LevelBlue

Secure What's Next.

MailMarshal

Evaluation Guide

October 2026



Legal Notice

Copyright © 2026 Trustwave Holdings, Inc.

The most current version of this document may be obtained from:

Support.LevelBlue.com/MailMarshal-SMTP/

Formatting Conventions

This manual uses the following formatting conventions to denote specific information.

Format and Symbols	Meaning
Blue Underline	A blue underline indicates a Web site or email address.
Bold	Bold text denotes UI control and names such as commands, menu items, tab and field names, button and check box names, window and dialog box names, and areas of windows or dialog boxes.
`Code`	Text in this format indicates computer code or information at a command line.
Italics	Italics are used to denote the name of a published work, the current document, or another document; for text emphasis; or to introduce a new term. In code examples italics indicate a placeholder for values and expressions.
[Square brackets]	In code examples, square brackets indicate optional sections or entries.
	**Note:** This symbol indicates information that applies to the task at hand.
	**Tip:** This symbol denotes a suggestion for a better or more productive way to use the product.
	**Caution:** This symbol highlights a warning against using the product in an unintended manner.

Copyright © 2026 Trustwave Holdings, Inc.

Definitions

This manual uses the following naming conventions.

Term	Definition
Service Provider	LevelBlue or the Reseller for a Customer.
Reseller	An organization that markets and manages hosted services to customers.
Reseller User	The personnel who manage application configuration and settings for customers of the Reseller.
Customer	An organization that subscribes to the hosted service.
Customer Administrator	The personnel who manage local configuration and email content security settings for the Customer organization.
User	Any individual email user within the Customer organization.

Copyright © 2026 Trustwave Holdings, Inc.

Table of Contents

Legal Notice . . . . . **ii**

Formatting Conventions . . . . . **iii**

Definitions . . . . . **iv**

List of Tables . . . . . **vii**

List of Figures . . . . . **viii**

1 Introduction **8**
1.1 What Is MailMarshal SMTP? 8
1.2 What Does MailMarshal Provide? 9
1.3 How MailMarshal Helps You 10
1.3.1 Filters Email at the Gateway 10
1.3.2 Delivers Layered Spam Protection 10
1.3.3 Protects Against Existing and Emerging Threats 11
1.3.4 Provides Unparalleled Performance 11
1.3.5 Includes Easy-to-Use Interfaces 11
1.4 How MailMarshal Works 11
1.4.1 Understanding What MailMarshal Does 12
1.4.2 Configuring MailMarshal 13
1.4.3 Monitoring and Reporting 13
1.5 LevelBlue MailMarshal Cloud 13

2 Installing MailMarshal **15**
2.1 Hardware and Software Requirements 15
2.2 Installing Prerequisite Software 16
2.3 Understanding the MailMarshal Evaluation Installation 18
2.4 Installing MailMarshal 18
2.5 Running the Configuration Wizard 19
2.6 Configuring Anti-Spam Settings 22
2.6.1 Spam Configuration and Rules 23
2.6.2 Configuring SpamCensor SpamProfiler, and YAE Updates 24
2.6.2.1 Configuring and Checking Automatic SpamCensor Updates 24
2.6.2.2 Configuring Proxy Settings for Updates 25
2.7 Configuring Anti-Virus and Anti-Malware Protection 26
2.7.1 Excluding MailMarshal Working Folders from AV Scanning 26
2.7.2 Default Anti-Malware Rules 27
2.7.3 Configuring MailMarshal to Use an Antivirus Product 27
2.7.4 Enabling Virus Scanning Rules 28
2.8 Configuring MailMarshal to Accept Test Email 29

Copyright © 2026 Trustwave Holdings, Inc.

2.9 Installing MailMarshal Web Components 30
2.10 What to Do Next 31

3 Guided Tour 33
3.1 MailMarshal Management Console - Configuration 33
3.1.1 System Configuration 35
3.1.1.1 Configuring MailMarshal 36
3.1.1.2 Configuring Individual Server Properties 38
3.1.2 Exploring Email Policy. 40
3.1.3 Policy Elements. 42
3.2 Configuring Spam Management 44
3.3 Configuring Folder Properties 45
3.4 Generating Sample Email Activity. 46
3.5 MailMarshal Management Console - Management 48
3.5.1 MailMarshal Console. 48
3.6 Spam Quarantine Management Website 49
3.6.1 Adding an Email Address for Spam Quarantine Management 51
3.7 Reviewing Blocked Email 51

4 Product Features 52
4.1 Anti-Spam and Anti-Malware 52
4.2 Anti-Virus. 54
4.3 Lexical Analysis. 55
4.4 Attachment Blocking 55
4.5 Automation and Time Saving 56
4.6 User Group Management 57
4.7 Administration 57
4.8 Usability. 59
4.9 Policy. 59
4.10 Security and Deployment 60
4.11 POP3 Email. 62
4.12 Archiving 62
4.13 Reporting. 63
4.14 Performance 63

5 Key Benefits at a Glance 65
5.1 Secures your email gateway against all threats 65
5.2 Delivers rapid Return on Investment. 65
5.3 Provides low Total Cost of Ownership 65
5.4 Enables you to fulfill a range of compliance obligations and Data Loss Prevention policies . . . 65
5.5 Provides unrivaled legal liability protection 65
5.6 Improves network efficiency and saves costs. 66
5.7 Improves employee productivity 66
5.8 Safeguards business reputation 66
5.9 Creates a safer working environment for employees 66

Copyright © 2026 Trustwave Holdings, Inc.

List of Tables

Table 1: MailMarshal component functions . . . 12
Table 2: Prerequisites for evaluation installation . . . 15
Table 3: Test email content and results . . . 47
Table 4: Anti spam features . . . 52
Table 5: Anti-virus features . . . 54
Table 6: Lexical analysis features . . . 55
Table 7: Attachment blocking features . . . 55
Table 8: Automation and time saving features . . . 56
Table 9: User group management features . . . 57
Table 10: Administration features . . . 57
Table 11: Usability features . . . 59
Table 12: Policy features . . . 59
Table 13: Security and deployment features . . . 60
Table 14: POP3 email features . . . 62
Table 15: Archiving features . . . 62
Table 16: Reporting features . . . 63
Table 17: Performance features . . . 63

Copyright © 2026 Trustwave Holdings, Inc.

List of Figures

Figure 1: Enabling Rules 29
Figure 2: Spam Quarantine Management configuration page 31
Figure 3: MailMarshal Management Console 33
Figure 4: MailMarshal Servers 35
Figure 5: MailMarshal Properties 36
Figure 6: Server (Node) properties window 39
Figure 7: MailMarshal Email Policy 41
Figure 8: Rule Wizard (Rule Actions window) 42
Figure 9: MailMarshal Policy Elements (Folder pane) 43
Figure 10: MailMarshal Console Dashboard 48
Figure 11: MailMarshal Console Folders view 49
Figure 12: Spam Quarantine Management website 50

Copyright © 2026 Trustwave Holdings, Inc.

1 Introduction

Email is an essential communication tool, but it also creates serious productivity and security issues. Email offers an entry point in your network for spam and other undesired non-business content, such as malicious code, large file attachments that consume valuable disk space, phishing attempts, information and identity theft attacks, and other damaging content and activity.

In addition, email can become a conduit for proprietary data and confidential information to leave the company. Spam, email viruses, malicious code, liability issues, and declining employee productivity are all risks associated with email.

Spam commonly accounts for more than half of the email companies receive. Email viruses, Trojan horses, and other malicious files can cause millions of dollars in damage in just a matter of hours. Reports of companies forced into legal action because of staff misuse of email are becoming commonplace.

Email remains the lifeblood of modern business communication, but the damages email can cause become more costly each year.

1.1 What Is MailMarshal SMTP?

MailMarshal SMTP is an email gateway security solution for organizations. It unifies email threat protection, content security, policy enforcement and data loss prevention into a single highly scalable, flexible and easy to manage enterprise solution.

MailMarshal acts as an email gateway to your organization by filtering all incoming and outgoing email at your network/Internet perimeter. MailMarshal blocks incoming email threats such as spam, phishing, viruses, malware and Denial of Service attacks. MailMarshal also enforces acceptable use standards and ensures compliance with Data Loss Prevention policies. MailMarshal can be deployed as a standalone solution or multiple, distributed MailMarshal servers can be easily configured into an array to support the largest of enterprise environments with minimal administration.

Key elements of the MailMarshal anti-spam solution include:

- **SpamProfiler,** an antispam pre-filter that can reject spam email without unpacking and full processing.
- **SpamCensor,** an advanced antispam engine that can filter most spam before it enters your network.
- **SpamBotCensor,** an optimized application of SpamCensor that can block spam generated by botnets with even greater efficiency.
- **Automatic updates** for SpamProfiler, SpamCensor, and Yara Analysis Engine, responding to the latest trends in spam and malware.
- **Zero Day updates** protecting you from significant spam and malware events.
- **DMARC verification**, to assist in authenticating that mail is sent from its purported source.

Copyright © 2026 Trustwave Holdings, Inc.

- **URLCensor**, to reject email based on URLs embedded in messages that are found on a DNS-based blocklist.
- **URL checking** for suspect URLs using a real-time lookup against a proprietary database.
- **TextCensor**, to analyze and filter inbound and outbound messages based on language content.

MailMarshal can be used with any internal company email system or cloud hosted mailbox offering, including Microsoft Exchange, Office 365/Exchange Online, Lotus Domino, Sendmail, and Linux email servers. MailMarshal provides your company with the layered security solution you need to manage email content, fight spam, and transparently enforce your email Acceptable Use Policy.

Many organizations today have created policies and guidelines for the appropriate use of email, and employee education programs to deal with the torrent of spam and viruses. MailMarshal can help your company automatically apply email policy and security at the gateway, so you can once again use email safely, securely and productively.

1.2 What Does MailMarshal Provide?

As a gateway content security solution, MailMarshal protects your network and your organization. MailMarshal enforces your Acceptable Use Policy to protect against spam, viruses, gateway email attacks, and other undesirable consequences of using email.

Easily supporting enterprises with tens of thousands of users, MailMarshal is by far the most powerful, feature rich email content security solution available.

MailMarshal scans the content of inbound and outbound email messages, including the headers, message body, and attachments. MailMarshal can detect many conditions, such as:

- Attempted message delivery from a server found on a DNS based blocklist
- Presence of a virus (using one or more supported virus scanners)
- Presence of particular phrases in header, message, or attachment
- Size or type of attachments
- Presence of URLs in header, message, or attachment that are found on a DNS-based blocklist

The product can also respond to messages that violate your Acceptable Use Policy, by taking actions such as:

- Refusing receipt of a message from a remote server
- Quarantining a message for later review by administrators or users
- Deleting a message
- Redirecting a message
- Archiving a message for future reference (including optional cloud based forensic archiving)

Copyright © 2026 Trustwave Holdings, Inc.

MailMarshal provides email administrators with granular control of policies and the ability to delegate email monitoring and control to other personnel. MailMarshal provides the following user interfaces to meet the needs of a variety of administrators and your email recipients:

Web Management Console

For email security administrators to configure the product, establish email policy, and configure permissions for other Console users and the Spam Quarantine Management website. For email administrators and helpdesk personnel to monitor and control product activity.

Spam Quarantine Management Website

For email recipients to verify quarantined email and customize spam blocking for their own email addresses.

Marshal Reporting Console

For auditors and email administrators to report on spam-blocking effectiveness and overall email use.

1.3 How MailMarshal Helps You

Unmonitored email presents both financial and legal dangers to a company. For example, spam represents a dramatic financial threat in terms of the cost of storage, bandwidth, and wasted employee time. Virus infection and malicious code can be costly in employee time, repair time, and lost data. Inappropriate and offensive email content wastes time and is a potential liability. Phishing raises financial, legal, and reputational risk.

Using MailMarshal, your company can earn a significant ROI as you secure your network, protect corporate assets, reduce the potential for corporate liability, and improve workplace productivity.

1.3.1 Filters Email at the Gateway

MailMarshal analyzes email content and attachments entering your network to deliver a greater than 97% spam detection rate with less than 0.001% false positives. MailMarshal protects your network and resources by reducing spam and eliminating other undesirable content before it enters your network. By scanning for viruses and detecting and preventing gateway attacks, MailMarshal helps ensure network availability for business purposes.

1.3.2 Delivers Layered Spam Protection

MailMarshal provides a multi-layered approach to email security, pioneering the latest technologies to protect your business from spam, gateway attacks, viruses, phishing attempts, and known malicious URLs embedded in email. Using proprietary SpamProfiler, SpamBotCensor, SpamCensor, URLCensor, and TextCensor technology to detect offensive and undesired content, MailMarshal responds to these emails with the actions you define to help enforce your email Acceptable Use Policy.

Copyright © 2026 Trustwave Holdings, Inc.

1.3.3 Protects Against Existing and Emerging Threats

MailMarshal integrates a wide variety of anti-spam and anti-threat technology to protect against known threats, as well as regular updates to meet emerging threats. The LevelBlue Labs team continually updates threat detection algorithms to detect new forms of spam, mass mailing worms, and phishing scams. MailMarshal can automatically download these updates to keep your protection levels current. The LevelBlue Labs team also publishes Zero Day updates to meet specific threats.

1.3.4 Provides Unparalleled Performance

In parallel with superior spam detection and multi-layered threat protection, MailMarshal provides exceptional performance, operating up to four times faster than other spam-detection products. MailMarshal is a fully native 64-bit application for optimized performance with modern hardware or virtual environments. Scalable configurations allow MailMarshal to work for small or large organizations and to grow as your company does. This hard-working product lets you configure for redundancy to meet demanding SLAs and operate MailMarshal in geographically separate locations from a central console.

1.3.5 Includes Easy-to-Use Interfaces

MailMarshal is easy to evaluate, install, and use. Default settings provide excellent anti-spam performance “out of the box.” The Web-based Management Console provides an intuitive interface that allows policy administrators to refine the rules MailMarshal uses to evaluate and reject or deliver email. The Console also allows email administrators to monitor product effectiveness and manage quarantined messages. A Web-based management console allows email users to review quarantined email, and establish and manage personal rules for acceptable and unacceptable email. Auditors and managers can easily produce reports using the Marshal Reporting Console. These user interfaces allow various users to easily access the information they need about the MailMarshal solution.

1.4 How MailMarshal Works

MailMarshal is a server-based Simple Mail Transfer Protocol (SMTP) email content scanning product that is easy to install in new or existing networks with other gateway applications. It complements and is compatible with traditional Internet firewalls, SMTP mail servers, antivirus scanners, and other security applications.

MailMarshal includes several components including the Array Manager, one or more email processing servers, a Microsoft SQL Server database, and management websites. Small organizations can install the components on a single computer, that could even act as the local SMTP/POP3 email server. Large organizations can install the components across several computers. Enterprises can manage a multi-site distributed array of email processing servers with a single Array Manager computer.

MailMarshal provides a number of user interfaces, including the Management Console, Spam Quarantine Management site, and optional Marshal Reporting Console. Security policy administrators can set email policy for the entire organization and manage blocked email from a central console. You can access these web-based interfaces securely from any network location as needed.

Copyright © 2026 Trustwave Holdings, Inc.

1.4.1 Understanding What MailMarshal Does

The MailMarshal installation functions as the email gateway of an organization. All inbound and outbound email passes through the MailMarshal Server. You can use multiple MailMarshal Servers to provide multiple gateways or to add bandwidth and redundancy to a single gateway.

Each MailMarshal Server runs several component services, including the Receiver, Engine, and Sender services.

Table 1: MailMarshal component functions

Receiver Functions	Engine Functions	Sender Functions
• Inbound TLS • SMTP Authentication • Blocked Hosts • Relaying Tables • DoS Protection • DHA Protection • Reputation Services (DNS Blocklists) • Global Header Rewriting • Connection Policy • DKIM, SPF, DMARC, and ARC-SEAL Evaluation • SpamProfiler rejection	• Content Analysis Policy • Malware Scanning • SpamBotCensor • SpamProfiler and SpamCensor quarantining • NDRCensor • Suspect URL Check • Blended Threats URL Rewriting • Message Archiving • Route Message To Host • Message Parking • DKIM and ARC-SEAL Signing • Azure Information Protection RMS decryption	• Domain Routing Tables • Outbound TLS • DANE validation • MTA-STS validation • SMTP Authentication

All inbound and outbound email enters the MailMarshal Server at the Receiver. At this stage, MailMarshal can apply SpamProfiler checks and Connection Policy rules to messages. Receiver blocking options offer powerful protection because they allow you to refuse incoming email based on criteria such as email not addressed to a recipient in your organization. Connection Policy rules that block email this way conserve resources for other legitimate email.

Next, the MailMarshal Engine unpacks each email, expanding any attached archive or compressed files. The Engine then checks each component against the Content Analysis Policy Rules you have enabled, including SpamCensor scripts, URLCensor, TextCensor scripts, and any other rules you have enabled. You can alter the effects of MailMarshal rules by changing the rule order and by changing specific characteristics of the rule.

MailMarshal also scans email for viruses using antivirus scanning software. MailMarshal supports several scanners with high-throughput interfaces. The product can also use most other antivirus scanners through a command line interface, if the scanner provides a scanning response in the correct format. However command line scanning provides limited throughput.

Copyright © 2026 Trustwave Holdings, Inc.

After the MailMarshal Engine evaluates each email component against the rules, it determines whether to accept, modify, or quarantine the email.

- Accepted email is passed to the MailMarshal Sender, which then delivers it to the appropriate recipients. TLS, MTA-STS, and DANE validation are supported.
- Modified email may be delivered to recipients with attachments removed.
- Email containing malware is quarantined.

MailMarshal can also notify administrators of specific actions or notify end-users of quarantined email. You can associate the appropriate rule action when you create or modify rules.

1.4.2 Configuring MailMarshal

You configure MailMarshal rules and settings using the Management Console interface, connected to the MailMarshal Array Manager. The Array Manager coordinates the activity of all other MailMarshal Servers in the array and connects with the user interfaces, optional Web server, and the database.

The initial configuration settings allow MailMarshal to act as the email gateway of an organization. You can enforce a wide variety of Acceptable Usage Policies by customizing the way MailMarshal processes email connections, content, and attachments.

1.4.3 Monitoring and Reporting

MailMarshal provides additional user interfaces for monitoring and daily email administration. The Management Console features the Dashboard and Status pages, to summarize MailMarshal activity and server health at a glance. Using the Console, email administrators can review email processing history for a message and view and release any quarantined message. Administrators can also review a list of connections rejected by policy.

The administrator can grant other users limited access to the Console. Using this feature, the administrator can delegate basic tasks to help desk or departmental personnel.

Email users can review and manage suspected spam and other quarantined email using daily email digests and the Spam Quarantine Management Web-based console.

Administrators and managers can generate reports on MailMarshal activity using the Marshal Reporting Console. Marshal Reporting Console uses SQL Server Reporting Services to product reports. This is a server application with a website interface. Marshal Reporting Console can deliver reports by web view, email, FTP, or local network files, and can schedule automatic delivery of reports.

Marshal Reporting Console is provided as a separate package from LevelBlue, and is available to all MailMarshal customers.

1.5 LevelBlue MailMarshal Cloud

MailMarshal Cloud is a managed service offered by LevelBlue. MailMarshal Cloud leverages the power and maturity of the MailMarshal processing engine to provide a powerful and cost effective

Copyright © 2026 Trustwave Holdings, Inc.

cloud hosted spam and malware filter. MailMarshal Cloud is an ideal companion to cloud hosted mailbox offerings. For more information about MailMarshal Cloud, contact LevelBlue.

Copyright © 2026 Trustwave Holdings, Inc.

2 Installing MailMarshal

This chapter provides the information you need to install MailMarshal so you can trial the product in a test environment. For the evaluation, you install the prerequisite software, and then install the MailMarshal product on a single computer. You can optionally install your antivirus product on the same computer. The evaluation installation process helps you set up the product and then send sample email using Mozilla Thunderbird or another POP3 email client.

Note: The hardware and software requirements in the *Evaluation Guide* are **not suitable** for a production email environment or testing with a live mail stream. For more information about the requirements for MailMarshal in a production environment, see the installation instructions in the *User Guide*.

2.1 Hardware and Software Requirements

Choose a computer in a test environment where you want to install MailMarshal for evaluation. The computer should not have any MailMarshal components installed. Remove any earlier versions of the product using Add/Remove Programs in Windows Control Panel. For more information about removing earlier versions of MailMarshal, see the *User Guide* for the installed version of the product.

Some prerequisite software is provided in the product installer. You can follow links from the installer to download additional required and optional software from the vendor websites.

The following table lists system hardware and software requirements for an evaluation installation of MailMarshal.

Table 2: Prerequisites for evaluation installation

Category	Requirements
Processor	**Minimum**: Pentium
Disk Space	**Minimum**: 10GB (NTFS)
Memory	**Minimum**: 4 GB (includes 1GB for operating system, 2 GB for MailMarshal, and 1 GB for SQL Express)
Supported Operating System with latest security updates	• Windows Server 2025 • Windows Server 2022 • Windows Server 2019 • Standard or Enterprise versions • Windows 11 *(not recommended for production)*
Network Access	• Port 80 (HTTP) and Port 443 (HTTPS) - for SpamCensor and SpamProfiler updates (Proxy usage is supported)

Copyright © 2026 Trustwave Holdings, Inc.

Table 2: Prerequisites for evaluation installation

Category	Requirements
Software	• Database server: SQL 2025 or 2025 Express, SQL 2022 or SQL 2022 Express, SQL 2019 or SQL 2019 Express, SQL 2017 or SQL 2017 Express. Install the latest Service Pack. For an Azure installation you can use Azure SQL Server. • Antivirus scanning software (optional but recommended) • Microsoft Internet Information Services (Microsoft IIS) with Windows Authentication enabled. • Microsoft .NET Framework 4.6.2 (or later 4.X). Additional .NET packages are included in the installer.

2.2 Installing Prerequisite Software

Install the required software before installing the MailMarshal product to avoid restarting the computer during setup.

To install prerequisites on the MailMarshal computer:

1. Log on to the MailMarshal computer with an account that has Administrator local permissions.
2. Install all operating system service packs and security updates to the latest version for your operating system.
3. Ensure that Microsoft .NET Framework 4.6.2 (or later 4.X) is installed on the MailMarshal computer.
   - If you already have a copy of the full installation package, you can install this item separately.
   - You can also download this item from the LevelBlue support website. Start the download from the Prerequisites tab of the MailMarshal setup window.
   - Complete the installation, and then rerun the MailMarshal distribution package.
4. Ensure that Microsoft IIS is installed on the MailMarshal computer. Include Windows Authentication.
5. *If you plan to use SQL Express to host the MailMarshal database:*
   If you are installing from the “With SQL Express” version of the Web package, you can install SQL Express 2022 as part of the Basic Install of MailMarshal (see “Installing MailMarshal” on page 18).

   To provide additional control of the installation, including instance name and install location, you can install SQL Express 2022 before installing MailMarshal, as follows:

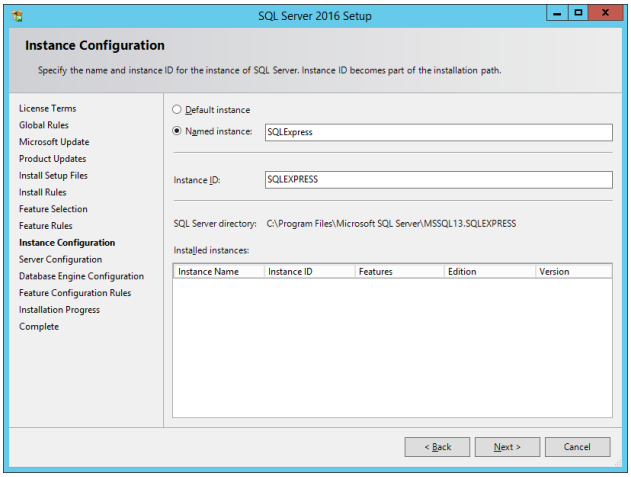
   a. On the MailMarshal setup window, click the Prerequisites tab.

   b. Click the link to install or download SQL Express.

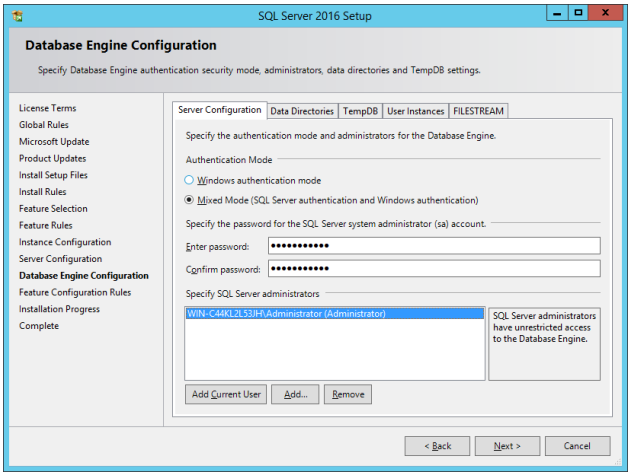
   c. The version of the SQL Express installer that is included in the MailMarshal web package is pre-configured with reasonable default values for an evaluation installation. These include enabling TCP connections and Mixed Mode authentication.

   d. Make a note of the instance name (by default, SQLEXPRESS).

Copyright © 2026 Trustwave Holdings, Inc.



e. Make a note of the password you specify for the **SA** account. MailMarshal uses Windows authentication for database connections by default, but you can also use SQL authentication to connect to the database remotely.



f. Complete the SQL Express installation. If necessary then rerun the MailMarshal distribution package.

6. *If you plan to use one of the integrated Marshal antivirus solutions:*
   a. On the MailMarshal setup window, click the Scanners tab.
   b. Click a link to download any of the listed software.
   c. Complete the main product installation before you install the antivirus solutions. These solutions check for an existing main product key, so they cannot be installed before the main product.

Copyright © 2026 Trustwave Holdings, Inc.

2.3 Understanding the MailMarshal Evaluation Installation

MailMarshal enables a set of email filtering rules by default. These rules include quarantine actions and other features designed for production use. For this evaluation installation, the default rules are assumed.



Note: It is also possible to use MailMarshal for “Monitoring Only” (using rules that log findings but take no action on messages). This mode does not provide any protection against malware or other threats. For assistance setting up a Monitoring Only installation, contact your LevelBlue sales representative.

2.4 Installing MailMarshal

If you have finished installing all prerequisite software, you are ready to install MailMarshal. The trial installation of MailMarshal installs the complete functioning product on one computer. You can evaluate the product for 30 days. When you are ready to purchase a product license, contact your sales representative.

For evaluation, you create a POP3 domain and send email through the MailMarshal product to observe how it handles various messages that you create. In a production setting, you do not typically use a POP3 service. In most production settings, you configure MailMarshal to deliver incoming email to your existing email server. For more information about installing MailMarshal in a production setting, see the *User Guide*.

To install MailMarshal for evaluation:

1. Log on to the MailMarshal computer with an account that has Administrator local permissions.
2. Ensure the Windows Simple Mail Transport Protocol service (if present) is stopped. To verify the Windows Simple Mail Transport Protocol service is not running:
    a. Click **Start > Settings > Control Panel > Administrative Tools > Services**.
    b. In the list, locate the Simple Mail Transport Protocol service.
    c. *If the service is present and the status is Started,* on the Action menu, click **Stop**. Ensure the startup type is set to **Manual.**
    d. Close the Windows Services MMC.
3. Run the MailMarshal setup program from the product installer package.
4. On the Setup tab, click **Install MailMarshal**.
5. On the Welcome window, click **Next**.
6. On the License Agreement window, carefully read the license information.
7. Select **I accept the terms of the license agreement,** and then click **Next.**
8. On the Setup Type window, select **Basic Install,** and then click **Next.**

Copyright © 2026 Trustwave Holdings, Inc.

9. MailMarshal attempts to connect to a SQL instance on the local computer using the Windows Local System account, and it creates a database named `MailMarshal`.



Note: If the process encounters problems connecting, you can use **Custom Install** for more options. If the database already exists, you can choose to use or re-create it. For full information about the available options, see LevelBlue Knowledge Base article Q12939.

10. The Settings Summary window displays the folder locations and database details for the installation. Review the settings, and then click **Next**.
11. On the Ready to Install window, click **Install**. The setup program displays a progress bar until the program is installed.
12. On the Finished window, ensure **Run Configuration Wizard** is selected, and then click **Finish** to run the Configuration Wizard.

You must complete the Configuration Wizard before MailMarshal can receive email and apply rules. For more information, see “Running the Configuration Wizard” on page 19.

2.5 Running the Configuration Wizard

When you click **Finish** on the final window of the MailMarshal Setup Wizard, MailMarshal runs the Configuration Wizard. If you do not complete the wizard after you run the setup program, MailMarshal runs the wizard the first time you start the MailMarshal Management Console.

To run the Configuration Wizard:

1. *If the Configuration Wizard is not running,* start the Wizard by browsing to the MailMarshal Management Console website. Use a supported browser (Chrome, Edge, Firefox, or Safari).
2. Log in to the Management Console. For a custom install use the Username and Password you entered in the Installation Wizard. For a basic install use Username `admin` and Password `admin`.

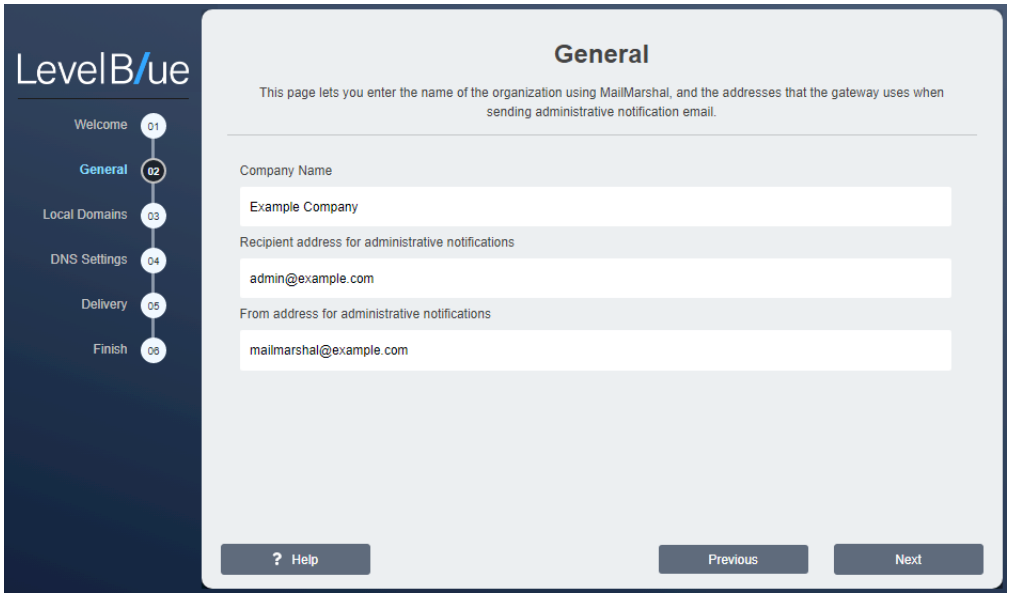


Note: For security, you should change the default password as soon as possible after completing the Wizard. See the Authorized Users item in the Management Console.

It is also possible to configure Windows Authentication or SAML Single Sign On (SSO) with Multi-FActor Authentication for the Console. See the *User Guide*.

3. On the Welcome window, click **Next.**
4. On the General window:

Copyright © 2026 Trustwave Holdings, Inc.



a. Type a company or organization name. This information identifies your organization when you request a license key for MailMarshal.

b. Enter a **Recipient Address**. MailMarshal sends administrative notifications (such as Dead Letter reports) to the address you specify in this field. This address should be a valid and appropriate mailbox or group alias within the local delivery domains of MailMarshal.

c. MailMarshal sends administrative and user notifications and other automated email from the address you specify in the **From Address** field. This address should be a valid address to allow for replies to notifications within the local delivery domains of MailMarshal.

5. Click **Next**.
6. On the Local Domains window, enter one or more domain names for which this MailMarshal server will accept incoming mail.

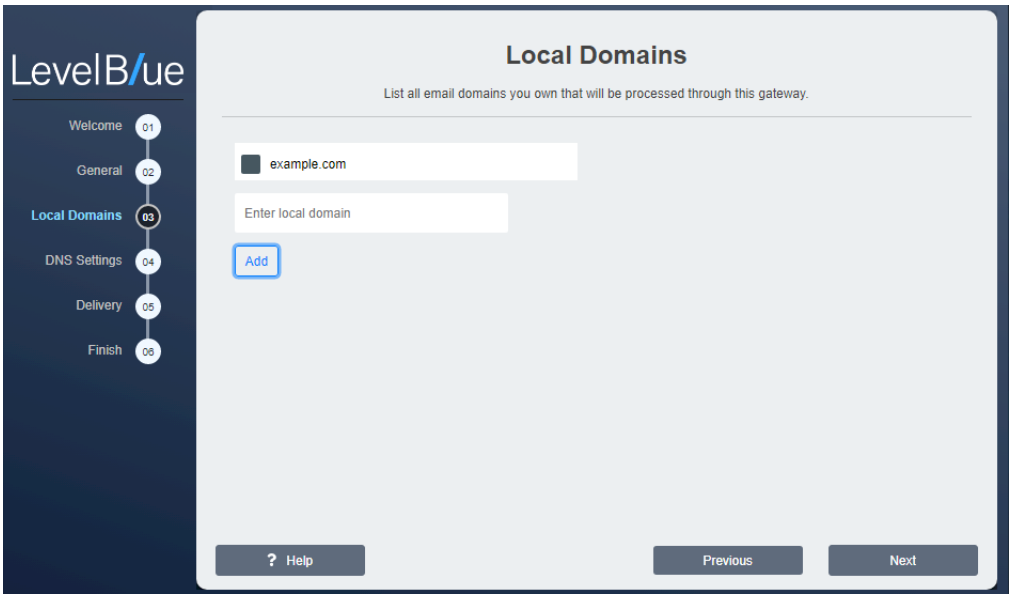
   a. Enter a domain name, and then click **Add**.

   b. Repeat the above steps for each local domain

   c. To delete an existing entry, select it and then click **Remove**.

Copyright © 2026 Trustwave Holdings, Inc.

7. To change an entry, delete it and then add the revised entry.

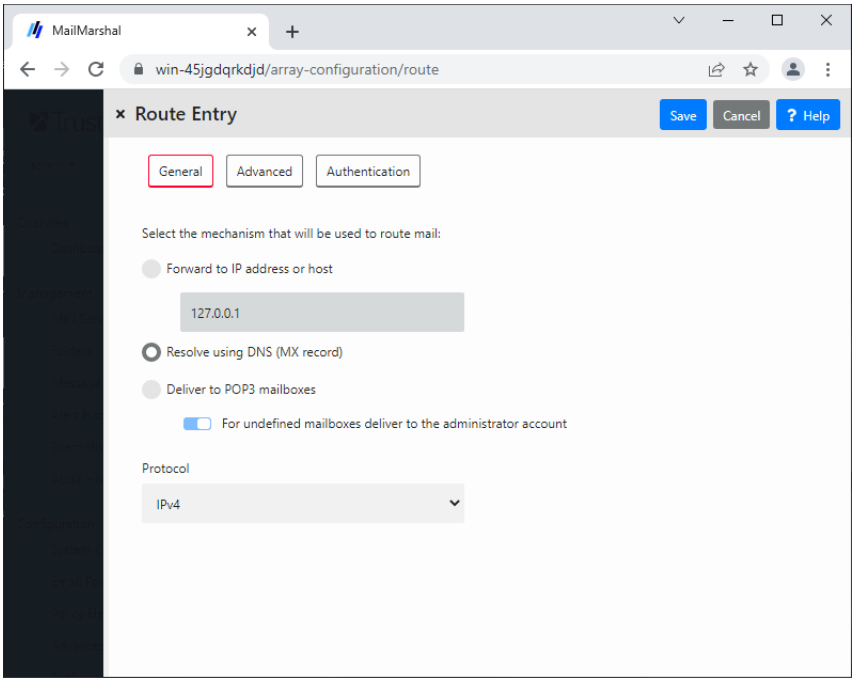


8. When you have included all your test email domains, click **Next**.
9. On the DNS Servers window, you can specify a valid IPv4 or IPv6 address for a **Primary DNS Server** and optionally for a **Secondary DNS Server**.

> **Note:** To assist you, MailMarshal automatically enters the DNS servers set in networking properties for the local computer. If other DNS servers are more suitable, change the entries. In daily operation, MailMarshal does not use Windows DNS settings.

10. Click **Next**.
11. On the Delivery window, enter a server name, Fully Qualified Domain Name, IPv4 or IPv6 address where MailMarshal will deliver incoming email.
    a. If you want test email to go to another server, enter the name or address of the other server.
    b. *If you want to use MailMarshal POP3 for testing,* enter `127.0.0.1 or ::1` (this entry will ensure that you can send test messages using Mozilla Thunderbird on the test server, via IPv4 or IPv6 respectively). You can change the delivery method to POP3 after completing the wizard.
12. Click **Next** to accept the default to deliver external email using DNS.
13. Review the Completing window, and then click **Finish**. The main MailMarshal Management Console window opens.
14. *If you want to use MailMarshal POP3:*
    a. In the left pane of the Management Console click **System Configuration.** In the System Configuration menu, click Routes.
    b. In the right pane, double-click to edit the entry Routing Table. Double-click to edit the entry Local Domains. Double-click the entry `127.0.0.1` or ::1.
    c. On the Route Entry Properties window, select **Deliver to POP3 mailboxes.**

Copyright © 2026 Trustwave Holdings, Inc.



d. Click **Save** until you return to the main Management Console page. To apply the change, click **Commit Pending Changes (at top right of the page).**

2.6 Configuring Anti-Spam Settings

Stopping unsolicited incoming email (commonly known as spam) is a primary goal for most organizations. MailMarshal SpamCensor technology provides a tested set of spam-detecting criteria that can help capture and quarantine spam based on the latest exploits. SpamBotCensor can block spam generated by botnets with even greater efficiency. LevelBlue offers regular updates to the MailMarshal SpamCensor and SpamBotCensor through the Web by HTTP and HTTPS. The SpamProfiler is a signature based check performed at the Receiver, that allows MailMarshal to refuse delivery of spam or quarantine it with minimal processing. For more information about availability of SpamCensor and SpamProfiler updates and eligibility for obtaining them, contact your sales representative.

By default, MailMarshal enables automatic updates for SpamCensor and SpamProfiler. You can configure update settings from the **System Configuration > MailMarshal Properties** window. You can also view current information about your license and last SpamCensor update on the MailMarshal Status page.

Note: To evaluate spam detection, you should ensure that MailMarshal updates are succeeding. For more information about configuring updates, see “Configuring SpamCensor SpamProfiler, and YAE Updates” on page 24.

Copyright © 2026 Trustwave Holdings, Inc.

2.6.1 Spam Configuration and Rules

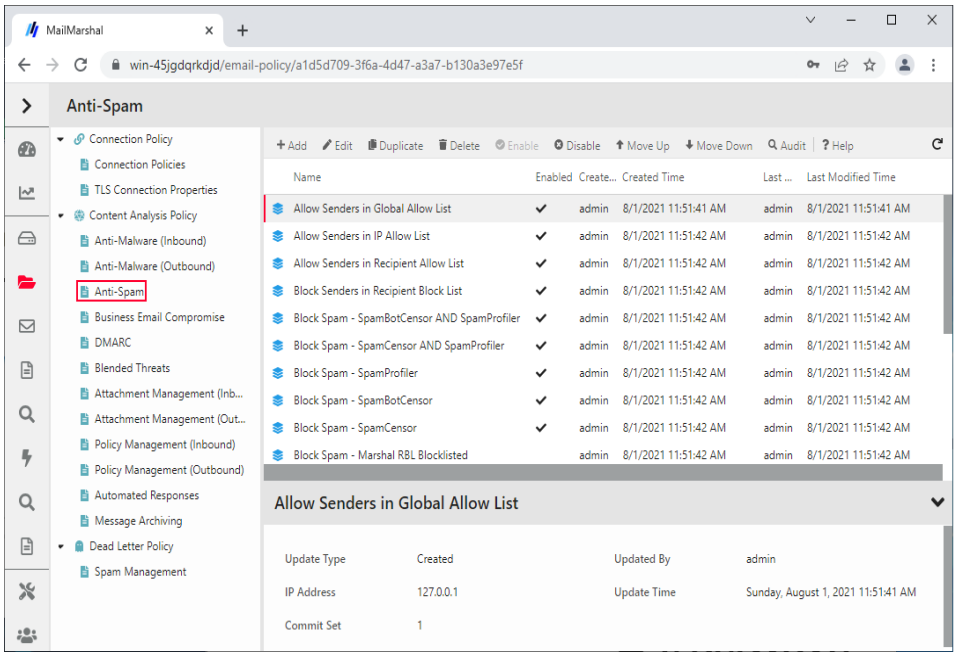
The default email policy provided with MailMarshal includes a policy group titled Spam. This policy group includes a number of rules to block spam. Some basic rules are enabled by default. You can enable and/or customize additional rules to suit your requirements.

MailMarshal provides other options to identify spam, including global settings and advanced customizable categorization. For more information, see the MailMarshal *User Guide* and white papers available from the LevelBlue website.

MailMarshal also allows you to delegate spam management. For more information about the management options, see “Installing MailMarshal Web Components” on page 30 and “Configuring Spam Management” on page 44.

To view the Spam policy group:

1. In the left pane of the Management Console, click the item **Email Policy.** Expand **Content Analysis Policy**.
2. Click the item **Anti-Spam**.



3. View details of each rule, including a description of its intended use, by double-clicking the rule in the right pane. Ensure **Preview** is selected to see all conditions and actions at the bottom of the panel.

The default rules include:

- Rules to quarantine spam using the SpamBotCensor, SpamCensor and SpamProfiler.

Note: To ensure the reliability of SpamCensor, SpamBotCensor, and SpamProfiler, verify that they are enabled and correctly configured. See “Configuring SpamCensor SpamProfiler, and YAE Updates” on page 24.

To ensure the reliability of SpamBotCensor, ensure that MailMarshal processing nodes accept messages directly from the Internet (with no relaying firewall or additional gateway).

Copyright © 2026 Trustwave Holdings, Inc.

- A rule to allow email messages from specific addresses.
- Rules to implement lists of blocked senders and safe senders for each user. Users can update these lists through the MailMarshal Spam Quarantine Management Website.
- A rule to quarantine email messages that contain specific text related to scams, using the MailMarshal TextCensor.
- A rule to block email that contains spam-related URLs in the message header or body. The rule uses the URLCensor function to compare URLs in received messages with listings maintained by external DNS-based blocklist sites. URLCensor decodes URLs intentionally obscured with decimal, octal, or hexadecimal notation. For more information about using URLCensor, see the LevelBlue Knowledge Base.



Note: To use URLCensor in production, you must ensure that MailMarshal uses a reliable, efficient DNS server. For more information, see "Configuring Default Delivery Options" in the MailMarshal *User Guide*.

2.6.2 Configuring SpamCensor SpamProfiler, and YAE Updates

LevelBlue provides updates for the SpamCensor, SpamProfiler, and Yara Analysis Engine (YAE) facilities to all trial installations, as well as customers with current MailMarshal maintenance contracts. The updates are delivered through the Web by HTTP and HTTPS.

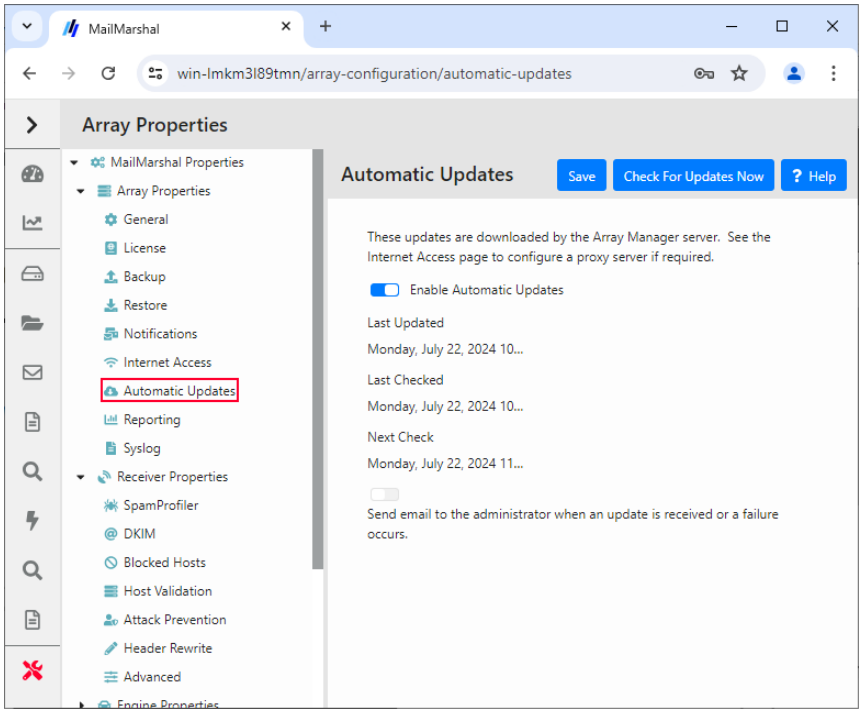
2.6.2.1 Configuring and Checking Automatic SpamCensor Updates

Automatic updating of the SpamCensor is enabled by default. You can choose to download updates manually or automatically.

To monitor and configure SpamCensor updates:

1. In the left pane of the Management Console, click **System Configuration**.
2. Select **Automatic Updates** from the right pane menu. The display shows the time and result of the last update attempt, and the time of the next attempt.

Copyright © 2026 Trustwave Holdings, Inc.



3. If you do not want the SpamCensor to update automatically, clear (toggle off) **Enable Automatic Updates.**
4. If you want to be notified by email when a SpamCensor update is received, select (toggle on) **Send email to the administrator.** MailMarshal sends an email message to the administrator address configured on the Notifications page of MailMarshal Properties.
5. Click **Save** to apply settings.
6. If you want to perform a check for SpamCensor updates immediately, click **Check for Updates Now.**

2.6.2.2 Configuring Proxy Settings for Updates

If the MailMarshal server(s) do not have direct access to the Web, you can configure MailMarshal to use a proxy server to download the SpamCensor and SpamProfiler updates.

SpamCensor updates are downloaded by the Array Manager. SpamProfiler updates are downloaded by each processing node.

To configure proxy settings for the updates:

1. In the left pane of the Management Console, click **System Configuration**.
2. Select **Internet Access** from the right pane menu.
3. You can configure the following settings for the Array Manager (SpamCensor updates) and for the processing nodes (SpamProfiler updates).
   a. If you want MailMarshal to access the Web directly, select **Direct Access.**
   b. If you want MailMarshal to use a specific proxy server, select **Proxy.** Enter a proxy server name and port. If necessary, enter a user name and password for proxy authentication.

Copyright © 2026 Trustwave Holdings, Inc.

4. To apply the proxy settings, click **Save** and then commit MailMarshal configuration changes.

2.7 Configuring Anti-Virus and Anti-Malware Protection

After you complete the Configuration wizard, MailMarshal starts a number of product services and displays the main view of the MailMarshal Management Console.

If your virus scanning product is configured to provide real-time scanning, the MailMarshal Engine Service may start and then stop, and your virus scanning product may alert you to a virus.

To start the MailMarshal services, you must configure your antivirus product to **exclude** the MailMarshal working folders from real-time virus scans and restart the MailMarshal services. Then you can configure MailMarshal to work with your antivirus (AV) program.

2.7.1 Excluding MailMarshal Working Folders from AV Scanning

MailMarshal checks for resident antivirus file scanning by writing a standard test virus file `eicar.com` *(not a real virus)* into some working folders. If your antivirus scanner removes this test file, or if the product denies MailMarshal access to the files, the MailMarshal Engine Service does not start.

In this case, MailMarshal sends an email notice to the administrator. If the check succeeds, MailMarshal deletes all copies of the `eicar.com` test virus except for one copy left in the `\Unpacking\avcheck` subfolder of the installation.

You must configure all your real-time scanning antivirus products to exclude these MailMarshal working folders from scanning even if you do not configure the antivirus product to scan MailMarshal email.

In an evaluation setting, you can exclude the entire MailMarshal installation folder and subfolders. In a production environment, exclude only specified subfolders. For more information, see the *User Guide.*

To exclude the MailMarshal product installation folder from your antivirus product for the evaluation:

1. Refer to your antivirus product documentation to determine how to exclude specific folders or files from antivirus scans.
2. Run the antivirus product control program.
3. Specify to exclude the MailMarshal program folder and all subfolders from scanning. If you installed MailMarshal in the default folder, exclude the `C:\Program Files\Trustwave\MailMarshal` folder and all subfolders.
4. *If the virus scanner does not allow you to exclude specific folders,* disable scanning completely during the evaluation period.
5. Close the antivirus product control program.
6. Browse to the MailMarshal Management Console website.
7. In the left pane, click **Mail Servers**.
8. *If the Status of the server in the list shows any service is not running:*
    a. Double-click the server line item.

Copyright © 2026 Trustwave Holdings, Inc.

b. In the services list, click **Restart All**.

c. Close the server item.

9. In the Mail Servers list, verify the server **State** is Running.

2.7.2 Default Anti-Malware Rules

The default email policy provided with MailMarshal includes two policy groups titled Anti-Malware (Inbound) and Anti-Malware (Outbound). These policy groups include a number of rules to block viruses and malware.

In addition to rules that enable traditional virus scanning, these policy groups include rules that implement Zero Day protection with updates from LevelBlue. These functions provide an additional layer of protection that delivers effective and timely results with lower resource usage than traditional scanning.

To ensure that the Zero Day functions are active, confirm that SpamCensor and SpamProfiler updating is enabled.

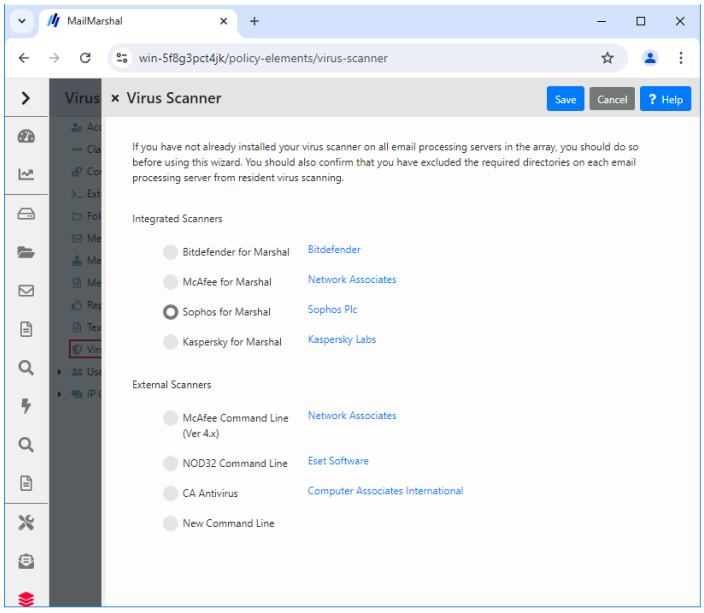
2.7.3 Configuring MailMarshal to Use an Antivirus Product

If you want to allow MailMarshal to use your existing antivirus product to scan email, configure MailMarshal to identify your antivirus product and enable the virus scanning rules of your choice.

To configure virus scanning in MailMarshal:

1. Ensure you have installed one or more supported antivirus scanners on the MailMarshal computer. You can install several integrated solutions from the links on the Scanners tab of the MailMarshal Setup window.
2. If necessary, configure the antivirus product to exclude the MailMarshal working folders. The integrated solutions, such as McAfee for Marshal, do not require this configuration. For more information, see “Excluding MailMarshal Working Folders from AV Scanning” on page 26.
3. Browse to the MailMarshal Management Console website.
4. In the left pane, click **Policy Elements**, and then select **Virus Scanners.**
5. On the toolbar above the list, click **Add**.
6. Select the installed antivirus scanner from the list.

Copyright © 2026 Trustwave Holdings, Inc.



7. *If you are configuring a command line scanner,* on the Configure Virus Scanner Path window, specify or browse to identify the location of the antivirus scanner program, such as `C:\McAfee\Scan.exe`.
8. For other command line scanners, enter required information. See Help for details.
9. Click **Save** to add the virus scanner.
10. *If you plan to use more than one virus scanner,* repeat the steps above for each scanner.

2.7.4 Enabling Virus Scanning Rules

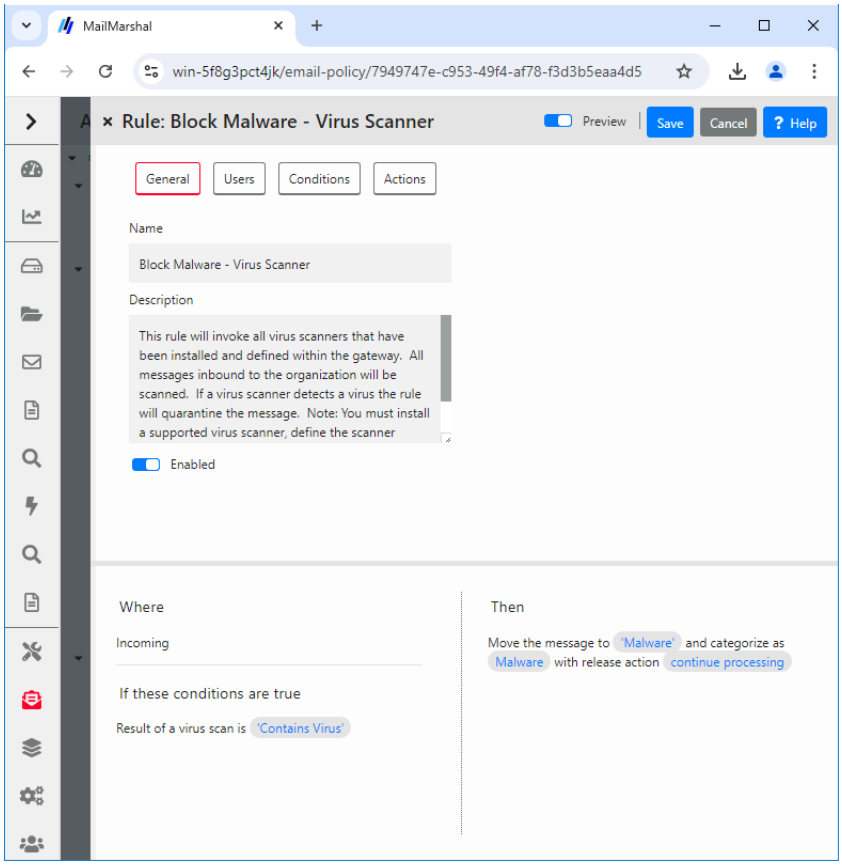
With your antivirus product installed and configured to exclude the MailMarshal working folders, you can now enable virus scanning of your inbound or outbound email.

To enable antivirus scanning of your inbound or outbound email:

1. In the Management Console, click **Email Policy.** Expand **Content Analysis Policy** and select **Anti-Malware (Inbound)**.
2. In the right pane, double-click each rule you want to enable. For example, select the **Block Malware - Virus Scanner** rule.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 1: Enabling Rules



3. Set the rule to **Enabled** using the toggle, and then click **Save**.
4. Select the Anti-Malware (Outbound) policy group, and enable rules in that group.
5. Click **Commit Pending Changes**.

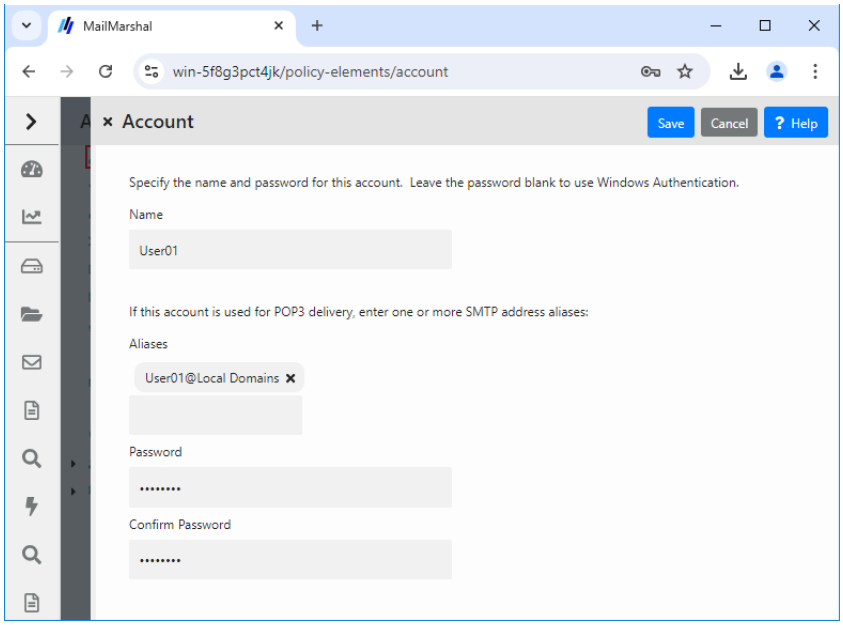
2.8 Configuring MailMarshal to Accept Test Email

To evaluate MailMarshal, you need to send email through the product. The procedure and values suggested in the following procedure help you create a POP3 email account and an administrator email account that allow you to experiment with MailMarshal interfaces, policies, and reports.

To configure MailMarshal to accept and deliver sample email:

1. In the left pane of the MailMarshal Management Console, click **Policy Elements.** Select **Accounts.**
2. On the toolbar, click **Add**.
3. Type the account name, such as `User01`, and a password.
4. Add one or more aliases (email addresses). If you enter an address with a domain part of **Local Domains,** MailMarshal automatically creates SMTP aliases for each local domain (for instance, `User01@mydomain.test`).

Copyright © 2026 Trustwave Holdings, Inc.



5. Click **Save.**
6. If you want MailMarshal to deliver administrative notifications, specify another account name and password. The administrative notification email address must match the Recipient Address you specified in the Configuration Wizard. By default MailMarshal sets this to `admin@mydomain.test` or the test domain you specified when you ran the Configuration Wizard.
7. Click **Save.**
8. In the left pane of the Management Console, select **System Configuration.** Int he right pane menu, select **Relaying.**
9. Double-click the item **Relay Table**. Verify that the source `127.0.0.1` is present and marked Allow. *If this address is not present,* click **Add** and add the address.
10. If you added the address, click **Save**.
11. Click **Commit Pending Changes.**
12. Set up an email account in Mozilla Thunderbird or another POP3 client for the sample address and the administrative notification address. For more information, refer to the product documentation for your email client.

2.9 Installing MailMarshal Web Components

MailMarshal includes a Spam Quarantine Management (SQM) console to allow email recipients to review and manage their quarantined email

You can install the SQM console on the MailMarshal evaluation computer if you install the required software on the computer before running the Web components installation program. For more information, see “Hardware and Software Requirements” on page 15.

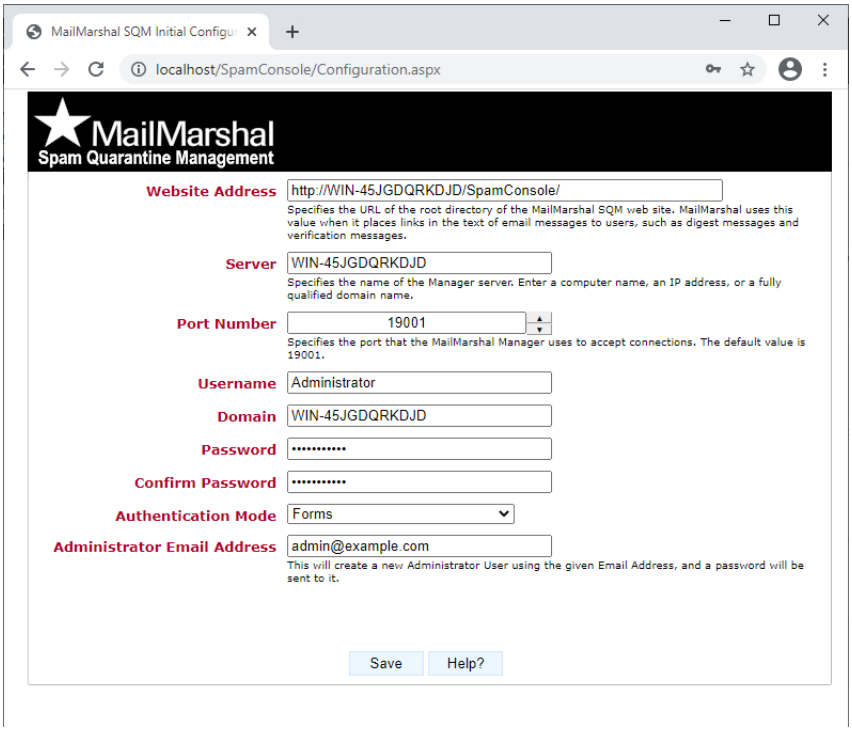
To install the MailMarshal SQM Console:

1. Run the installer package.

Copyright © 2026 Trustwave Holdings, Inc.

2. On the Setup tab, click **Install Web Components**.
3. Follow the instructions to install the SQM component on the local computer.
4. On the Setup Wizard Complete window, click **Finish.**
5. To complete configuration of the Spam Quarantine Management website, open the site by clicking the Spam Quarantine Management item in the MailMarshal program group.

Figure 2: Spam Quarantine Management configuration page



6. In the **Server** field, specify the name of the MailMarshal computer.
7. For **Port Number**, accept the default port `19001`**.**
8. Specify a Windows **User**, **Domain**, and **Password** for an account with Administrator local permissions on the MailMarshal computer.
9. For authentication mode, select **Windows without AD integration.**
10. Click **Save.** MailMarshal records the configuration, and then opens the Spam Quarantine Website to the default view.

You can open the SQM website by using the Start menu item. You can also open the website from other computers that have access, using the appropriate URL. Access the site using a recent version of supported browsers.

2.10 What to Do Next

Now that you have installed MailMarshal, explore the product by continuing through the guided tour in the following chapter.

Copyright © 2026 Trustwave Holdings, Inc.

For more information about product details, see Chapter 4, “Product Features.” For more information about MailMarshal components and architecture for a production installation, see the *User Guide*.

Copyright © 2026 Trustwave Holdings, Inc.

3 Guided Tour

This chapter guides you through the user interfaces to demonstrate the features and power of MailMarshal SMTP. The tour includes the following user interfaces:

- MailMarshal Management Console - Configuration
- Spam Quarantine Management console
- MailMarshal Management Console - Management

In addition, this chapter guides you through the process of customizing your spam-blocking policy and generating sample email activity to view the effect of using MailMarshal SMTP to manage your email.

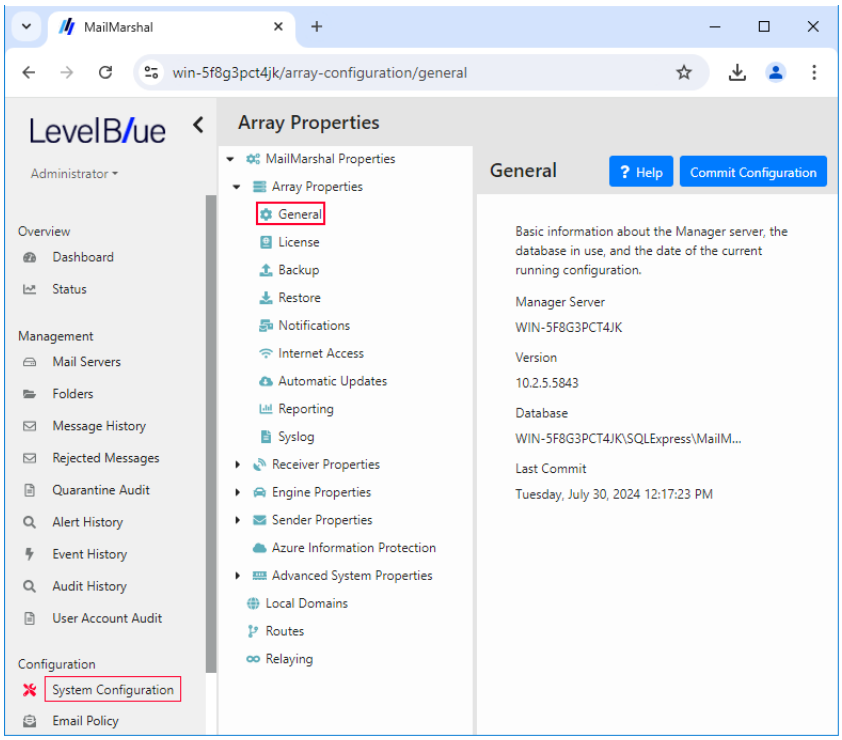
3.1 MailMarshal Management Console - Configuration

The MailMarshal Management Console allows product administrators to create and edit email policy, control email delivery settings, and configure the product.

To follow along with this tour, open the MailMarshal Management Console site (default website on the standalone server installation).

The following figure shows the Management Console open to the System Configuration page. To view this page, in the left pane of the Management Console, click **System Configuration**.

Figure 3: MailMarshal Management Console



Copyright © 2026 Trustwave Holdings, Inc.

Items in the Configuration section of the menu at the left let you control MailMarshal configuration, define your email policy rules, and define other elements of policy, such as return message templates and MailMarshal user groups.

The following list defines the left pane items and the product areas the Management Console lets you control:

Dashboard

Provides a view of email processing, blocked threats, and recommended configuration.

Status

Provides a view of system health, updates, and licensing.

Mail Servers

Lets you review status and configure detailed settings for each processing server.

Folders

Lets you find and review messages in the MailMarshal quarantine and local archives.

Message History

Lets you find and review handling records as well as messages in folders in a searchable unified list.

Lets you find and review messages in the MailMarshal quarantine and local archives.

Rejected Messages

Lets you find and review handling records for messages or connections rejected by server policy or connection rules.

Alert History, Event History, Audit History

Lets you review system events and configuration changes.

System Configuration

Lets you configure MailMarshal components including the Array Manager properties, routing and relaying settings, the Array configuration, and individual Server properties.

Email Policy

Lets you define rules that determine how MailMarshal evaluates and acts on email.

Copyright © 2026 Trustwave Holdings, Inc.

Policy Elements

Lets you customize how MailMarshal connects to your directory servers and manage MailMarshal user groups. Also lets you specify how MailMarshal customizes email notifications, message templates, stamps, and classifications.

Advanced Settings

Lets you control expert-level settings that are not included in the graphical interface.

Authorized Users

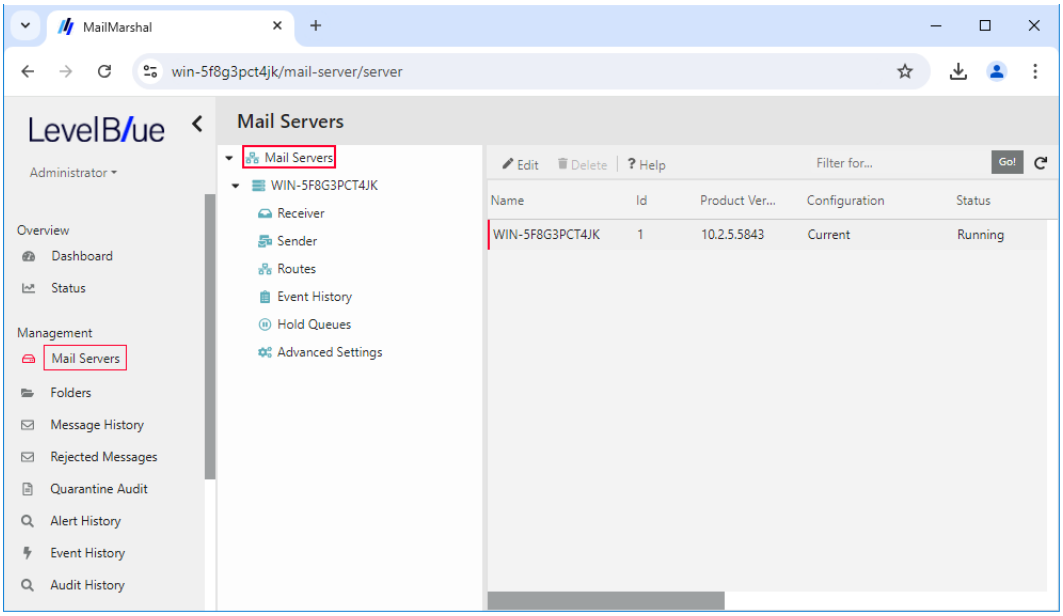
Lets you control access to the Management Console (visible to Superusers only).

3.1.1 System Configuration

When you install MailMarshal as you have for this evaluation, MailMarshal installs the Array Manager and Server components on one computer. The MailMarshal Management Console lets you configure the Array Manager to which all the MailMarshal servers report. The Management Console also lets you monitor the status of all your MailMarshal servers and, when necessary, customize settings for specific servers.

In the left pane, click **Mail Servers** to quickly check the status of your servers and configure individual servers. For evaluation, you should have just one MailMarshal Server, similar to Figure 4.

Figure 4: MailMarshal Servers



In the right pane, you can quickly assess the status of each server in the array. In the above example, the Engine service is not running.

The **System Configuration** item lets you access configuration for the Array Manager and all servers in the installation.

Copyright © 2026 Trustwave Holdings, Inc.

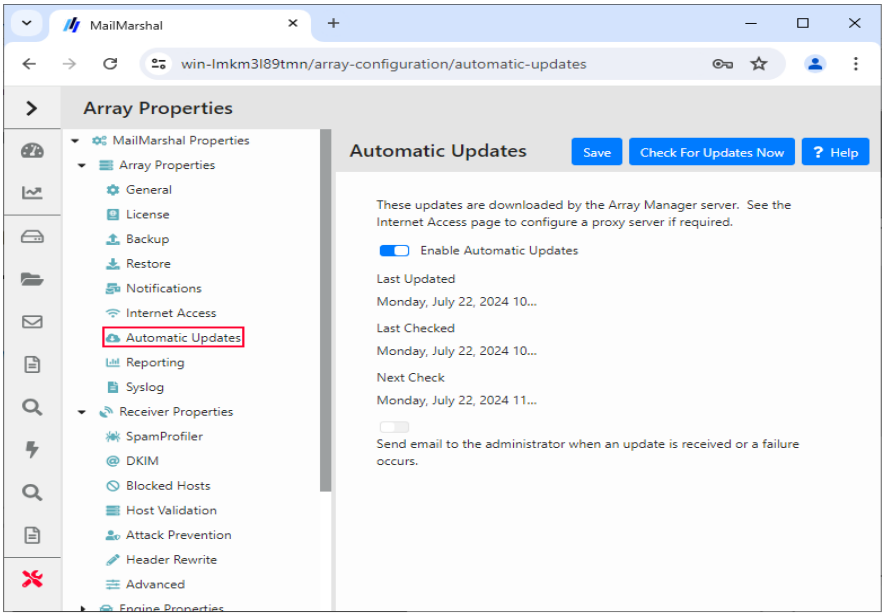
3.1.1.1 Configuring MailMarshal

The MailMarshal Properties window lets you configure attributes of the array of servers. MailMarshal Properties controls email filtering rules applied to all email, such as restrictions on relaying, Directory Harvest Attack prevention, and use of Transport Layer Security certificates.

To open the MailMarshal Properties panel, select System Configuration from the left menu.

Figure 5 shows the MailMarshal Properties window. To see additional options, expand items in the menu such as the Receiver, Engine, and Sender.

Figure 5: MailMarshal Properties



The MailMarshal Properties window lets you configure the following properties:

General

Provides information about the MailMarshal Array Manager server, software version, and database name. Also lets you back up and restore the product configuration.

License

Lets you review current licenses, add new licenses, and specify product behavior if the license expires.

Backup

Allows you to configure automatic configuration backup and retention settings, and make a backup manually.

Restore

Allows you to restore configuration from an available backup.

Copyright © 2026 Trustwave Holdings, Inc.

Notifications

Allows you to edit the email addresses the product uses when it delivers administrative email notifications.

Internet Access

Allows you to edit the information the product uses to access the Internet, to download SpamCensor and SpamProfiler updates.

Automatic Updates

Allows you to control how frequently to check for automatic SpamCensor updates to implement the latest spam blocking techniques.

Reporting

Lets you set the data retention period for reporting.

Syslog

Lets you configure data format and content to send to a Syslog server. You must create a database for temporary data storage using the MailMarshal Server Tool before enabling Syslog sending.

SpamProfiler

Allows you to enable or disable SpamProfiler, and configure the SpamProfiler option that checks for known spam at the message receipt level.

DKIM

Allows you to enable or disable use of DomainKeys Identified Mail (DKIM) validation. To use DKIM for signing you must also enter a private key for each local domain, and include public keys in DNS records.

Blocked Hosts

Allows you to maintain a list of servers from which MailMarshal will never accept email messages.

Host Validation

Allows you to configure the product to verify hosts by the host PTR record in DNS.

Attack Prevention

Allows you to configure the product to prevent Denial of Service (DoS) and Directory Harvest Attacks (DHA). On this tab you can also specify servers to exempt from attack prevention (safe list).

Copyright © 2026 Trustwave Holdings, Inc.

Header Rewrite

Allows you to globally change the contents of email headers (recommended only for experienced users). For example, you may want to delete internal email host names from outbound email to hide sensitive information about internal email servers.

Blended Threats

Allows you to configure global exclusions for the Blended Threat analysis services.

Executive Name List

Allows you to configure names of company executives for use in fraud detection rules.

Delivery

Allows you to configure how MailMarshal forwards email to external email domains.

Outbound Security (TLS)

Allows you to configure when to enforce Transport Layer Security (TLS) certificates to connect securely with external email servers.

Azure Information Protection

Allows you to enter the information required to decrypt and scan AIP protected documents.

Advanced items and Advanced System Properties

Allow you to set additional options that affect MailMarshal operation (recommended only for experienced users).

3.1.1.2 Configuring Individual Server Properties

You can use the MailMarshal Management Console to configure the settings for an individual server.

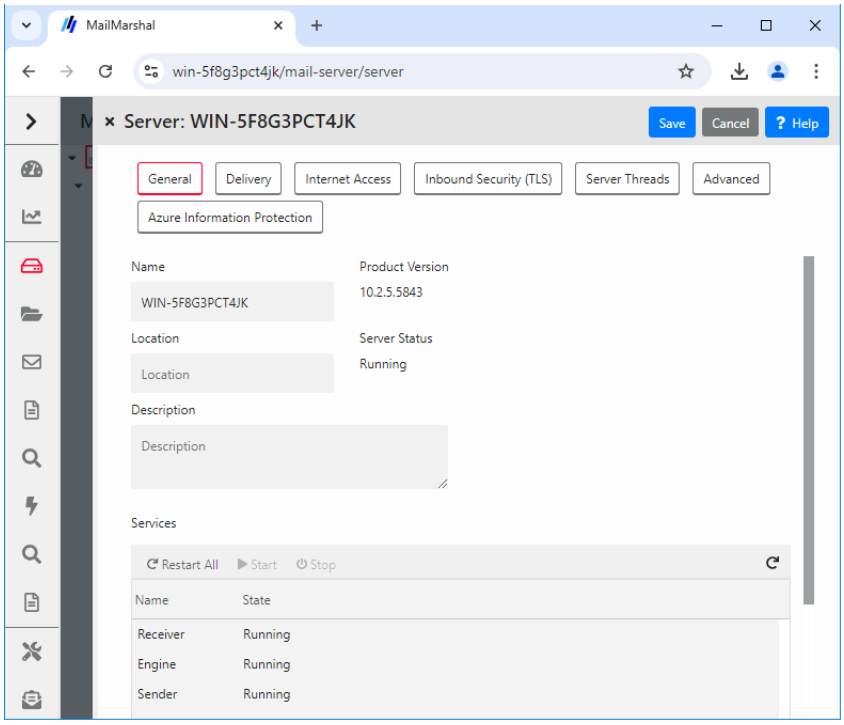
To display and configure MailMarshal Server properties:

1. In the left pane, select **Mail Servers.**
2. In the list at the right of the right pane, double-click the server you want to configure.

MailMarshal displays a window to let you configure your specific server.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 6: Server (Node) properties window



The Server Properties window lets you configure the following properties:

General

Lets you add information about the server and start or stop the MailMarshal Server services, including the Receiver, Engine, Sender, and optional POP3 server.

Delivery

Lets you customize DNS lookup options and specify email delivery options, such as direct delivery or forwarding.

Internet Access

Allows you to edit the information the product uses to access the Internet from this server, to download SpamProfiler updates.

Inbound Security (TLS)

Lets you create Transport Layer Security certificates and manage the security configuration including PFS support.

Server Threads

Lets you configure performance settings for an individual server.

Copyright © 2026 Trustwave Holdings, Inc.

Advanced

Lets you configure advanced settings such as receiver port bindings, host name, and hosts to deliver notifications.

Azure Information Protection

Lets you review the status of the Azure Information Protection (AIP) Rights Management client on this server. The AIP client allows you to unpack and scan AIP protected messages.

3.1.2 Exploring Email Policy

Email Policy in MailMarshal defines how the product handles each email it processes.



Note: So that MailMarshal can detect and block email with explicit language, such as profanity and pornographic language, the Email Policy rules and the TextCensor scripts must contain that explicit language. Anyone with permission to run the MailMarshal Management Console may be exposed to this explicit language. Since this language may be objectionable, please follow your company's policy about employee exposure to potentially objectionable content.

The Email Policy includes Connection Policy, Content Analysis Policy, and Dead Letter Policy.

- Connection Policy is evaluated while MailMarshal is receiving messages from a remote server. Connection Policy rules can accept or reject a message based on limited criteria.
- Content Analysis Policy is evaluated once a message is fully received and all content has been unpacked. Content Analysis Policy rules can scan a message for viruses and other inappropriate content, and quarantine the message or take many other actions.
- Dead Letter Policy allows you to control how MailMarshal treats messages that could not be fully scanned because they are malformed.

Within each policy type you can define one or more policy groups. Each policy group contains one or more rules. Each rule has three parts:

User Matching

Defines to which users or groups the product will apply the rule.

Conditions

Defines the conditions in which the rule applies.

Actions

Defines the actions MailMarshal should take when an email meets the rule conditions.

To evaluate an email, MailMarshal applies User Matching criteria to see if the policy applies to the recipient.

If the email meets the User Matching criteria, MailMarshal evaluates the header, message, and attachments according to the User Matching and Conditions sections of each rule in the group.

Copyright © 2026 Trustwave Holdings, Inc.

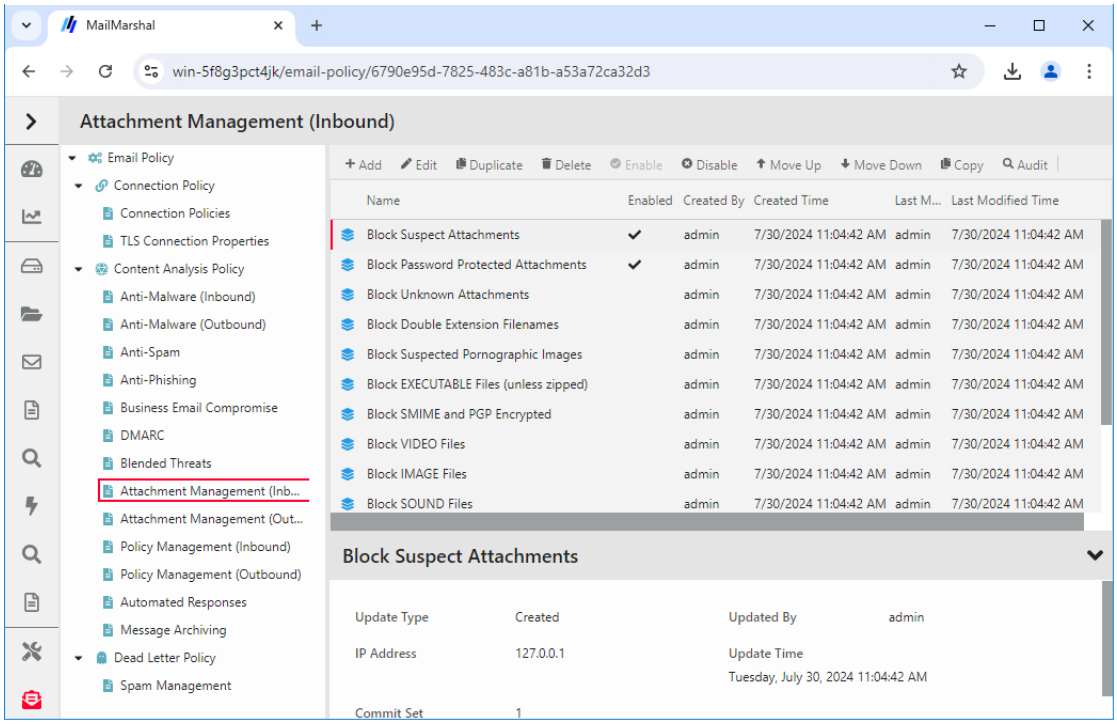
MailMarshal rules let you apply policy based on many email features, such as content of subject lines, name of sending host, URLs specified in the message, and many more options.

If the email meets the criteria of a rule, MailMarshal applies the specified actions to the message. Using rule actions, MailMarshal can redirect or quarantine email, send notifications, and even modify message content.

To explore email policy:

1. In the left menu, select **Email Policy**. Select **Connection Policy, Content Analysis Policy**, or **Dead Letter Policy**.

Figure 7: MailMarshal Email Policy



2. In the left pane, select a policy group, such as **Attachment Management (Inbound)**.
3. In the right pane, double-click to edit a rule, such as **Block EXECUTABLE Files.**

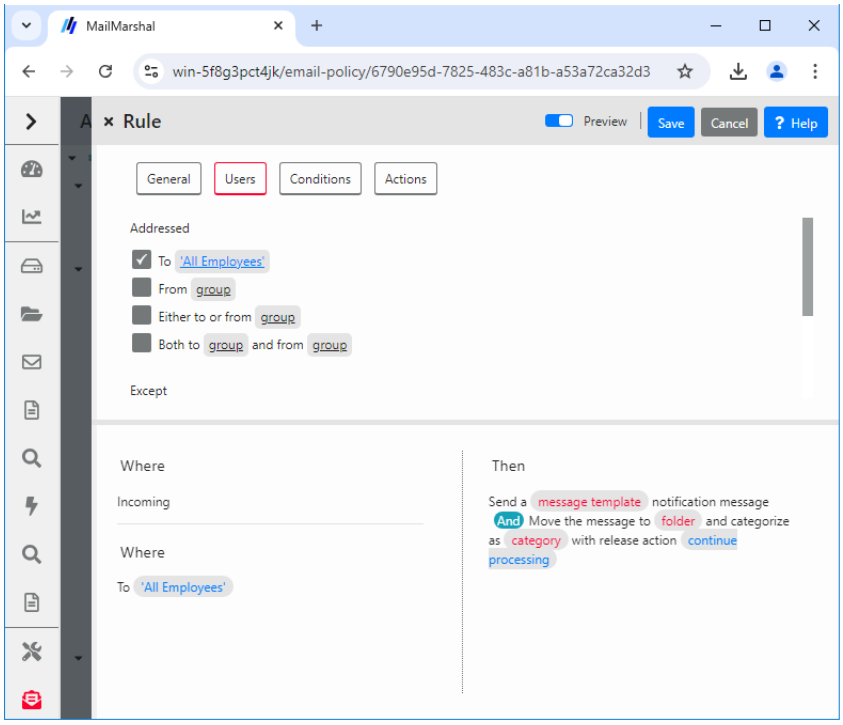
The window displays the rule name, comment, and description. To see a full narrative of the rule, make sure that **Preview** is enabled (toggle at the top of the panel).

The following figure shows a window in the Rule Wizard General tab.

Links and fields on each tab of the window let you customize the rule and choose the policy conditions you want to enforce.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 8: Rule Wizard (Rule Actions window)



Take some time and explore the rules that the product includes. Customize a few of them so you can understand how the user matching, conditions, and actions could apply the rule to members of your organization.

3.1.3 Policy Elements

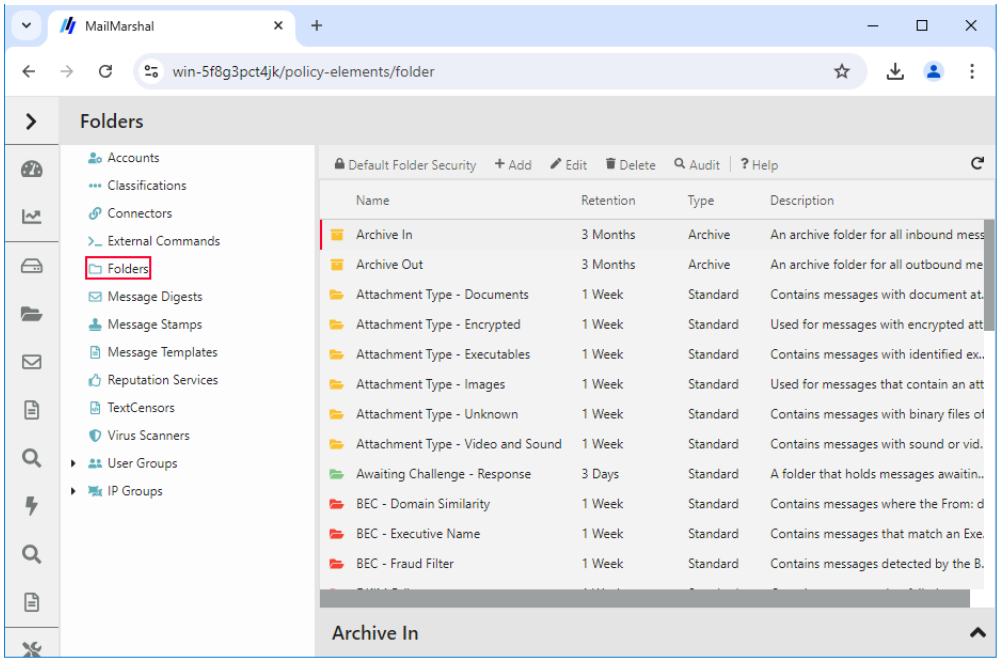
MailMarshal Policy Elements are building blocks you can use when you create MailMarshal policy groups and rules. These elements help you specify complex rule conditions and rule actions.

To work with Policy Elements:

1. In the left pane, select **Policy Elements**.
1. Select a Policy Element, such as **Folders**.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 9: MailMarshal Policy Elements (Folder pane)



The right pane displays the folders available and the current message retention period for each folder.

You can create or edit many policy elements on the fly while you are editing email policy. You can also create elements in advance. Spend a few minutes exploring the default elements and the options available.

MailMarshal provides the following policy elements:

Connectors

Allow you to import user and group information from Azure Entra, Active Directory or LDAP servers.

Accounts

Allow you to grant permission to relay email through MailMarshal for specific users. Also allow you to set up POP3 service on the MailMarshal server for a limited number of users.

Classifications

Allow you to record the results of MailMarshal evaluations. You can report on classification actions using Marshal Reporting Console.

External Commands

Allow you to extend MailMarshal functionality with customized conditions and actions.

Copyright © 2026 Trustwave Holdings, Inc.

Folders

Allow you to quarantine or copy messages. You can report on folder actions using Marshal Reporting Console.

Message Digests

Allow you to notify users about quarantined email on a schedule you specify, and allow them to release the quarantined messages.

Message Stamps

Allow you to add signatures or disclaimers, and to notify email users and administrators about MailMarshal actions within an existing email message. You can include specific information about a message using variables.

Message Templates

Allow you to notify email users and administrators about MailMarshal actions by sending a new email message. You can include specific information about a message using variables.

Reputation Services

Allow you to configure DNS-based services that provide information about the reputation of other email servers. You can use these services in rules to help MailMarshal decide whether to accept a message.

TextCensors

Allow you to apply policy based on the textual content of email messages and attachments. You can create complex conditions using weighted combinations of Boolean and proximity searches.

Virus Scanners

Allow you to check email messages for virus content. If your antivirus scanner finds a virus in a message, MailMarshal can quarantine it.

User Groups

Allow you to apply policy based on email addresses. MailMarshal can retrieve groups from Active Directory or LDAP servers. You can also create local groups and enter members using wildcards.

IP Groups

Allow you to apply policy to specific IP addresses or IP ranges.

3.2 Configuring Spam Management

When MailMarshal quarantines a suspicious email, the recipient or sender may still want the message to be released to its destination. If an organization generates a large amount of quarantined email, the

Copyright © 2026 Trustwave Holdings, Inc.

email administrator may not have time to review all the quarantined email. This situation is likely to arise with messages that MailMarshal has classified as Spam.

MailMarshal provides several options that allow the administrator to delegate responsibility to the email recipient or other reviewer to determine if the email should be released. For example, the following people may be candidates to review quarantined email:

- Departmental administrators or help desk personnel can have permission to process the messages in selected quarantine folders, using the MailMarshal Management Console. Permissions can be granted using MailMarshal roles, and either Windows users/groups or MailMarshal users (depending on the authentication method chosen for the Management Console).
- Email recipients who receive a daily summary of their incoming quarantined messages from MailMarshal digest emails.

Each email user can have permission to review and release messages quarantined in one or more folders, through the MailMarshal Spam Quarantine Management Website. This facility is specifically designed to allow users to review messages that MailMarshal classifies as Spam, but you can use it for other classifications. It also allows each user to refine the Spam classification by maintaining personal lists of safe and blocked senders.

3.3 Configuring Folder Properties

The primary purpose of the Spam Quarantine Management Website is to allow users to review messages that MailMarshal has quarantined as spam. The site can be used to manage one or more folders for this purpose. The site can also be used to manage folders that are used for other purposes.

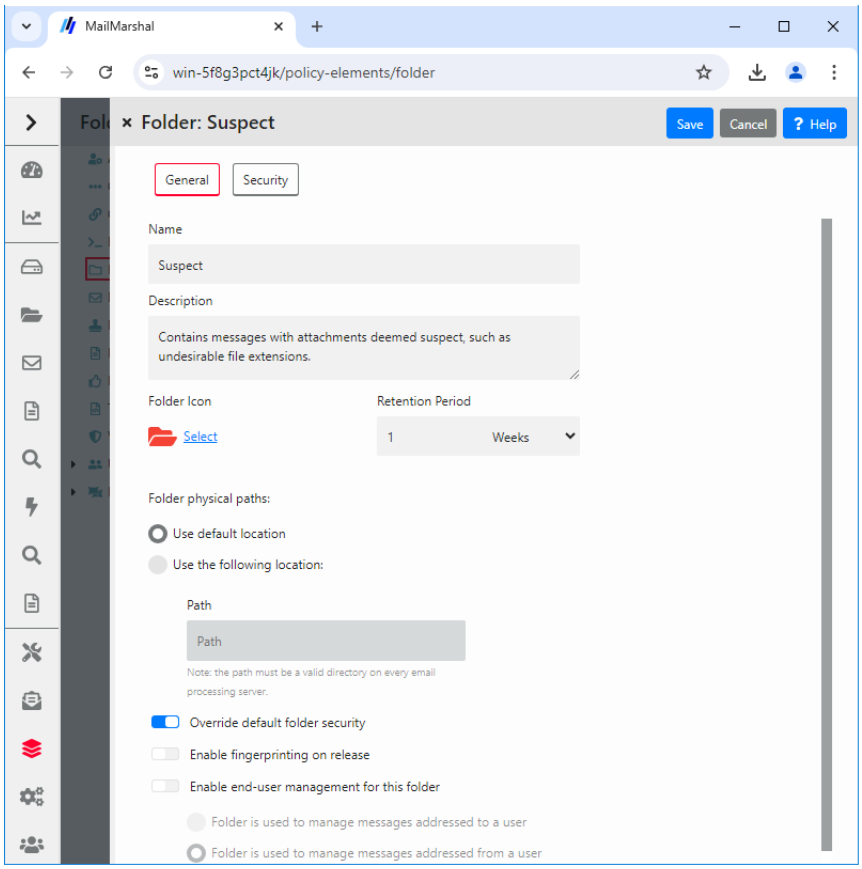
Each folder managed by the Spam Quarantine Management Website can contain either messages sent to local users or messages sent by local users, but not both.

To set up folders to manage spam with the Spam Quarantine Management Website:

1. In the menu of the Management Console, click Policy Elements. From the right pane menu, click Folders.
2. Double-click a folder in the list such as the Suspect folder.
3. In the folder properties, select (toggle on) **Enable End-user Management for this folder.**
4. Choose the setting **Folder is used to manage messages addressed to a user**.

Copyright © 2026 Trustwave Holdings, Inc.

5. Click **Save**.



6. *If you want each user to receive a summary of messages quarantined in this folder,* in **Policy Elements**, click **Message Digests.**
7. Double-click to edit the item Spam Digest. Click the **Folders** tab.
8. Click **Add,** select the folder Suspect from the list, and then click **Save.**
9. You can review and change other features of the digest using the other tabs of the properties window.
10. Click **Save** to close the window, and then commit configuration changes.

3.4 Generating Sample Email Activity

To see the features of MailMarshal in action, you can send sample email through the system using your current email client. For more information, see “Configuring MailMarshal to Accept Test Email” on page 29.

You can review how MailMarshal handles these messages using the MailMarshal Console, Spam Quarantine Management Website, and Marshal Reporting Console.

You can send sample email through your Mozilla Thunderbird or other POP3 email client to trigger MailMarshal rules so you can evaluate the product.

Copyright © 2026 Trustwave Holdings, Inc.

The following table provides some test samples. The samples are simple emails that trigger some default rules. In production, MailMarshal recognizes much more sophisticated cases of spam and other undesirable content.



Note: MailMarshal spam detection relies on several layers that evaluate the entire message including the source and header information as well as text. Spam signatures and heuristic algorithms are updated frequently. For these reasons it is not possible to define an example message that "looks like spam" and will always trigger spam detection. To see the full power of spam detection in action, use a MailMarshal server to process real messages.

The cases in the table use default email policy rules. You can experiment with additional features by enabling rules found in other policy groups, such as Content Security and Anti-Virus policy groups. You may want to test other rules that block attached files by type, such as Block EXECUTABLE files.

The results shown here are expected if you use the default MailMarshal rules without customizing. You can see the actual results by using the MailMarshal interfaces as described later in this chapter.

To test MailMarshal, create emails with the following subject line, email body, and any specified attachments. Send the email to your sample email account (such as `sample@mydomain.test`). For more information about setting up a sample email account, see "Configuring MailMarshal to Accept Test Email" on page 29.

Table 3: Test email content and results

Email Content	MailMarshal Result
Subject: `Hello World` Body: `Hi there`	Delivered and logged in Mail History
Subject: `Spam 1` Body: `XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X`	Quarantined in the Spam - Confirmed folder. • **Note:** Copy the provided string into the email body as a single line. This string is a standard Spam test string known as GTUBE ("Generic Test for Unsolicited Bulk Email").
Subject or Body contains: `MailMarshal-Anti-Spam-Test`	Quarantined in the Spam - Suspected folder.
Subject: `Attached bat file` Body: `Hi there` Attachment: any file with extension .BAT	Quarantined as Suspect. Recipient receives a notification email.
Subject: `Attached passworded Zip` Body: `Hi there` Attachment: any ZIP file with a password	Quarantined as Encrypted. MailMarshal cannot fully unpack and scan password protected files, so it places them in quarantine for manual review.
Subject: `make money at home` Body: `C@sh`	If the rule "Anti-Spam\ Block Spam - Administrator Maintained Keyword list" is enabled, this message is quarantined as Spam - Suspected based on the word found in the body.

When MailMarshal examines email, in addition to checking the extension of all file attachments, MailMarshal also opens attachments to check the file structure. MailMarshal blocks files by

Copyright © 2026 Trustwave Holdings, Inc.

examining both the extension and file structure to detect risky attachments, even when a file extension has been changed.

3.5 MailMarshal Management Console - Management

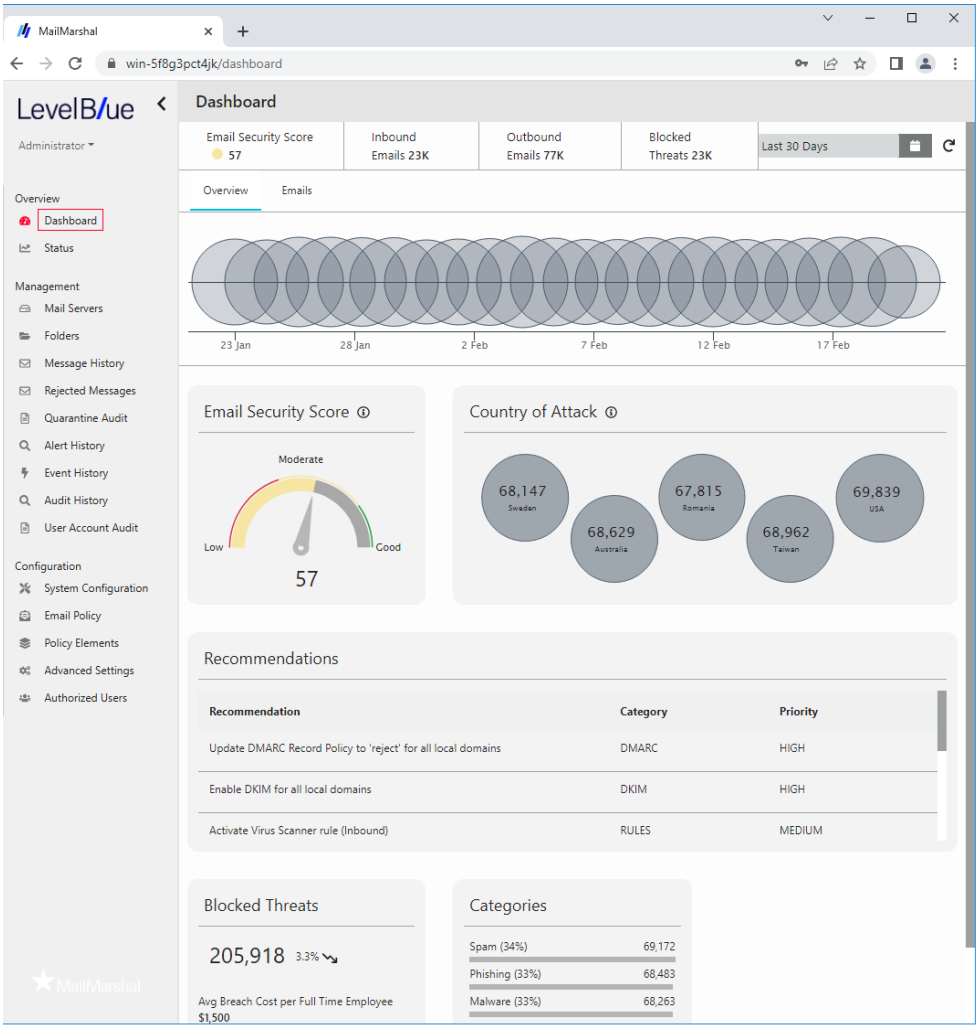
The Management section of the MailMarshal Management Console allows you to monitor MailMarshal operation and email flow. This section provides summary information on the current state of MailMarshal, as well as administrative access to the quarantine folders and message sending services.

If you have sent sample email as suggested above, you can see the results of MailMarshal rules here.

3.5.1 MailMarshal Console

When you first open the MailMarshal Management Console item, the Console displays the Dashboard page. The Dashboard provides a graphical overview of security status and threats detected.

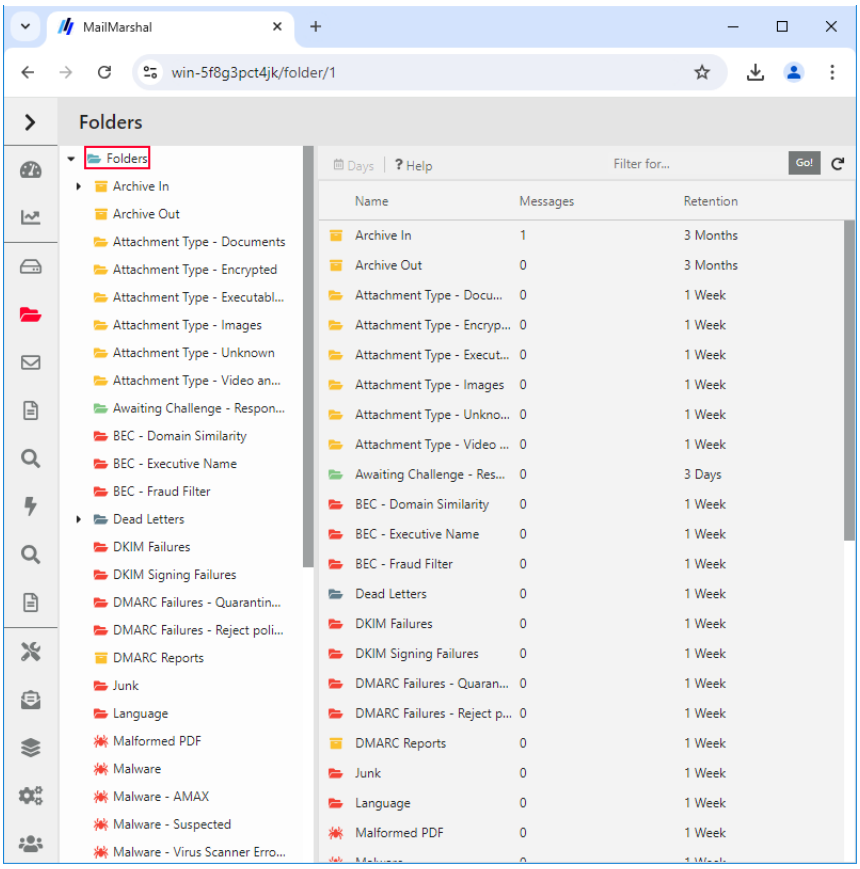
Figure 10: MailMarshal Console Dashboard



Copyright © 2026 Trustwave Holdings, Inc.

The Folders item under Management in the left pane allows you to review the contents of MailMarshal quarantine folders individually. Each folder is organized with daily subfolders for easy access.

Figure 11: MailMarshal Console Folders view



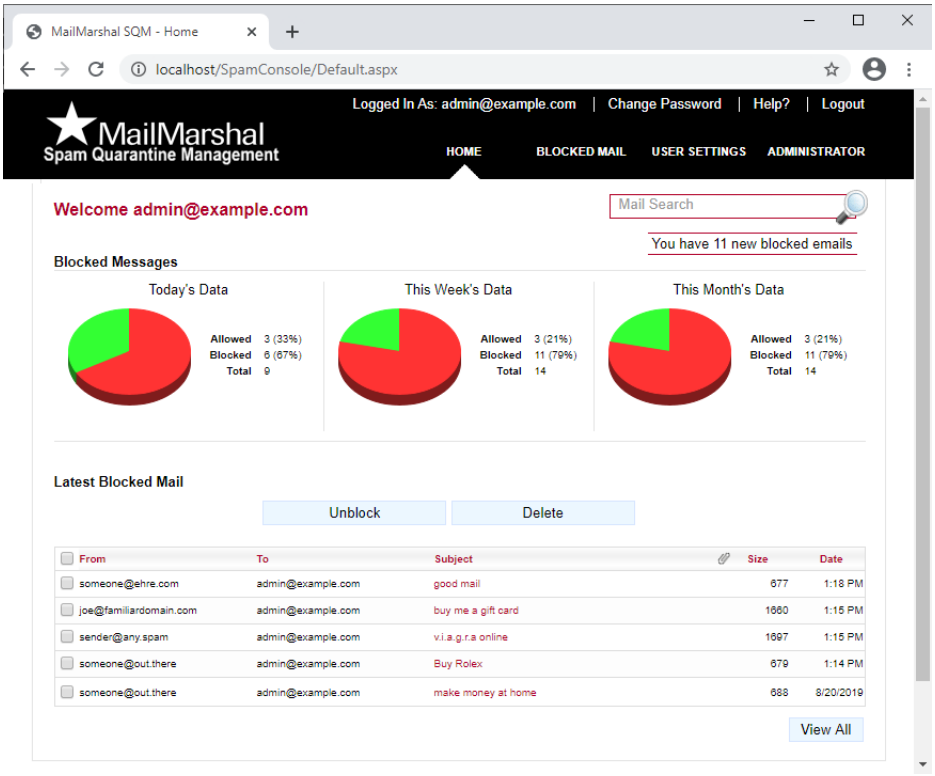
The Message History item under Management in the left pane allows you to see the result of processing for each message that MailMarshal has processed. These results can include delivery, quarantine, and logging classification, among others. You can search for specific messages by address, subject, and time.

3.6 Spam Quarantine Management Website

The MailMarshal Spam Quarantine Management (SQM) Website allows users to review email that MailMarshal SMTP quarantined as spam. Users can review their messages and release them. When messages are addressed to more than one recipient, each recipient can decide whether to release the email.

Copyright © 2026 Trustwave Holdings, Inc.

Figure 12: Spam Quarantine Management website



The SQM site offers the following features:

Blocked Mail

Allows users to review email messages addressed to them that MailMarshal has quarantined in one or more folders.

Manage Senders

Allows users to maintain personal lists of safe senders and blocked senders. If you use the default MailMarshal rules, the product does not block email from safe senders, and it always blocks mail from blocked senders. You can choose not to use one or both of these lists.

Email Addresses

Allows users to maintain a list of additional email addresses at which they receive email. Users can use this feature to aggregate and manage email for several email aliases using the SQM site with a single logon.

Delegates

Allows users to delegate rights to review their blocked email. For example, a manager could delegate SQM review of email to a personal assistant.

Copyright © 2026 Trustwave Holdings, Inc.

User Settings

Allows users to choose site look and feel options, such as a default language for the site. Level-Blue provides English, French and Spanish versions of the site. You can add other languages.

Administrator

Allows nominated administrators to configure site settings and manage users.

3.6.1 Adding an Email Address for Spam Quarantine Management

You can add more email addresses to manage using SQM.

To add an email address:

1. Start a web browser and in the address bar, type the following address: `http://localhost/SpamConsole`.
2. Click **User Settings** and select the **Email Addresses tab.**
3. Type `sample@mydomain.test`, and then click **Add.**
4. SQM delivers a confirmation email to the address.
5. Retrieve the confirmation email using your email client and click the confirmation link.
6. The authorization page indicates **Successfully verified email alias.** Close this window.
7. Refresh the Email Addresses window. The list displays the added address, `sample@mydomain.test`.

3.7 Reviewing Blocked Email

If you have set up a local email address and folder, you can use the SQM site to review sample email you have sent. For more information, see “Configuring MailMarshal to Accept Test Email” on page 29 and “Configuring Folder Properties” on page 45.

To review blocked email:

1. On the SQM main window, click **Blocked Mail.**
2. The Blocked Mail page shows a list of email quarantined for all email addresses associated with the login. Click the message subject to see more details.
3. Click **Release** to release the message for delivery.

Copyright © 2026 Trustwave Holdings, Inc.

4 Product Features

Use the following feature lists to compare MailMarshal SMTP with other products for features and performance.

4.1 Anti-Spam and Anti-Malware

MailMarshal provides a full set of features and tools to detect and manage spam and malware. After initial installation MailMarshal manages spam with very little overhead.

Table 4: Anti spam features

Feature	Description
SpamCensor	Incorporates an advanced heuristic anti-spam engine. Provides better than 97% spam detection rate with less than 0.001% false positives. SpamCensor ranks among the world's best in spam detection and accuracy, straight out of the box without need for customization.
SpamBotCensor	Provides detection optimized for recognition of messages generated by spambot networks.
SpamProfiler	Provides a signature-based anti-spam function that can be used to very quickly and accurately identify messages that resemble known examples of spam. Macin receives signature updates from LevelBlue as frequently as every 10 minutes. SpamProfiler can also identify spam messages in a variety of languages.
Yara Analysis Engine	Provides a script-based anti-malware function as a further layer in spam detection.
Email Compromise Fraud Detection	Provides heuristic detection for targeted fraud spam. You can customize this feature by adding information about local executive names and email addresses ("Executive Names List").
Machine Learning Technologies	Incorporates several proprietary Machine Learning/AI based engines to recognize Phishing and other threats.
Dynamic Anti-Spam Updates	Provides the ability to automatically update anti-spam technology via the Internet. Updates include spam pattern definitions and the SpamCensor engine. MailMarshal is always up-to-date with the latest developments from LevelBlue.
Spam Classifications	Allows you to classify spam based on the confidence rating of the identification. Apply different policy to different types of Spam. Explicit spam, made up of offensive spam and other items identified with high confidence, can be managed separately from suspect spam. Spam Classifications dramatically reduce the cost and inconvenience of managing spam. End users can manage suspect spam using the Spam Quarantine Management Website (see below).
Spam Customization	Allows you to create customized and fine-tuned filtering for spam criteria. Block spam according to keywords, IP range, domain name, foreign character sets, and even number of recipients.

Copyright © 2026 Trustwave Holdings, Inc.

Table 4: Anti spam features

Feature	Description
Blocked Spam Report	Can deliver a summarized email digest notification to individual users. Provides summary information on quarantined spam for a specified period. Users can link directly from the Blocked Spam Report to the SQM system.
Spam Quarantine Management (SQM)	Allows users to manage quarantined spam with an easy-to-use Web interface. Users can delete or release suspected spam from quarantine, manage personal lists of safe and blocked senders, specify email aliases for consolidated management, and delegate rights to others to manage these functions. With the SQM system, potential false positive messages are not lost or deleted.
Delegate Administration of Spam	Allows users to assign spam quarantine management to another user. For example, an executive could assign spam management to a personal assistant.
Anti-Spam Personalization	Allows users to customize anti-spam preferences by defining lists of safe and blocked email senders. If a message is falsely classified as spam, users can release it and add the sender to their personal safe list to be excluded from future spam analysis. Users can also add persistent spammer email addresses into a personal block list.
Anti-Relaying	Prevents spammers from using company email servers as relay hosts, a practice which effectively hides the spammer and frames the company. MailMarshal secures email servers against relaying by default. MailMarshal also allows for relaying exceptions to provide legitimate users the ability to relay through the company email server.
Reputation Service Support	Allows you to use the Marshal IP Reputation Service and third-party, fee-based reputation services such as Spamcop and Spam Haus. These services provide real-time listings of known spam sources as an added defense against spam.
Spam Reporting	Provides comprehensive and meaningful reporting on all aspects of email activity including spam. MailMarshal can show what proportion of incoming email is spam, categorize spam activity by classification, detail messages managed by end users, and provide an ROI savings estimate.
Blended Threat Checking	Provides a real-time check of URLs in email bodies for malicious behavior when the URL is clicked, using a cloud service.
Suspect URL Checking	Provides a check of URLs in email bodies when the message is evaluated by MailMarshal, using a cloud service that uses a frequently updated list of suspect URLs.
Deep Image Analysis	Scans images based on visual features using a neural network. Detects many different categories of images with high reliability and low false positive rate. Commonly used categories are pornography and QR code images.

Copyright © 2026 Trustwave Holdings, Inc.

4.2 Anti-Virus

MailMarshal can provide virus scanning at the email gateway using one or more third party scanning products.

Table 5: Anti-virus features

Feature	Description
Email Anti-Virus Scanning at the Gateway	Allows integration with a wide range of antivirus products to provide real-time antivirus scanning of messages at the email gateway. Blocks infected messages at the gateway and prevents them from entering the network. This method is more secure and logical than server-based virus scanning alone. MailMarshal supports multiple antivirus products from vendors such as Bitdefender, McAfee, and Sophos so you can choose the virus scanners you want to use.
Use Multiple Scanners Simultaneously	Allows use of multiple antivirus products together for comprehensive gateway antivirus protection. Running multiple scanners increases the chances of detecting viruses and reduces the vulnerabilities from delays in patch updates.
Anti-Virus Keyword and Code Command Scanning	Provides detection of suspected viruses based on keywords or code commands. MailMarshal can proactively block viruses based on known keywords or other characteristics. MailMarshal can also identify common code commands embedded in scripted viruses, not common in legitimate business email.
Anti-Virus Blocking by Attachment Type	Allows proactive blocking of potentially dangerous or malicious files by file type, such as SCR and EXE. MailMarshal identifies files by their inherent structure and does not trust the file name or file extension which is often falsified.
Unpack Archive File Types	Provides unpacking of archive and compound file types such as ZIP files and Microsoft Office documents, which may contain embedded viruses or other prohibited content.
Block Encrypted or Password Protected Files	Identifies and manages files that cannot be virus scanned, such as encrypted or password protected files. Ensures that all email and files entering the network are successfully scanned for viruses.
Virus Management Options	Supports a range of virus management rules that allow greater options when reporting and notifying of viruses. Logs specific virus names for reporting, and allows custom management of password protected or corrupted files.
Anti-Virus Reporting	Provides comprehensive and meaningful reporting on all aspects of email activity, including virus incidents. MailMarshal can show what proportion of emails contained viruses, provide a breakdown of top virus incidents and virus names, and even provide a Return on Investment savings estimate.

Copyright © 2026 Trustwave Holdings, Inc.

4.3 Lexical Analysis

MailMarshal can scan text within email messages and attachments using an advanced lexical analysis engine.

Table 6: Lexical analysis features

Feature	Description
TextCensor	Provides an advanced lexical analysis engine. TextCensor places key words into the context of phrases, other keywords, and the meaning of the entire document. TextCensor is intuitive and easy-to-use. TextCensor allows for Boolean and proximity operators and weighted scoring. MailMarshal supplies a full complement of default TextCensor scripts for profanity, harmful code commands, and other common uses.
Scan Text in Email Header, Subject Line, Message Body and Attachments	Allows you to scan any component of an email message including the header, the subject line, the body text and text inside attachments such as Word and PDF documents. You can select one or all of these message components for text analysis.
Logical Operators (Boolean Searching)	Supports the use of logical search operators such as “AND” or “NOT”. Relational expressions assist in reducing false triggers.
Proximity Operators	Supports the use of search operators such as “NEAR”, “PRECEDEDBY”, or “FOLLOWEDBY”.
Weighted Text Scoring	Supports increased or decreased relevance of a key word based on repetition and other key words.
Wildcards and Special Character Matching	Allows matching based on partial words and symbols, such as HTML tags.
TextCensor Script Testing	Allows you to test new scripts against real content before deploying live.

4.4 Attachment Blocking

MailMarshal can block files based on attachments.

Table 7: Attachment blocking features

Feature	Description
Policy-Based Management of Attachments	Allows you to manage email attachments based on the requirements of your organization’s Acceptable Use Policy. Define groups of users authorized to receive specific file types or sizes. MailMarshal can take a variety of actions on attachments, including rejecting, stripping, deleting, copying, forwarding, and quarantining for user review.
Block by File Type	Identifies more than 175 distinct file types by their inherent structure. MailMarshal does not rely on the file name or file extension and is therefore much harder to circumvent.
Block by Size	Determines the size of a message and each attachment. Allows you to set policies for groups for various attachment sizes.

Copyright © 2026 Trustwave Holdings, Inc.

Table 7: Attachment blocking features

Feature	Description
Block by Number of Attachments	Allows you to set policy based on multiple attachments. For instance, block joke emails containing multiple JPG image attachments.
Strip Attachments	Provides the option to remove undesirable or prohibited file attachments while allowing the message text to be passed through to the user. Optionally allow users to release the original email message, including the original attachment(s), on their own authority.
Fingerprinting	Allows MailMarshal to recognize specific files such as company logos. You can specify exceptions to policy for those particular files.
Recursive File Unpacking	Allows unpacking of nested archives to a configurable depth (20 levels by default).
Detects Embedded Files in Office and PDF Documents	Prevents users from circumventing policy by placing files inside Office documents, such as PowerPoint and Word files, or Adobe Acrobat PDF files.

4.5 Automation and Time Saving

MailMarshal provides a number of features to automate tasks and save time.

Table 8: Automation and time saving features

Feature	Description
Message Stamps	Allows you to append legal disclaimers or corporate signatures to outgoing emails, set different stamps by department or user, and schedule message stamps with a start and expiry date. Includes a message stamp editor so you can easily customize message stamps.
Automatic Notifications (Message Templates)	Provides customized warning notifications when messages are blocked. Different notifications can be sent to different recipients. Notifications can contain specific variable details for the message in question, such as the sender, subject line, and reason the message was blocked.
Email Auto-Responders	Allows you to respond to messages based on common text sent to specific email addresses. Use this feature to reduce administration overhead and increase service levels to customers.
Automated Self-Service Message Release Notifications	Provides users the ability to release messages from quarantine simply by replying to a notification. Enhances convenience and saves time.
Insert Notification Variables or Attachments	Allows you to insert variable information specific to the message being processed. Provides the ability to customize notifications, and send messages, logs, or other files as attachments.
Run External Third Party Utilities	Allows you to run batch or executables from a command line. Use this feature to extend the functionality of MailMarshal, automate processes, and save time and money.

Copyright © 2026 Trustwave Holdings, Inc.

4.6 User Group Management

MailMarshal allows you to apply email policy selectively by grouping users. You can import users and groups from a directory server.

Table 9: User group management features

Feature	Description
User Groups	Allows you to define user matching criteria in MailMarshal rules. Create MailMarshal groups and import information from Azure Entra, Active Directory and LDAP servers. Establish groups around departments such as Marketing and Accounts, offices, teams, or any other logical group.
LDAP Support	Allows for the retrieval of user group information from industry standard directory servers such as Exchange, Lotus Notes, or Netscape. LDAP support saves significant administration time by streamlining the MailMarshal setup process and automating the process of updating user group information.
Azure Entra Support	Provides a direct link to cloud hosted Entra groups. MailMarshal can maintain these user groups automatically. This feature is particularly useful for customers hosting mailboxes in the Microsoft 365 environment. Entra intergration saves significant time and effort in creating, maintaining, and updating user information.
Active Directory Support	Provides a direct link into AD user groups. MailMarshal can maintain these user groups automatically. AD integration saves significant time and effort in creating, maintaining, and updating user information.
IP Groups	Allows you to define user matching criteria in MailMarshal rules based on the sender IP. Populate groups with CIDR specifications, ranges, and individual IP addresses.

4.7 Administration

MailMarshal provides a number of intuitively designed interfaces that allow full control of its many powerful features.

Table 10: Administration features

Feature	Description
MailMarshal Management Console (Configuration section)	Provides the policy creation and management center of MailMarshal. Within this section you can customize “Policy Elements” such as Message Stamps, TextCensor Scripts, LDAP connections, and User Groups. These policy elements are then combined into policies using the Policy Creation Wizard.
MailMarshal Management Console (Management section)	Provides the day-to-day MailMarshal administration center. Within the Console you can view up-to-the-minute details on server status and services, logging information, message processing, rejected messages, and performance counters. You can also perform extensive searching of message archives and quarantined messages.

Copyright © 2026 Trustwave Holdings, Inc.

Table 10: Administration features

Feature	Description
Dashboard	Provides details of MailMarshal email filtering at a glance. Located within the MailMarshal Management Console, the Dashboard displays summary data on MailMarshal message processing, inappropriate content, messages quarantined, and refused connections.
Status	Providers details of MailMarshal server health at a glance. The Status page includes information on licensing, automatic updates, processing service status, and processing server health.
Quarantine Folders	Provides the structure where MailMarshal stores blocked or copied messages. You can create folders with special settings for message archiving, end user management, and delayed message delivery. You can customize user access and security settings on each folder.
Email Archive Searching	Allows you to search the quarantine folders. Customize a search using a wide range of criteria including message name, sender, recipient, size, classification, subject, time, date, and much more. Locating particular messages or groups of similar messages is easy and efficient.
Delegated Administration	Allows you to delegate administrative tasks. For instance, you can give help desk staff limited power to monitor server health and release messages for all users. You can also give a manager or supervisor full power to review messages for their department or team.
Commit Scheduling	Allows you to defer the application of changes to a scheduled time relative to the processing server's timezone. Changes can be made in office hours and applied out of hours.
Change Review	Changes made in the Management Console website can be reviewed in detail before being committed for processing. You can alter any change before it is committed.
Auditability	Changes in configuration and user accounts are logged to Audit History. You can search for changes and see the responsible user and the set of changes made at the same time.
REST API	Allows you to integrate Console management functions and some configuration functions with an external application.
Syslog Integration	Allows you to send message handling records (quarantine, delivery, release, and content) to a Syslog server such as LevelBlue SIEM for correlation and central monitoring.

Copyright © 2026 Trustwave Holdings, Inc.

4.8 Usability

MailMarshal is designed from the ground up to be easy to use.

Table 11: Usability features

Feature	Description
Policy Creation Wizard	Provides a plain English interface that guides you through the process of creating an email policy. Rules are laid out in simple, clear English and include a description field so you can document the intent and function of a rule for future reference.
Extensive Online Help	Provides a comprehensive and searchable documentation archive, including suggestions and tips on how to get the most out of MailMarshal.
Dynamic Rule Changes 'On-The-Fly'	Allows you to activate new rules and configuration changes with no server restarts or disruption to services. MailMarshal applies changes seamlessly to the next received message.
Wildcard Support	Allows quick entry of patterns and ranges for user matching, local domain entry, TextCensor scripts, reporting, and searching. Category Scripts and header rewriting functions support more comprehensive regular expression syntax.
Intuitive Configuration	Provides convenience and saves time with simple touches. For instance, the product automatically populates email address domain information when you create multiple email addresses. MailMarshal also lets you create new email policy elements, such as folders, as you create policy.

4.9 Policy

MailMarshal allows you to set up customized policies in support of your organization's Acceptable Use Policy for email usage.

Table 12: Policy features

Feature	Description
End User Quarantine Management	Allows users to manage their own blocked email through an intuitive and easy-to-use Web interface. The primary use of this feature is to manage blocked spam for false positives. However, you can use this feature to allow users to manage whatever messages your policy permits.
Message Parking	Allows you to prioritize business email by parking high-bandwidth, bulk email for off-peak delivery. This feature ensures that priority business email is not delayed by bulk messages during peak times.
Scheduled Rules	Allows scheduled activation and expiry of rules. Schedule application of a message stamp or embargo on particular content.
Printable Policy Configuration	Allows you to print your policy configuration in plain English for policy audits. Allows administrators to easily understand the configured policy.

Copyright © 2026 Trustwave Holdings, Inc.

Table 12: Policy features

Feature	Description
Evaluation and Policy Testing	Provides the ability to employ rules that log information about email for later reporting but take no other actions. This function is useful for testing rules in a “what if” scenario before going live or to investigate email habits of your organization to proactively identify areas of concern.
Go-To Rules	Allow you to skip portions of the email policy based on a rule result. For instance, specify that an oversized message should not be parked if the previous rule detected the presence of the key word “URGENT” in the subject line. MailMarshal can apply very complex polices under specific conditions and circumstances.
DMARC Enabled	Allows you to participate in the DMARC (Domain Message Authentication Reporting & Conformance) validation system based on SPF and DKIM checks.
SMTP TLS reporrting	Provides reporting on potential problems with TLS connections using the standard described in RFC-8460.

4.10 Security and Deployment

You can deploy MailMarshal in a variety of scenarios to provide secure management of email for any size environment.

Table 13: Security and deployment features

Feature	Description
Gateway Security	Provides a checkpoint through which all inbound or outbound email must pass. This is the most logical and appropriate strategic location to deploy an email content security solution to enforce corporate Acceptable Use Policy.
DMZ Deployment Option	Provides a higher degree of network protection by adding an additional layer of security over the trusted environment. An array of MailMarshal servers deployed in the DMZ can be connected through a single firewall port for added security.
Array Manager/Enterprise Deployment	Delivers a management platform to handle the requirements of even the largest enterprise organizations. Administrators can define policy, apply changes, and manage quarantined items from hundreds of email processing servers through a centralized management console. MailMarshal can be deployed across geographically separated arrays and management applied over low-speed links. MailMarshal is also fault tolerant. Array servers can be temporarily disconnected from the central MailMarshal database and policy management servers without affecting message processing or losing any reporting/logging data.

Copyright © 2026 Trustwave Holdings, Inc.

Table 13: Security and deployment features

Feature	Description
ESMTP Supported Connection Policy Rules	Allows MailMarshal to take action based on the initial packets of data transmitted when a connection is established. MailMarshal can reject messages from denied senders or oversized messages by simply dropping the connection. This ability saves time and bandwidth as the message is rejected before the body is sent.
DKIM Validation and Signing	Allows MailMarshal to validate incoming messages using the DomainKeys Identified Mail standard (DKIM), and to sign outgoing messages. DKIM allows the recipient of a message to check for message tampering and validate the integrity of the message.
ARC validation and signing	Allows MailMarshal to validate incoming messages based on information in the ARC-SEAL header (if present), and to extend the ARC chain. ARC (Authentication Received Chain) is a standard that preserves a record of authentication results from each server that processed a message.
Folder Permissions	Allows folder access and management functions to be assigned to users or groups. This function provides the ability to delegate limited email management powers to various users.
Strict RFC Compliance	Ensures strict compliance with the SMTP email standards RFC 2821 and RFC 2822. Corrupted, non-compliant, or malformed messages are not permitted to enter the trusted network and exploit weaknesses on internal mail servers. MailMarshal allows you to relax the rigidity of certain aspects of the RFC enforcement if your organization requires it.
Header Rewriting	Allows MailMarshal to mask confidential network details, such as internal IP addresses and server names, which can be harvested maliciously to exploit weaknesses in an organization's network.
Transport Layer Security (TLS)	Provides transmission of email over a secure tunnel. Allows rule-based validation of remote server certificates for inbound connections. Supports Perfect Forward Secrecy (PFS) for enhanced security.
MTA-STS	Provides validation of recipient servers to the MTA-STS standard (Mail Transfer Agent Strict Transport Security).
DANE	Provides validation of recipient servers to the DANE standard (Domain-based Authentication of Named Entities).
User-Based Routing	Allows the MailMarshal gateway to direct messages to specific internal servers based on the user name.
Single Sign On with Multi-Factor Authentication	Allows integration of MailMarshal Management Console logins with a centralized security repository such as Entra ID, using SAML SSO. Provides MFA ability for Console logins.

Copyright © 2026 Trustwave Holdings, Inc.

4.11 POP3 Email

MailMarshal supports the POP3 protocol for both maintaining local POP3 mailboxes and collecting incoming email, providing flexibility for smaller organizations.

Table 14: POP3 email features

Feature	Description
Standalone POP3 Email Server	Provides a self-contained POP3 email server to offer a cost-effective email system for the small business as well as a useful tool in test environments.
Dial-up Support	Allows scheduled connections to the Internet for small or remote installations.
POP3 Collection	Provides the ability to collect incoming messages from an ISP through a multi-POP mailbox. Applies MailMarshal rules and delivers email to POP3 mailboxes or relays email to your internal email server for delivery.

4.12 Archiving

MailMarshal can archive and log email for later retrieval, re-sending, or analysis.

Table 15: Archiving features

Feature	Description
Email Archiving and Logging	Reports on historical activity and lets you retrieve archived messages. Also helps you analyze email traffic and plan for growth. Archives can serve as a backup for lost email and to preserve email for industry or legal compliance.
Multiple Archive Folders	Allows you to sort inbound and outbound email or sort based on source or destination domains.
Searchable Archives	Provides an advanced message search facility to make finding messages as easy as possible. You can use a wide range of search options including date, time, sender, recipient, subject line, policy classification, and much more.
Low Disk Checking	Allows graceful recovery if the disk containing archived email or processing logs is full.
Operational Logging	Provides detailed information on message processing to allow tracing and aid in troubleshooting.

Copyright © 2026 Trustwave Holdings, Inc.

4.13 Reporting

MailMarshal provides detailed reporting on email traffic and email filtering activity.

Table 16: Reporting features

Feature	Description
Marshal Reporting Console	Provides a web-based interface for reporting on MailMarshal, ECM, and WebMarshal activity. Allows scheduled generation and delivery of reports. Included in licensing for all MailMarshal trial users and customers (installed separately).
Email Activity Reporting	Provides detailed, customizable reporting on all aspects of email activity providing management meaningful insight into email use and policy compliance. Also provides drill-down accessibility from summaries to individual user activity. Saves or emails reports. Provides broad coverage, from individual user behavior to bandwidth usage, spam information, virus reports, policy breaches, and ROI.
SQL Server or SQL Express	Logs reporting data to Microsoft SQL Server or SQL Express database.
Schedule Reports	Allows you to produce reports periodically.
Export Reports	Sends reports in dynamic HTML, Microsoft Word, comma separated values (CSV), and other available formats.
Email Reports	Allows you to email reports directly to individuals or distribution lists.
Billing	Calculates the cost of email traffic by user group for billing purposes.

4.14 Performance

MailMarshal is one of the fastest and most robust email content security products available.

Table 17: Performance features

Feature	Description
Native 64-bit architecture	Takes advantage of the additional memory and processing enhancements available on current Windows systems using 64-bit code.
Modest System Requirements	Operates on readily available hardware with low speed and capacity requirements. A 1000-user site may require only a 2GHz Pentium 4 server with 20GB available disk space, and 1GB of RAM.
Scalable Distributed Architecture	Allows for expansion by using modular architecture. MailMarshal can handle more email by adding more email processing servers with minimal reconfiguration. With third party load-balancing software, MailMarshal can provide redundancy and performance improvement.
Cost-effective Cloud Installation	Integrates with Azure SQL Server for cost-effective performance of medium-sized installations on Azure.

Copyright © 2026 Trustwave Holdings, Inc.

Table 17: Performance features

Feature	Description
Performance Monitors	Provides graphical performance charts showing key performance data for each MailMarshal component using Windows Performance Monitor software so counts and charts can be easily combined with other metrics.

Copyright © 2026 Trustwave Holdings, Inc.

5 Key Benefits at a Glance

MailMarshal SMTP is an email gateway security solution for organizations. It unifies email threat protection, content security, policy enforcement and data loss prevention into a single highly scalable, flexible and easy to manage enterprise solution.

5.1 Secures your email gateway against all threats

MailMarshal SMTP restores the real business value in email by making it safe and efficient to use. MailMarshal protects against all email threats including blocking spam, phishing, email compromise fraud, blended threat attacks, viruses, Trojans, worms, denial-of-service attacks, directory harvesting attacks and spoofed messages.

5.2 Delivers rapid Return on Investment

Comprehensive and meaningful management reports highlight anti-spam and security effectiveness as well as identifying attempted policy breaches; this enables system administrators to demonstrate a rapid return on investment.

5.3 Provides low Total Cost of Ownership

Easy deployment, minimal administration overhead, consolidation of all email security functions into a single management interface along with Zero-Day security updates and detailed but clear reporting are all part of what makes MailMarshal the ultimate email security solution.

5.4 Enables you to fulfill a range of compliance obligations and Data Loss Prevention policies

MailMarshal SMTP enables organizations to place restrictions on who can send confidential information via email, what data can be sent and ensures that sensitive communications are secured against prying eyes. MailMarshal also provides context-sensitive email archiving such as archiving all messages on a related topic or all email exchanges with specific domains. MailMarshal allows you to deliver message handling information to a Syslog server for correlation and central storage.

5.5 Provides unrivaled legal liability protection

Inappropriate or offensive content is filtered out of incoming email and outgoing email is automatically checked for policy compliance. MailMarshal allows enterprises to show that all reasonable measures to protect employees and fairly enforce policies have been put in place.

Copyright © 2026 Trustwave Holdings, Inc.

5.6 Improves network efficiency and saves costs

By controlling bandwidth consumption MailMarshal maintains consistent and reliable network performance and prevents excessive non-business email use. When installed in the Azure cloud, MailMarshal can significantly reduce bandwidth usage inbound to the corporate network by filtering spam in the cloud.

5.7 Improves employee productivity

Enforcing email acceptable use policies means that employees spend less time managing spam, sending personal email or on other time-wasting, non-business activities.

5.8 Safeguards business reputation

MailMarshal SMTP upholds organizational acceptable use standards. It prevents the unauthorized distribution of confidential or sensitive information via email and ensures that users are not in a position to embarrass your organization through defamation or inappropriate email use

5.9 Creates a safer working environment for employees

Through consistent and thorough application of security and acceptable use policies, the risk from issues such as harassment is reduced and controlled.

Copyright © 2026 Trustwave Holdings, Inc.

About LevelBlue

LevelBlue reduces risk and builds lasting resilience so organizations can innovate and advance their mission with confidence. As the world's most analyst-recognized and largest pure-play managed security services provider, LevelBlue elevates client outcomes that matter: stronger defense, faster response, and sustained business continuity. LevelBlue combines AI-powered security operations, advanced threat intelligence, and elite human expertise to provide the most comprehensive portfolio of strategic advisory, managed security, offensive security, and incident response services.