



Release Notes

Table of Contents

1 New Features in GWGuardian	5
1.1 Phishing.....	5
1.2 Language Filtering	6
1.3 Message Audit Logs	7
1.3.1 Database Formats	7
1.3.2 Creating an MS SQL Message Audit Database	8
1.3.3 Creating a PostgreSQL Message Audit Database	11
1.4 GroupWise Alias Update Wizard.....	12
2 Changes to the GWGuardian Administration Console	13
2.1.1 Administration Console.....	13
2.1.2 License Keys	13
2.1.3 Quarantine Reports	15
2.1.4 Reverse DNS.....	16
3 Features Removed from the GWGuardian Administration Console	17
3.1 Quarantine Report.....	17
3.2 Security > Properties > Mail Relay	17
4 Bug Fixes	19

1 New Features in GWGuardian

Detailed information about the functionality of the new features can be found in the GWGuardian Installation & Configuration Guide.

1.1 Phishing

Phishing spam has become more prevalent and, as such, GWGuardian now isolates it as a separate feature. GWGuardian manages mail with phishing content as it does viruses. Messages can be quarantined or deleted by users but not released. Only Administrators can release these messages.

The functionality of the Phishing feature however, will mimic that of spam. The definition files are updated by the spam engine and, by default, the update occurs every 15 minutes. Custom scripts remain intact.

- The auto-cleanup and performance (caching) settings are configured in the Spam tab and Phishing will adopt the same configuration.
- The Phishing category has been added to the GWGuardian Administration Console in the Menu Bar, under Threats, as a tab in the Icon Bar and as a separate field in WebAdmin and WebQuarantine.
- The Phishing scanning level mimics that of Spam: Normal, Strong or Extreme.
- Under the **Find > Quarantine** feature, Hoax has been removed and Phishing has been added in its place.
- Under Quarantine, a Phishing tab has been added, separating Phishing messages from the Spam categories.

In order to effect any change or customization to the phishing settings, system administrators must grant privileges to domain administrators and users. This is done through the Administration Console by choosing **WebAdmin > Privileges**.

Admin Console

Phishing references can be found by choosing the following:

- **Domains > Preferences > Phishing**
- **Users > Preferences > Phishing**
- **Quarantine > Phishing**
- **Phishing > Preferences > Options**
- **Web > WebAdmin > Privileges**

WebAdmin

Phishing references can be found by choosing the following:

- **Domains > Phishing**
- **Users > Phishing**

WebQuarantine

Phishing references can be found by choosing the following:

- **Settings > Email Filtering > Phishing**
- **Quarantine**
- **Quarantine Report**

1.2 Language Filtering

GWGuardian provides the option to scan for foreign language content:

- Scanning for language content occurs:
 - after virus and attachment scanning
 - after the trusted and blocked lists
 - before spam scanning by the SCA engine
- Custom filters based on language content are supported and trusted addresses bypass language filtering.
- Messages containing words or characters in several languages are given a language probability rating based on the weight of the content.
 - For example, if the bulk of a message is in Italian, GWGuardian will consider it as such and this is the code that will appear in the header envelope.
- The probability rating determines whether the message is filtered or not.
 - If the bulk of the message is in a 'permitted' language but contains words or characters in blocked languages, the message will pass through.
- Messages considered SPAM are displayed in the 'low spam probability' section of the Quarantine Reports and can be released by the user.
- The header tag is accessible to Sieve scripts and allows for the creation of custom rules based on language, such as exclusion rules.

Language Filter settings can be changed at the system, domain and user levels. In order to effect any change or customization, system administrators must grant privileges to domain administrators and users. This is done through the Console by choosing **WebAdmin > Privileges**.

Admin Console

Language filter references can be found by choosing the following:

- **Domains > Preferences > Language Filter**
- **Users > Preferences > Language Filter**
- **Rules > Properties > Language Filter**
- **Web > WebAdmin > Privileges**

WebAdmin

Language filter references can be found by choosing the following:

- **Domains > Language Filter**
- **Users > Language filter**

WebQuarantine

Language filter references can be found by choosing the following:

- **Settings > Email Filtering > Language Filter**

1.3 Message Audit Logs

System administrators are provided with a current status tracking for all messages. The information is presented in the Message Audit view of the Monitoring application.

All message transactions are displayed in a 1-line per message summary. This feature tracks message traffic – inbound external mail, outbound local mail and mail from local user to local user.



The ODBC MDAC driver for the SQL Server should be at version 2000.86.1830. Messaging Architects recommends MDAC 2.8. Messaging Architects also recommends that WebQuarantine and SQL server not be installed on the same machine as this could impact performance.

1.3.1 Database Formats

The following table provides the recommended database format for GWGuardian:

Database	MS SQL2000+	MS SQL Express	PostgreSQL	MS Access & MSDE
Quarantine	✓	✓	✓	✓
Monitoring	✓	✓	✓	✓
Audit	✓	✓	✓	✗
Sieve	✓	✓	✓	✓

- MS Access and MSDE have a size limitation of 2GB
 - These are not recommended for large environments but are acceptable in small environments
- SQL Express has a size limitation of 4GB
 - It can be used in medium-sized environments
- MySQL can be used for the Quarantine database but is not recommended
- There are update scripts for the Monitoring and Quarantine databases that should run automatically during the install
 - If the user account indicated in the ODBC connection and in the GWGuardian Administration Console is not the default "SA" account, check the account's permissions for the database
 - It must have full access, including db_datawriter
 - This should be verified before the installation to prevent problems with the update



Due to a potential traffic load with this function, you have the option to run it system-wide or only for specific domains and/or users. To enable the feature for domains and/or users only:

- Ensure that the feature is enabled in **Logs > Properties > Message Audit**
- Go to **Domains > Properties > Message Audit** to enable it for specific domains
- Go to **Users > Properties > Message Audit** to enable it for specific users

Admin Console

Audit message log references can be found by choosing the following:

- **Logs > Properties > Message Audit** (master system control)
- **System > Properties > Message Audit Database**

- **Domains > Preferences > Message Audit**
- **Users > Preferences > Message Audit**
- **Web > WebAdmin > Privileges**

WebAdmin

Audit message log references can be found by choosing the following:

- **Domain > Message Audit**
- **User > Message Audit**

WebMonitor

The Message Audit feature can be found in the GWGuardian WebMonitor.

Searching Messages

The search feature allows you to search for specific messages in the message audit log. Search fields include email address, subject and message status, among others.

Search Results

The search results view can be configured to provide up to seven columns of information. The complete message audit can be exported in CSV or HTML format.

In addition to the information available in the search results view, clicking on a particular message opens the log detail view which provides the full transaction history for the message. The log details can be forwarded by the Postmaster account; blocked messages can be released to their destined recipients and exported in HTML or text format.

1.3.2 Creating an MS SQL Message Audit Database

- Go to the SQL Enterprise Manager
- Create a database and name it **Audit**
- Select **Properties** and go to **Options**
 - Ensure that *Auto update statistics* is **enabled**
 - Ensure that *Auto shrink* is **disabled**
- Click on **OK**
- Start the **SQL Query Analyzer**
- Select your database (Audit)
- Choose **File > Open** and go to **...Messaging Architects\GWGuardian\DBStructures\SQL Server\Audit**
- Run the following scripts, in the following order:
 - audit_tables.sql
 - audit_procs.sql
 - audit_jobs.sql
- Once the tables have been created, choose **System > Properties > Message Audit Database** in the GWGuardian Administration Console.
 - Enter the required information

- Click on **Apply**
- In the Console, choose **Logs > Properties > Message Audit**
 - Enable **Audit Logging** and **System-Wide Logging**.
 - Click **Apply**.
- Choose **System > Properties > Services** and stop/start all services.
- Go to a Command Prompt and type **iisreset** <enter> to restart the IIS service
- The Message Audit feature has been configured for use in WebMonitor.

Security Enhancements

To improve security, the audit database user should have **minimum** privileges.

- No server administrator role

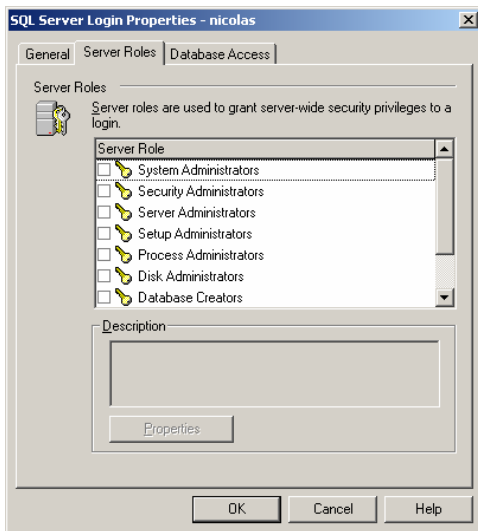


Figure 1: SQL Login Server Roles

- Access granted to the Audit database **only**

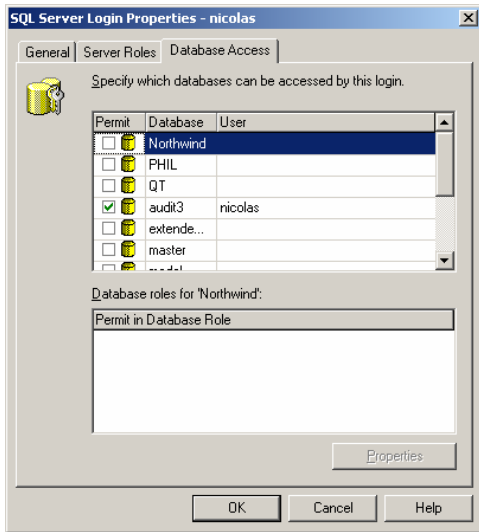


Figure 2: SQL Login Database Access

- Only db_datareader and db_datawriter permissions for the Audit database

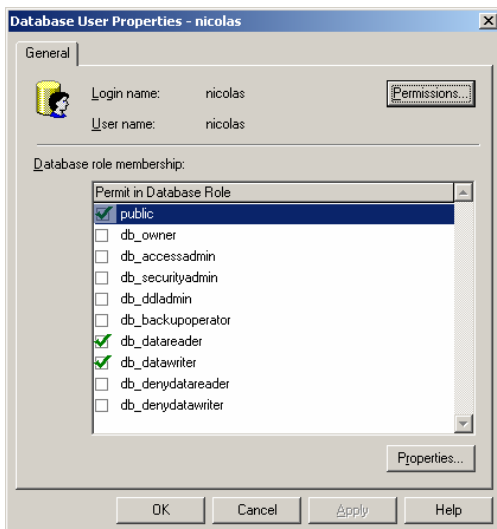


Figure 3: SQL Database User Role

- No permission to create, drop, or alter Audit tables (starting with mt_audit*)
- No permission to use audit tables directly (no select, no insert, no update, no delete)
- Permission to execute all audit DB stored procedures (starting with mp_audit*)

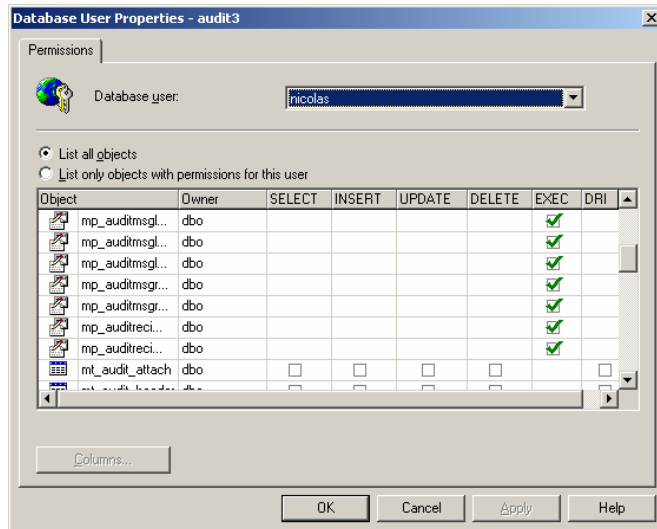


Figure 4: SQL Database User Permissions



If the SQL Server is installed on the same machine as the WebQuarantine and the Message Audit is enabled, you will, likely, experience performance problems.

1.3.3 Creating a PostgreSQL Message Audit Database

- Open the pgAdmin III program or your favorite administration program for PostgreSQL
- Create a database and name it **Audit**, making sure to select **UNICODE** for the encoding
- Open the Query editor for your database (Audit)
- Click on **File > Open** and go to **...Messaging Architects\GWGuardian\DBStructures\PostgreSQL\Audit**
- Run the following scripts, in this order:
 - audit_tables.sqisresetl
 - audit_procs.sql
- Once the tables have been created, choose **System > Properties > Message Audit Database** in the Console
 - Enter the required information
 - Click on **Apply**
- In the Console, choose **Logs > Properties > Message Audit**
 - Enable **Audit Logging** and **System-Wide Logging**
 - Click **Apply**
- Choose **System > Properties > Services** and stop/start all services
- Go to a Command Prompt and type **iisreset** <enter> to restart the IIS service
- The Message Audit feature has been configured for use in WebMonitor

1.4 GroupWise Alias Update Wizard

The GroupWise Alias Update Wizard allows GroupWise administrators to synchronize the number of users in the GroupWise system with the number of users in GWGuardian. With the GroupWise Alias Update Wizard, administrators can configure and schedule the GroupWise Alias Update Wizard to run automatically to perform a variety of administrative tasks. The GroupWise Alias Update Wizard can be used when you are performing a fresh installation of GWGuardian, or when you are upgrading your existing GWGuardian system. For more information, see the *GroupWise Alias Update Wizard Installation and Configuration Guide*.



In order to access the Help file for the GroupWise Alias Update Wizard, the Help file must be manually copied into the directory where the application was installed.

2 Changes to the GWGuardian Administration Console

Detailed information about the functionality of these changes can be found in the *GWGuardian Installation & Configuration Guide*.

2.1.1 Administration Console

The following changes have been made to the GWGuardian Administration Console:

Changes to the Menu Bar

The Menu Bar has been reorganized and grouped according to administrative tasks:

- Domains, Users and Quarantine are now grouped together under **Admin**
- Security, Virus, Phishing and Spam are grouped together Under **Threats**
- Attachments, Rules and Language Filter are grouped under **Policies**
- System, Authentication, Logs and Web are grouped under **Config**

Changes to the Icons

The icons have been regrouped to reflect the Menu Bar changes.

- Anti-Spam and Anti-Virus have been renamed Spam and Virus respectively
- Phishing has been added
- Rules has been added
- Forbidden Attachments has been renamed to F.A.

Changes to Find

Search For items have been reorganized:

- MIME Parsing Errors has been removed
- Blocked Senders has been moved from the Spam Categories to **Search For**
- Custom (in Spam Categories) has been replaced by Blocked by Rules in **Search For**
- Hoax (in Spam Categories) has been replaced by Phishing in **Search For**

Logs > Properties > File Config

In an effort to optimize system performance, the default maximum file size for the log file has been increased from 10,000KB to 40,000KB. Any change that was made to this number by the Administrator will remain.

2.1.2 License Keys

General Information

- One activation key will be issued per product instance and kept throughout your relationship with Messaging Architects.
 - The key format is 6x4
- Details for your software package are stored in a text file that is downloaded and installed on your server.
 - This file contains an encrypted signature that is verified and decoded by the activation key to unlock the features

- The file also includes details about the licensed product package
 - Any changes made to the package will be transmitted to this file via a secure connection
- License key validation and file updates are performed regularly with updates to the scan and virus engines.

Changes to the Installation Process

- During the installation process, to validate and activate the product, you must enter the license key provided to you at time of purchase.
- The license key is activated once the installation begins and decodes the encrypted signature to unlock the program's functions.
- Should the license key decryption fail, the GWGuardian installation will continue but the services will not start.
 - In the event that the installation fails, contact Messaging Architects and your license file will be emailed to you
 - Once the file has been saved to your server, you will be prompted to manually activate your license key via the Administration console
 - If the license key is not activated manually, activation will occur during the next auto-update process

Changes to the Product Update Process

- During product updates, the license key is validated and the text file associated with your key is checked for any changes to package details.
 - The information stored within the file determines what is updated and whether the update is permitted as per your support plan and license key expiry dates.
 - If the update is not permitted, the services will be restarted and the program will run in its original state
 - You will receive an on-screen notification of the problem and instructions to contact Messaging Architects

Changes to the Update Expiry Process

- Every auto-update expires after a period of 14 days.
- If the auto-update system cannot connect for 2 consecutive days, GWGuardian will issue warnings to the system administrator.
 - These warnings will appear as pop-up messages when the Administration Console is opened and will also be emailed to the local postmaster address
- If the auto-update cannot connect for 7 consecutive days, the license key enters a grace period and behaves as an expired perpetual key for an additional 5 days.
- If a connection cannot be established after 14 consecutive days, GWGuardian goes into an expired state.
 - The 14-day period includes the initial 7-day warning and 5-day grace periods
- The final expiry behavior depends on whether the key is subscription or perpetual.

Changes to License Expiry

License expiry differs for Subscription (trial or temporary) license keys and Perpetual license keys:

- Subscription (trial) keys:

- When the expiry date is reached:
 - GWGuardian continues to route mail to the mail server but all filtering stops
 - All security options are disabled except for SMTP Auth and all scan operations stop
- Perpetual (permanent) keys:
 - When the expiry date is reached, the program continues to run under the existing build with the existing scan filter libraries but:
 - The filter definitions will not be updated
 - GWGuardian cannot be updated to a newer build
 - The license must be renewed in order to obtain any updates
- Automated messages advising that the license has expired are sent to the local postmaster and Messaging Architects

2.1.3 Quarantine Reports

Any custom Quarantine Reports that you have will be lost when you upgrade your version of GWGuardian. New custom reports can be easily created with the new interface in v4.4. Please refer the *GWGuardian Installation & Configuration Guide* for more details.

The Delete function has been optimized:

- Access to the Quarantine Reports from WebAdmin has been optimized, if you run the following script:
 - SQL Server
 - Open the Query Analyzer
 - Run `mssql_quarantine_manual_upgrade.sql`
 - This script can be found in `...\DBStructures\SQL Server\Quarantine`
 - PostgreSQL
 - Open pdAdmin III
 - Run `pg_quarantine_manual_upgrade.sql`
 - This script can be found in `...\DBStructures\PostgreSQL\Quarantine`

Language Settings

The language of the Quarantine Report will be determined by the permanent mailbox language settings in the Administration Console:

- **System > Properties > Settings**

Quarantine Report Settings

Quarantine Report references can be found in the following panels:

- **Domains > Preferences > Reporting**
- **Domains > WebAdmin > Privileges**
- **Users > Preferences > Reporting**
- **System > Properties > Quarantine Reports**
- **Web > WebAdmin > Privileges**

WebAdmin

Quarantine Report references can be found in the following panels:

- **Domain > Reporting**
- **Users > Reporting**

WebQuarantine

If the administrator has granted you rights, you may configure your Quarantine Report preferences by choosing:

- **Settings > Email Filtering > Quarantine Report Preferences**

2.1.4 Reverse DNS

The Reverse DNS feature has been modified in **Security > Properties > Sender Validation & Accreditation**. Previously, when **Perform a look up for the SMTP host in the DNS** was enabled, you were able to select both **Reject Connection Immediately on Lookup Failure** and **Accept Unknown Hosts** simultaneously. With GWGuardian v4.4, you will now have three options from which to choose but you may only use one.

Perform a look up for the SMTP host in the DNS

- **Reject Connection Immediately On Lookup Failure**
 - GWGuardian will not accept messages when the reverse DNS of the SMTP host has failed.
- **Postpone the rejection until authentication**
 - GWGuardian will verify the SMTP AUTH connection before performing the reverse lookup.
- **Do not reject connection (Accept all hosts)**
 - GWGuardian will log the DNS lookup results and will process the message whether the lookup fails or not.

3 Features Removed from the GWGuardian Administration Console

The following features were removed from the GWGuardian Administration Console:

3.1 Quarantine Report

The Blocked Sender feature has been removed because:

- Messages have already been filtered and quarantined
- Users still can add addresses and domain names to their Blocked Senders List in WebQuarantine by choosing **Settings > Email Filtering > Blocked Senders**

3.2 Security > Properties > Mail Relay

- **Allow relaying for any user in a local domain** has been removed
 - If this feature had been enabled and you want to turn the feature off or on, open the Registry Editor
 - Go to **HKEY_LOCAL_MACHINE\Software\Messaging Architects\VopMail**
 - Find **NoThirdParyRelay** and disable/enable it
- **Verify in the domain that the user has been removed**
 - If this feature had been enabled and you want to turn the feature off or on, open the Registry Editor
 - Go to **HKEY_LOCAL_MACHINE\Software\Messaging Architects\VopMail**
 - Find **NoThirdParyRelayUserName** and disable/enable it

4 Bug Fixes

The following fixes have been implemented in this release:

- 3817: Fixed a bug where image spam was not being properly detected.
- 3868: Fixed a bug whereby GWGuardian ignored the bounce that greylisting mail servers send.
- 4032: Fixed a bug where some domain settings were lost when editing the routes.
- 4121: Fixed a bug so that now when a temporary key expires while services are running, the mail will not be left undelivered in the "invirus" folder.
- 4253: Fixed bug where the release link was not available for mail caught by the language filter.
- 4308: Fixed problem with the Quarantine page in the Administration Console (showed Phishing in the spam page).
- 4397: Fixed a bug whereby the Y-axis for WebQuarantine traffic was incorrect.
- 4467: Fixed a bug where encoded subjects were not displayed properly in WebMonitor.
- 4578: Fixed a display bug with the WebMonitor Login page.
- 4590: Fixed the quarantine search for from: and to: fields in WebAdmin so that it only returns results pertaining to the current users.
- 4594: Fixed a bug so now, if a message is blacklisted or whitelisted, the scan result is 'Blacklisted by XXX' or 'Whitelisted by XXX'.
- 4619: Fixed a bug for inconsistent behavior of SMTPDS when sending back a DSN.
- 4624: Fixed a bug in GWGuardian whereby administrators could not change passwords in WebAdmin.
- 4636: Corrected a typo in the Quarantine Report.
- 4661: Fixed a bug whereby if reverse DNS was set to Postpone the rejection until authentication, the trusted IP list was ignored.
- 4692: Fixed a bug where the Norwegian and Chinese languages were not synchronized correctly when selecting them as "permanent" from WebQuarantine.
- 4715: Fixed a memory leak in PostgreSQL processes.
- 2885: An auto-cleanup feature has been added to purge all AV .dat files older than 1 month from the ...\\MessagingArchitects\\GWGuardian\\{McAfee/Norman}\\Backup directory
- 2919: The default encoding of WebQuarantine was changed to utf-8 to support all languages so that the text in the subject line appears properly
- 3158: Fixed the "Mark as Read" for the Quarantine find results screen and disabled F5 in search.
- 3179: Added validation in message view for release and report for FA, Blocked by Rules and other types of message.
- 3190: Paperclip option is available again
- 3439: Fixed a problem with French characters (accents) not displaying properly
- 3441: Improvement: WebQuarantine now shows total entries per list count for Trusted/Blocked Senders lists so that users know how many they have in their lists
- 3443: Added <body id="loginpage"> to the Login.aspx and <body id="listpage"> to the List.aspx to facilitate customizing WebQuarantine
- 3489: Added a field to configure the SMTP encryption port in the Administration Console to resolve an issue with SMTPRS STARTLS failing if the inbound port is something other than port 25.
- 3652: Added option to configure RBL check after AUTH login

- 3732: Fixed a bug where passwords were visible, in clear text, in the error logs
- 3818: Fixed intermittent problem with login to WebAdmin.
- 3824: Fixed an issue with passwords starting with an '=' in the System panel of the console.
- 3827: Fixed a bug where it was not possible to log into WebAdmin as an administrator.
- 3855: Now the "After all scanning" and the "Before all scanning" scripts will not be executed for released from the quarantine messages.
- 3873: Fixed a bug so that if monitoring is stopped for a few days, it will restart.
- 3903: Added a setting that will prevent the checking of the mandatory fields "mailNickname" and "displayName" when authenticating against AD. This could be necessary when the client uses AD authentication but not an Exchange mail server.
- 3945: Added the ability to disable domains & mailboxes stats in WebAdmin.
- 4024: Fixed a problem whereby SPF check was not always turned off even if disabled in console.
- 4032: Fixed a bug where some domain settings were lost when editing the routes.
- 4139: Improvements related to #3652: Verify SMTP auth before rejecting connection and reverse DNS lookup options have been added.