



Trustwave SEG Evaluation Guide

Legal Notice

Copyright © 2017 Trustwave Holdings, Inc.

All rights reserved. This document is protected by copyright and any distribution, reproduction, copying, or decompilation is strictly prohibited without the prior written consent of Trustwave. No part of this document may be reproduced in any form or by any means without the prior written authorization of Trustwave. While every precaution has been taken in the preparation of this document, Trustwave assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

While the authors have used their best efforts in preparing this document, they make no representation or warranties with respect to the accuracy or completeness of the contents of this document and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Neither the author nor Trustwave shall be liable for any loss of profit or any commercial damages, including but not limited to direct, indirect, special, incidental, consequential, or other damages.

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

www.trustwave.com/support/

Trademarks

Trustwave and the Trustwave logo are trademarks of Trustwave. Such trademarks shall not be used, copied, or disseminated in any manner without the prior written permission of Trustwave.

Formatting Conventions

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




Format and Symbols	Meaning
<u>Blue Underline</u>	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>Code</code>	Text in this format indicates computer code or information at a command line.
<i>Italics</i>	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 software in an unintended manner.

Table of Contents

Legal Notice.	ii
Formatting Conventions	iii
List of Tables	vii
List of Figures	viii
1 Introduction	9
1.1 What Is Trustwave Secure Email Gateway?	9
1.2 What Does Trustwave SEG Provide?	10
1.3 How Trustwave SEG Helps You	11
1.3.1 Filters Email at the Gateway	11
1.3.2 Delivers Layered Spam Protection	11
1.3.3 Protects Against Existing and Emerging Threats	11
1.3.4 Provides Unparalleled Performance	12
1.3.5 Includes Easy-to-Use Interfaces	12
1.4 How Trustwave SEG Works	12
1.4.1 Understanding What Trustwave SEG Does	12
1.4.2 Configuring Trustwave SEG	14
1.4.3 Monitoring and Reporting	14
1.5 Trustwave SEG and Trustwave ECM	14
2 Installing Trustwave SEG	15
2.1 Hardware and Software Requirements	15
2.2 Installing Prerequisite Software	16
2.3 Understanding the Trustwave SEG Evaluation Installation	18
2.4 Installing Trustwave SEG	18
2.5 Running the Configuration Wizard	19
2.6 Configuring Anti-Spam Settings	21
2.6.1 Spam Configuration and Rules	22
2.6.2 Configuring SpamCensor SpamProfiler, and YAE Updates	23
2.6.2.1 Configuring and Checking Automatic SpamCensor Updates	23
2.6.2.2 Configuring Proxy Settings for Updates	24
2.7 Configuring Anti-Virus and Anti-Malware Protection	24
2.7.1 Excluding Trustwave SEG Working Folders from AV Scanning	24
2.7.2 Default Anti-Malware Rules	25
2.7.3 Configuring Trustwave SEG to Use an Antivirus Product	26
2.7.4 Enabling Virus Scanning Rules	27
2.8 Configuring Trustwave SEG to Accept Test Email	28

2.9 Installing Trustwave SEG Web Components	29
2.10 What to Do Next	30
3 Guided Tour	31
3.1 Trustwave SEG Configurator	31
3.1.1 Server and Array Configuration.	32
3.1.1.1 Configuring Trustwave SEG	33
3.1.1.2 Configuring Individual Server Properties	36
3.1.2 Exploring Email Policy.	37
3.1.3 Policy Elements.	39
3.2 Configuring Spam Management	41
3.3 Configuring Folder Properties	42
3.4 Generating Sample Email Activity.	43
3.5 Trustwave SEG Console.	44
3.5.1 Trustwave SEG Console.	45
3.5.2 Trustwave SEG Web Console	46
3.6 Spam Quarantine Management Website	47
3.6.1 Adding an Email Address for Spam Quarantine Management	49
3.7 Reviewing Blocked Email	49
4 Product Features	50
4.1 Anti-Spam and Anti-Malware	50
4.2 Anti-Virus.	52
4.3 Lexical Analysis.	53
4.4 Attachment Blocking	53
4.5 Automation and Time Saving	54
4.6 User Group Management	55
4.7 Administration	55
4.8 Usability.	56
4.9 Policy.	57
4.10 Security and Deployment	58
4.11 POP3 Email.	59
4.12 Archiving	59
4.13 Reporting.	59
4.14 Performance	60
5 Key Benefits at a Glance	61
5.1 Secures your email gateway against all threats	61
5.2 Delivers rapid Return on Investment.	61
5.3 Provides low Total Cost of Ownership	61
5.4 Enables you to fulfill a range of compliance obligations and Data Loss Prevention policies . . .	61
5.5 Provides unrivalled legal liability protection.	61
5.6 Improves network efficiency and saves costs	61

5.7 Improves employee productivity 62

5.8 Safeguards business reputation 62

5.9 Creates a safer working environment for employees 62

List of Tables

Table 1:	Trustwave SEG component functions	13
Table 2:	Prerequisites for evaluation installation	15
Table 3:	Test email content and results	44
Table 4:	Anti spam features	50
Table 5:	Anti-virus features	52
Table 6:	Lexical analysis features	53
Table 7:	Attachment blocking features	53
Table 8:	Automation and time saving features	54
Table 9:	User group management features	55
Table 10:	Administration features	55
Table 11:	Usability features	56
Table 12:	Policy features	57
Table 13:	Security and deployment features	58
Table 14:	POP3 email features	59
Table 15:	Archiving features	59
Table 16:	Reporting features	59
Table 17:	Performance features	60

List of Figures

Figure 1:	Enabling Rules	27
Figure 2:	Spam Quarantine Management configuration page	30
Figure 3:	Trustwave SEG Configurator	31
Figure 4:	Trustwave SEG Configurator Servers	33
Figure 5:	Trustwave SEG Properties	34
Figure 6:	Server (Node) properties window	36
Figure 7:	Trustwave SEG Email Policy	38
Figure 8:	Rule Wizard (Rule Actions window)	39
Figure 9:	Trustwave SEG Policy Elements (Folder pane)	40
Figure 10:	Trustwave SEG Console Dashboard	45
Figure 11:	Trustwave SEG Console Folders view	46
Figure 12:	Trustwave SEG Web Console	47
Figure 13:	Spam Quarantine Management website	48

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 Trustwave Secure Email Gateway?

Trustwave Secure Email Gateway 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.

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

Key elements of the Trustwave SEG 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 and reporting**, to assist in authenticating that mail is sent from its purported source.
- **URLCensor**, to reject email based on blacklisted URLs embedded in messages.

- **URL checking** for suspect URLs using a real-time lookup against a database maintained by Trustwave.
- **TextCensor**, to analyze and filter inbound and outbound messages based on language content.

Trustwave SEG can be used with any internal company email system, including Microsoft Exchange, Novell GroupWise, Lotus Domino, Sendmail, and Linux email servers. Trustwave SEG 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. Trustwave SEG 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 Trustwave SEG Provide?

As a gateway content security solution, Trustwave SEG protects your network and your organization. Trustwave SEG 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, Trustwave SEG is by far the most powerful, feature rich email content security solution available.

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

- Attempted message delivery from a blacklisted server
- 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 blacklisted URLs in header, message, or attachment

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

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

Configurator

For email security administrators to configure the product and establish email policy.

Console

For email administrators and helpdesk personnel to monitor and control product activity. Also available as a Web based application.

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 Trustwave SEG 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.

Using Trustwave SEG, 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

Trustwave SEG analyzes email content and attachments entering your network to deliver a greater than 97% spam detection rate with less than 0.001% false positives. Trustwave SEG 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, Trustwave SEG helps ensure network availability for business purposes.

1.3.2 Delivers Layered Spam Protection

Trustwave SEG 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, Trustwave SEG responds to these emails with the actions you define to help enforce your email Acceptable Use Policy.

1.3.3 Protects Against Existing and Emerging Threats

Trustwave SEG 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 Trustwave Labs team continually updates threat detection algorithms to detect new forms of spam, mass mailing worms, and phishing

scams. Trustwave SEG can automatically download these updates to keep your protection levels current. The Trustwave 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, Trustwave SEG provides exceptional performance, operating up to four times faster than other spam-detection products. Trustwave SEG is a fully native 64-bit application for optimized performance with modern hardware or virtual environments. Scalable configurations allow Trustwave SEG 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 Trustwave SEG in geographically separate locations from a central console.

1.3.5 Includes Easy-to-Use Interfaces

Trustwave SEG is easy to evaluate, install, and use. Default settings provide excellent anti-spam performance “out of the box.” The Configurator provides an intuitive interface that allows policy administrators to refine the rules Trustwave SEG uses to evaluate and reject or deliver email. The Console allows email administrators to monitor product effectiveness using a local client or a Web-based interface. 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 Trustwave SEG solution.

1.4 How Trustwave SEG Works

Trustwave SEG 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.

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

Trustwave SEG provides a number of user interfaces, including the Configurator, Console, Web console, Spam Quarantine Management site, and optional Marshal Reporting Console. The Configurator lets security policy administrators set email policy for the entire organization from a central console. You can install additional user interfaces on other computers throughout the network as needed.

1.4.1 Understanding What Trustwave SEG Does

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

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

Table 1: Trustwave SEG component functions

Receiver Functions	Engine Functions	Sender Functions
<ul style="list-style-type: none"> • Inbound TLS • SMTP Authentication • Blocked Hosts • Relaying Tables • DoS Protection • DHA Protection • Reputation Services (DNS Blacklists) • Global Header Rewriting • Connection Policy • SPF Evaluation • SpamProfiler rejection 	<ul style="list-style-type: none"> • Content Analysis Policy • Malware Scanning • SpamBotCensor • SpamProfiler and SpamCensor quarantining • SpamCensor advanced usage (spam types) • NDRCensor • Suspect URL Check • Blended Threats URL Rewriting • Message Archiving • Route Message To Host • Message Parking • DKIM Signing 	<ul style="list-style-type: none"> • Domain Routing Tables • Outbound TLS • SMTP Authentication

All inbound and outbound email enters the Trustwave SEG Server at the Receiver. At this stage, Trustwave SEG 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 Trustwave SEG 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 Trustwave SEG rules by changing the rule order and by changing specific characteristics of the rule.

Trustwave SEG also scans email for viruses using antivirus scanning software. Trustwave SEG supports several scanners with high-throughput interfaces. The product can also use any antivirus scanner that provides a scanning response in the correct format (most antivirus scanners do).

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

- Accepted email is passed to the Trustwave SEG Sender, which then delivers it to the appropriate recipients.
- Modified email may be delivered to recipients with attachments removed.
- Virus-laden email is quarantined, or can optionally be cleaned and delivered.

Trustwave SEG 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 Trustwave SEG

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

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

1.4.3 Monitoring and Reporting

Trustwave SEG provides additional user interfaces for monitoring and daily email administration. The Console features the Dashboard to summarize Trustwave SEG 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.

The administrator can grant other users access to specific Console functions or specific quarantine folders. Using this feature, the administrator can delegate basic tasks to help desk or departmental personnel. Trustwave SEG also offers a Web version of the Console to allow remote access to the Console capabilities.

Email users can review and manage suspected spam and other quarantined email using daily email digests and the Spam Quarantine Management Web-based console. This console is a Web application you can easily deploy on your intranet Web server running Microsoft Internet Information Services (IIS).

Administrators and managers can generate reports on Trustwave SEG activity using the Marshal Reporting Console. Marshal Reporting Console uses SQL Server Reporting Services to produce 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 Trustwave, and is available to all Trustwave SEG customers.

1.5 Trustwave SEG and Trustwave ECM

Trustwave SEG is a gateway solution that applies email content security for email inbound from or outbound to the Internet. Trustwave ECM (formerly known as MailMarshal ECM or MailMarshal Exchange) provides email content security for email sent or received **internally** when you use Microsoft Exchange as your email server. Trustwave ECM lets you scan internal email and apply your internal Acceptable Use Policy.

If you require both internal and external email content security, you can use both products. With adequate computer resources, Trustwave SEG and Trustwave ECM can run on a single computer.

For more information about Trustwave ECM, see the *User Guide* for Trustwave ECM.

2 Installing Trustwave SEG

This chapter provides the information you need to install Trustwave SEG so you can trial the product in a test environment. For the evaluation, you install the prerequisite software, and then install the Trustwave SEG 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 Windows Mail 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 Trustwave SEG 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 Trustwave SEG for evaluation. The computer should not have any Trustwave SEG 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 Trustwave SEG, 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 Trustwave SEG.

Table 2: Prerequisites for evaluation installation

Category	Requirements
Processor	Minimum: Pentium
Disk Space	Minimum: 10GB (NTFS)
Memory	Minimum: 3GB (includes 1GB for operating system, 1 GB for Trustwave SEG, and 1 GB for SQL Express)
Supported Operating System with latest security updates	<ul style="list-style-type: none"> • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012 • Windows Server 2008 R2 with Service Pack 1 • Standard or Enterprise versions • Windows 7 (SP1) • Windows 8 • Windows 10
Network Access	<ul style="list-style-type: none"> • Port 80 (HTTP) and Port 443 (HTTPS) - for SpamCensor and SpamProfiler updates (Proxy usage is supported)

Table 2: Prerequisites for evaluation installation

Category	Requirements
Software	<ul style="list-style-type: none"> Database server: SQL 2016 or SQL 2016 Express, SQL 2014 or SQL 2014 Express, SQL 2012 or SQL 2012 Express, SQL Server 2008 R2 (SP3) or SQL 2008 R2 Express (SP3) Antivirus scanning software (optional but recommended) Microsoft Internet Information Services (Microsoft IIS), if you plan to evaluate the Web components Microsoft .NET Framework 3.5 SP1 Microsoft .NET Framework 4, if you plan to evaluate the Web components or install SQL Server.

2.2 Installing Prerequisite Software

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

To install prerequisites on the Trustwave SEG computer:

1. Log on to the Trustwave SEG 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. *If you plan to evaluate the Trustwave SEG Web components*, ensure that Microsoft .NET Framework 4 is installed on the Trustwave SEG computer. Installation of .NET 4 requires Windows Installer 4.5, and in many cases requires a server restart.
 - If you already have a copy of the full installation package, you can install this item separately.
 - You can also download this item from Trustwave. Start the download from the Prerequisites tab of the Trustwave SEG setup window.
 - Complete the installation, and then rerun the Trustwave SEG distribution package.
4. *If you plan to evaluate the Trustwave SEG Web components*, ensure that Microsoft IIS is installed on the Trustwave SEG computer.
5. *If you plan to use SQL Express to host the Trustwave SEG database:*
If you are installing from the “With SQL Express” version of the Web package, you can install SQL Express 2016 as part of the Basic Install of Trustwave SEG (see “Installing Trustwave SEG” on page 18). To provide additional control of the installation, including instance name and install location,

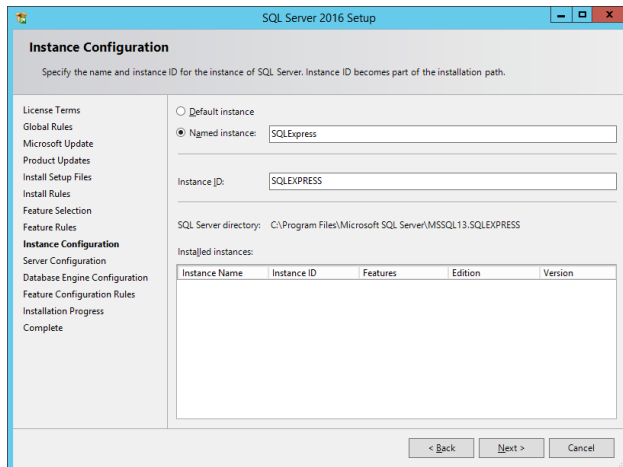


Note: SQL 2016 requires a minimum of Windows Server 2012. If you want to install on an earlier OS version you can obtain SQL Express 2008 R2 from the Database Setup link on the Prerequisites tab of the setup window. The SQL Express installation package will install .NET Framework 4.6.

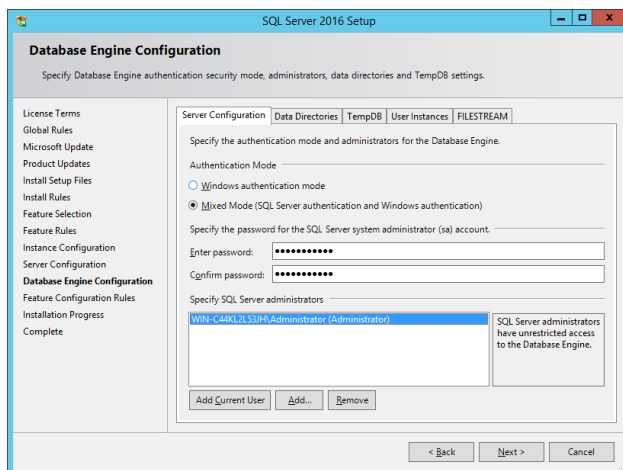
you can install SQL Express 2016 before installing Trustwave SEG, as follows:

- a. On the Trustwave SEG setup window, click the Prerequisites tab.

- b. Click the link to install or download SQL 2016 Express.
- c. The version of the SQL Express 2016 installer that is included in the Trustwave SEG 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).



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



- f. Complete the SQL 2016 Express installation. If necessary then rerun the Trustwave SEG distribution package.
6. *If you plan to use one of the integrated Marshal antivirus solutions:*
 - a. On the Trustwave SEG setup window, click the Scanners tab.
 - b. Click a link to install or download any of the listed software.
 - c. Complete the product installation, and then rerun the Trustwave SEG distribution package.

2.3 Understanding the Trustwave SEG Evaluation Installation

Trustwave SEG 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 Trustwave SEG 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 Trustwave sales representative.

2.4 Installing Trustwave SEG

If you have finished installing all prerequisite software, you are ready to install Trustwave SEG. The trial installation of Trustwave SEG 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 Trustwave SEG 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 Trustwave SEG to relay email through your existing email server. For more information about installing Trustwave SEG in a production setting, see the *User Guide*.

To install Trustwave SEG for evaluation:

1. Log on to the Trustwave SEG computer with an account that has Administrator local permissions.
2. Ensure the Windows Simple Mail Transport Protocol service 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 Trustwave SEG setup program from the product installer package.
4. On the Setup tab, click **Install Trustwave SEG**.
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**.

9. Trustwave SEG attempts to connect to a SQL instance on the local computer using the Windows Local System account, and it creates a database named [TrustwaveSEG](#).



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 Trustwave 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 Trustwave SEG can receive email and apply rules. For more information, see “Running the Configuration Wizard” on page 19.

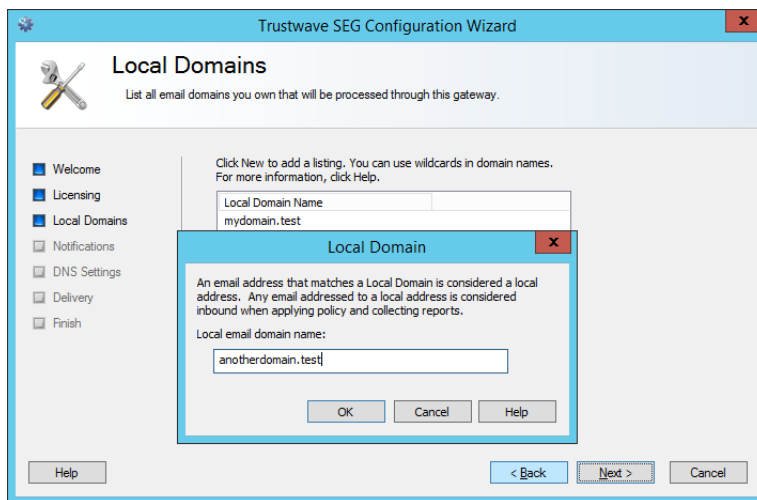
2.5 Running the Configuration Wizard

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

To run the Configuration Wizard:

1. *If the Configuration Wizard is not running*, start the wizard by running Trustwave SEG Configurator from the Trustwave SEG program folder.
2. On the Welcome window, click **Next**.
3. On the License window, type your company or organization name. This information identifies your organization when you request a permanent license for Trustwave SEG. The License window also reports details of your current license. You can supply another license key at a later time. For more information, see the *User Guide*.
4. Click **Next**.
5. On the Local Domains window, click **New** to add a Local Domain. Local domains are the domains of “inbound email” addresses.
 - a. Specify a test email domain name, such as [mydomain.test](#), and then click **OK**.

- b. *If you want to specify additional test domains, click **New** and repeat Step a.*



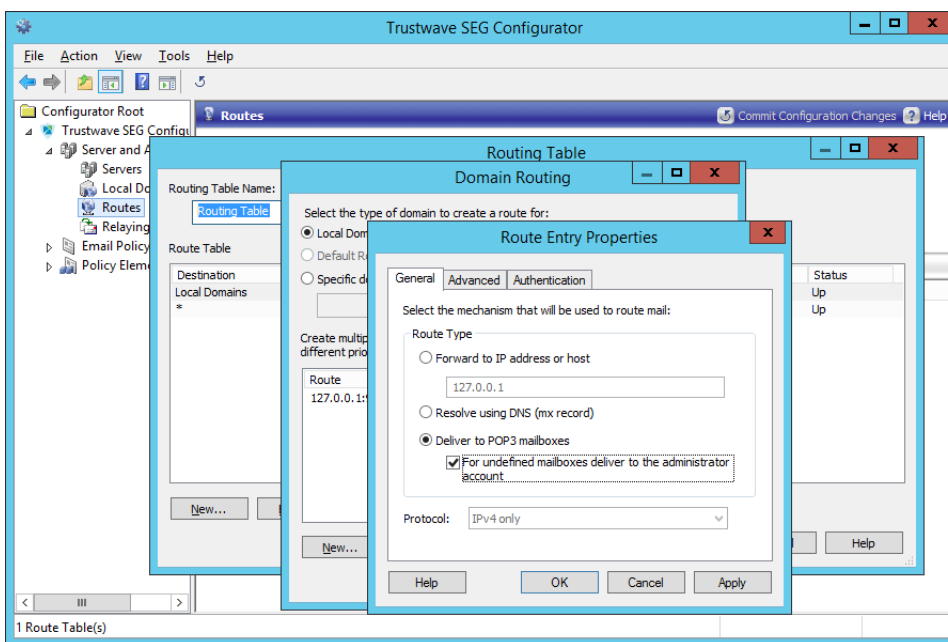
6. When you have included all your test email domains, click **Next**.
7. Accept the default **Recipient Address** to identify where to send administrative notifications, such as Dead Letter reports.
8. Accept the default email address for the **From Address**. Trustwave SEG uses this email address for email notifications to users.
9. Click **Next**.
10. 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, Trustwave SEG automatically enters the DNS servers set in networking properties for the local computer. If other DNS servers are more suitable, change the entries.

11. Click **Next**.
12. On the Delivery window, enter a server name, Fully Qualified Domain Name, IPv4 or IPv6 address where Trustwave SEG 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 Trustwave SEG POP3 for testing, enter 127.0.0.1 or ::1 (this entry will ensure that you can send test messages using Windows Mail on the test server, via IPv4 or IPv6 respectively). You can change the delivery method to POP3 after completing the wizard.*
13. Click **Next** to accept the default to deliver external email using DNS.
14. Review the Completing window, and then click **Finish**. The main Trustwave SEG Configurator window opens.
15. *If you want to use Trustwave SEG POP3:*
 - a. In the left pane of the Configurator expand **Server and Array Configuration** and select 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**.



- d. Click **OK** until you return to the main Configurator window. To apply the change, on the Tools menu, click **Commit Configuration**.

2.6 Configuring Anti-Spam Settings

Stopping unsolicited incoming email (commonly known as spam) is a primary goal for most organizations. Trustwave SEG 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. Trustwave offers regular updates to the Trustwave SEG SpamCensor and SpamBotCensor through the Web by HTTP and HTTPS. The SpamProfiler is a signature based check performed at the Receiver, that allows Trustwave SEG 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, Trustwave SEG enables automatic updates for SpamCensor and SpamProfiler. You can configure update settings on the **Trustwave SEG Properties** window. You can also view current information about your license and last SpamCensor update on the Trustwave SEG Console Dashboard.



Note: To evaluate spam detection, you should ensure that Trustwave SEG updates are succeeding. For more information about configuring updates, see "Configuring SpamCensor SpamProfiler, and YAE Updates" on page 23.

2.6.1 Spam Configuration and Rules

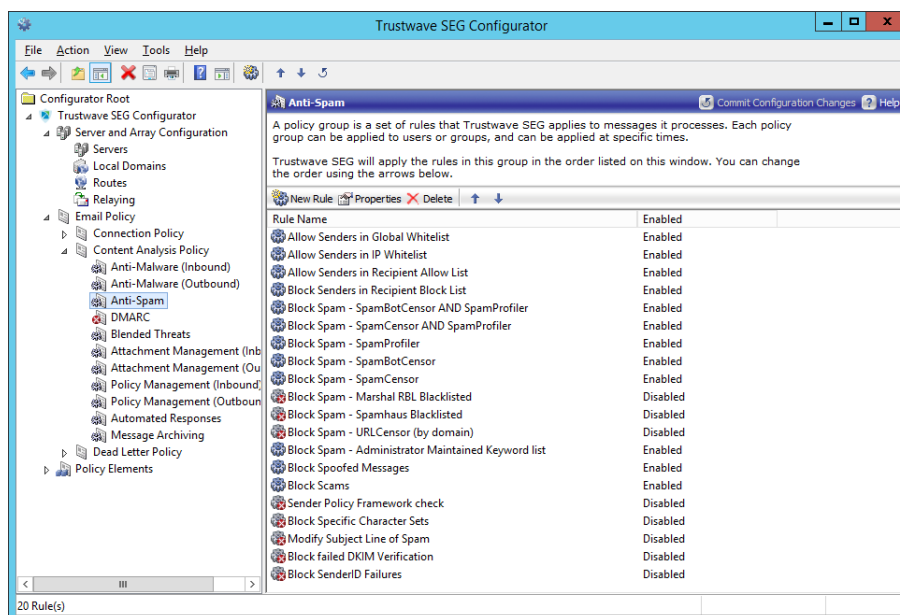
The default email policy provided with Trustwave SEG includes a policy group titled Spam. This policy group includes a number of rules to block spam. Some basic rules are enabled by default. You can enable and/or customize additional rules to suit your requirements.

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

Trustwave SEG also allows you to delegate spam management. For more information about the management options, see “Installing Trustwave SEG Web Components” on page 29 and “Configuring Spam Management” on page 41.

To view the Spam policy group:

1. In the left pane of the Configurator, expand the item **Email Policy > Content Analysis Policy**.
2. Expand the item **Anti-Spam**.



3. View details of each rule, including a description of its intended use, by selecting the rule in the right pane and choosing **Properties** from the toolbar of the MMC or the taskpad.

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 23.

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

- 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 Trustwave SEG Spam Quarantine Management Website.
- A rule to quarantine email messages that contain specific text related to scams, using the Trustwave SEG TextCensor.
- A rule to blacklist senders of spam email that contains URLs in the message header or body. The rule uses the URLCensor function to compare URLs in received messages with blacklists maintained by external blacklist sites. URLCensor decodes URLs intentionally obscured with decimal, octal, or hexadecimal notation. For more information about using URLCensor, see the Trustwave Knowledge Base.



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

2.6.2 Configuring SpamCensor SpamProfiler, and YAE Updates

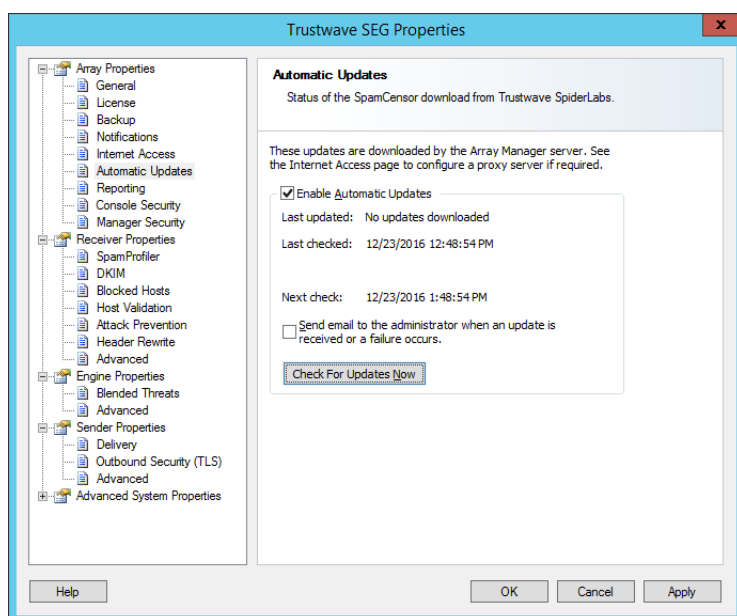
Trustwave provides updates for the SpamCensor, SpamProfiler, and Yara Analysis Engine (YAE) facilities to all trial installations, as well as customers with current Trustwave SEG maintenance contracts. The updates are delivered through the Web by HTTP and HTTPS.

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 Configurator, select **Trustwave SEG Properties** from the Tools menu.
2. Select **Automatic Updates** from the left pane. The display shows the time and result of the last update attempt, and the time of the next attempt.



3. If you do not want the SpamCensor to update automatically, clear the check box **Enable Automatic Updates**.
4. If you want to be notified by email when a SpamCensor update is received, select the check box **Send email to the administrator**. Trustwave SEG sends an email message to the administrator address configured on the Notifications page of Trustwave SEG Properties.
5. 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 Trustwave SEG server(s) do not have direct access to the Web, you can configure Trustwave SEG 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 Configurator, select **Trustwave SEG Properties** from the Tools menu.
2. Select **Internet Access** from the left pane.
3. You can configure the following settings for the Array Manager (SpamCensor updates) and for the processing nodes (SpamProfiler updates).
 - a. If you want Trustwave SEG to access the Web directly, select **Direct Access**.
 - b. If you want Trustwave SEG 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.
4. To apply the proxy settings, click **OK** to go back to Trustwave SEG Properties and then commit Trustwave SEG configuration changes.

2.7 Configuring Anti-Virus and Anti-Malware Protection

After you complete the Configuration wizard, Trustwave SEG starts a number of product services and the Trustwave SEG Configurator.

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

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

2.7.1 Excluding Trustwave SEG Working Folders from AV Scanning

Trustwave SEG 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 or cleans this test file, or if the product denies Trustwave SEG access to the files, the Trustwave SEG Engine Service does not start.

In this case, Trustwave SEG sends an email notice to the administrator. If the check succeeds, Trustwave SEG 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 Trustwave SEG working folders from scanning even if you do not configure the antivirus product to scan Trustwave SEG email.

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

To exclude the Trustwave SEG 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 Trustwave SEG program folder and all subfolders from scanning. If you installed Trustwave SEG in the default folder, exclude the `C:\Program Files\Trustwave\Secure Email Gateway` 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. *If it is not already running*, start the Trustwave SEG Configurator from the Trustwave SEG program group.
7. In the left pane, expand **Trustwave SEG Configurator**.
8. *If the State of the server in the right pane shows any service is not running:*
 - a. In the right pane, select the server.
 - b. In the tool bar, click **Server Properties**.
 - c. Click **Restart All**.
 - d. Click **OK**.
9. In the right pane, verify the server **State** is Running.

2.7.2 Default Anti-Malware Rules

The default email policy provided with Trustwave SEG 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 Trustwave. These functions provide an additional layer of protection that delivers effective and timely results with lower resource usage than traditional scanning.

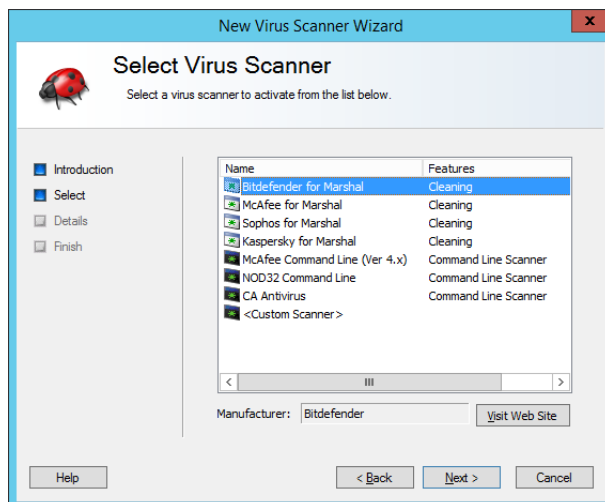
To ensure that the Zero Day functions are active, confirm that SpamCensor and SpamProfiler updating is enabled.

2.7.3 Configuring Trustwave SEG to Use an Antivirus Product

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

To configure virus scanning in Trustwave SEG:

1. Ensure you have installed one or more supported antivirus scanners on the Trustwave SEG computer. You can install several integrated solutions from the links on the Scanners tab of the Trustwave SEG Setup window.
2. If necessary, configure the antivirus product to exclude the Trustwave SEG working folders. The integrated solutions, such as McAfee for Marshal, do not require this configuration. For more information, see “Excluding Trustwave SEG Working Folders from AV Scanning” on page 24.
3. *If it is not already running*, start the Trustwave SEG Configurator from the Trustwave SEG program group.
4. In the left pane, expand **Trustwave SEG Configurator > Policy Elements**, and select **Virus Scanners**.
5. On the Action menu, click **New Virus Scanner**.
6. On the Welcome window, click **Next**.
7. On the Select a Virus Scanner window, select your antivirus scanner from the list.



8. *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`.
9. *If the scanner is installed remotely*, on the Configure Virus Scanner Location window, specify the server name or IP address and port where the scanner can be accessed.
10. *If your scanner is not in the list*, select **Custom Scanner**. Specify the details of your antivirus software, and then click **Next**.
11. On the Completing the New Virus Scanner window, click **Finish** to add the virus scanner.

12. If you plan to use more than one virus scanner, repeat Steps 5 through 11 for each scanner.

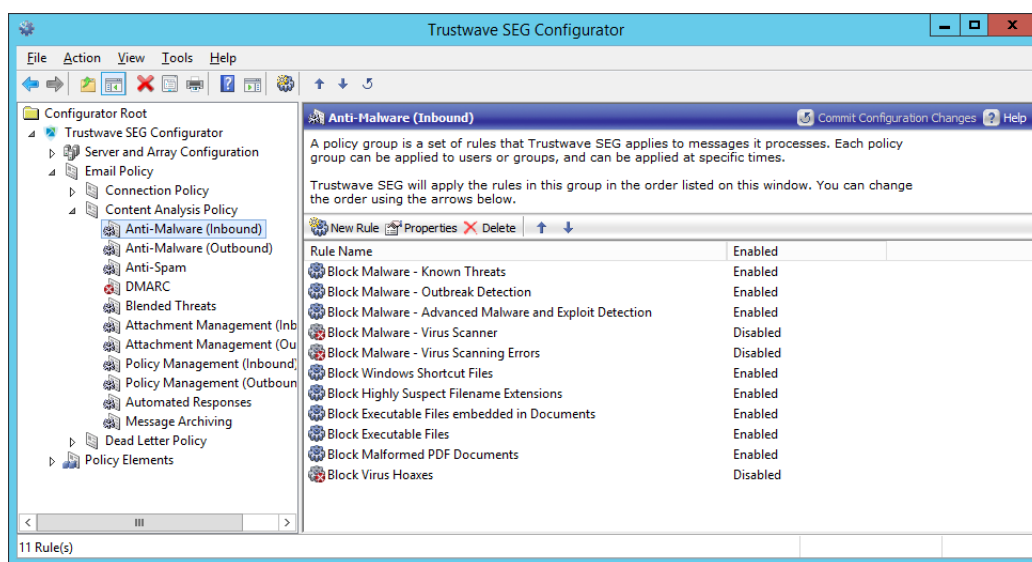
2.7.4 Enabling Virus Scanning Rules

With your antivirus product installed and configured to exclude the Trustwave SEG 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 left pane of the Configurator, expand **Email Policy > Content Analysis Policy** and select **Virus & Threats (Inbound)**.
2. In the right pane, select the virus scanning rules you want to enable. For example, select the **Block Virus** and **Virus Scanning Errors** rules.

Figure 1: Enabling Rules



3. On the Action menu, click **Enable**. You can also right click the rule and click **Enable** on the right-click context menu.
4. In the left pane, select **Virus & Threats (Outbound)**.
5. In the right pane, select the virus scanning rules you want to enable. For example, select **Block Virus** and **Virus Scanning Errors**.
6. On the Action menu, click **Enable**.
7. In the left pane, click **Trustwave SEG Configurator**.
8. On the Action menu, click **Commit Configuration**. You can also click **Commit Configuration** in the task pad tool bar.



Note: Trustwave SEG can also implement virus cleaning with selected scanners. For information about configuring cleaning rules, see Help and the User Guide.

2.8 Configuring Trustwave SEG to Accept Test Email

To evaluate Trustwave SEG, 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 Trustwave SEG interfaces, policies, and reports.

To configure Trustwave SEG to accept and deliver sample email:

1. In the left pane of the Trustwave SEG Configurator, expand **Trustwave SEG Configurator > Policy Elements**, and click **Accounts**.
2. On the Action menu, click **New Account**.
3. Type the account name, such as `User01`, and a password. Trustwave SEG automatically creates SMTP aliases for each local domain (for instance, `User01@mydomain.test`). The value **LocalDomains** is a placeholder for all local aliases.

4. Click **Add**.
5. If you want Trustwave SEG 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 Trustwave SEG sets this to `admin@mydomain.test` or the test domain you specified when you ran the Configuration Wizard.
6. Click **Add**.
7. Click **Close**.
8. In the left pane of the Configurator, expand **Server and Array Properties** and 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 **New** and add the address.
10. Click **OK** until you return to the main Configurator window.
11. On the Anti-Relaying tab, click **OK**.
12. If prompted, on the Tools menu, click **Commit Configuration**.
13. Set up an email account in Windows Mail 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 Trustwave SEG Web Components

Trustwave SEG includes the following Web-based consoles:

- Spam Quarantine Management console to allow email recipients to review and manage their quarantined email
- Web Console to provide email administrators clientless access to the Trustwave SEG Console

You can install the consoles on the Trustwave SEG 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 Trustwave SEG Web components:

1. Run the installer package.
2. On the Setup tab, click **Install Web Components**.
3. Follow the instructions to install **Both** Web components 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 Trustwave SEG program group.

Figure 2: Spam Quarantine Management configuration page

The screenshot shows a web browser window with the address bar displaying 'localhost/SpamConsole/Configuration.aspx'. The page title is 'Trustwave Spam Quarantine Management'. The form contains the following fields and values:

- Website Address:** http://VM-EXAMPLETW45/SpamConsole/
- Server:** vm-exampletw45
- Port Number:** 19001
- Username:** administrator
- Domain:** vm-exampletw45
- Password:** (masked with dots)
- Confirm Password:** (masked with dots)
- Authentication Mode:** Forms
- Administrator Email Address:** admin@example.com

At the bottom of the form are 'Save' and 'Help?' buttons.

6. In the **Server** field, specify the name of the Trustwave SEG 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 Trustwave SEG computer.
9. For authentication mode, select **Windows without AD integration**.
10. Click **Save**. Trustwave SEG records the configuration, and then opens the Spam Quarantine Website to the default view.

You can open either website by using the Start menu items. You can also open the websites from other computers that have access, using the appropriate URL. Access the sites using a recent version of Internet Explorer or Firefox (Chrome is supported for the Spam Quarantine website only).

2.10 What to Do Next

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

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

3 Guided Tour

This chapter guides you through the user interfaces to demonstrate the features and power of Trustwave Secure Email Gateway. The tour includes the following user interfaces:

- Trustwave SEG Configurator
- Spam Quarantine Management console
- Trustwave SEG Console

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 Trustwave Secure Email Gateway to manage your email.

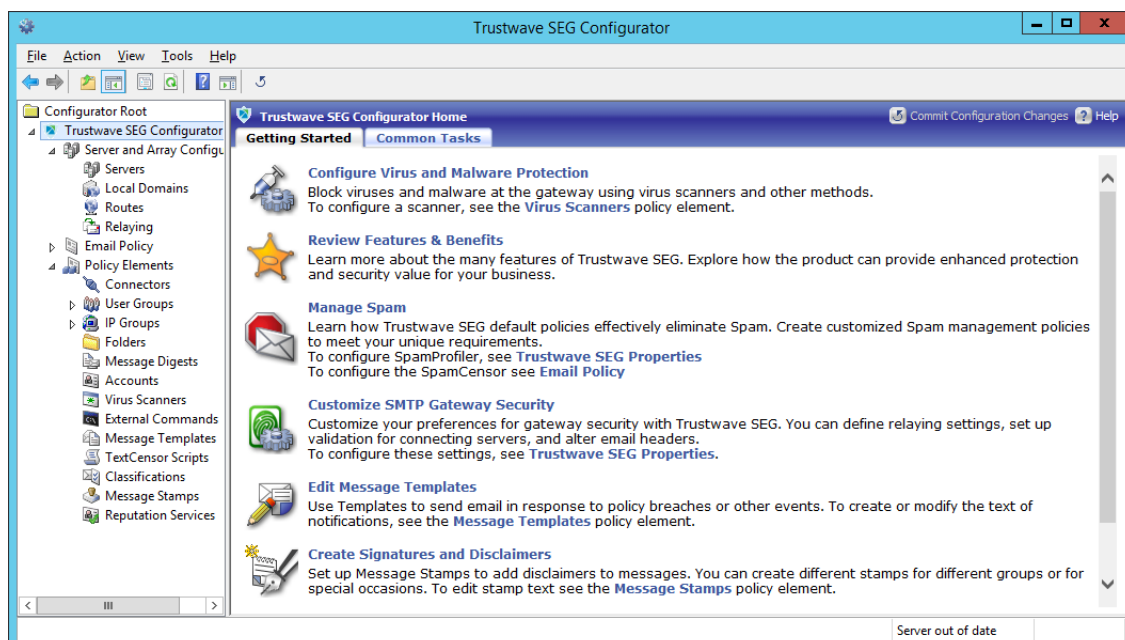
3.1 Trustwave SEG Configurator

The Trustwave SEG Configurator allows product administrators to create and edit email policy, control email delivery settings, and configure the product.

To follow along with this tour, start the Trustwave SEG Configurator from the Trustwave SEG program group or by clicking **Start > Programs > Trustwave SEG > Trustwave SEG Configurator**.

The following figure shows the Trustwave SEG Configurator with all left pane items expanded. To view this page, in the left pane of the Configurator, click **Trustwave SEG Configurator**.

Figure 3: Trustwave SEG Configurator



The Getting Started and Common Tasks tabs in the right pane help you understand many of the features and benefits of the product. These task pads also help you get started using the product and provide shortcuts to performing common tasks with Trustwave SEG.

Items in the left pane let you control Trustwave SEG configuration, define your email policy rules, and define other elements of policy, such as return message templates and Trustwave SEG user groups.

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

Server and Array Configuration

Lets you configure Trustwave SEG 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 Trustwave SEG evaluates and acts on email.

Policy Elements

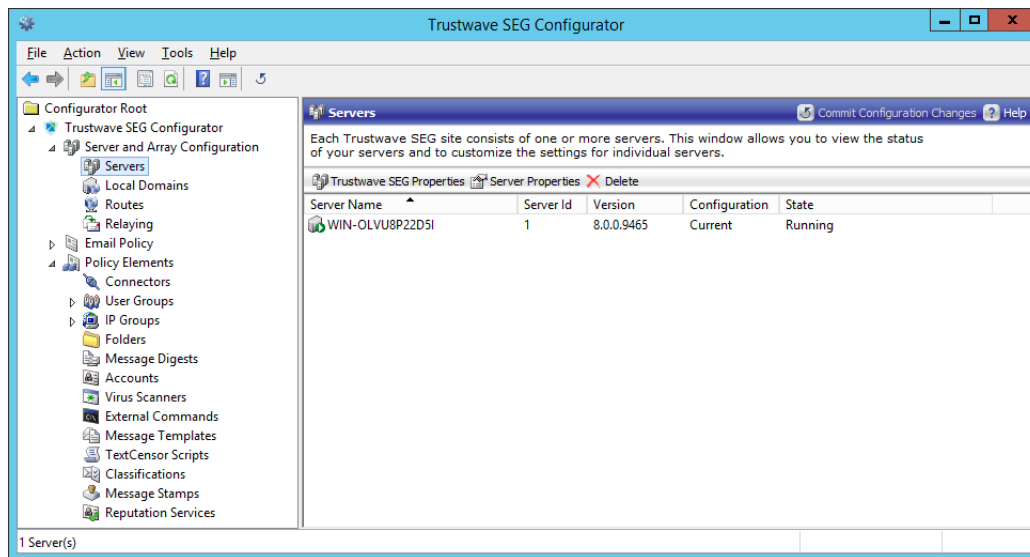
Lets you customize how Trustwave SEG connects to your directory servers and manage Trustwave SEG user groups. Also lets you specify how Trustwave SEG customizes email notifications, message templates, stamps, and classifications.

3.1.1 Server and Array Configuration

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

In the left pane, click **Server and Array Configuration** to quickly check the status of your servers. For evaluation, you should have just one Trustwave SEG Server, similar to Figure 4.

Figure 4: Trustwave SEG Configurator Servers



In the right pane, you can quickly assess the status of each server in the array. In the above example, the red icon on the server indicates a problem. A green icon indicates a running server.

The **Server and Array Configuration** item also lets you access configuration for the Array Manager, the Trustwave SEG Server or array of servers, and when necessary, configure individual server properties.

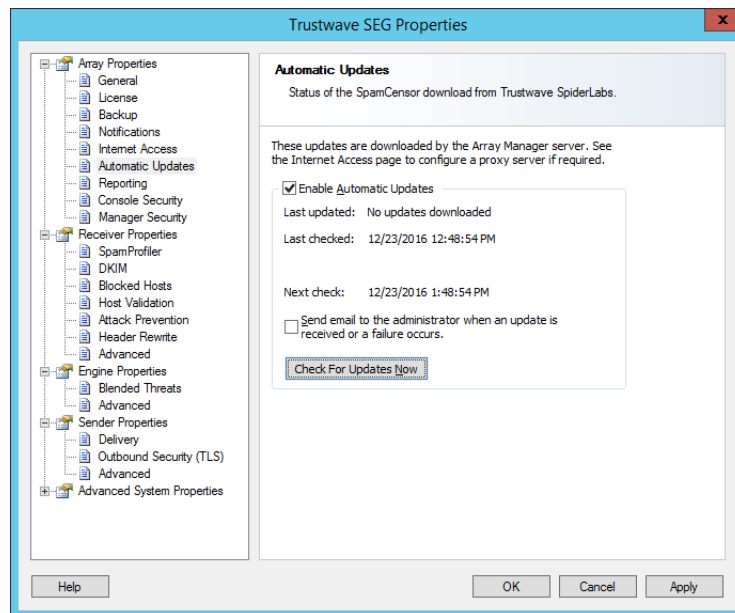
3.1.1.1 Configuring Trustwave SEG

The Trustwave SEG Properties window lets you configure attributes of the array of servers. Trustwave SEG 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 Trustwave SEG Properties window select **Trustwave SEG Properties** on the Tools menu.

Figure 5 shows the Trustwave SEG Properties window.

Figure 5: Trustwave SEG Properties



The Trustwave SEG Properties window lets you configure the following properties:

General

Provides information about the Trustwave SEG 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.

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, define classification groups for Virus and Spam reporting, and specify whether to display the message count for the top quarantine folders on the Dashboard in the Trustwave SEG Console.

Console Security

Lets you set access control permissions for Administrators using the Trustwave SEG Console by specifying Windows user accounts or groups and activities for each Console user. For more information about the Trustwave SEG Console, see "Trustwave SEG Console" on page 44.

Manager Security

Lets you specify the permissions for the Array Manager service account.

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.

SpamProfiler

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

Blocked Hosts

Allows you to maintain a list of servers from which Trustwave SEG will never accept email messages (blacklist).

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).

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.

Delivery

Allows you to configure how Trustwave SEG 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.

Advanced items and Advanced System Properties

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

3.1.1.2 Configuring Individual Server Properties

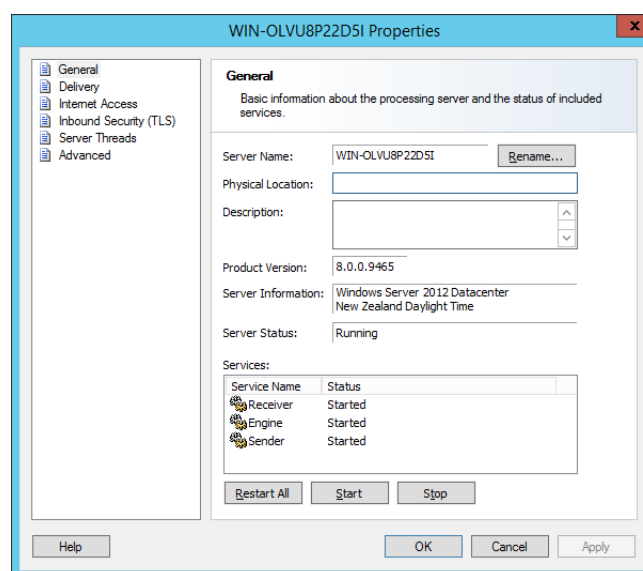
You can use the Trustwave SEG Configurator to configure the settings for an individual server.

To display and configure Trustwave SEG Server properties:

1. In the left pane, expand **Server and Array Configuration** and click **Servers**.
2. In the right pane, select the server you want to configure.
3. On the **Servers** window click the **Server Properties** link in the task pad toolbar.

Trustwave SEG displays a window to let you configure your specific server.

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 Trustwave SEG Server services, including the Receiver, Engine, Sender, and optional POP3 server.

Internet Access

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

Delivery

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

Inbound Security (TLS)

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

Advanced

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

3.1.2 Exploring Email Policy

Email Policy in the Trustwave SEG Configurator defines how the product handles each email it processes.



Note: So that Trustwave SEG 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. An/one with permission to run the Trustwave SEG Configurator 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 Trustwave SEG 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 Trustwave SEG 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 Trustwave SEG should take when an email meets the rule conditions.

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

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

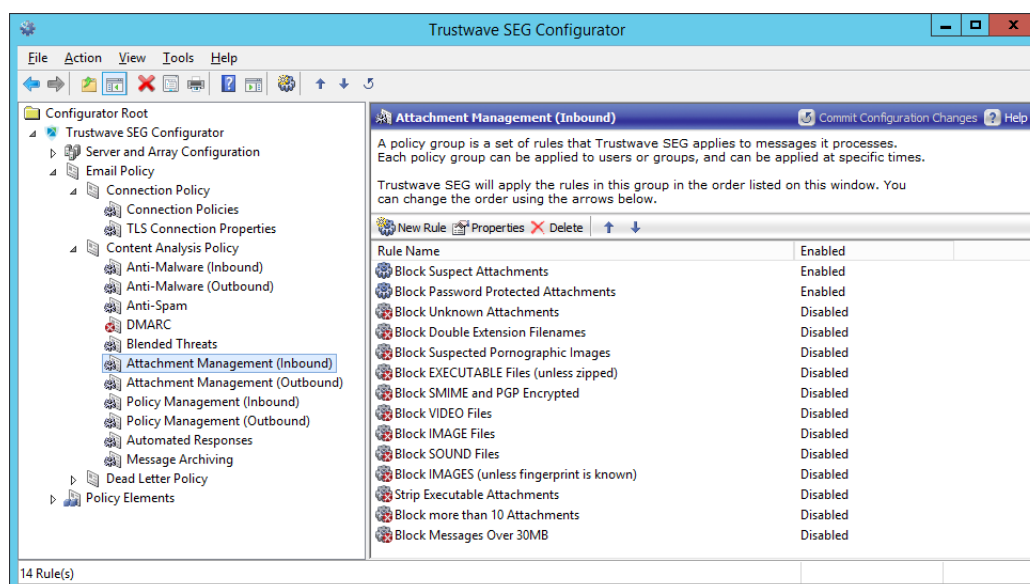
Trustwave SEG rules let you apply policy based on many email features, such as content of subject lines, name of sending host, URLs specified in the message, and many more options.

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

To explore email policy:

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

Figure 7: Trustwave SEG Email Policy

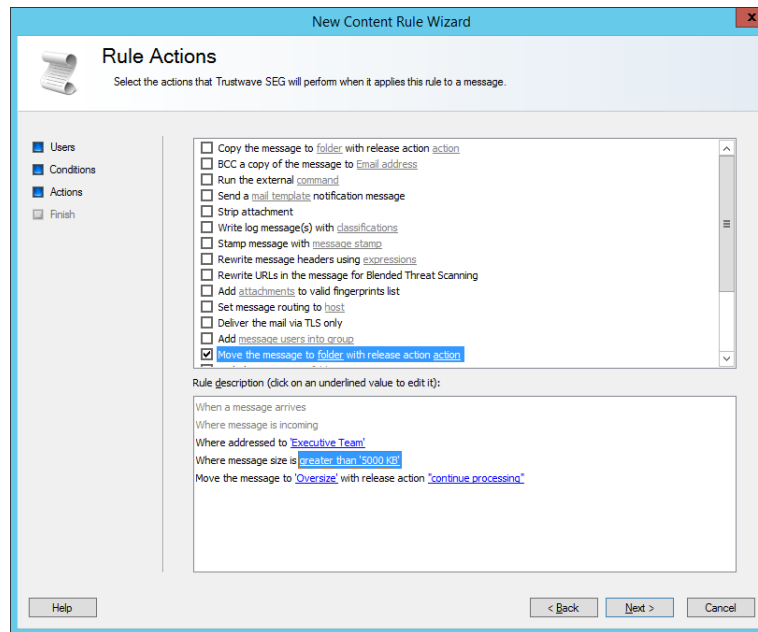


2. In the left pane, select a policy group, such as **Attachment Management (Inbound)**.
3. In the right pane, select a rule, such as **Block EXECUTABLE Files**.
4. Click the Properties icon on the Trustwave SEG Configurator tool bar or click **Properties** in the task pad toolbar.

Trustwave SEG starts the Rule Wizard to help you through the process of creating, reviewing, or modifying a rule. The window displays the rule name, comment, and description.

Links in the description window let you customize the rule and choose the policy conditions you want to enforce. The following figure shows a window in the Rule Wizard. Click a link in the Rule Description box to customize the rule.

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.

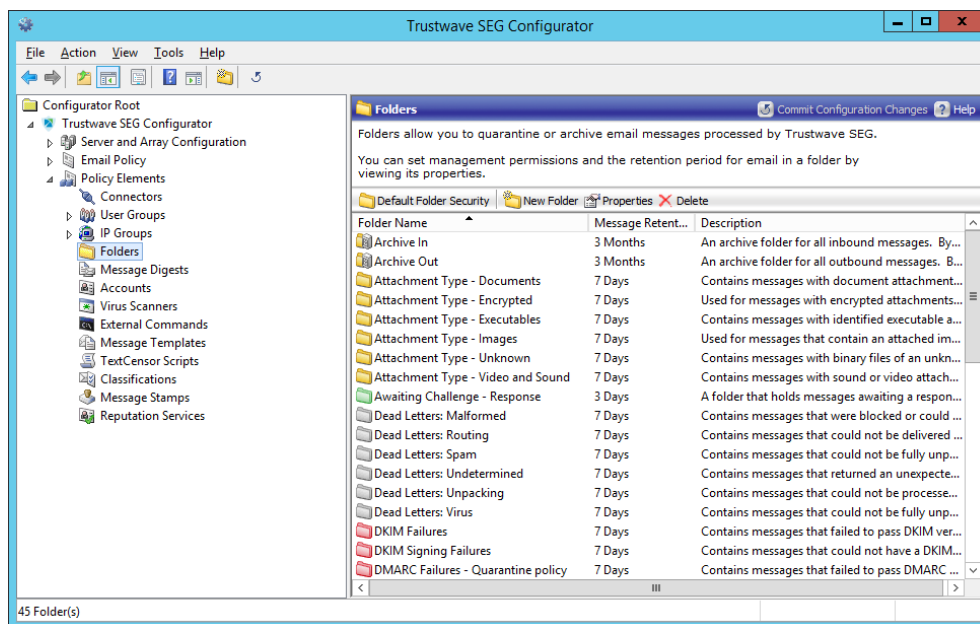
3.1.3 Policy Elements

Trustwave SEG Policy Elements are building blocks you can use when you create Trustwave SEG 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**.

Figure 9: Trustwave SEG 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.

Trustwave SEG provides the following policy elements:

Connectors

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

User Groups

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

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.

Accounts

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

Virus Scanners

Allow you to check email messages for virus content. If your antivirus scanner finds a virus in a message, Trustwave SEG can attempt to clean it.

External Commands

Allow you to extend Trustwave SEG functionality with customized conditions and actions.

Message Templates

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

TextCensor Scripts

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.

Message Classifications

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

Message Stamps

Allow you to add signatures or disclaimers, and to notify email users and administrators about Trustwave SEG actions within an existing 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 Trustwave SEG decide whether to accept a message.

3.2 Configuring Spam Management

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

Trustwave SEG 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 Trustwave SEG Console or Web Console.
- Email recipients who receive a daily summary of their incoming quarantined messages from Trustwave SEG digest emails.

Each email user can have permission to review and release messages quarantined in one or more folders, through the Trustwave SEG Spam Quarantine Management Website. This facility is specifically designed to allow users to review messages that Trustwave SEG 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 (whitelists and blacklists).

3.3 Configuring Folder Properties

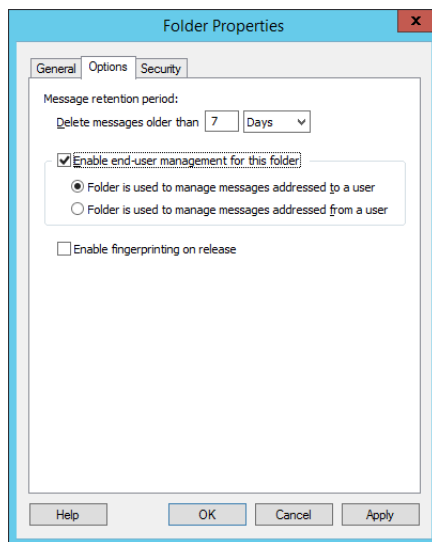
The primary purpose of the Spam Quarantine Management Website is to allow users to review messages that Trustwave SEG has quarantined as Spam. The site can be used to manage one or more folders for this purpose. The site can also be used to manage folders that are used for other purposes.

A folder managed by the Spam Quarantine Management Website can contain either inbound or outbound messages, but not both.

To set up a folder to manage Spam with the Spam Quarantine Management Website:

2. In the Trustwave SEG Configurator, expand **Trustwave SEG Configurator > Policy Elements** and click **Folders**.
3. In the right pane, select the **Suspect** folder.
4. Click **Properties** in the taskpad header. You can also click the Properties icon in the Trustwave SEG Configurator tool bar.

5. On the Options tab, select **Enable end-user management for this folder**.



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

3.4 Generating Sample Email Activity

To see the features of Trustwave SEG in action, you can send sample email through the system using your current email client. For more information, see “Configuring Trustwave SEG to Accept Test Email” on page 28.

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

You can send sample email through your Windows Mail or other POP3 email client to trigger Trustwave SEG rules so you can evaluate the product.

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

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 Windows Mail to send the messages and use the default Trustwave SEG rules without customizing. You can see the actual results by using the Trustwave SEG interfaces as described later in this chapter.

To test Trustwave SEG, 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 Trustwave SEG to Accept Test Email” on page 28.

Table 3: Test email content and results

Email Content	Trustwave SEG Result
Subject: Hello World Body: Hi there	Delivered and logged in Mail History
Subject: Spam 1 Body: viagra online	Quarantined in the Spam folder
Subject: Spam 2 Body: Generic cialis and viagra online http://0.0.0.0	Quarantined in the Spam 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. Trustwave SEG cannot scan password protected files, so it places them in quarantine for manual review.
Subject: make money at home Body: C@sh	If the rule “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 Trustwave SEG examines email, in addition to checking the extension of all file attachments, Trustwave SEG also opens attachments to check the file structure. Trustwave SEG blocks files by examining both the extension and file structure to detect risky attachments, even when a file extension has been changed.

3.5 Trustwave SEG Console

The Trustwave SEG Console is the interface administrators and help desk staff use to monitor Trustwave SEG operation and email flow. The Trustwave SEG Console provides summary information on the current state of Trustwave SEG, as well as administrative access to the quarantine folders and message sending services.

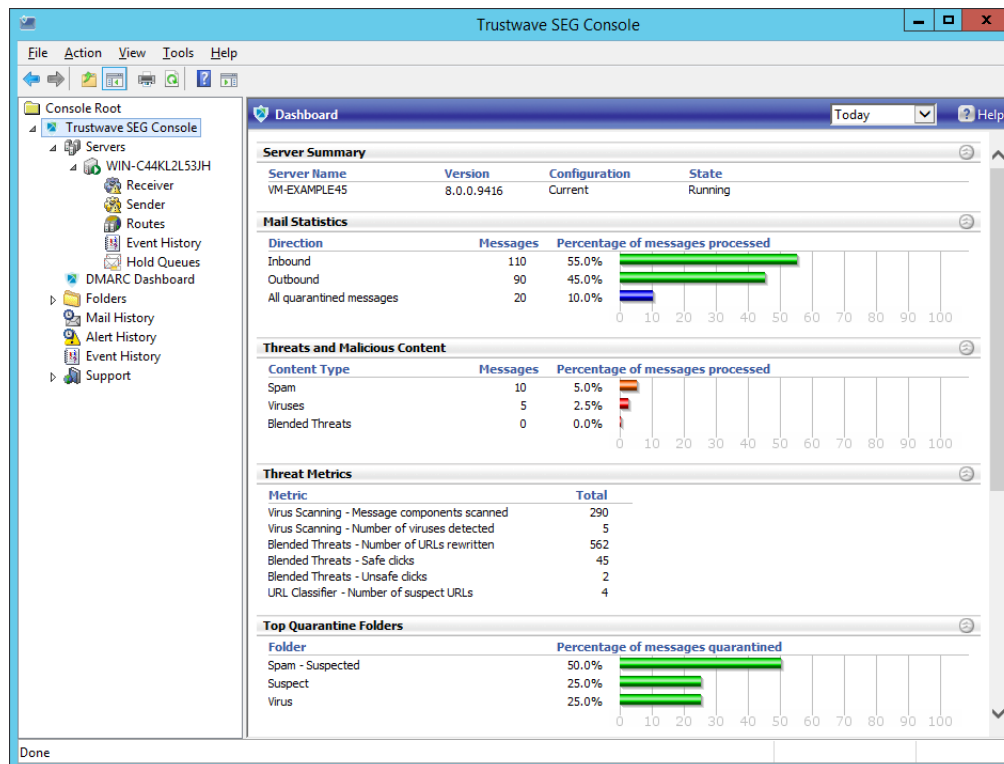
You can install the Trustwave SEG Console on any computer that can connect to the Trustwave SEG Array Manager. The Basic install option installs the Trustwave SEG Console on the same computer as the other Trustwave SEG components.

If you have sent sample email as suggested above, you can see the results of Trustwave SEG rules by running the Trustwave SEG Console.

3.5.1 Trustwave SEG Console

When you select the Trustwave SEG Console item in the left pane, the Console displays the Dashboard page. The Dashboard provides a graphical overview of email traffic and filtering activity for a selectable period.

Figure 10: Trustwave SEG Console Dashboard

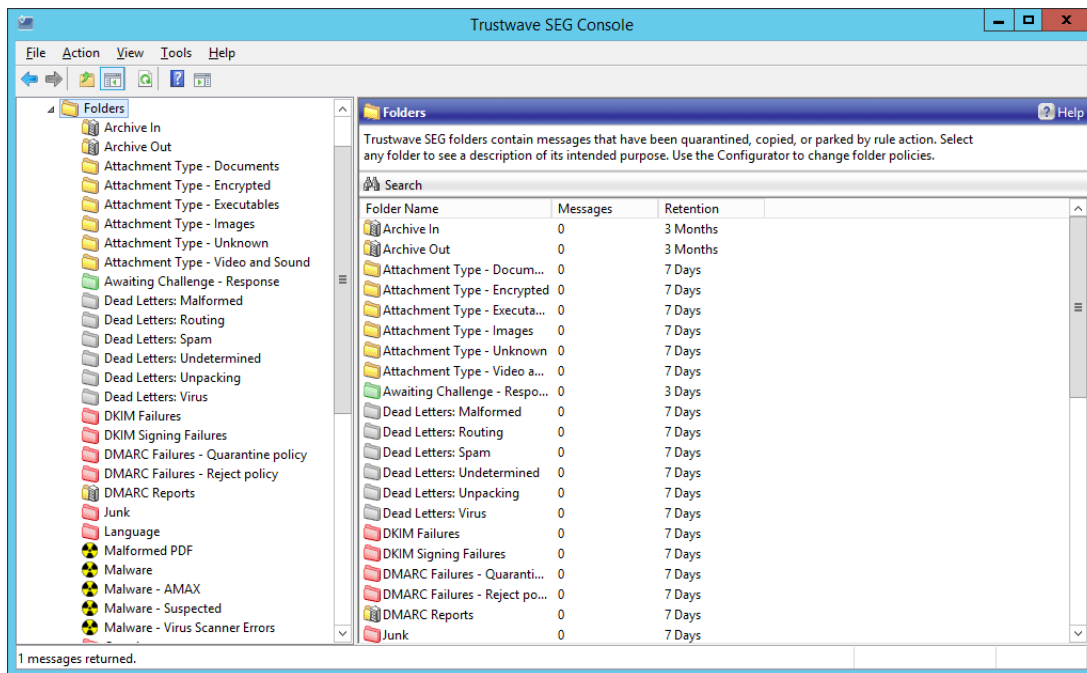


The sections include the following status reports:

- **Server Summary** shows the status of your Trustwave SEG email processing servers
- **Mail Statistics** include totals for inbound and outbound email
- **Threats and Malicious Content** shows blocked spam and viruses
- **Threat Metrics** shows the number of message components scanned for threats and the number of threats found
- **Top Quarantine Folders** shows messages quarantined in various folders
- **Mail Transport Policies** shows connections refused based on global policies applied at the SMTP connection level

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

Figure 11: Trustwave SEG Console Folders view

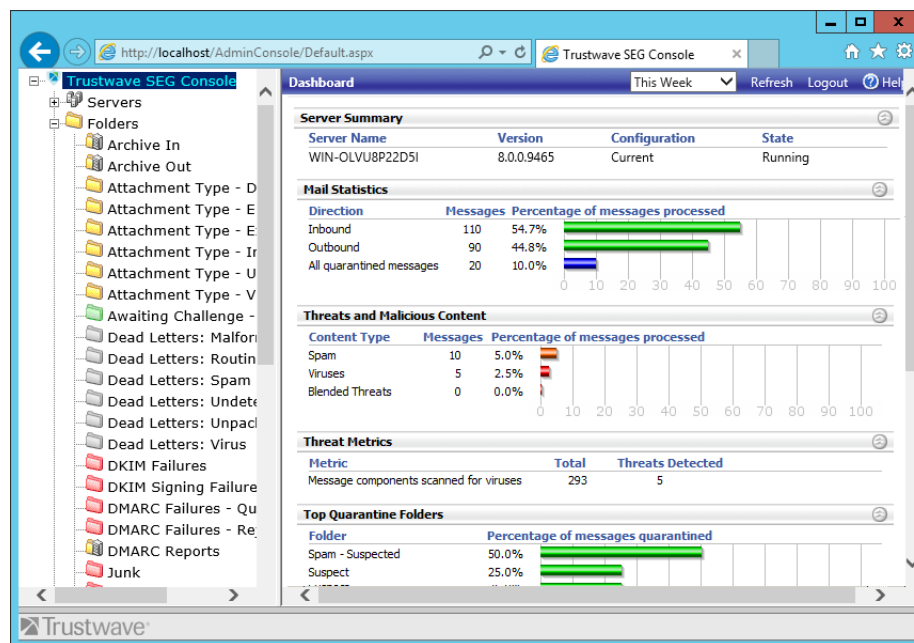


The Mail History item in the left pane allows you to see the result of processing for each message that Trustwave SEG has processed. These results can include delivery, quarantine, and logging classification, among others. You can search for specific messages by address, subject, and time.

3.5.2 Trustwave SEG Web Console

You can access most Trustwave SEG Console features using the Trustwave SEG Web Console. The Web Console installs in a virtual directory under Microsoft IIS. You can access the Web Console from any computer that can browse to the server where you installed the Web Console. Figure 12 shows the Dashboard as displayed in the Web Console.

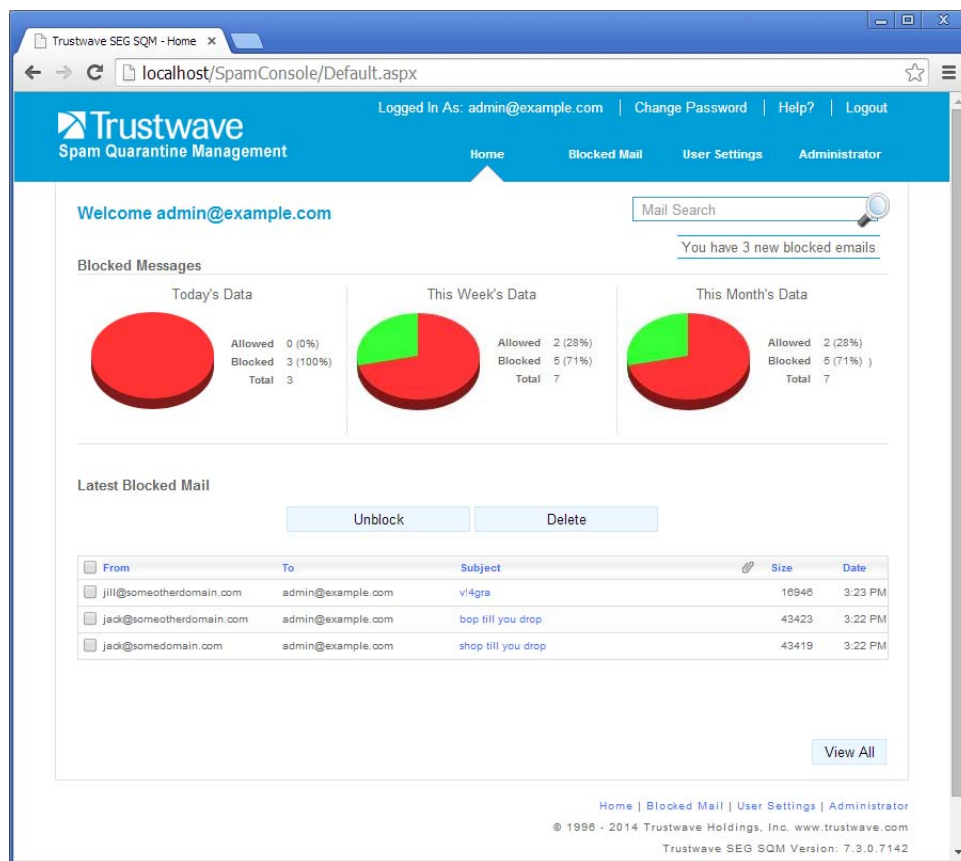
Figure 12: Trustwave SEG Web Console



3.6 Spam Quarantine Management Website

The Trustwave SEG Spam Quarantine Management (SQM) Website allows users to review email that Trustwave Secure Email Gateway 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.

Figure 13: Spam Quarantine Management website



The SQM site offers the following features:

Blocked Mail

Allows users to review email messages addressed to them that Trustwave SEG 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 Trustwave SEG 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 login.

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.

User Settings

Allows users to choose site look and feel options, such as a default language for the site. Trustwave 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 Internet Explorer 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 Trustwave SEG to Accept Test Email” on page 28 and “Configuring Folder Properties” on page 42.

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.

4 Product Features

Use the following feature lists to compare Trustwave Secure Email Gateway with other products for features and performance.

4.1 Anti-Spam and Anti-Malware

Trustwave SEG provides a full set of features and tools to detect and manage spam and malware. After initial installation Trustwave SEG 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. SpamProfiler receives signature updates from Trustwave 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.
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. Trustwave SEG is always up-to-date with the latest developments from Trustwave.
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.
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.

Table 4: Anti spam features

Feature	Description
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. Trustwave SEG secures email servers against relaying by default. Trustwave SEG 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. Trustwave SEG 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 Trustwave SEG, using a cloud service that uses a frequently updated list of suspect URLs.

4.2 Anti-Virus

Trustwave SEG 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. Trustwave SEG supports multiple antivirus products from vendors such as Bitdefender, Kaspersky, 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.
Virus Cleaning	Provides the option of virus cleaning where it is supported by virus scanners. Messages can be automatically disinfected or repaired and cleared through to the intended recipient.
Anti-Virus Keyword and Code Command Scanning	Provides detection of suspected viruses based on keywords or code commands. Trustwave SEG can proactively block viruses based on known keywords or other characteristics. Trustwave SEG 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. Trustwave SEG 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. Trustwave SEG 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.

4.3 Lexical Analysis

Trustwave SEG 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. Trustwave SEG 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", "PRECEDED BY", or "FOLLOWED BY".
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

Trustwave SEG 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. Trustwave SEG 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. Trustwave SEG 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.
Block by Number of Attachments	Allows you to set policy based on multiple attachments. For instance, block joke emails containing multiple JPG image attachments.

Table 7: Attachment blocking features

Feature	Description
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 Trustwave SEG 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

Trustwave SEG 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 Trustwave SEG, automate processes, and save time and money.

4.6 User Group Management

Trustwave SEG 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 Trustwave SEG rules. Create Trustwave SEG groups and import information from 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 Trustwave SEG setup process and automating the process of updating user group information.
Active Directory Support	Provides a direct link into AD user groups. Trustwave SEG can maintain these user groups automatically. As with LDAP support, this feature saves significant time and effort in creating, maintaining, and updating user information.

4.7 Administration

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

Table 10: Administration features

Feature	Description
Trustwave SEG Configurator	Provides the policy creation and management center of Trustwave SEG. Within the Configurator 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. The Configurator uses the familiar Microsoft MMC interface.
Trustwave SEG Console	Provides the day-to-day Trustwave SEG administration center. Within the Console you can view up-to-the-minute details on server status and services, logging information, message processing, and performance counters. You can also perform extensive message archive and quarantine searching. The Console also uses the MMC interface.
Web Console (Remote Management)	Allows you to administer Trustwave SEG remotely through a fully functional Web-based version of the Console.
Dashboard	Provides details of Trustwave SEG activity at a glance. Located within the Trustwave SEG Console, the Dashboard displays summary data on Trustwave SEG servers, services, message processing, inappropriate content, messages quarantined, and refused connections. The Dashboard is your quick and easy reference on how Trustwave SEG is performing and on the health of your email gateway.

Table 10: Administration features

Feature	Description
Getting Started	Highlights Trustwave SEG key features and benefits as well as guiding administrators in the initial setup to ensure Trustwave SEG is configured to deliver the recommended security benefits.
Common Tasks	Highlights quick links to many of the product's most frequently used tools, such as releasing quarantined messages or generating reports.
Quarantine Folders	Provides the structure where Trustwave SEG 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.

4.8 Usability

Trustwave SEG 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. The award winning Policy Creation Wizard is the heart of the product's ease-of-use philosophy. 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.
Drag 'n Drop; Copy 'n Paste	Provides familiar but important ease-of-use functionality with drag 'n drop, copy 'n paste management of rules, users, policy elements, and messages.
Extensive Online Help	Provides a comprehensive and searchable documentation archive, including suggestions and tips on how to get the most out of Trustwave SEG.
Dynamic Rule Changes 'On-The-Fly'	Allows you to activate new rules and configuration changes with no server restarts or disruption to services. Trustwave SEG 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.

Table 11: Usability features

Feature	Description
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. Trustwave SEG also lets you create new email policy elements, such as folders, as you create policy.

4.9 Policy

Trustwave SEG 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 Configurations	Allows you to print your policy configuration in plain English for policy audits. Allows administrators to easily understand the configured policy.
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. Trustwave SEG can apply very complex policies 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.

4.10 Security and Deployment

You can deploy Trustwave SEG 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 Trustwave SEG 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. Trustwave SEG can be deployed across geographically separated arrays and management applied over low-speed links. Trustwave SEG is also fault tolerant. Array servers can be temporarily disconnected from the central Trustwave SEG database and policy management servers without affecting message processing or losing any reporting/logging data.
ESMTP Supported Connection Policy Rules	Allows Trustwave SEG to take action based on the initial packets of data transmitted when a connection is established. Trustwave SEG 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 Trustwave SEG 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.
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. Trustwave SEG allows you to relax the rigidity of certain aspects of the RFC enforcement if your organization requires it.
Header Rewriting	Allows Trustwave SEG 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.
User-Based Routing	Allows the Trustwave SEG gateway to direct messages to specific internal servers based on the user name.

4.11 POP3 Email

Trustwave SEG 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 Trustwave SEG rules and delivers email to POP3 mailboxes or relays email to your internal email server for delivery.

4.12 Archiving

Trustwave SEG 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.

4.13 Reporting

Trustwave SEG 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 Trustwave SEG, Trustwave ECM, and WebMarshal activity. Allows scheduled generation and delivery of reports. Included in licensing for all Trustwave SEG trial users and customers (installed separately).

Table 16: Reporting features

Feature	Description
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.
DMARC Reports	Provides information on DMARC compliance.

4.14 Performance

Trustwave SEG 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. Trustwave SEG can handle more email by adding more email processing servers with minimal reconfiguration. With third party load-balancing software, Trustwave SEG can provide redundancy and performance improvement.
Performance Monitors	Provides graphical performance charts showing key performance data for each Trustwave SEG component using Windows Performance Monitor software so counts and charts can be easily combined with other metrics.

5 Key Benefits at a Glance

Trustwave Secure Email Gateway 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

Trustwave Secure Email Gateway restores the real business value in email by making it safe and efficient to use. Trustwave SEG protects against all email threats including blocking spam, phishing, 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 Trustwave SEG the ultimate email security solution.

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

Trustwave Secure Email Gateway 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. Trustwave SEG also provides context-sensitive email archiving such as archiving all messages on a related topic or all email exchanges with specific domains.

5.5 Provides unrivalled legal liability protection

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

5.6 Improves network efficiency and saves costs

By controlling bandwidth consumption Trustwave SEG maintains consistent and reliable network performance and prevents excessive non-business email use.

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

Trustwave Secure Email Gateway 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.

About Trustwave®

Trustwave helps businesses fight cybercrime, protect data and reduce security risk. With cloud and managed security services, integrated technologies and a team of security experts, ethical hackers and researchers, Trustwave enables businesses to transform the way they manage their information security and compliance programs. More than three million businesses are enrolled in the Trustwave TrustKeeper® cloud platform, through which Trustwave delivers automated, efficient and cost-effective threat, vulnerability and compliance management. Trustwave is headquartered in Chicago, with customers in 96 countries. For more information about Trustwave, visit <https://www.trustwave.com>.