FREQUENTLY ASKED QUESTIONS

Trustwave MailMarshal (SEG) Blended Threat Module

Table of Contents

1 What is a Blended Threat?

A Blended Threat is an attempt to compromise information security that uses multiple vectors. Blended Threat email messages are typically crafted so that they appear to be from a trusted sender. They contain links to a website hosting malicious code, or attempting to entice the user into providing personal information. Blended Threat emails are sometimes targeted to a specific individual or individuals.

2 What is the Blended Threat Module?

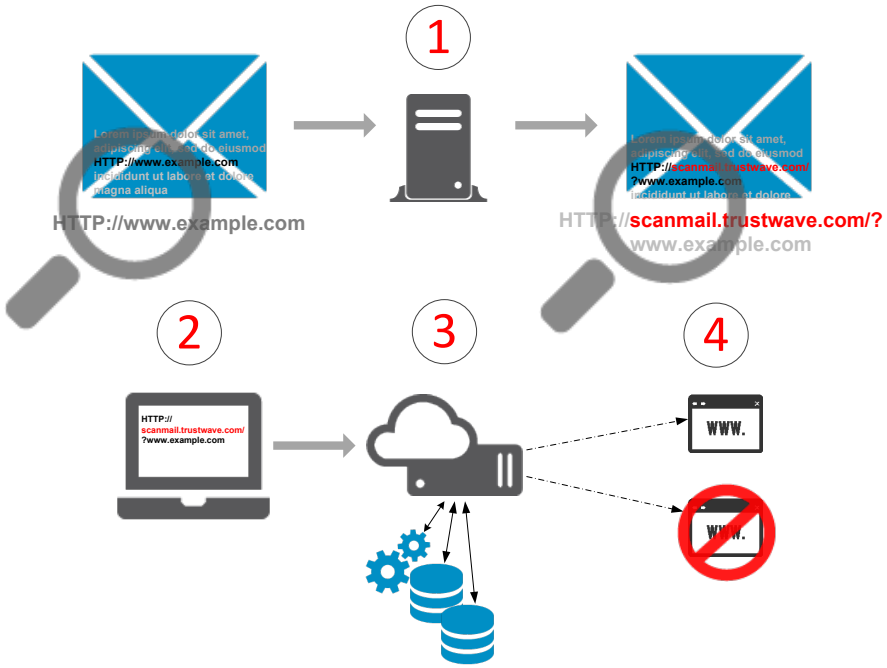
The Trustwave MailMarshal Blended Threat Module uses a number of validation methods, including real-time behavioral analysis and content inspection as well as information from a number of industry standard sources, to identify and block sites that serve suspicious or malicious code.

Because validation is performed in real time by a cloud service when a link is clicked, it provides superior effectiveness in catching and neutralizing new exploits for all users on any device from any location.

3 How Does the BTM Work?

The BTM functions as follows:

1. MailMarshal scans email messages and rewrites URL links before delivering the email.
2. Clicking a link invokes the Trustwave Link Validator cloud service.
3. The Link Validator passes the URL to one or more validation services.
4. Depending on the results of validation, the Link Validator redirects the request to the original site, or blocks the request, as described below.

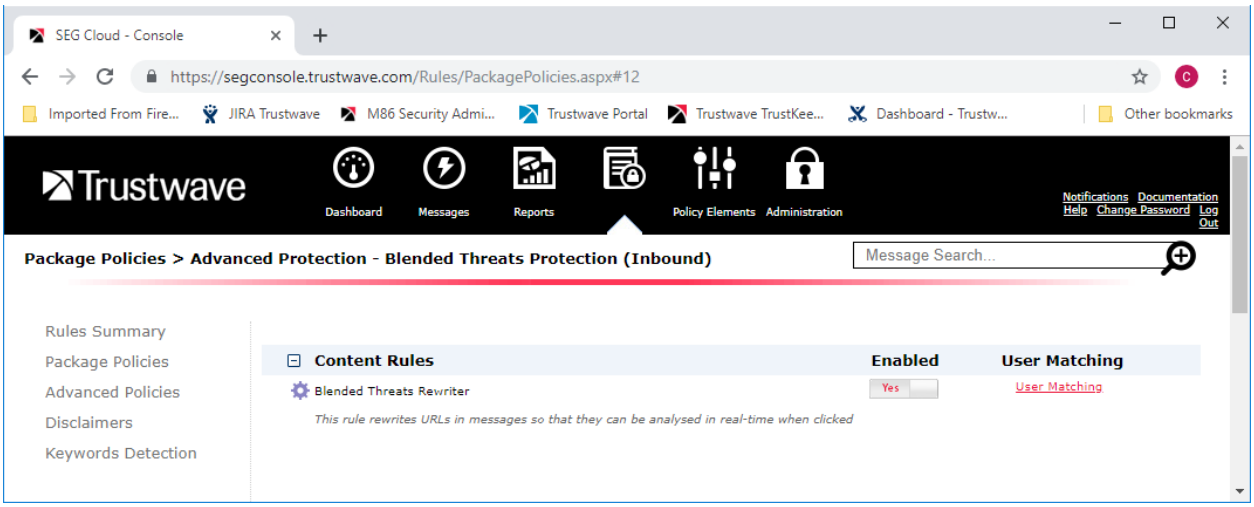


4 How Do I Enable the BTM?

The BTM is implemented as a Rule Action in MailMarshal.

4.1 MailMarshal (SEG) Cloud

Customers who are entitled to the Advanced Protection package see this Package in the Customer Console. The Package contains a single rule, which is enabled by default. The customer can choose to bypass scanning for some users, as described later in this document.

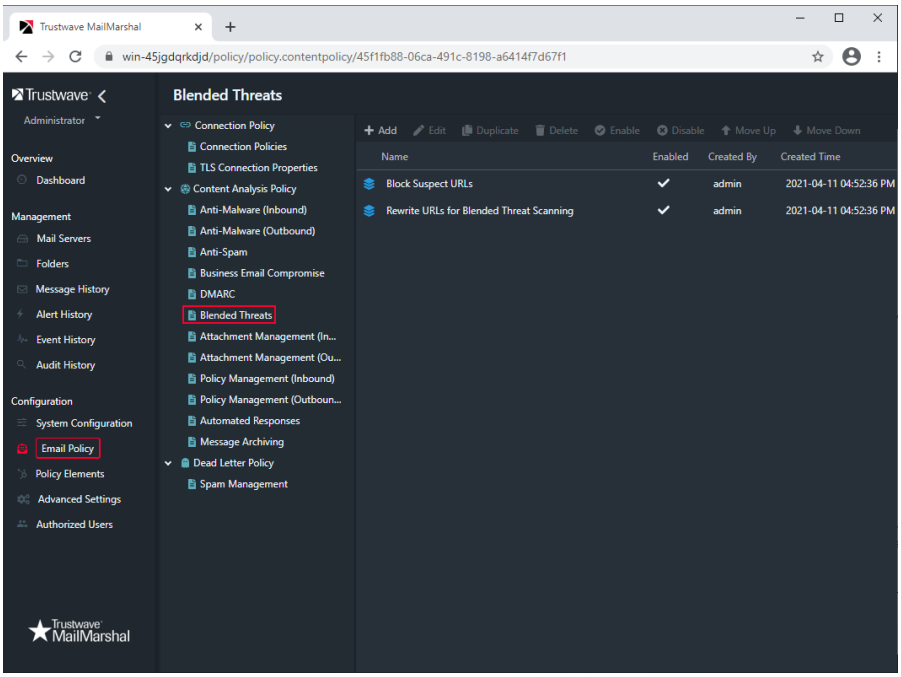


4.2 MailMarshal (SEG) Premises

MailMarshal Premises installations require Web access from the Array Manager server. The required URLs are:

- `https://mailmarshal.licensing.marshal.com` (used to validate licensing for this feature)
- `https://stats.scanmail.trustwave.com` (used to retrieve information about URL rewriting activity from the cloud service)

MailMarshal includes a default Policy Group (Blended Threats), and a Rule to enable the BTM. This rule is disabled by default because the BTM is separately licensed. To use the rule, simply enable it and then commit configuration. Customers who have not licensed this feature will not be able to enable this rule.



Note: MailMarshal Premises installations that were upgraded from version 6.9 or below do not include this default rule. The customer must create a rule using the action *Rewrite URLs in the message for Blended Threat Scanning.* This rule should be placed after anti-virus and spam blocking rules.

5 What URLs Does the BTM Rewrite and Check?

The BTM attempts to rewrite any link or text in the body of an email message that might be clickable when the user reads the message. In HTML message bodies, the link location (href) is rewritten. In both HTML and plain text message bodies, text URLs are rewritten.

The BTM does not rewrite links in attached files such as PDF or Office documents. The BTM does rewrite links in attached email messages.

Links that may be rewritten include text that “looks like” a URL either with or without the protocol part like http:// as well as IPv4 and IPv6 addresses and obfuscated links.

In MailMarshal Premises only, the BTM also rewrites text links in the message subject.

The BTM does not rewrite URLs of the customer’s local domains (domains used for inbound email delivery), or private network IP addresses.

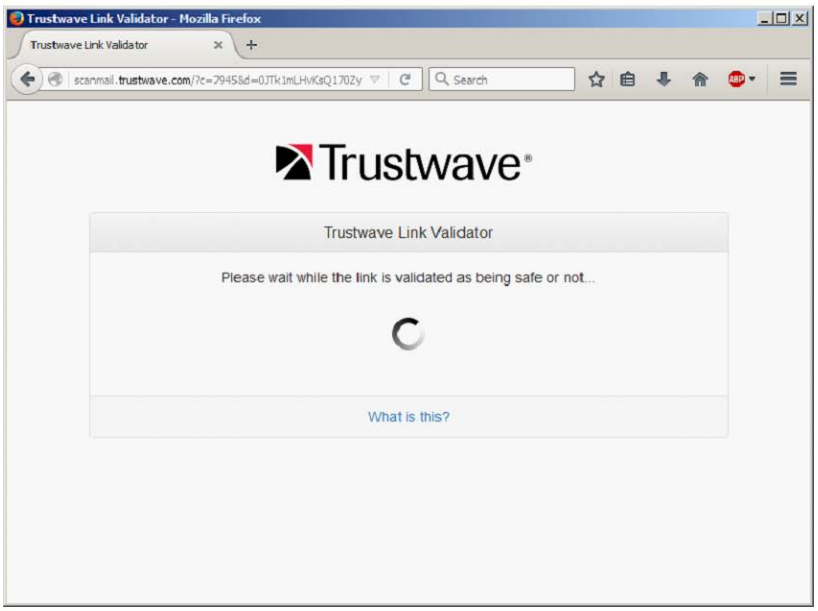
For full technical details of the types of links that are rewritten and excluded from rewriting, see Trustwave Knowledge Base article Q14548.

6 What Do End Users See?

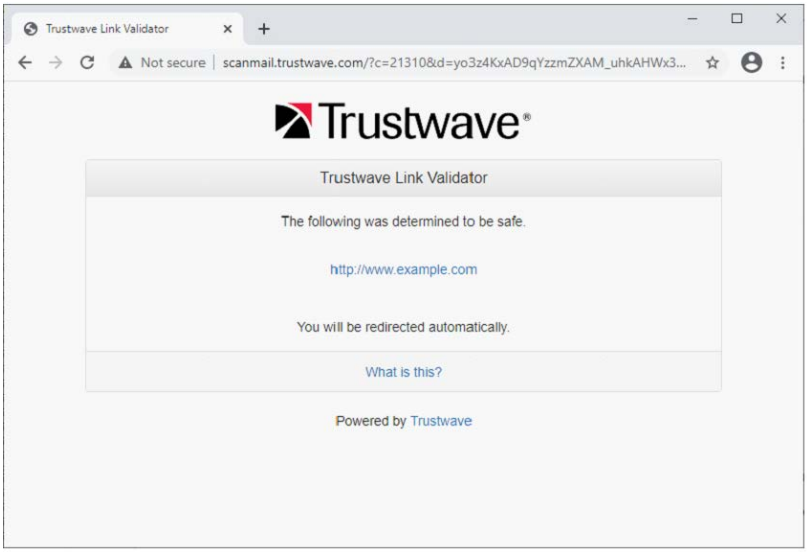
When a user opens a message, if the message is displayed in plain text all links will be visibly altered. HTML messages will not be visibly altered, but hovering over a link shows the rewritten URL.

The URL of the Link Validator cloud service accessed by the email clients is:
`http://scanmail.trustwave.com/`

When the user clicks a link, the URL is passed to the Trustwave Link Validator for evaluation. An information page displays briefly.

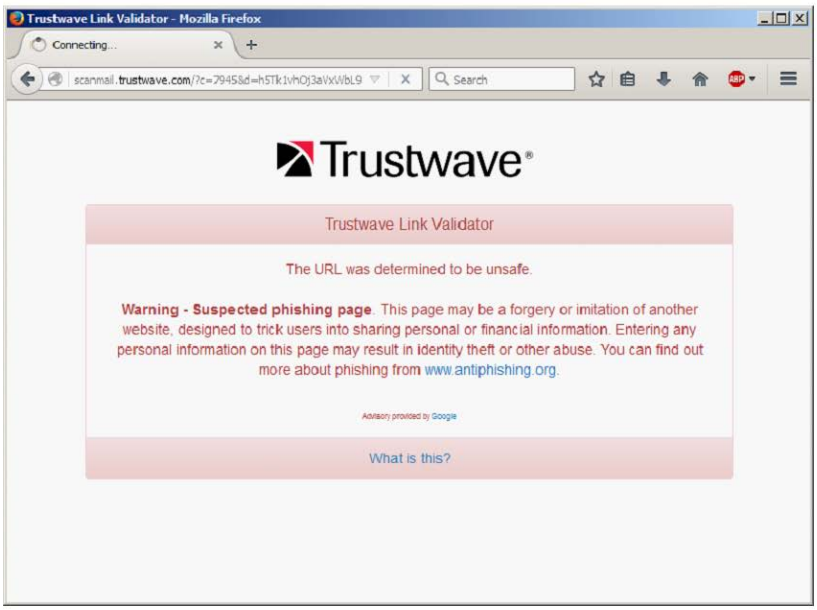


When a result is available it is reported.



If the result is “safe”, the user is automatically redirected to the original URL.

If the result is “unsafe”, a block page displays. In some cases a link with more specific information about the block source is included.



If the validator cannot check the URL, the user will be informed and will be offered the opportunity to click through to the site without validation.

This could occur if

- the BTM license of the customer company that originally rewrote the URL is expired
- the validator encounters an error accessing the site

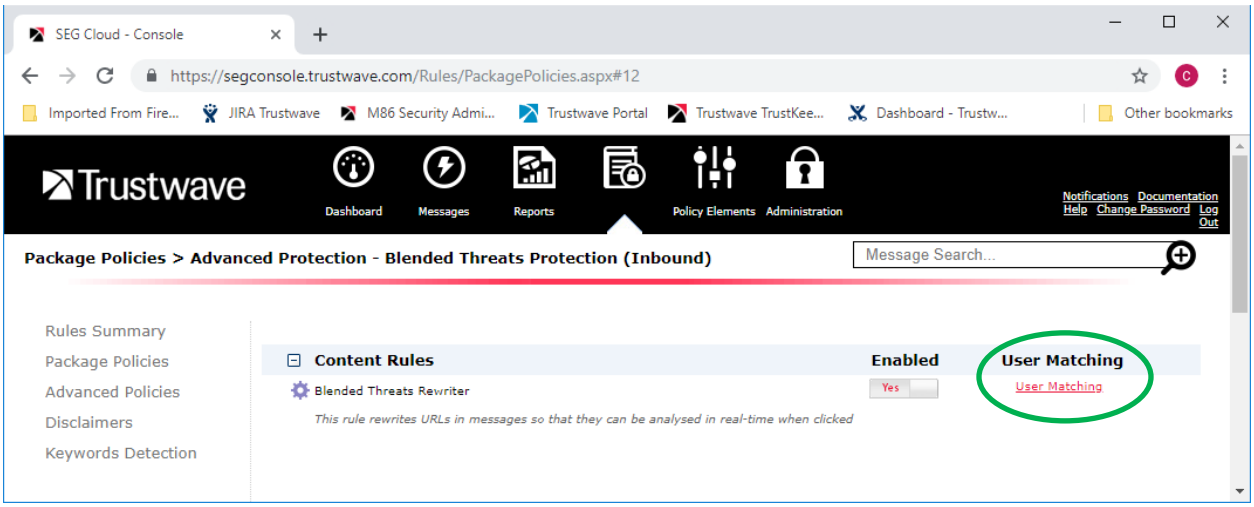
7 Can I Bypass the BTM for Some Users or URLs?

You can configure BTM to not rewrite some URLs, or not rewrite content for some users.

Caution: Trustwave strongly recommends you do not bypass rewriting if at all possible. “Trusted” sites and “busy executive” users are among the highest risks for Blended Threats.

7.1 MailMarshal (SEG) Cloud

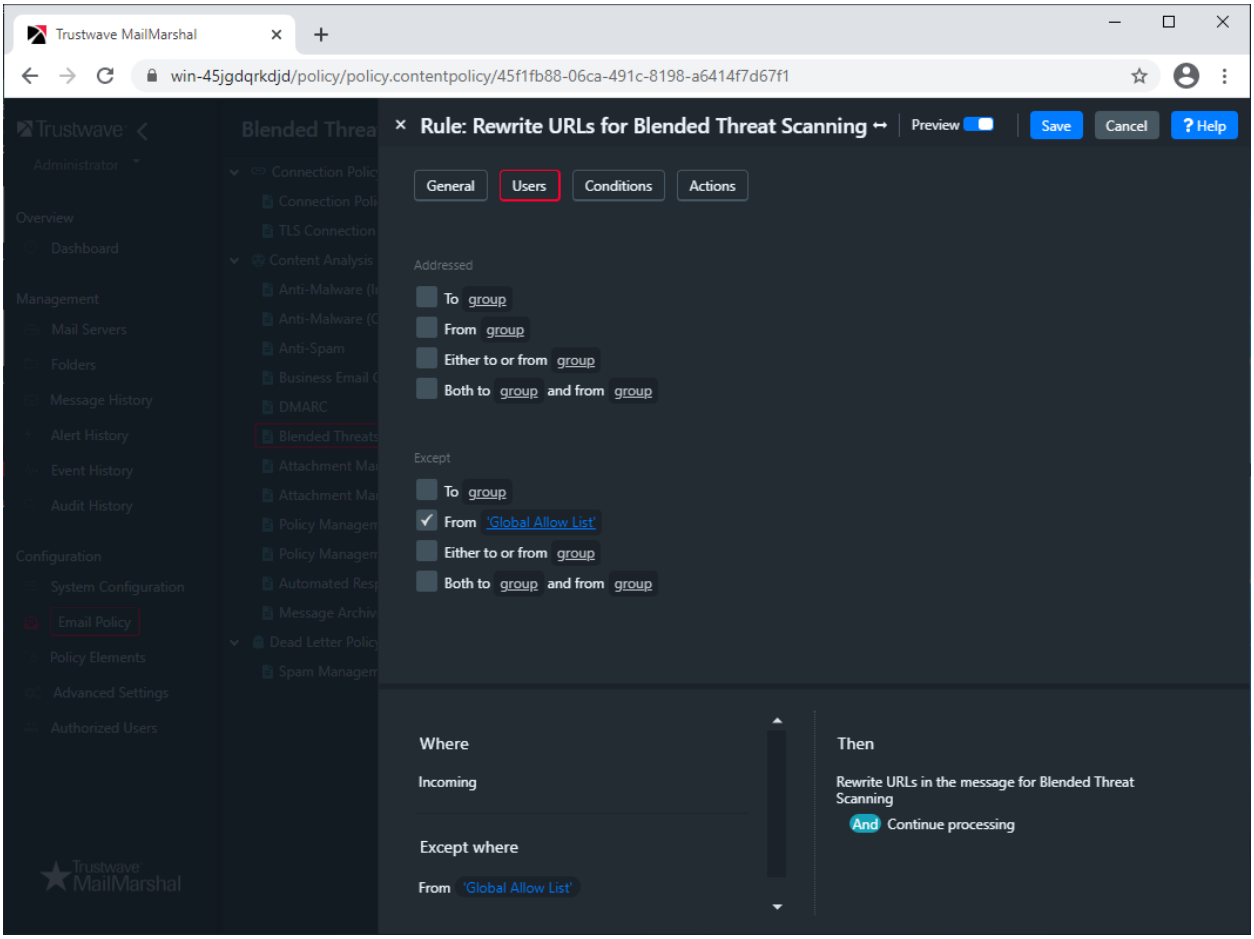
To bypass BTM rewriting, configure User Matching on the Blended Threats Scanner Rule. You can choose to bypass rewriting for messages that are addressed to certain internal users, or from certain external addresses. For testing purposes only, you can choose only to rewrite messages addressed to, or from, specific addresses.



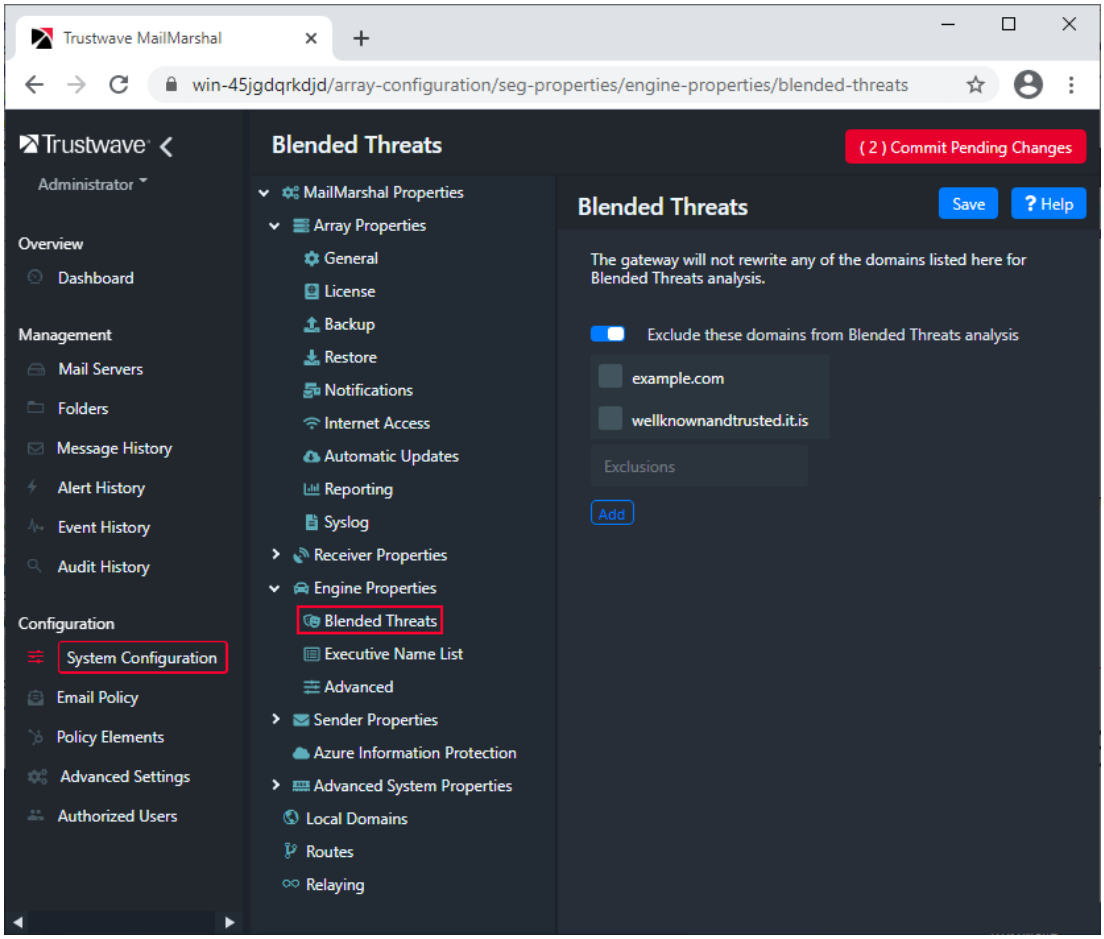
For more information about User Matching, see Help for this page of the Customer Console.

7.2 MailMarshal (SEG) Premises

To bypass BTM rewriting, you can add User Matching conditions to the Rewrite URLs for Blended Threat Scanning Rule.

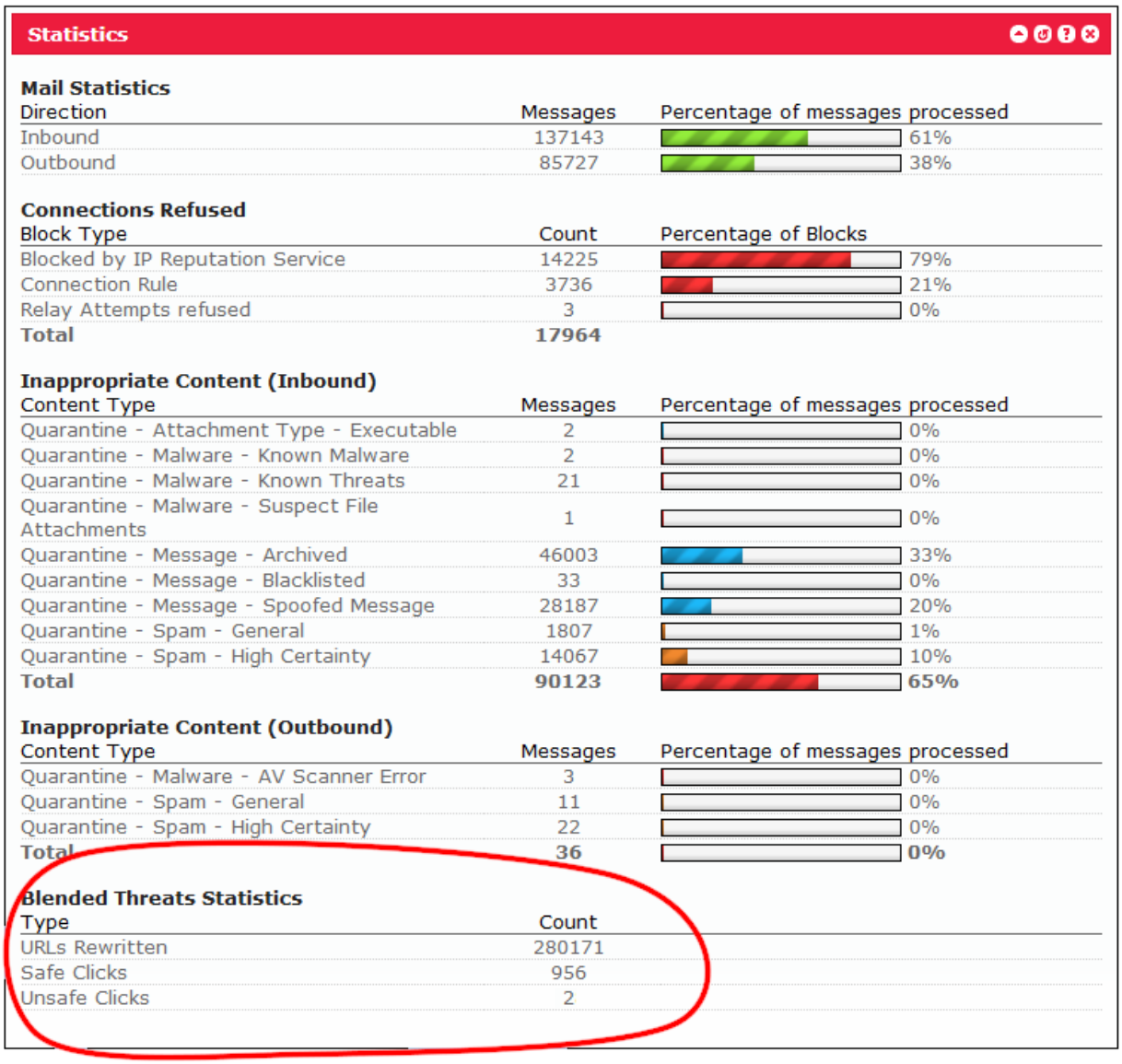


You can also exclude specific domains from rewriting. In the Management Console, navigate to MailMarshal Properties > Engine Properties > Blended Threats. (For Trustwave SEG 8.X, see Trustwave SEG Properties > Engine Properties > Blended Threats.)



8 What Reporting on BTM is Available?

Statistics of URLS rewritten, “safe” clicks, and “unsafe” clicks display on the MailMarshal Premises Console Dashboard and the MailMarshal Cloud Customer Console Dashboard.



Statistics

Mail Statistics

Direction	Messages	Percentage of messages processed
Inbound	137143	61%
Outbound	85727	38%

Connections Refused

Block Type	Count	Percentage of Blocks
Blocked by IP Reputation Service	14225	79%
Connection Rule	3736	21%
Relay Attempts refused	3	0%
Total	**17964**	

Inappropriate Content (Inbound)

Content Type	Messages	Percentage of messages processed
Quarantine - Attachment Type - Executable	2	0%
Quarantine - Malware - Known Malware	2	0%
Quarantine - Malware - Known Threats	21	0%
Quarantine - Malware - Suspect File Attachments	1	0%
Quarantine - Message - Archived	46003	33%
Quarantine - Message - Blacklisted	33	0%
Quarantine - Message - Spoofed Message	28187	20%
Quarantine - Spam - General	1807	1%
Quarantine - Spam - High Certainty	14067	10%
Total	**90123**	**65%**

Inappropriate Content (Outbound)

Content Type	Messages	Percentage of messages processed
Quarantine - Malware - AV Scanner Error	3	0%
Quarantine - Spam - General	11	0%
Quarantine - Spam - High Certainty	22	0%
Total	**36**	**0%**

Blended Threats Statistics

Type	Count
URLs Rewritten	280171
Safe Clicks	956
Unsafe Clicks	2

9 Can I Report URLs to Trustwave?

If you find a URL that you think is wrongly classified by BTM validation, you can report it to Trustwave using the web form at https://www.trustwave.com/support/submit-URL.asp

Use this form to report URLs that should be blocked by BTM, or blocked URLs that you believe are legitimate and safe.

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.