

WASP 2.0

Installation and Admin Guide

Contents

Deverview 4 Obtaining WASP2 4 Starting and stopping WASP2 4 Licensing and Support 5 Where to install WASP2 6 Installation 7 GWAVA 4 Server Activation 13 Creating a WASP2 Scanner 15 Remote Scanner Installation 19 Configuration 24 General Settings 24 Scanning Configuration 25 Antivirus 25 Text filtering 25 Oversize 25 Oversize 25 Source address filter (From:), Destination filter (To:) 25 Signature 26 Global Quarantine 26 Blind Carbon Copy 26 Exceptions 26 Scanner Information 26 Status 26 Scanner Information 26 Status 26	System Requirements
Obtaining WASP24Starting and stopping WASP24Licensing and Support5Where to install WASP26Installation7GWAVA 4 Server Activation13Creating a WASP2 Scanner15Remote Scanner Installation19Configuration24General Settings24Scanning Configuration25Antivirus25Text filtering25Oversize25Source address filter (From:), Destination filter (To:)25Message services26Signature26Blind Carbon Copy26Exceptions26Scanner Information26Status26 </th <th>Overview</th>	Overview
Starting and stopping WASP2 4 Licensing and Support 5 Where to install WASP2 6 Installation 7 GWAVA 4 Server Activation 13 Creating a WASP2 Scanner 15 Remote Scanner Installation 19 Configuration 24 General Settings 24 Scanning Configuration 25 Antivirus 25 Text filtering 25 Mime filtering 25 Oversize 25 Fingerprinting 25 Source address filter (From:), Destination filter (To:) 25 Signature 26 Signature 26 Signature 26 Scanner Information 26 Scanner Information 26 Status 26	Obtaining WASP2 4
Licensing and Support 5 Where to install WASP2 6 Installation 7 GWAVA 4 Server Activation 13 Creating a WASP2 Scanner 15 Remote Scanner Installation 19 Configuration 24 General Settings 24 Scanning Configuration 25 Antivirus 25 Text filtering 25 Mime filtering 25 Oversize 25 Fingerprinting 25 Attachment types 25 Source address filter (From:), Destination filter (To:) 25 Message services 26 Signature 26 Blind Carbon Copy 26 Exceptions 26 Status 26 Status 26 Status 26 Status 26 Status 26	Starting and stopping WASP24
Where to install WASP26Installation7GWAVA 4 Server Activation13Creating a WASP2 Scanner15Remote Scanner Installation19Configuration24General Settings24Scanning Configuration25Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Blind Carbon Copy26Exceptions26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26Status26	Licensing and Support
nstallation7GWAVA 4 Server Activation13Creating a WASP2 Scanner15Remote Scanner Installation19Configuration24General Settings24Scanning Configuration25Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Blind Carbon Copy26Exceptions26Scanner Information26Status26Status26Status26Statistics26<	Where to install WASP2
GWAVA 4 Server Activation13Creating a WASP2 Scanner15Remote Scanner Installation19Configuration24General Settings24Scanning Configuration25Antivirus25Text filtering25Mime filtering25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Blind Carbon Copy26Exceptions26Status26Status26Status26Statistics26	Installation7
Creating a WASP2 Scanner15Remote Scanner Installation19Configuration24General Settings24Scanning Configuration25Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Status26Status26Statistics26St	GWAVA 4 Server Activation
Remote Scanner Installation19Configuration24General Settings24Scanning Configuration25Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Blind Carbon Copy26Exceptions26Status26Status26Statistics26Statistics26	Creating a WASP2 Scanner15
Configuration24General Settings24Scanning Configuration25Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Statistics26	Remote Scanner Installation
General Settings24Scanning Configuration25Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Statistics26	Configuration
Scanning Configuration25Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Scanner Information26Status26Status26Status26Status26Status26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26Statistics26	General Settings
Antivirus25Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Status26Status26Status26Status26Statistics26Statistics26	Scanning Configuration
Text filtering25Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Status26Statistics26	Antivirus
Mime filtering25Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Status26Status26	Text filtering
Oversize25Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Statistics26	Mime filtering
Fingerprinting25Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Statistics26	Oversize
Attachment types25Source address filter (From:), Destination filter (To:)25Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Statistics26	Fingerprinting
Source address filter (From:), Destination filter (To:)25Message services26Signature.26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Status26Status26	Attachment types
Message services26Signature26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Statistics26Statistics26	Source address filter (From:), Destination filter (To:)
Signature.26Global Quarantine26Blind Carbon Copy26Exceptions26Scanner Information26Status26Statistics26Statistics26	Message services
Global Quarantine 26 Blind Carbon Copy 26 Exceptions 26 Scanner Information 26 Status 26 Statistics 26 Statistics 26	Signature
Blind Carbon Copy 26 Exceptions 26 Scanner Information 26 Status 26 Statistics 26	Global Quarantine
Exceptions	Blind Carbon Copy
Scanner Information	Exceptions
Status	Scanner Information
Statistics	Status
	Statistics
Configure WASP Settings	Configure WASP Settings
Manage Scanner Object	Manage Scanner Object
Scanner Event Actions	Scanner Event Actions
our State Checkboxes	Four State Checkboxes

Uninstalling WASP2 scanner	28
Licensing	29
Uninstalling WASP 2	31
	33
WASP 2 notifications	33

Copyright Notices

The content of this manual is for informational use only and may change without notice. GWAVA 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. Windows is copyrighted by Microsoft. © 2005 GWAVA Inc. All rights reserved.

WASP[®] and GWAVA [®] are registered trademarks of GWAVA Inc. NetWare[®], GroupWise[®], and WebAccess[®] are registered trademarks of Novell, Inc.

System Requirements

GWAVA 4 (build 108 or later) WebAccess 7 (or later) Java 1.4x (or later) OS Platforms – Netware 6.5, SLES 9, 10, OES 1, 2 (In remote mode only) Windows NT* Server, Windows 2000 Server, or Windows 2003 Server, plus the latest Service Pack for your version of Windows

Overview

WASP2, (Web Access Server Protection version 2), is a content scanning solution for GroupWise WebAccess. WASP2 hooks into the WebAccess servlet, working between the message composition interface of WebAccess and the WebAccess agent. This allows WASP2 to scan all messages for viruses and any defined content before they are sent to the GroupWise server. If a problem is found, the message will not be sent and the user is notified of the problem. Effectively, WASP2 fills the protection gap in WebAccess for the GroupWise mail system.

Obtaining WASP2

Browse to <u>http://www.gwava.com/products/dev_downloadform.php</u> and fill out the information requested. After the information has been completed, you will be presented with the opportunity to download GWAVA4, which includes the WASP2 package.

Starting and stopping WASP2

Because of the way WASP2 is built into the WebAccess servlet, there is a recommended start and stop order to ensure the best results from your WASP scanner.

When starting or stopping WASP2, it is a best practice to have GWAVA4 be the first program started, and the last program stopped. Because WASP2 and WebAccess are servlets inside Tomcat, stopping Tomcat also shuts down WASP2 and WebAccess.

Common commands for starting / stopping Tomcat and WASP: (Start and stop commands may differ depending on the installation of WebAccess and your OS.)

Linux: Sles 9x – rctomcat (start/stop/restart) Linux: Sles 10x – rctomcat5 (start/stop/restart) NetWare: (Start – stop commands) tomcat5 - tc5stop tomcat4 - tc4stop

Logs

The log level of WASP is determined by the log setting in the GWAVA management console. (Found under Server/Scanner Management, expand your server, open Server Management, and select the

Configure Server object.) WASP 2 program logs are kept with the GWAVA4 logs, (.../gwava4/services/logs/wasp), unless you are running WASP 2 in remote mode, which then writes the logs to the local machine. The WASP 2 remote log files are kept in the WebAccess application logs directory. (Usually this is found at ...groupwise/webaccess/logs/wasp.)



When WASP starts up, it launches a thread to connect to GWAVAMAN, reads configuration information (from GWAVAMAN), opens log files, etc. Wasp will wait for this initialization to complete. If the initialization completes before the specified amount of time, Wasp continues processing. If the specified time elapses before initialization completes (this may happen if GWAVAMAN is not running), Wasp continues processing anyway. If this happens and the log files have not been opened, any data written to the log files will be written to the WebAccess application log. WebAccess has its own log level, and may not record all messages. This is intended mainly for diagnostic purposes.

Licensing and Support

If your WASP 2 install is not an evaluation, obtain the license file for WASP 2 at <u>https://licenses.gwava.com/</u>, or contact your sales representative.

GWAVA 4 and WASP 2 support and support information can be found on the web at <u>http://support.gwava.com</u>.

Preparation

We will first install GWAVA 4 and then the WASP2 package will be installed to the GWAVA 4 server. After WASP 2 is installed, we can create and install the WASP 2 scanner. When the scanner is created, WASP 2 will be connected to the WebAccess system. WebAccess needs to be installed and working before a WASP 2 scanner can be created. If you already have an existing GWAVA 4 server in your network, you may install WASP 2 on that server.

If you have a running installation of WASP 1, it should be uninstalled before installing WASP 2.

The necessary packages are: WebAccess GWAVA 4 Unified installer package Know the location of the active webacc.cfg Know the working directory of Tomcat, (path to the 'webapps' sub directory).

You can find the install files for both WASP2 and GWAVA 4 at <u>http://www.gwava.com/solutions/trial-downloads.html</u>. Fill out the requested information and then download the product of your choice.

Where to install WASP2

Wasp can be installed where any GWAVA 4 server is located. WASP 2 utilizes the scanning engine of GWAVA 4, and must have access to the scanner. Locally scanning the WebAccess system is the best option, but WASP 2 also has the ability to access the GWAVA scanning engine over the network, through TCP, to remotely scan a WebAccess system. To scan a WebAccess system not on the local machine, the GWAVA 4 scanner port must be available and open between the remote WebAccess machine and the GWAVA 4 server. See the <u>Remote Scanning</u> section for details.

Installation

WASP 2 is installed using the GWAVA unified installation package, which can install both WASP 2 and GWAVA 4. This package can be run to install to Linux or Netware. To start the installation for NetWare, a Microsoft Windows computer with access and admin

rights to the NetWare server must be used, double click on the GwavaSetup.
build#>.jar from the Microsoft Windows compute to initiate the installation program.



For Linux, if your system has associated .jar files to be run automatically with your java system, you may simply double-click the icon on the desktop. Otherwise, and for most systems, you must open a terminal in the GUI and run the installer from the command line using the following command:

java –jar gwava_setup.jar

Once the installer is run, you should be greeted by the following screens.



Click 'Next' to continue.



Specify that you agree to the license and click 'Next' to continue.



The Readme provides important change and feature information. Please read then select 'Next' to continue.



From Windows, the Linux installation platform will not be available. If installing to Linux, perform the Linux install on the local machine. Select your platform and select 'Next'.



The installer can modify the autoexec.ncf, or the default runlevel, to make GWAVA and WASP automatically run on system boot. The option to start GWAVA and WASP when the installer has finished is only available on Linux. Select your settings, and click 'Next'.

🔤 GWAVA Installer 🛛 🔀					
GWAVA	Proxy Configuration				
	GWAVA 4 and WASP 2 require access to the internet to retrieve anti-virus definitions and program updates from the web. If you use a proxy to contact the internet, provide the correct information here. If you do not use a proxy in your system, click "Next" to proceed.				
	Proxy Server (ex: proxy.myfirewall.com:8080): Proxy Username:				
	Proxy Password:				
	Cancel Back Next				

WASP 2 and GWAVA 4 receive program updates and virus definitions from the internet, and must have access to the internet for this to work. If your system uses a firewall or a proxy that utilizes a login to receive port 80 access to the internet, specify it here. This is critical to keep your system up to date.

If you do not use a proxy or login to connect to the internet, leave the settings blank, and select 'Next'.



You will be asked to select the GWAVA 4 and WASP 2 installation directory. The default assumes a mapped drive to the desired target volume or location. For the NetWare installation, if you do not have a mapped drive, you must specify the correct destination.



The installer now asks to verify all your provided settings. Double check all your settings. Once you click 'Next', all files will be copied to the system. This is your last chance to cancel the installation before the installation is performed.



Once the installation starts, it may take a while to complete. The status bar shows the status of the current action, and not the completed status of the total installation.



Once the installation has completed, you will be given a report of the installation status and connection information.

If you installed to NetWare, you must add a search path before you can start GWAVA 4. From the system console type:

Add a search path to the GWAVA 4 bin directory.

Search Add <volume>:\<gwava_install_dir>\assets\bin (Example : Search Add gwvol:\gwava4)

Start your server, (if it is not already running), then connect to the web management console. Start commands:

NetWare:	Linux:	
gwavaup		rcgwavaman start
Stop commands:		
NetWare:	Linux:	
gwavadn		rcgwavaman stop

When you have completed the tasks, click 'Finish'.

To continue, make sure that the GWAVA 4 service is running and then open a browser and continue to the setup and server activation by going to:

http://<server_ip>:49282

GWAVA 4 Server Activation

From your workstation, enter the URL <u>http://<your_server_ip>:49282</u>. For example: <u>http://192.168.10.60:49282</u>, then click 'Go' or press ENTER.

 CWUXA 4 Management Console - Microsoft Internet Explorer

 File
 Edit View Favorites
 Tools
 Help

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer
 Image: Console - Microsoft Internet Explorer

 Image: Console -

Choose the default, 'this is a new GWAVA server' and click 'Continue'

Enter the requested information for your environment.

Because this is the first, or only GWAVA m network, we need to gather some rudiment and prepare it for installing the scanner app mail system.	anagement server in yo ory settings to secure th plications that will protec	ur e server t your e-		
Server Param	eters			
Server identifying Name	NW65 (NetWare)	•		
Client connection address	192.168.10.60:49282	4)		
Administration Inf	ormation		i i i i i i i i i i i i i i i i i i i	
GWAVA administrator Login Name	Admin	9		Remember this
GWAVA administrator password	•••••	•		password. You will
Verify administrator password	•••••	()		need this to login
Internet Domain (eg. GWAVA.com)	gwava.com	•		after this sten is
GWAVA administrators full name	GWAVA Four	9		complete
GWAVA administrator e-mail address	gwava4@gwava.com	(i)		complete.
Mail Relay / User Aut	thentication			
SMTP server for notification/authentication	127.0.0.1	•		
SMTP AUTH username	gwava4	•		
SMTP AUTH password	•••••	4)		
Continue]			
			į	

Confirm that the information is accurate and click 'Install'.

Please verify the information below is correct and accurate, and press the install button to proceed with server activation.		
Server identifying name		
Address to access server	192.168.10.60:49282	
Administrator login	Admin	
Administrator password	[concealed]	
Administrator full name		
Administrator e-mail address	gwava4@gwava.com	
SMTP server address		
SMTP AUTH username		
SMTP AUTH password	[concealed]	
	Install	

After the server has been activated, the following screen should appear. This is what you should see when you login to the web interface in the future.

GWAVA 4	Management Console
Network Status	Server Activation Completed
Servers online: 1 Servers offline: 0	Click here to enter the management console. You will require a valid login name and password to enter.
	Enter Management Console

Now that the server is activated, we can proceed with creating a WASP scanner.

To connect to the GWAVA4 Management Console in the future, open any browser that has access to the server and type the URL <u>http://<server_ip>:49282</u>

Scanner creation Management Console Network Status Servers online: 1 Servers offline: 0 Click here to enter the management console. You will
require a valid login name and password to enter. - Enter Management Console --

Log into your GWAVA 4 Management Console to being

Connect to 192.1	68.1.101 ? 🔀
The server 192.168.1 username and passwo	I. 101 at GWAVA Console requires a ord.
User name:	S
Password:	
	Remember my password
	OK Cancel

Creating a WASP2 Scanner

After you have logged into the server, you may begin. On the left-hand pane, expand your view below **Server/Scanner Management**.

X	GWAVA 4
Home	GWAVA.com Support Help Logout
	ome Pages
6	Welcome
V	🗿 Quarantine manager
🕨 в	ookmarks
D 🖉	ocumentation
D S	ystem Management
👿 s	erver/Scanner Management
	BERRE (BLARDANA)
	Server menogement
Ē	i Server management
	Install/create new scanner
	Migrate GWAVA 3 config
	Manage scanners
	Con no menu items available

Expand your server, open the Wizards folder, and Click 'Install/create new scanner' to install a scanner.

۵	Select the type of scanner you wish to install					
	 GroupWise GWIA Mail Interface GroupWise MTA Mail Interface GroupWise POA Scheduled Scan Job WASP Interface 					
	Continue					

Select the WASP Interface and Click Continue

*	Create new WASP scanner
	Welcome to the WASP scanner creation wizard.
	To ensure a smooth installation of this interface, some information about your mail system needs to be supplied. You may also undertake some of these steps manually after the GWAVA network has been configured if you wish to maintain control of the process yourself.
	Prerequisites:
	 Web Access installed, configured and verified that it is running correctly. Location of Web Access directory.
	Post install:
	There are no post installation requirements.
	Continue

To create a scanner you must know the correct information for the location of the Web Access directory and the active Tomcat directory. Click **Continue.**

(The WebAccess startup file is the webacc.cfg – specify the entire path, including the webacc.cfg filename.)

(The Tomcat directory desired is the one containing the 'webapps' directory from which your WebAccess is run. In a standard SLES 10.x system, the path would be: /usr/share/tomcat5. If you have several instances of Tomcat on the same machine, locate the working webapps directory by searching the webacc.cfg file for the "Templates.path=..." line. It will specify the Tomcat path that WebAccess is using. The correct webapps directory will also contain a gw folder - .../webapps/gw.)

It is important to specify the tomcat instance that WebAccess is running on. There may be several instances of Tomcat installed on the same machine at the same time, depending on the way WebAccess was installed.

2	Create new WASP scanner				
	Scanner Name	WASP2			
	Install on this server	linux-o3in (Linux)			
	GroupWise WebAccess startup file	/opt/novell/groupwise/webaccess/webacc.cfg			
	Groupwise webaccess startup he	(example: /opt/novell/webaccess/webacc.cfg)			
	Tomcat Directory	/srv/www/tomcat5/base			
	Tomcat Directory	(example: /tomcat/4)			
		Continue			

Enter the correct information and click **Continue**.



To enable protection from viruses, select an anti-virus engine. On Linux, the Kaspersky engine will be selected for you. On NetWare, you may have other engines to choose from in addition to the Kaspersky engine.

Click Continue.

*	Create new WASP sca	anner
	The requisite information has is correct, press the install be	been collected and is ready to be deployed. If you are satisfied that the installation information utton to commit the installation procedure to the GWAVA network.
	Scanner name	wasp scanner
	Install to server	TEST (NetWare)
	WebAccess startup file	sys:\novell\webaccess\webacc.cfg
	Tomcat directory	sys:\tomcat\5.0
	Stop Viruses	Yes
		Install

Double check all the information for accuracy, then click **Install** if it is correct. Use the back button on your browser if you need to correct any of the information.

Installing WASP scanner

Installation tasks are now being performed. On completion, you will be able to continue to configure the scanner services to start protecting your messaging system.

DO NOT change pages during this procedure or the installation will not complete. Please wait until you are taken to the completion response page.

Wait until the next page appears. This may take several minutes depending on the speed of the machine and current load. Please be patient.

Ž	WASP scanner installation finished
	Activating virus scanning
	Activating Attachment Blocking
	Setting up Fingerprinting
	Scanner 'wasp scanner' was created successfully.
	Your GroupWise WebAccess agent needs to be restarted for this WASP scanner to become active. Click the onumber of the Parameters of the P

Once this page appears, your scanner has been successfully created and you can browse away from the scanner creation interface.

NOTE: Your WASP scanner will be dormant until Tomcat is restarted and a browser calls the Web Access interface. This is required to initiate the WASP servlet for the web server. Restart the Tomcat instance you installed WASP to before testing the scanner.

OES and OES2 SYSTEMS: Novell OES systems set the Tomcat User and Group differently than standard Linux systems. Before WASP will function, the User and Group for the WASP scanner must be corrected in the GWAVA 4.5 management interface. The setting is found under Server/Scanner Management | <Server Name> | Manage scanners | <your new WASP scanner> |Configure WASP settings | Mail interface settings. Expand the Show Advanced File System Options link.

Home GWAVA.com Support Help Logout	🗸 😽 WASP interface	
Server/Scanner Management Server/Scanner Management Server manageme	Bypass message scanning Maximum scan threads Scanner timeout	16 3
	(For OES this will need to be changed to noviwww.) (For OES2 this will need to be changed to www.run for the user an Tomcat User: tomcat Tomcat Group: tomcat	d www for the group.)
 	Show Advance Clustering Options	

Change the User and Group according to the requirements of your specific system. The variables are listed in the interface.

OES: change user and group to "novlwww"

OES 2: change user to "wwwrun" and change the group to "www".

WASP 2 scanners rebrand the WebAccess login and mailbox screens to alert users that WASP 2 is in use. If you do not want this and wish to return to the original branding and artwork, the files were renamed and reside in the following directories:

For GroupWise 7: <tomcat_path>/webapps/gw/com/novell/webaccess/images/splash.png

For GroupWise 8: <tomcat_path>/webapps/gw/webaccess/<build_date>/images/install_watermark_n.png

WASP 2 has renamed these to *.bak, (or .bak0 if .bak already exists). Simply rename the file to the original and restart your WebAccess system to return them to default.

Remote Scanner Installation

Running WASP 2 in remote mode means that WASP 2 needs to transfer the mime files via the network to GWAVA 4 in order to be scanned. To create a remote WASP 2 scanner, you will need the following information:

The location of the WebAccess configuration file on remote computer (webacc.cfg) The location of the Functioning WebAccess Tomcat directory – Or IIS directory (The folder containing the 'webapps' directory. See notes <u>above</u>.)

Start the scanner creation wizard as above, but when prompted for the path to the files requested, place invalid paths in the defined areas.

2	Create new WASP scanner	
	Scanner Name	WASP 2
	Install on this server	bitterlinux (Linux)
	GroupWise WebAccess startup file	not/valid/path (example: /opt/novell/webaccess/webacc.cfg)
	Tomcat Directory	/not/valid/path (example: /tomcat/4)
		Continue

The installer will try to verify the path to the installation files, but will fail. This triggers the remote install mode for the scanner.

In remote mode, the installer creates a wasp user and password to connect to GWAVA 4. The Username is created automatically, but you must specify the password. Any password will do. Configure as desired.

2	Create new WASP scanner
	Unable to open WebAccess startup file: not/valid/path Unable to verify Tomcat Path /not/valid/path
	If this is not a remote install, click here to go back to the previous page and correct the paths Password for Remote Install:
	9 Your gwava system already has one or more scanners configured. Choose this option to share an existing scanner configuration
	You can quickly setup the scanner with some of the most common default security options
	Stop Viruses
	This server will use Kaspersky AV engine to scan for viruses
	Enabling virus scanning includes enabling virus sanner services and detecting file types that frequently include viruses with attachment type scanning (i.e. *.vbs, *.pif, *.exe etc) and fingerprinting of attachments.
	advanced settings
	Continue

Verify all information, and click 'install' when the information is correct. Use the 'back' button on your browser if you need to change any of the information before you continue.

*	Create new WASP sca	nner
	The requisite information hat press the install button to con	s been collected and is ready to be deployed. If you are satisfied that the installation information is correct, nmit the installation procedure to the GWAVA network.
	Scanner name	WASP 2
	Install to server	bitterlinux (Linux)
	WebAccess startup file	not/valid/path
	Tomcat directory	/not/valid/path
	Stop Viruses	Yes
		Install

You MUST wait until this page is shown. WASP 2 requires you to copy some files and edit the webacc.cfg on the remote machine for the installation to be successful.

 Second second sec	WASP scanner installation finished
	Activating virus scanning
	Activating Attachment Blocking
	Setting up Fingerprinting
	Scanner 'wasp' was created successfully.
	You will need to edit the remote webacc.cfg file and find the following line Provider.GWAP.class This will need to be changed to Provider.GWAP.class=com.gwava.wa.provider.Wasp with this line.
	Copy the next part and paste it at the end of the file
	Provider.Wasp.gwavaman.address=10.1.1.101:49282 Provider.Wasp.gwavaman.username=wswasp Provider.Wasp.gwavaman.password=D144B72E9D Provider.Wasp.reference.id=149hege.149hgis.h3
	You will need to copy the following files to the remote Tomcat folder. mail.jar needs to go into tomcat/webapps/gw/WEB-INF/lib/ and tomcat/common/lib/ activation.jar needs to go into tomcat/webapps/gw/WEB-INF/lib/ and tomcat/common/lib/ wasp.jar needs to go into tomcat/webapps/gw/WEB-INF/lib/
	Your GroupWise WebAccess agent needs to be restarted for this WASP scanner to become active. Click the 🕑 for WebAccess restart instructions.

The files that need to be downloaded are linked from this page. Create a backup of the current versions of the files you are copying over. Clicking on the name will download the necessary files you need to copy to the locations defined. You must restart Tomcat after the files have been copied over, and the lines added, before the WASP 2 scanner will become active.

Testing your WASP scanner

Now that the scanner has been installed, we need to test the scanner to make sure that it is scanning mail sent from your WebAccess system.

Open your browser of choice and connect to your WebAccess mailbox.

Create a quick test message and send it to a recipient. (It may be handy to send to 'admin' or another account you can log into and manage.)

Once the message has been sent, return to the GWAVA4 Management console.

Under Server/Scanner Management, Manage Scanners, select your WASP Scanner and open the Scanner Information folder.

Select the Status object.



The Status page gives a quick report on when the scanner became active and the last time that the scanner status was received.



From the left menu, select the **Statistics** object.

The statistics page shows the number of messages that have been scanned and what actions have been taken, if any. Our simple test message has been scanned and is logged. (You may need to click on **Request stats refresh** to obtain current information.)

Z Statistics				• 🕹	ž	\mathcal{Z}	2
Statistics recorded at 10:	30:17 on 05/13/08		Reset statistic	Reque s All	st stat	s refres	sh
Statistic	Overall	Today					
Messages processed	1	1					
Viruses detected	0	0					

To test the antivirus scanning of the WASP engine, it is recommended to use the Eicar test string. See the webpage <u>http://www.eicar.org/anti_virus_test_file.htm</u> and read the information provided there. Download the Eicar test file of your choice. (Your local machine must have virus protection disabled or the test file may be deleted before you can use it.)

Return to the WebAccess account and attach the Eicar test string to a message, and then send it.

When you attempt to send the message with the 'infected' attachment, you should receive this notification:

The page at http://10.1.1.10	says:	×
Your message was blocked b An attachment to this messa may rectify the problem and help.	y the GWAVA WASP content filtering service for the following reason(s): ge is not allowed; A virus was detected in one of the attachments. You resend your message. Please see your system administrator for additional	

The test string will not allow the message to be sent. Repeat this test as desired.

You can also check the statistics page, (and click **request stats refresh**), to ensure that proper reporting is working correctly.

	<u>//</u> 9	Statistics	H 🛼 🕹 🗹 🥲		
		Statistics recorded at 10:31:	46 on 05/14/08	Request stats refresh Reset statistics All 💽 Go	-
		Statistic	Overall	Today	
		Messages processed	6	6	
		Viruses detected	4	4	
- 1					

Configuration

WASP 2 is configured by default to block and delete all corrupted or infected files and messages that are detected. The GWAVA4 defaults for the rest of the scanner settings are also in effect. If you wish to change the configuration of WASP 2, you can change it at any time.





The current configuration of your WASP 2 scanner and the option to change the configuration is found under **Server/Scanner Management**, your **server name**, **Manage Scanners**, and your **WASP2 scanner** – as shown.

Some of the options in this configuration, which are standard for GWAVA4, are ineffective for a WASP scanner because WASP only scans mail uploaded to the GroupWise system through WebAccess. GWAVA4 scans mail that comes to the GroupWise system from the internet. Because WebAccess passes mail either through the GWIA or directly to the destination post office if the mail is internal, some of the options in the configuration do not apply or are redundant if you have a GWIA scanner installed.

The options that are ineffectual to configure on the WASP2 interface are the **Antispam** options, (Heuristics, SURBL, RBL, Spam auto-learn, and Non-spam auto-learn). Antispam would only be applied to valid GroupWise system users who are sending mail through the WebAccess system. It is best to disable all Antispam scanner settings in the WASP configuration.

Also, any configuration settings that are duplicated on a GWIA scanner will add duplicate affects to the messages. For instance, BCC and Global Quarantine message services enacted on messages that also go through a GWIA scanner, (external destination), with the same settings will have two copies sent BCC and the quarantine.

General Settings

The general settings contain the Administrator email address, notification templates and notification address for the scanner. If you wish the notifications coming from the WASP2 scanner to be sent to a different location than is default for GWAVA4, you may specify it here. The notification templates are available for editing. Make a backup copy of the files before you edit. They are found in

.../gwava4/assets/global/template and are associated with the event they are listed next to on the Notification page.

Scanning Configuration



Antivirus

The setting for antivirus scanning is contained here for WASP2. The default setting is shown here, and designates that the Antivirus engine is configured to block infected messages and files, regardless of exceptions or any other settings, and to never quarantine the message. The gold locks used here, or four-state checkboxes, are explained <u>below</u>.

Text filtering

The text filter will search the text of the messages sent through WebAccess for the string that you specify. For example; if you wanted to make sure that everyone using WebAccess could not send a message that contained the characters 'ESPN' through the mail system, you could specify ESPN as a text filter and set the filter to block detected messages. In this case, WASP 2 would not allow an offending message to be sent, and displays a notification that "The content of the message was disallowed". (It may be a good idea to inform the users of text filter regulations as they may become frustrated when WASP 2 does not allow them to send their message.)

MIME filtering

The mime filter also allows for a search on a matching string, but this scanner searches the entire mime of a message, and allows matching on objects not found in the message text.

Oversize

Messages that are larger than the size specified in this scanner will be blocked as well. This counts the entire message size and not the size of single attachments.

Fingerprinting

Every file type has a specific pattern that can be read like a fingerprint, allowing the fingerprinting scanner to check for executables or other file types that are misnamed to mask their attributes. Any file type that is specified in this scanner will have the associated action taken when that file type is identified, regardless of the extension.

Attachment types

This blocks attachments based on the extension, you may add extensions to block file types that are not listed.

Source address filter (From:), Destination filter (To:)

These filters have very limited use in the WebAccess system. Namely, this will only be able to keep your users from sending mail from WebAccess, in case you don't want a particular user to be able to send mail from the WebAccess system but still be able to log into, and view messages that have been sent to the user. The Destination filter will block users from sending mail to a specific location/address. Example; an employee is not longer working at a company, but still has mail in the system that they need access to. You can add their address to both the destination and source list, keeping them from sending or receiving any more mail in the system, without locking them out of the actual system itself.

Message services

Signature

The signature service in WASP 2 is unavailable, and will not function.

Global Quarantine

This will place a copy of every message sent through WebAccess into the GWAVA Quarantine. Again, this will be a redundant setting and action for all outbound mail if the GWIA scanner is also set to global quarantine.

Blind Carbon Copy

The BCC service will make a copy of each message and send it to the address of choice. This will also be redundant for outbound mail if the GWIA scanner is also set to create a blind carbon copy.

Exceptions

The exceptions for the WASP 2 engine will allow you to exempt a particular user or message string from the filters listed above. NOTE: if the <u>four state checkbox</u> has been enabled for an action, as it is set by default on antivirus, then the exception will not apply to that scanner. Otherwise, the exception will apply to all events selected under that exception.

To add an exception, enter the desired address or string into the new exception text box, then select the

add button. Once the exception has been added, you still need to apply the exception to at least one scanner before it will be saved to the configuration database.

Select which scanners you wish this exception to apply to by placing a checkmark in the associated box, and the save changes disk icon in the top right will highlight. Click the **save changes** button and the exception will become active as the scanner reloads the configuration. (This should happen within the next couple minutes.)

Scanner Information

Status

The status page gives a quick status report of the engine. How long it has been active and when it last reported to the system.

Statistics

The statistics window displays detailed statistics on the amount of messages that have been processed, (total), the amount detected by any particular scanner (antivirus, text filter, blacklists, etc.), and the actions taken on those messages, (deleted, blocked, quarantined).

The stats page can be refreshed by selecting the **Request stats refresh** link at the top right. This sends a request to the scanner engine for the latest statistical information.

Configure WASP Settings

Mail Interface Settings – Mail Interface Settings allow you to specify the maximum amount of scan threads, or the amount of messages that WASP 2 will be able to scan at the same time. The default is 16. This window also allows you to place the WASP 2 scanner into bypass mode, which makes the scanner



act as though it was not installed. You may also set the scanner timeout value here. The timeout value is how long the scanner will wait for a scan thread to become available before alerting the user that all scan threads are busy, and to try sending again. This value is in seconds and is set at default to 3. If either of these settings are set below or equal to zero, then the default value will be used.

Manage Scanner Object

Scanner properties – This page displays the properties for the scanner: the different IDs, name, and the option to uninstall the scanner from the system. Removing the configuration returns the system back to the way it was before you created the WASP2 scanner. It does not remove the WASP2 package from the GWAVA4 package management system.

Scanner Event Actions

There are five, (six for some), optional actions for every scanner event or filter that fires on a message: Block, Notify Sender, Notify Recipient(s), Notify Administrator, Quarantine, and, for some, Notify

Defined Addresses. The action icons work as a global button. Selecting the icon globally activates, or deactivates, the event for every listed option.

	<	Ser	vices	>	
1	2	s		20	

The block and the quarantine options are not the same. If you select to quarantine a message, but do not select the block action, then the message will have a copy placed in the quarantine, but still be allowed to reach the destination mailbox. Blocking a message without selecting quarantine will simply prevent a message from entering the GroupWise system.

The different notification options are exactly as they are named and are active for every time the event

fires. The Notify Defined Addresses sends a notification to the addresses defined under the services carousel. To access the — different options, click on either arrow to the sides of the word **Services** above the action icons until you reach the desired option. Select **Edit** to open the defined address list for this action.



	<	Sen	vices	>		
1	2		2	20		
	<	Add	resses	>		
	د گ	Add	resses	> 85	0	

When you have defined the addresses you desire, select **OK** and enable the action.

Four State Checkboxes

29

The locks you see next to the options are always visible on the Antivirus scanning settings, but are invisible, and unavailable to configure for the rest of the system, unless you enable the option "Enable Four State Checkboxes". The four state checkbox allows setting the 'gold locks' on any checkbox in the rest of the system. A closed lock indicates an overriding option. (This Dr overrides any exceptions or settings in the rest of the system.) Four state locks are a powerful 05 option and they are not standard in any area except in the Antivirus section. Both images show here are set to the same setting: always block, never quarantine. For the events that these settings are active for, the messages will always be blocked and never quarantined, regardless

	<	Ser	vices	>	
1	2	ß	.	20	(2)
2 0					

of exceptions or other actions that are active on that message.

Uninstalling WASP2 scanner

To uninstall the scanner- click on the uninstall scanner link on the Manage Scanner Object page, and select the objects you wish to remove from the system. For most all situations, select all available options and select **uninstall scanner** to completely uninstall the WASP2 scanner.

Sec	🔅 Scanner properties						Ľ	2
		Scanner name	WASP2					1
		Database ID	142k49h.142k5r0.kj					
		Engines associated with this scanner	engine of WASP2 (id: 142k49h.142k5r0.5s)					
		Interfaces associated with this scanner	interface of WASP2 (id: 142k49h.142k5r0.5o)					
		Deployed on servers	linux-o3in (Linux) (id: 142k49h)					
	Per	form Operations						
	Uni	nstall scanner						

🔅 Sc	anner u	ininstall		🔶	🔰 😢	<mark>،</mark> (2)	
6	WARNING! You are about to uninstall scanner 'WASP2' with database id: 142k49h.142k5r0.kj						
_	This un the rele	install procedure will remove all compone evant server to remove any support files	ents associated with this scanner and where necessary send an that have been installed.	uninsta	all script t	0	
		Engine to be removed:	engine of WASP2 (id: 142k49h.142k5r0.5s)				
		Interface to be removed:	interface of WASP2 (id: 142k49h.142k5r0.5o)				
		Server to uninstall from:	linux-o3in (Linux) (id: 142k49h)				
	✓	Remove statistics:	Statistics data for this scanner will be purged from server linu 142k49h)	x-o3in ((Linux) (ia	i:	
	Files to be removed/modified during cleanup Remove WASP settings from /opt/novell/groupwise/webaccess/webacc.cfg Remove WASP Libraries from '/srv/www/tomcat5/base\webapps\gw\WEB-INF\lib'. Remove GWAVA startup switches from GWAVA services.conf (linux)						
			Uninstall Scanner				

Copyright © 2008 GWAVA Inc. All rights reserved.

The connection between WASP and GWAVA4 is now severed, but the wasp.jar is still active in the WebAccess system. Because the connection to GWAVA4 is unavailable to WASP, WebAccess will be non-functional until Tomcat is restarted. Restarting Tomcat will remove the wasp settings from the WebAccess configuration and wasp.jar will no longer be running.

If you wish to completely uninstall the WASP2 package from your system, you need to return to the package manager and remove the WASP2 package by clicking on the recycle bin icon to completely remove the package from the GWAVA4 system.

Package List			
Package ID	Package Description	Actions	Status
WASP2	WASP 2 plug in for GWAVA 4	11 🧿	5



Installing the license file for WASP 2 is exactly the same as installing the license for GWAVA 4. It is located under Server/Scanner Management | <server name> | Server management | Licensing

Select the Licensing object to open the licensing window.

If you do not have a license installed, your licensing page should look like the one pictured below.



To install a license, click the 'Browse' button to open the browse window.

File Upload				-	-	-	? 🔀
Look in:	🧟 share on 10.1.	1.101	~	6	1 🖻		
My Recent Documents Desktop My Documents My Computer	Totc Totc	shots so Jnx_multi.tar.gz re	E notes.txt readme_500 Retain 160A v4license.pe wv4license.pe wasplicence.	7722.htr oha5.zip m	nl		
	File name:	wasplicence.pen	n		~		Open
My Network	Files of type:	All Files			~		Cancel

Browse to where the license file is located, select your license file and click 'open'.

You will be returned to the license upload window. Click on the 'upload' button.

GWAVA 4 will automatically install the license file to the appropriate location when you click the upload button. When you have successfully installed the license, the license should appear as installed, as shown below.

R	Licensing	\diamondsuit	¥	Ľ	2
	Last action: Installed license file wasplicence.pem				^
	Install license (pem) file Install Install				
	Installed license files Image: state of the sta				
	Licenses on this server are located in /opt/beginfinite/gwava/license/				

Restart GWAVA 4 to cause the license to immediately take effect.

Uninstalling WASP 2

To fully uninstall WASP 2, there are three things to remove: the scanner, the .jar files, and the WASP 2 package.

First remove the scanner from the GWAVA 4 management console. The uninstall option is found under Server/Scanner Management, Manage Scanners, select your WASP Scanner, open the Manage Scanner Object folder, and select Scanner Properties.

Select the 'uninstall scanner' link on the Scanner properties page.

You will see a confirmation page, asking for each part you wish to uninstall. Remove all modules to ensure complete uninstall.

7	Server/Scanner Management
	_
	🣁 bitterlinux (Linux)
	🗉 📁 Server management
	🗉 📁 Wizards
	🖃 💋 Manage scanners
	🗄 📁 Gwia Scanner (GWIA)
	🖃 💋 WASP 2 (WASP)
	🖲 📁 General settings
	Image: Image: Search in the search is the search in the search is the
	🗄 📁 Message services
	Exceptions
	🗉 📁 Scanner Information
	🗉 💋 Configure WASP settings
	🗉 🃁 Manage scanner object
	Scanner properties

	WARNING! You are about to uninstall scanner 'WASP 2' with database id: 149hege. 149hgis. 1vb					
r	This uninstall procedure will remove all components associated with this scanner and where necessary send an uninstall script to the relevant server to remove any support files that have been installed.					
		Engine to be removed:	engine of WASP 2 (id: 149hege. 149hgis. 1ki)			
	V	Interface to be removed:	interface of WASP 2 (id: 149hege. 149hgis. 1ke)			
		Server to uninstall from:	bitterlinux (Linux) (id: 149hege)			
	✓	Remove statistics:	Statistics data for this scanner will be purged from server bitterlinux (Linux) (id: 149hege)			
	V	Files to be removed/modified during	Remove WASP settings from /invalid/path			
		cleanup	Remove WASP Libraries from '/invalid/path\webapps\gw\WEB-INF\ib' .			
			Remove GWAVA startup switches from GWAVA services.conf (linux)			
	Uninstall Scanner					

If you installed a remote scanner, simply reverse the process you used to install the scanner. WASP cannot remove or edit the files on the remote machine, so this must be completed manually.

Remove or comment out the lines you added to the webacc.cfg file:

Provider.Wasp.gwavaman.address=* Provider.Wasp.gwavaman.username=wswasp Provider.Wasp.gwavaman.password=* Provider.Wasp.reference.id=*

Replace the original files back to their original directories: Mail.jar and Activation.jar to where they were originally, one of two places: ...tomcat/webapps/gw/WEB-INF/lib/ and-or ...tomcat/common/lib/ Delete wasp.jar from .../tomcat/webapps/gw/WEB-INF/lib Second, remove the WASP2 switches from the webacc.cfg file. These settings should be at the bottom of the file, and should be marked as WASP settings. Comment out or remove all lines that begin with "Provider.Wasp..."

Return the Provider.GWAP.class line in the webacc.cfg back to the original provider. It should be simply commented out, which you can return to original function by removing the hash mark, (Linux), or the semicolon, (NetWare). The original line for webaccess 7 is as follows: Provider.GWAP.class=com.novell.webaccess.providers.gwap.XGWAP

Third, remove the wasp.jar file from the WebAccess system. It will be located in the .../webaccess/gw/WEB-INF/lib directory.

To remove the rebranding of WASP 2 in the WebAccess interface, return the original picture files to the default. WASP renamed them to .bak and restart your WebAccess system. You will find them in the following locations:

For GroupWise 7 <tomcat_path>/gw/com/novell/webaccess/images/splash.png

For GroupWise 8 <tomcat_path>/gw/webaccess/200808220638/images/install_watermark_n.png

WASP 2 is no longer a functioning package on your system. But if you wish to completely remove WASP 2, complete the last step by removing WASP 2 from the package manager in GWAVA 4.

In the GWAVA 4 management console, under the System Management Tab, expand the System Management tree and select the Package manager. Click the recycle bin icon for the WASP 2 package to delete the package from the system. Click 'Ok' to confirm, and WASP 2 will be removed.

ackage Manager		ĥ	8	٤	\mathcal{Z}	2
This page provides the fac system.	This page provides the facility to install 3rd party add on packages, snap-ins and discreet updates to your GWAVA system.					
If you have obtained an installable package please follow the instructions provided with the package where applicable. Packages can be uploaded to the system through this interface, or copied directly into the packages directory on your gwava server. Package installation requires several steps to complete depending on the package. Once installed, the actions available for the package will be indicated by the icons in the action column of the package list. Upload a new package						
Package List						
Package ID	Package Description	Actions			Status	
WASP2	WASP 2 plug in for GWAVA 4	1			5	

WASP 2 is now completely uninstalled.

Appendix

WASP 2 notifications

The different notifications for WASP 2 should be clear, but the most common notifications are listed here with their corresponding events for reference. WASP 2 will respond with the following notifications when the corresponding scanner filter is triggered with a block event.

Antivirus scanner:	A virus was detected in one of the attachments
Destination address blacklist:	The recipient list includes a restricted address.
Source address blacklist:	This account is not permitted to send messages
Attachment filter:	An attachment to this message is not allowed
IP address blacklist:	The computer you are sending from is not permitted to send
Text filters (all text filters):	The content of the message is not allowed
Oversize message scanner:	The message is too large