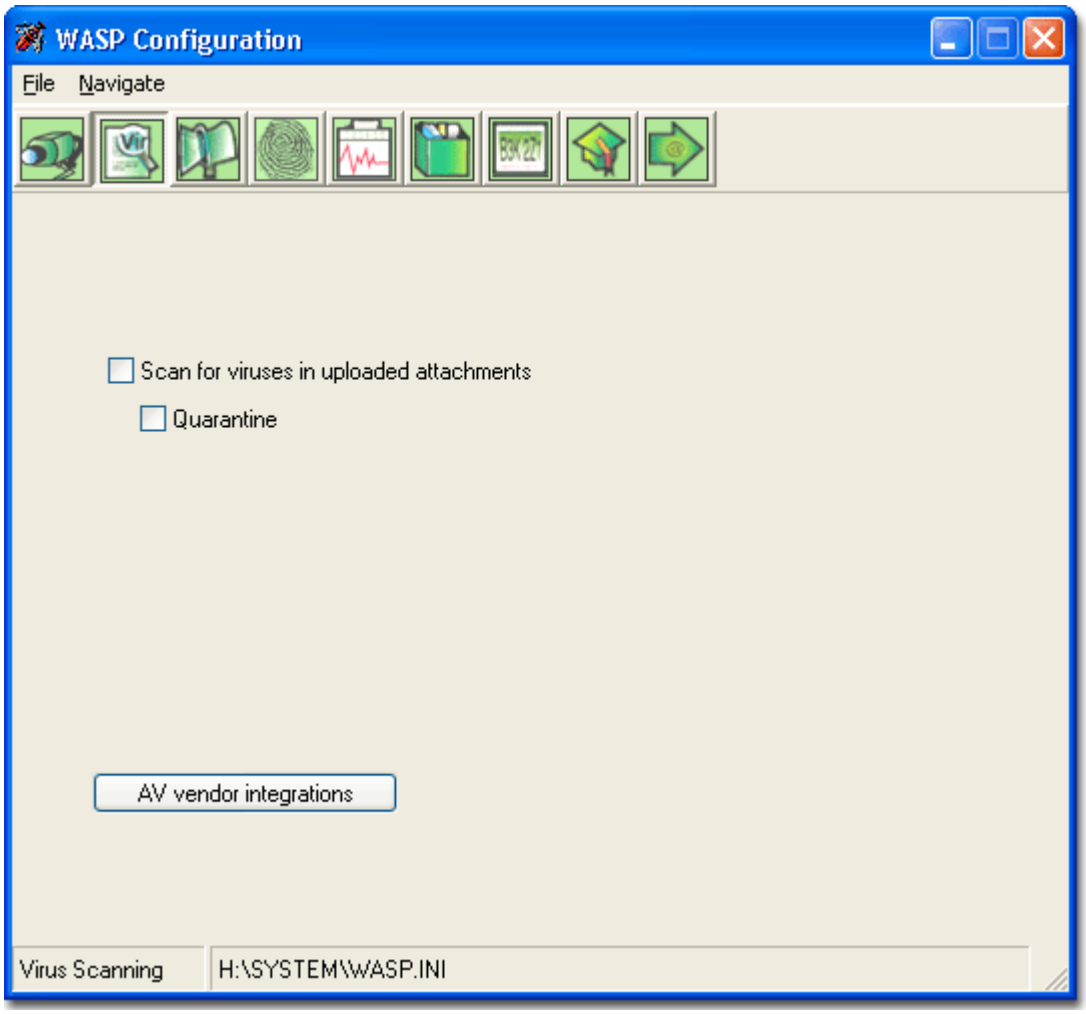
Finally, there is a data entry field for locating the WebAccess working directory for uploaded files. This path must be populated for WASP to function.

For WASP to protect your WebAccess installation:

- It must be installed **on the server running the WebAccess servlet**, and
- It must have access to the file upload directory. Specify this path in UNC format in the data entry field at the bottom of the window. The file upload directory is normally \\servername\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, which is normally installed in \\servername\sys\novell\webaccess
- Note that at this time, WASP supports uploaded file protection exclusively, not downloaded files.

Virus Scanning

Configure WASP's virus scanning options.



We recommend you first install your AV NLM and test it separately before installing WASP. This will facilitate debugging and optimization.

- WASP's only specific AV NLM requirements are that they must allow the exclusion/inclusion of specific directories for scanning and also permit the deletion and moving of infected files.

Turn on virus scanning by clicking the **Scan for viruses** checkbox. The currently selected configuration (see the bottom of the screen) will now be protected by WASP once the setting is saved by selecting **Save** from the **File** menu. The **Quarantine** checkbox will store infected attachments rather than delete them. The quarantine location is determined by your antivirus settings.

AV vendor integrations

To configure your AV engines, click the **AV vendor integrations** button. This presents a new window for configuring WASP's antivirus settings.

AV Engine Options

WASP allows administrators to configure single or multiple AV engines to protect GroupWise Web Access.

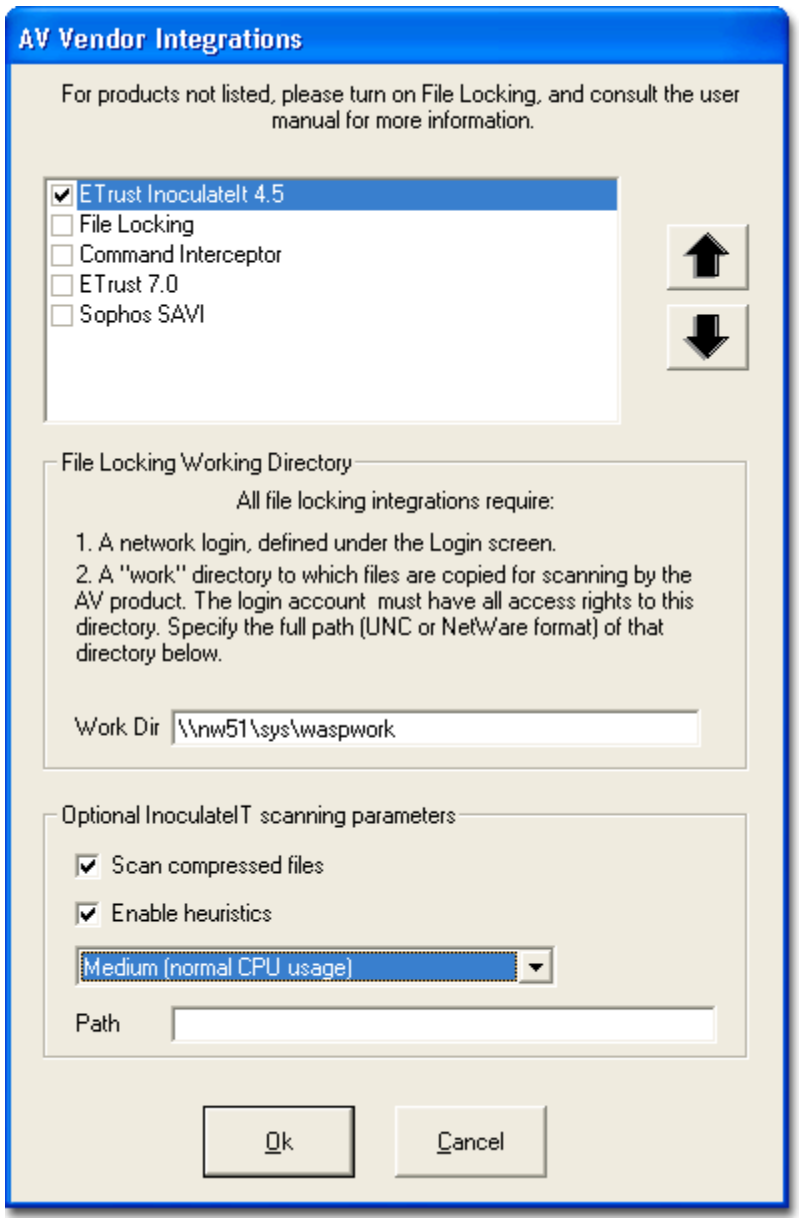
To select which will be used by WASP click **AV Vendor Integrations** and click to enable one or more options. If you are running **McAfee Netshield, Norton Corporate Edition, Sophos** (without SAVI), **Trend Micro, Panda, Kaspersky or Command Antivirus** (not Interceptor), please be certain to select **File Locking**.

File Locking

The working directory for file locking must be specified at log-in with all rights and permissions. You may wish to create a directory with a specific name, prior to entering the UNC path in the data entry field provided.

Special options for ETrust InoculateIT

Scanning options for ETrust InoculatIT are also configured from this screen including: checkboxes to enable **Scan Compressed Files and Enable Heuristics**; **CPU load preferences** and the **Path** to the VIRSIG.DAT file (Normally in `sys:inoculan`). CPU load preferences are managed by a drop down menu at the bottom of the window. The options available are **low**, **medium** and **high**. The default is medium.



Integration Order

WASP has the ability to alter the order of your AV integrations. Select the active AV integration in the AV Vendor Integrations window, then use the **Up** and **Down** arrows to the right to alter the scanning order.

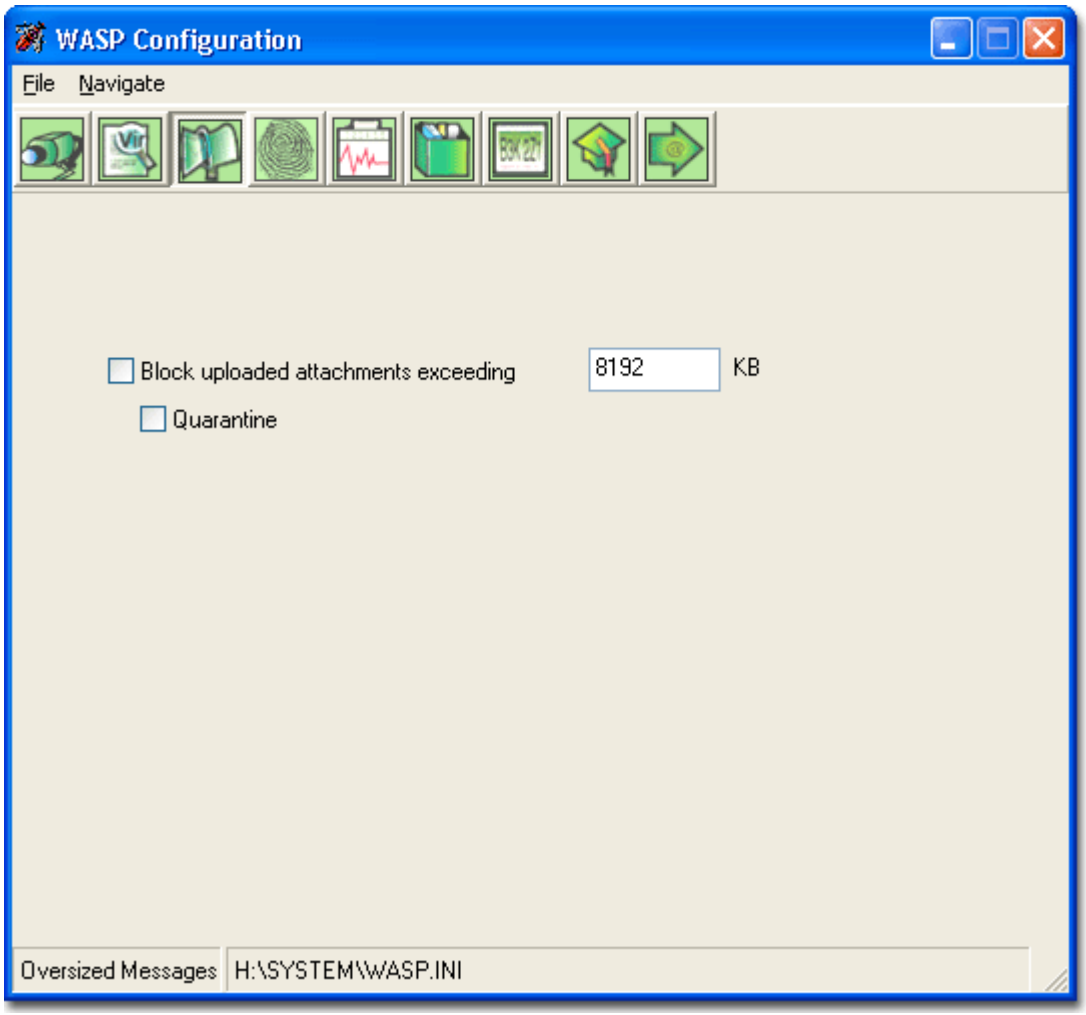
Once you have edited your AV settings, click **OK** to save or **Cancel** return to the previous screen without making any changes.

Configuring AV engines

For more about configuring AV engines to work with WASP, see the appendix at the end of this manual.

Oversized Messages

This section configures how WASP blocks attachments based upon their size.

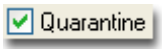


Turn on oversized message blocking by clicking the **Block attachments exceeding** checkbox.

To set the upper limit on attachments that can be uploaded to your GroupWise environment via web access, enter a figure in kilobytes in the data entry field next to the check box.

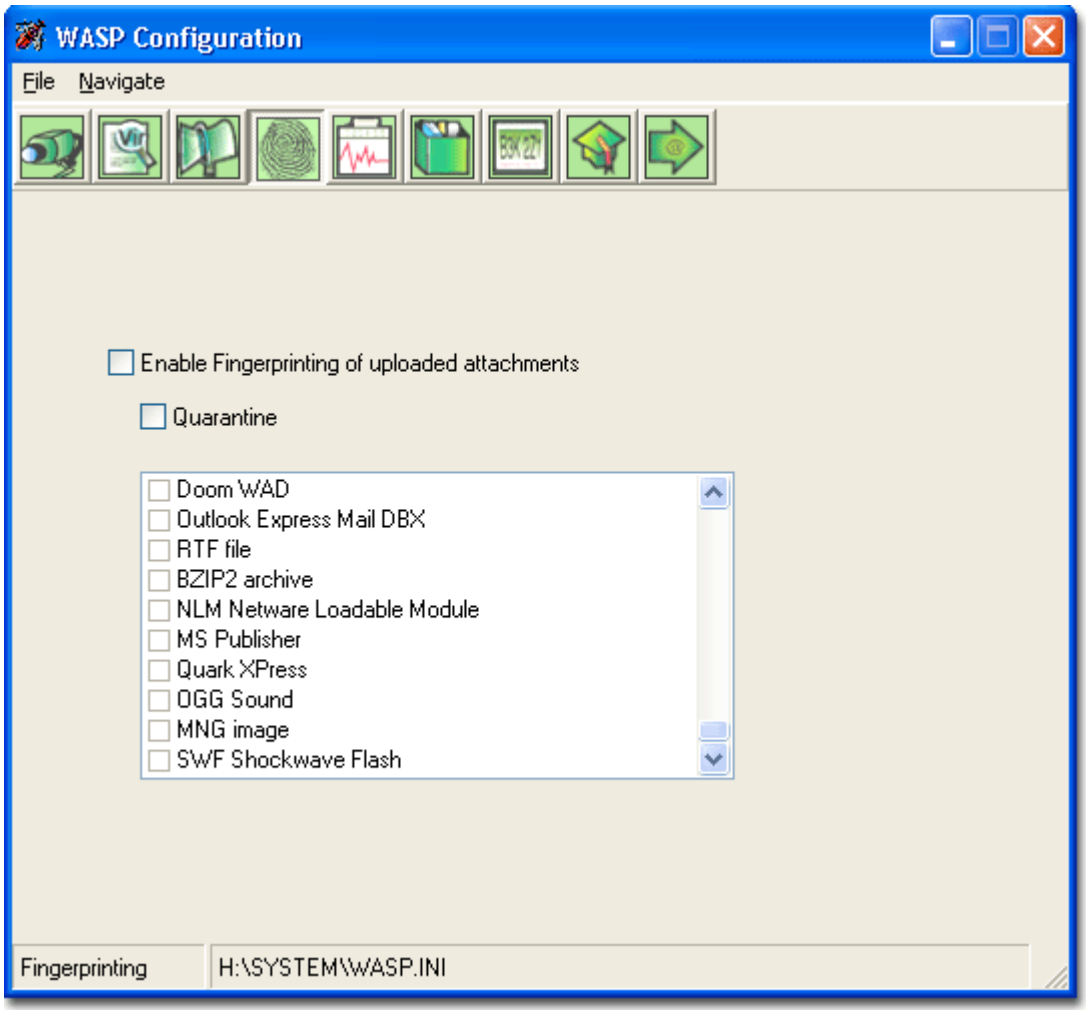
Quarantine

To quarantine *oversized* files, enable the **Quarantine** checkbox. Files will be stored rather than deleted when this is enabled. Quarantine of fingerprinted or infected files being transmitted through Web Access must be enabled separately.



Fingerprinting

This screen configures options for identifying file types.



Differences between Fingerprinting and Conventional Attachment Blocking

Fingerprinting is *similar to, but different from* conventional Attachment Blocking: Attachment Blocking is based on file **name**, and Fingerprinting = block by file **format**

An attachment block for *.SCR* would only block a SCR file that has an extension of SCR, like *test.scr*. If you were to rename *test.scr* to *test.abc* the attachment would not be blocked.

Fingerprinting ignores the file name and extension and concentrates on the file's format, so a renamed PIF file like *test.abc* could not slip past WASP's Fingerprinting.

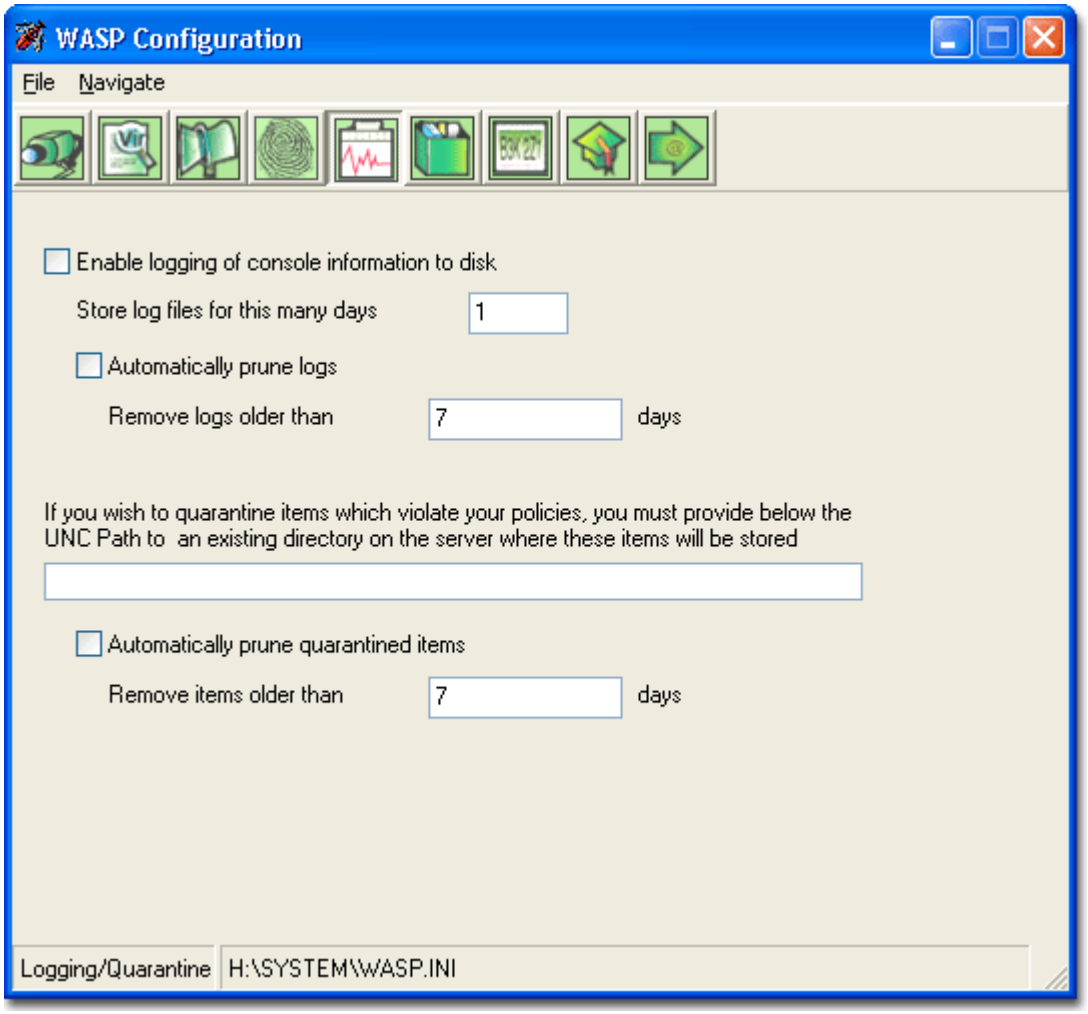
To enable fingerprinting, click the **Enable Fingerprinting of uploaded attachments** box in the Fingerprinting window; then, enable the checkboxes in the list provided to search for the file types desired, regardless of current extensions.

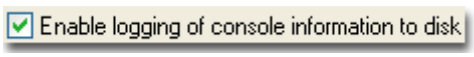
Quarantine

To quarantine fingerprinted files, enable the Quarantine checkbox. Files will be stored rather than deleted when this is enabled. Quarantine of oversized or infected files being transmitted through Web Access must be enabled separately.

Logging

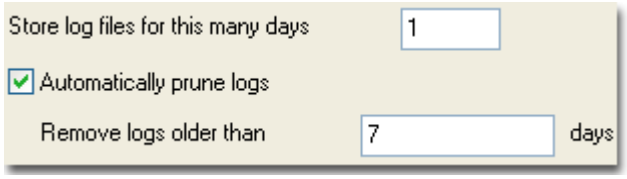
The Event Logging screen is where WASP's reporting is configured.





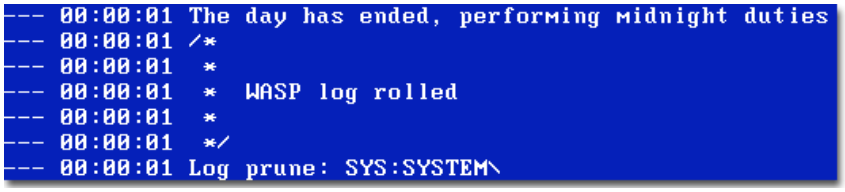
To turn on logging, click the Enable logging of console information to disk checkbox.

When enabled, WASP will write activity logs in the same directory that the WASP program file is running. You can limit the length of time a log file is stored by entering a number of days in the **Store log files for this many days** field. If you enter 7 in this field, log files will be purged after one week.



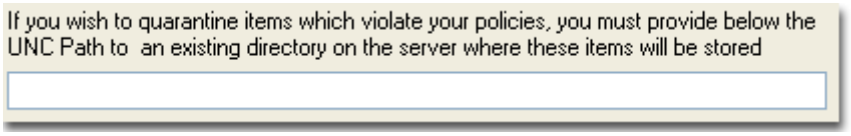
Prune Logs

Another means of limiting the size of log files is to enable the **Automatically Prune Logs** checkbox. Enabling this checkbox activates the items beneath: **Remove archives older** than and **Remove at** what time. The defaults for these are seven days and 2 a.m. respectively. **Note**: the time of day must be specified using a 24-hour clock.

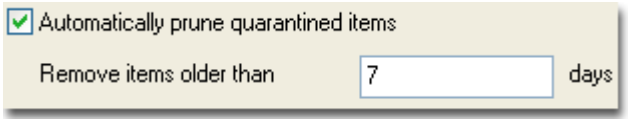


Quarantine Options

If you wish to set WASP to hold infected, oversize or fingerprinted attachments, you must set the storage location for them. Please ensure that the volume has enough space available for your needs; then enter the full UNC path to the quarantine location in the data entry field on this screen of the WASP configuration program.

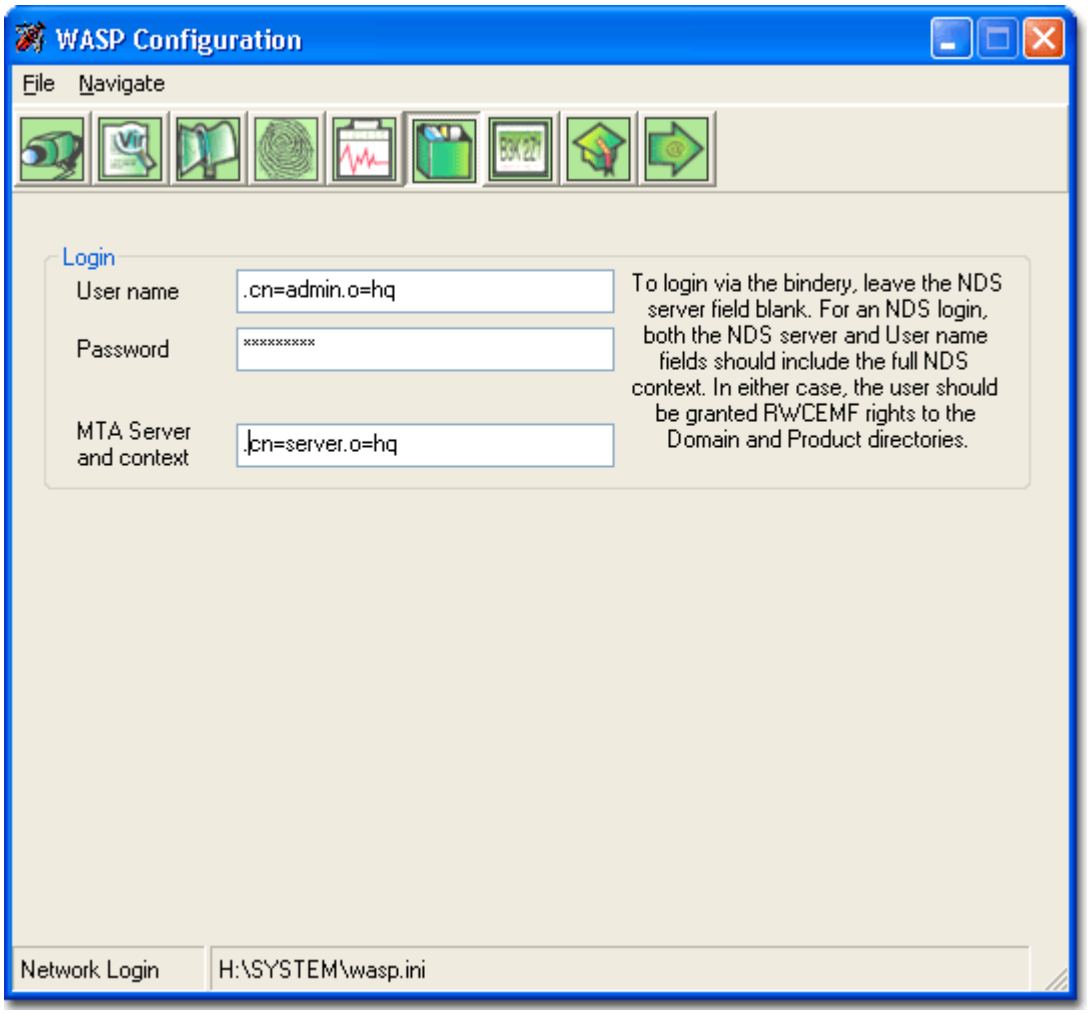


Another means of controlling the size of your quarantine directory is to enable the **Automatically prune quarantined** items checkbox. Use **the Remove items older than** data entry field to determine how long files are kept. The default is seven days.



Log-In

Network login information is specified here 



Network login is only required if you have selected **File Locking** in WASP's anti-virus settings.

For NDS logins, the **User Name** should be the FDN (.CN=Admin.O=Company), and the **NDS Server Context** should be the FDN as well (For example, .CN=MyServer.O=Company).

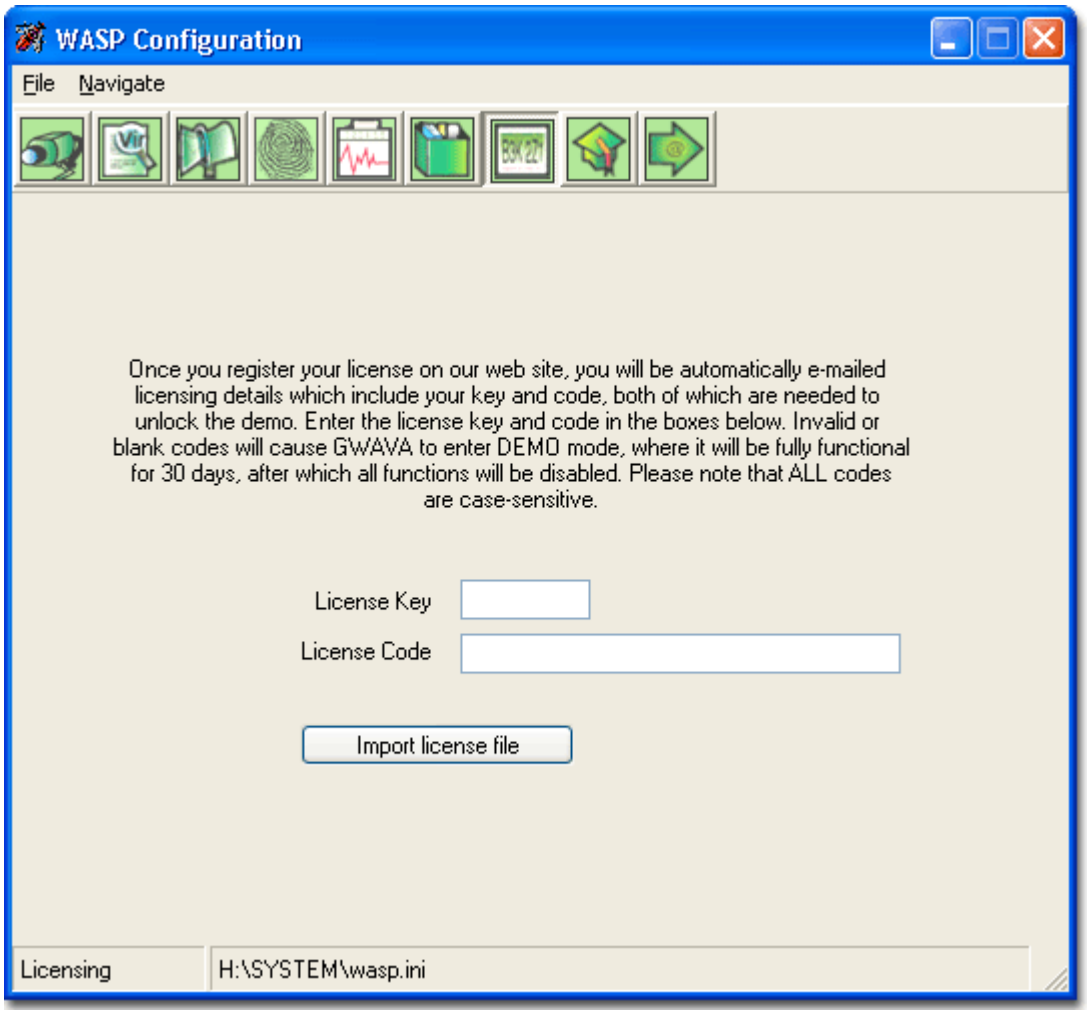
NOTE: The user account should have RWCEMF rights to the following directories:

1. The directory in which WASP.NLM and WASP.INI was installed (e.g. SYS:SYSTEM)
2. The WebAccess file upload directory (normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, which is normally installed in \\server\sys\novell\webaccess)
3. The working directory for file locking (if you are using a file flocking AV NLM). See the Virus Scanning section for more information.
4. The Quarantine directory (if quarantining is enabled).

For bindery login, please ensure your server is running bindery emulation, and that you have specified a leaf object in the Bindery Context (for example, .admin). You do not need to complete the NDS Server Context when performing a bindery login.

Licensing

This screen unlocks the WASP demo once you have purchased your per user license.



Unlocking WASP

- Launch WASP
- Select **Licensing** from either the **Navigation** menu or the button bar.
- Copy & Paste in your License Key and License Code
- Click **Save** from the **File** menu.

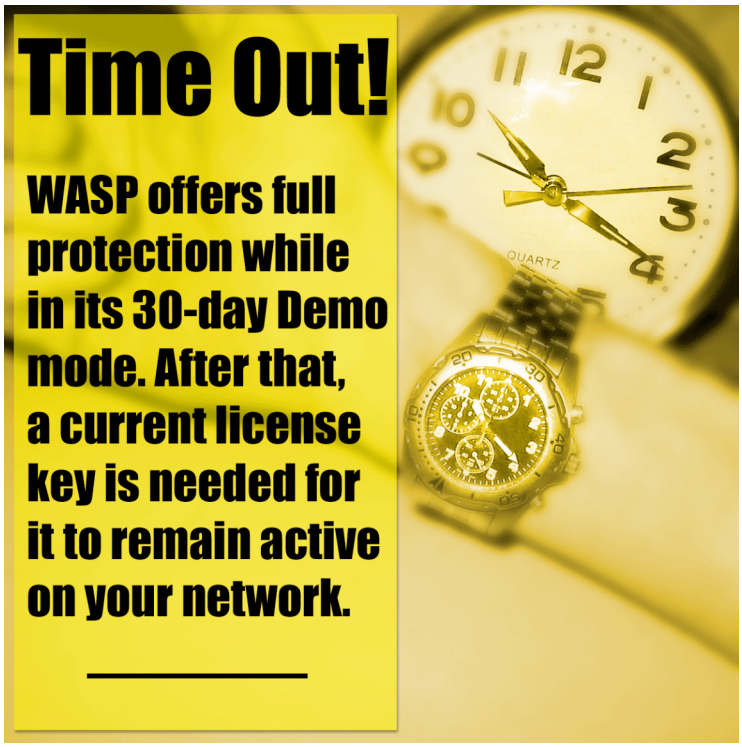
Once you register your license on our web site, you will be automatically e-mailed your license key and code, **both** of which are needed to unlock the demo. Note that the Key and Code are case sensitive. There is no need to re-install and reconfigure WASP as it remembers all of your settings and customizations.

If your license is delivered to you in the form of a license file, you can also import an existing license key by means of the **Import License File** button. To use this feature, click the button and navigate to your existing license key file.

Two-part combination

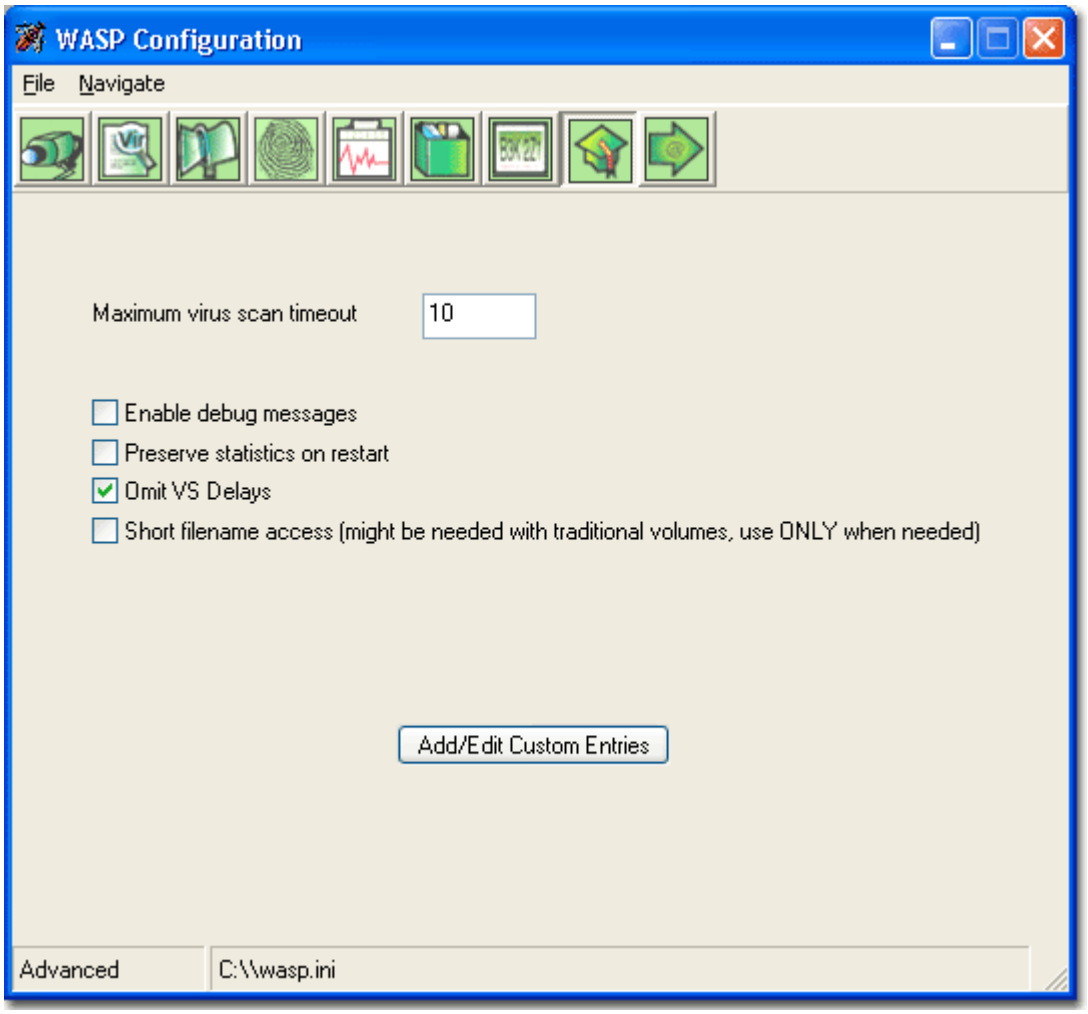
WASP uses a two-part combination. There is a License *Key* and a License *Code*. For WASP to work properly, and not time out after 30 days, you must enter both pieces of information correctly.

Invalid keys and codes or fields left blank will cause WASP to remain in demo mode.



Advanced

Settings for fine-tuning your WASP installation —use with caution.

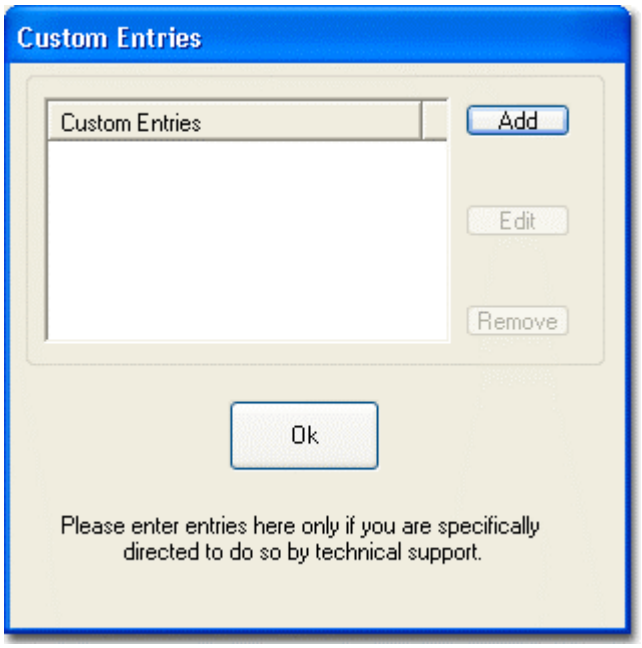


Please avoid making any changes to these settings unless you are doing so with the guidance of GWAVA technical support.

- **Maximum virus scan timeout**: This specifies how long before a virus scan is timed out. WASP's default setting is 10 minutes.
- **Enable debug messages.** Outputs more verbose information to the log that may be helpful for troubleshooting.
- **Preserve statistics on restart:** Keeps cumulative statistics on the WASP NLM screen.
- **Omit VS delays:** Performance setting for virus scanning. If you have difficulty catching viruses, it may be necessary to change the default.
- **Short filename access** (might be needed with traditional volumes, use ONLY when needed.)

Custom Entries

These should not be adjusted unless you are instructed to do so by WASP support. This section is informational so that in the event you are ever instructed to adjust these settings you will be familiar with the interface. Click the **Add/Edit Custom Entries** button to begin.

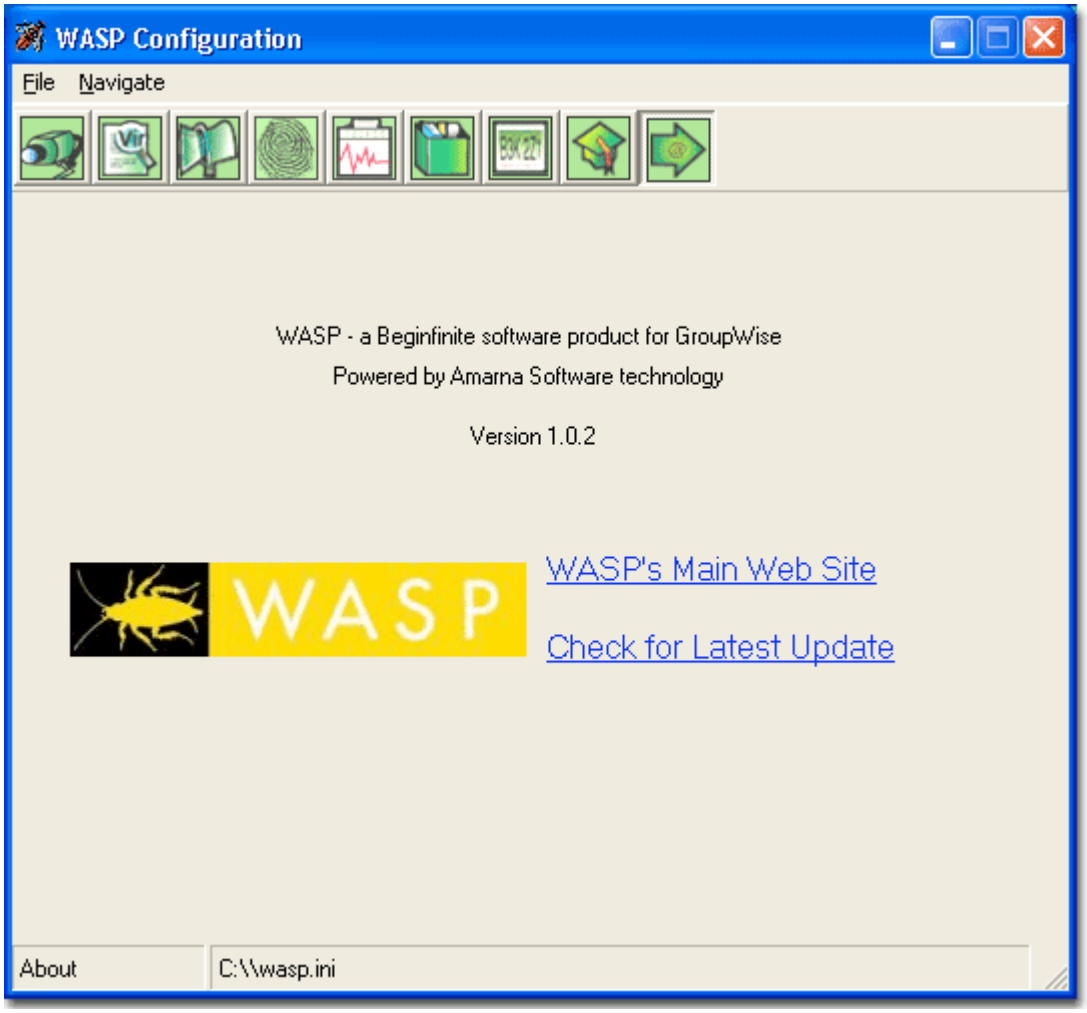


To open the Custom Entries dialogue box, click **Add** or **Edit** Custom Entries when you are instructed to add an entry by our support team.

In the space provided, enter the custom entry field you are instructed by Beginfinite Technical Support. Click **Ok** twice to return to WASP's **Advanced** settings screen.

About

This informational screen shows information about your build and installation of WASP.



You can confirm your GWAVA version number from this screen, as well as check for updates.

30-day demo

If you are evaluating WASP without a valid license, you automatically enter Demo mode. WASP's demo is fully-featured, and can provide your system with protection for thirty days.

Removing WASP

Uninstalling WASP from your GroupWise environment is straightforward. Other than adding several files into SYS:SYSTEM, there are no changes made to the server.

- No NDS schema modifications are made by WASP.
- No modifications are made to the GroupWise domains, GroupWise post offices, or message store.

To remove the WASP.EXE configuration program and other dependencies on the Windows workstation, use Add/Remove Programs in the Windows Control Panel.

To deactivate the server-based NLMs:

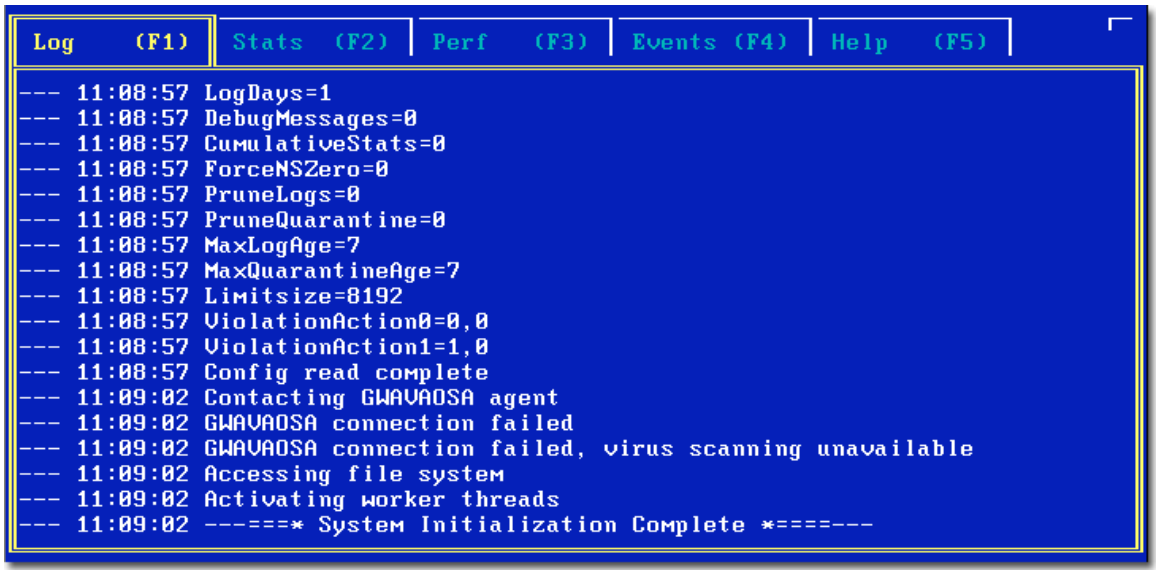
- From the server console, unload WASP.
- From the server console, unload GWAVAOSA.NLM
- Remove the following files from SYS:SYSTEM:
  - WASP.NLM
  - WASP.INI
  - GWAVAOSA.NLM (if not used by another GWAVA product)

Optional

If your AV NLM was being used exclusively in conjunction with GWAVA, follow the vendor's instructions for uninstalling the AV NLM.

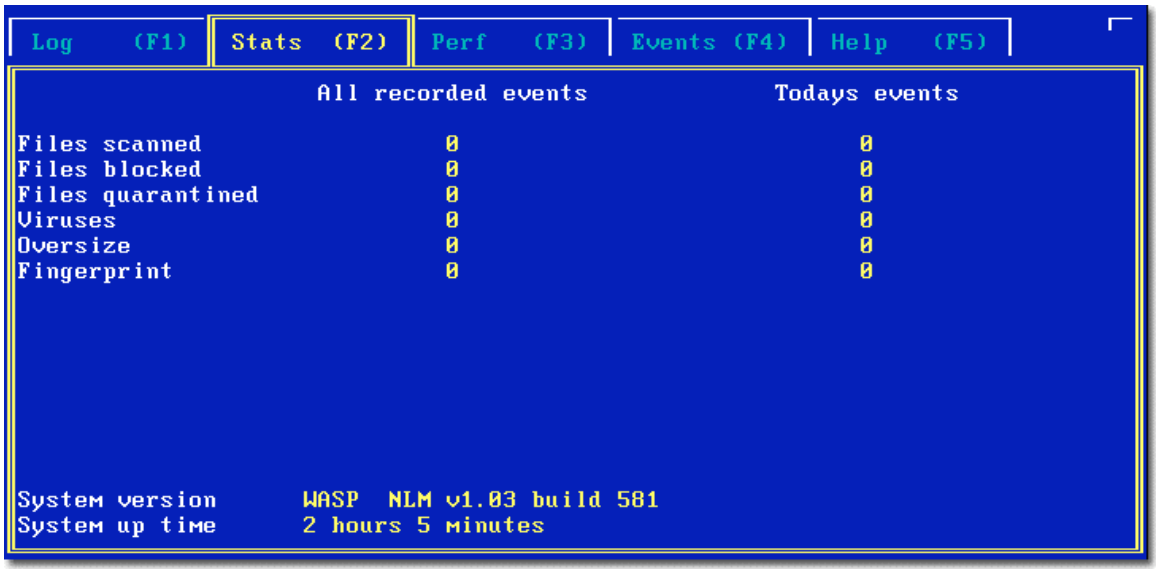
The Wasp Program Interface

The Log Screen



The default screen is the Log screen. It is available by pressing **F1**. It summarizes ongoing operations of WASP in your installation.

Statistics

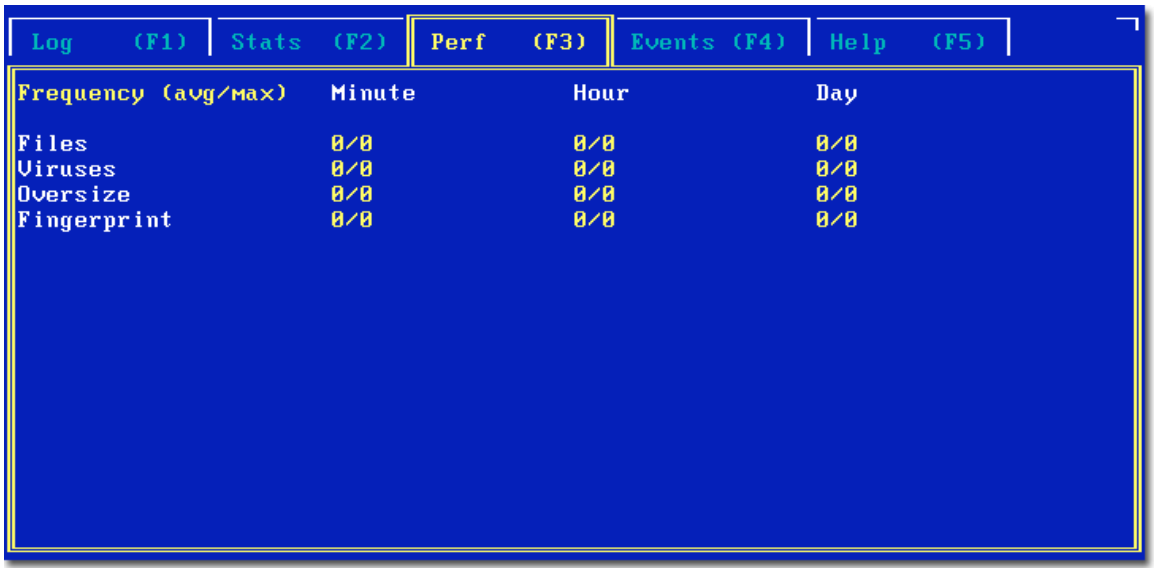


The Statistics screen reports the cumulative ongoing operations of WASP. Statistics available include:

- Files Scanned
- Files Blocked
- Files Quarantined
- Viruses
- Oversized Messages
- Fingerprinting
- System version
- System Uptime

These are broken down further into all recorded events overall and per message as well as overall today and per message today. This screen is presented by pressing **F2**.

Performance



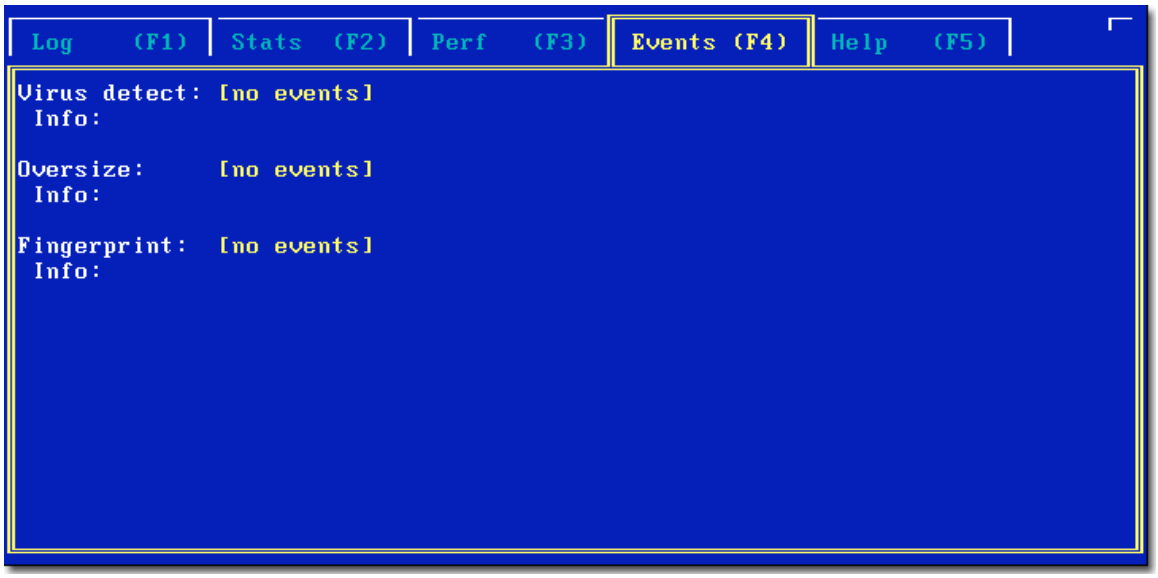
The Performance screen reveals how often events occur. It is useful when identifying spikes in viruses or spam. Statistics available include:

- Files
- Viruses
- Messages Oversized
- Fingerprint

These are broken down further into the frequency of recorded events per minute, per hour and per day.

This screen is presented by pressing **F3**.

Events



The Events screen reports WASP events including:

- Virus Detections
- Oversize Detections
- Fingerprint Detections

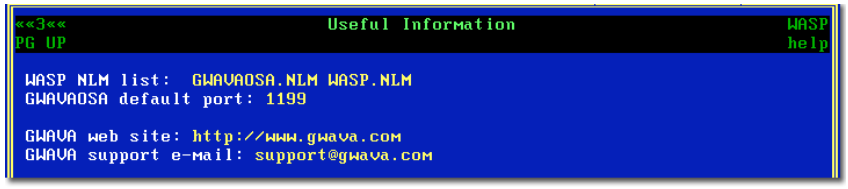
Summary details from the From header and other information are also included for each category. This screen is presented by pressing **F4**.

Help

The WASP Program also has a help file which lists key commands for the WASP NLM. Pressing **F5** presents the list. This spans several pages. Use the **Page Down** and **Page Up** keys to navigate through these screens. WASP supports the following keyboard commands:

- **F1** - Log Screen
- **F2** - Statistics Screen
- **F3** - Performance Screen
- **F4** - Events Screen
- **F5** - Help (Page Down/Up for additional screens)
- **F7** - Exit Wasp
- **CTRL+S** - Reload the system configuration
- **CTRL+T** - Tests the configuration file

Page down again to see the version of your WASP installation and product URLs.



Appendix: AV Engine Configuration

CA eTrust Antivirus (Formerly InoculateIT) 4.5 or higher

- **Note:** If eTrust was not installed to the SYS volume, create the following folder: SYS:INOCULAN and copy VIRSIG.DAT into the newly created directory.
- Install eTrust Antivrus (InoculateIT), and run it (ISTART4.NCF).
- In the Configuration, and Real-Time Monitor menu, set Direction to Disabled. Save your changes.
- In the WASP Configuration Manager, click on the AV vendor integrations button, and select eTrust InoculateIT 4.5 from the menu. Save your changes by clicking OK.
- **Note**: If the virus scanner engine is not loaded when WASP starts, it will not use the integration. You cannot enable this after the fact, so the AVENGINE.NLM must be loaded prior to WASP.

CA eTrust 7.x

- Install eTrust Antivrus. Run it by typing AVLAUNCH INOSTART at the server console.
- In the WASP Configuration Manager, click on the AV vendor integrations button, and select eTrust 7.0 from the menu. Save your changes by clicking OK.
- Configure your exclusions via the eTrust Antivirus Realtime settings (using the Exclusions section of the Filters tab on the Realtime Monitor Options dialog). Add the WebAccess file upload directory. This is normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, and normally installed in \\server\sys\novell\webaccess
- **Note**: If the virus scanner engine is not loaded when WASP starts, it will not use the integration. You cannot enable this after the fact, so the AVENGINE.NLM must be loaded prior to WASP.

NAI Netshield 4.11/4.5/4.6 (or higher)

- Install Netshield, and load the server-based NLM (NETSHLD.NCF). Then run the Netshield Console.
- Right-Click the NetShield On-Access Monitor and select Properties.
- In Scan, files written to and from the server should be scanned.
- In What To Scan, All Files should be scanned.
- In Actions, either Move Infected files to a folder or Delete Infected Files Automatically can be selected.
- Under Exclusions, add the WebAccess file upload directory. This is normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, and normally installed in \\server\sys\novell\webaccess.

Norton Antivirus Corporate Edition 7/7.5/7.6/8.0 (or higher)

- Options for the server-based NLM are configured in the Symantec System Console (SSC), which requires an NT workstation or server machine.
- After you install the SSC and the server-based NLM, load the server based NLM as instructed. (LOAD VPSTART /INSTALL the first time, and VPSTART afterwards).
- Run the SSC.
- Select the Server, unlock it, and Choose the Server RealTime Protection Options
- The Enable file system realtime protection checkbox should be checked.
- Set File Types to All Types.
- In Macro Virus options, set the primary action to Quarantine, and the secondary action to Delete. Repeat for Non-Macro viruses.
- The Exclude selected files and folders checkbox should be checked.
- Click Exclusion and add the WebAccess file upload directory. This is normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, and normally installed in \\server\sys\novell\webaccess.
- You may wish to enable/disable Display Message on infected computer.

Command Interceptor

- Interceptor is not the same as Command Antivirus. If you do not have Command Interceptor, please follow the Command Antivirus configuration or contact Command Software for information regarding Interceptor.
- Install the NLM, run it (LOAD CSSCAN).
- If you also have Command Antivirus running on your WASP server, disable realtime scanning or exclude the **entire** Domain and Post Office directories.
- In the WASP Configuration Manager, click on the AV vendor integrations button, and select Command Interceptor from the pull-down menu. Save changes by clicking OK.
- **Note**: If the virus scanner engine is not loaded when WASP starts, it will not use the integration. You cannot enable this afterwards, so the CSSCAN.NLM must be loaded prior to WASP.
- You can optionally edit the Virus notifications in the Location of files section of the WASP configuration manager and add the %%VirusName variable which is compatible with this AV NLM.

Command AntiVirus for NetWare 4.58 (or higher)

- Options for the server-based NLM are configured in a Windows based program (Command AntiVirus for Netware Administration).
- Install the NLM, run it (LOAD F-PROT), and run the Command AntiVirus for NetWare Administration.
- Select the Server, and under the Task Menu, choose Real-Time Scans
- In Settings, set Action on Infection to Quarantine or Delete.
- In Settings, select both Scans On Opens and Scans on Closes.
- In Exclude, add the WebAccess file upload directory. This is normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, and normally installed in \\server\sys\novell\webaccess. All subdirectories will automatically be added, although the interface does not make this obvious.

Trend Micro's ServerProtect for NetWare 3.71/5.0/5.1 (or higher)

- Options for the server-based NLM are configured in a Windows based program (Supervisor Configuration Utility).
- Install the NLMs. Make sure they are running (SPNW.NCF), then run the Supervisor Configuration Utility.
- Double-click the server, and unlock it. Then choose File Checking from the Configure Menu.
- In the RealTime tab, make sure ALL Files are selected for DOS.
- In the RealTime tab, enable all the Incoming/Outgoing File Checking options—all 5 checkboxes should be checked.
- In the Exception Tab, add the WebAccess file upload directory. This is normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, and normally installed in \\server\sys\novell\webaccess.
- In the Action Tab, set Action on Virus Identification to Wipe Out or Move.
- You may wish to disable the BROADCAST message for Configure Actions.

Panda Antivirus 2.5 (or higher)

- Options for the server-based NLM are configured in a Windows based program (Panda Administrator)
- Install Panda Antivirus, and load the server-based NLM (PAV.NLM). Then run the Panda Administrator.
- Select the server and the Configure button.
- In the Configuration of the Permanent Protection tab, under General Options, all boxes should be checked.
- In the Configuration of the Permanent Protection tab, under If a virus is found, select either Delete file or Quarantine file.
- Under Exclusions, add the WebAccess file upload directory. This is normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, and normally installed in \\server\sys\novell\webaccess.

Sophos SAVI

- Sophos SAVI is not the same as Sophos Sweep. If you do not have Sophos SAVI, contact Sophos for information regarding SAVI.
- Install the program files. Typically the virus definitions go into SYS:\SOPHOS\SAVI and the NLMS (SAVI and VEEX) got into SYS:\SYSTEM
- If you also have Sophos Sweep running on your WASP server, disable real time scanning or exclude the ENTIRE Domain and Post Office directories (Ignore the directory exclusion instructions earlier.
- In the WASP Configuration Manager, click on the AV vendor integrations button, and select Sophos SAVI from the pull-down menu. Save changes by clicking OK.
- **Note**: SAVI may be safely loaded before WASP starts. Alternatively WASP will automatically load it when needed.

Kaspersky AntiVirus for NetWare 3.5 (or higher)

- Options for the server-based NLM are configured through a snapin for NetWare Administrator (NWADMN32.EXE)
- Install Kaspersky Antivirus, and load the server-based NLM (AVKERNEL.NLM). Then run NetWare Administrator.
- Double-click on the AVPN object in order to access the configuration.
- In the Real-time Scanning tab, under Exclude These Folders and add the WebAccess file upload directory. This is normally \\server\sys\novell\webaccess\temp. It is specifically defined in webacc.cfg, and normally installed in \\server\sys\novell\webaccess.
- In the Real-time Scanning tab, under Files to Scan, check the Except These Extensions box and add *.DB.
- In the Actions tab, under Actions to Take with Infected Files and Action to Take with Suspicious Files, select either Delete or Move to Quarantine Directory.

Contact WASP

For all of your support and purchasing needs, please visit our home page at www.gwava.com.

100 Alexis Nihon, Suite 500
Montreal, QC, H4M 2P1, Canada.
E-Mail: info@gwava.com