LevelBlue

Secure What's Next.

FREQUENTLY ASKED QUESTIONS

MailMarshal Blended Threat Module

Table of Contents

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

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?

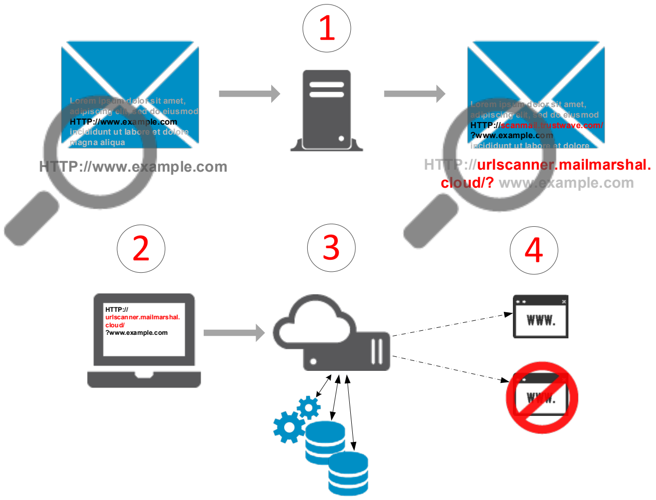
The MailMarshal Blended Threat Module uses a number of validation methods, including real-time behavioral analysis and content inspection as well as information from a number of industry standard sources, to identify and block sites that serve suspicious or malicious code.

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 Blended Threat 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.


1
Lorem ipsum dolor sit amet,
adipiscing elit, sed do eiusmod
HTTP://www.example.com
incididunt ut labore et dolore
magna aliqua
HTTP://www.example.com
Lorem ipsum dolor sit amet,
adipiscing elit, sed do eiusmod
HTTP://scanmail.trustwave.com/
?www.example.com
incididunt ut labore et dolore
HTTP://urlscanner.mailmarshal.
cloud/? www.example.com
2
3
4
HTTP://
urlscanner.mailmarshal.
cloud/
?www.example.com
WWW.
WWW.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

4 How Does URL Validation Work?

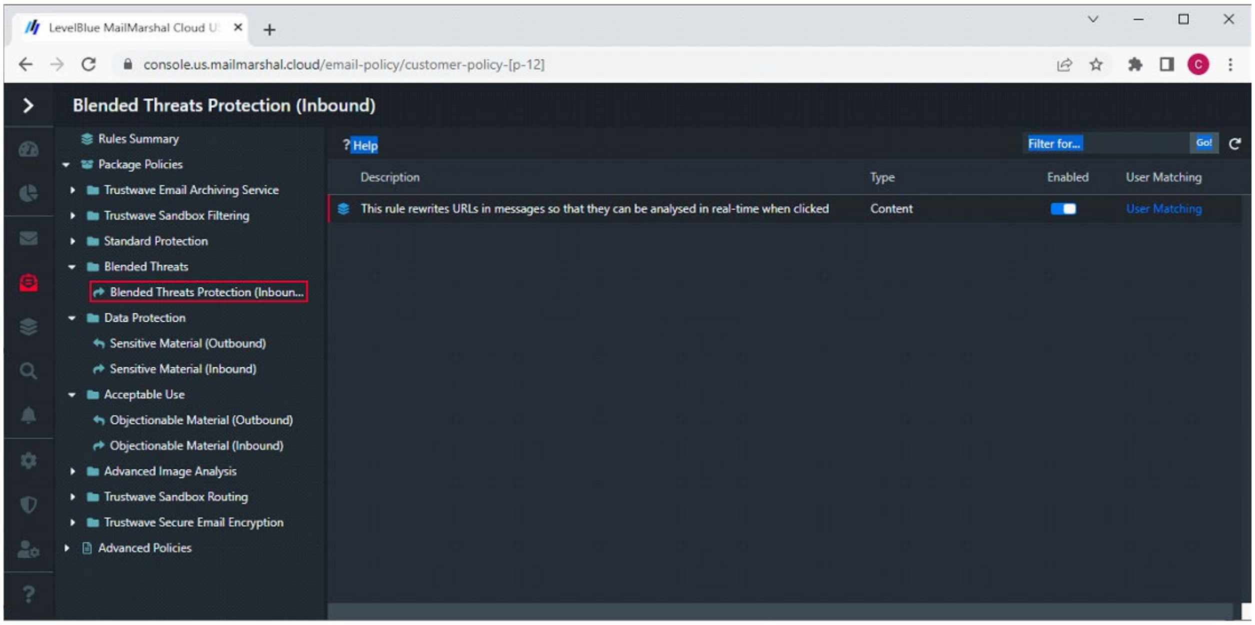
URLs are loaded, followed if they contain redirects, and subjected to a range of different URL validation services. These include various URL reputation services that check whether the URL has been associated with phishing or other malicious activity. URLs are also subject to real-time checking of page content using a proprietary URL classifier, based on machine learning technology, which is continuously trained on real-world data to recognize phishing and other threats. Real-time scanning helps detection of new threats in the window of time before URLs become listed in reputation lists.

5 How Do I Enable the BTM?

The BTM is implemented as a Rule Action in MailMarshal.

5.1 MailMarshal Cloud

All MailMarshal Cloud customers have access to the Blended Threats package. The Package contains a single rule to rewrite URLs, which is enabled by default. The customer can choose to bypass scanning for some users, as described later in this document.


LevelBlue MailMarshal Cloud U
console.us.mailmarshal.cloud/email-policy/customer-policy-[p-12]
Blended Threats Protection (Inbound)
Rules Summary
Package Policies
Trustwave Email Archiving Service
Trustwave Sandbox Filtering
Standard Protection
Blended Threats
Blended Threats Protection (Inboun...
Data Protection
Sensitive Material (Outbound)
Sensitive Material (Inbound)
Acceptable Use
Objectionable Material (Outbound)
Objectionable Material (Inbound)
Advanced Image Analysis
Trustwave Sandbox Routing
Trustwave Secure Email Encryption
Advanced Policies
? Help
Filter for...
Go!

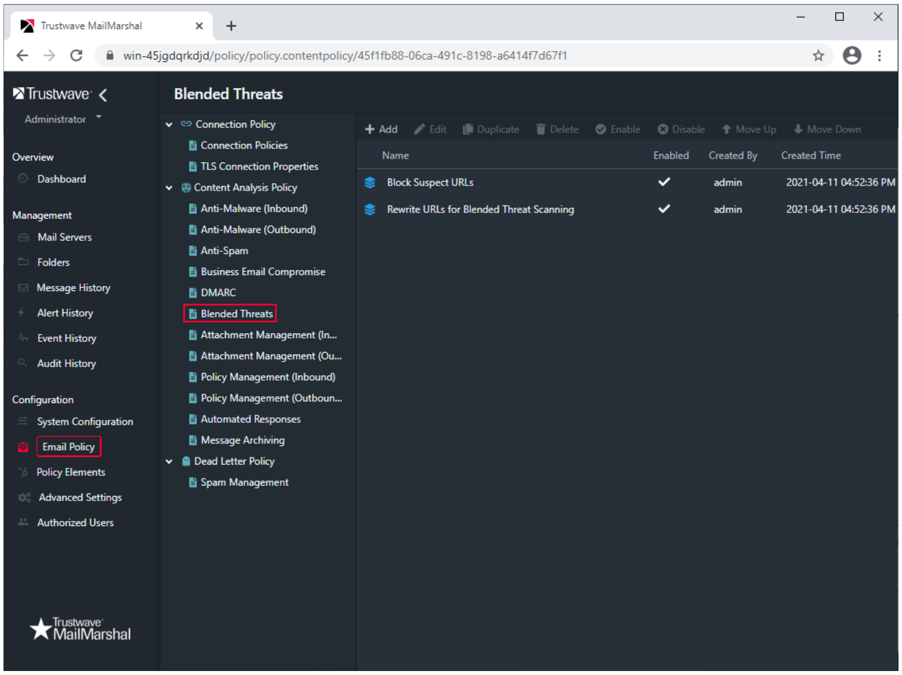
Description	Type	Enabled	User Matching
This rule rewrites URLs in messages so that they can be analysed in real-time when clicked	Content	●	User Matching

5.2 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://urlscanner.mailmarshal.cloud` (used to retrieve information about URL rewriting activity from the cloud service). For versions below 11.2, the URL is `https://stats.scanmail.trustwave.com`

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.



Name	Enabled	Created By	Created Time
Block Suspect URLs	✓	admin	2021-04-11 04:52:36 PM
Rewrite URLs for Blended Threat Scanning	✓	admin	2021-04-11 04:52:36 PM

Note: MailMarshal Premises installations that were originally installed using versions below 7.0 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.

6 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.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

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.

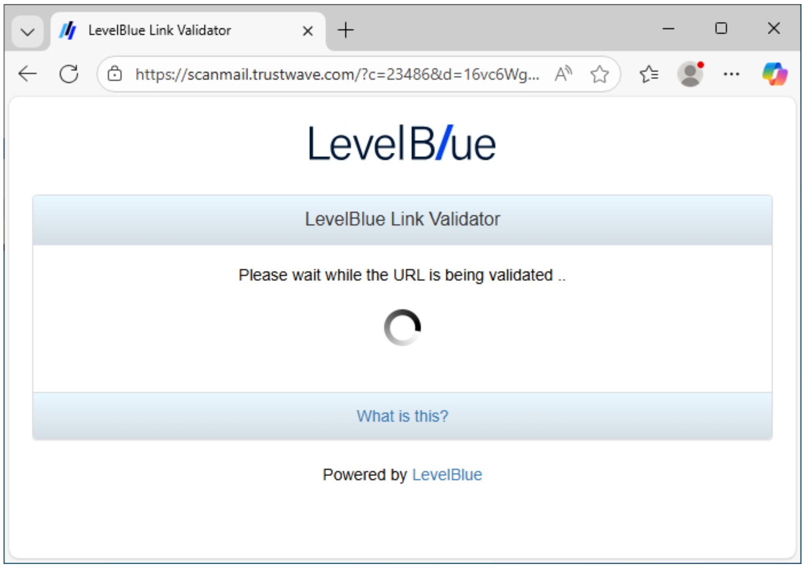
For full technical details of the types of links that are rewritten and excluded from rewriting, see Knowledge Base article Q14548.

7 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.



LevelBlue Link Validator

https://scanmail.trustwave.com/?c=23486&d=16vc6Wg...

LevelBlue

LevelBlue Link Validator

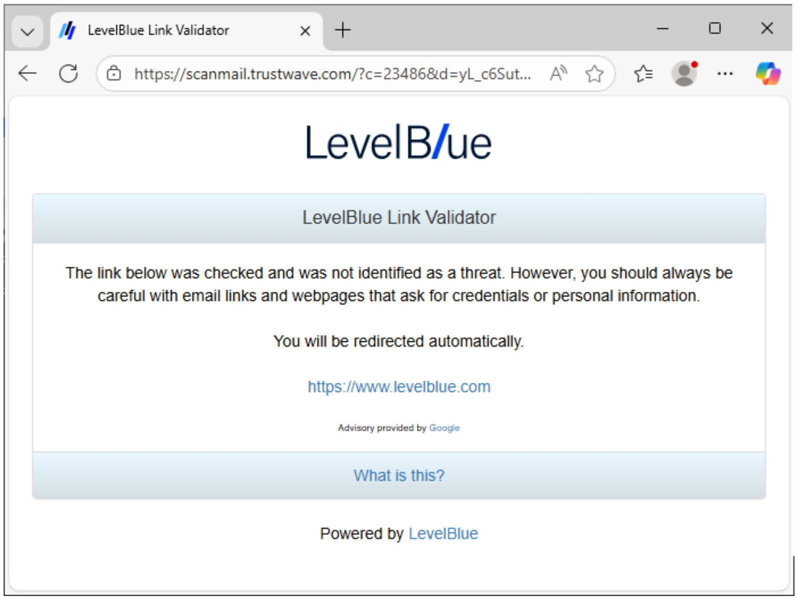
Please wait while the URL is being validated ..

What is this?

Powered by LevelBlue

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

When a result is available it is reported.



LevelBlue Link Validator

The link below was checked and was not identified as a threat. However, you should always be careful with email links and webpages that ask for credentials or personal information.

You will be redirected automatically.

https://www.levelblue.com

Advisory provided by Google

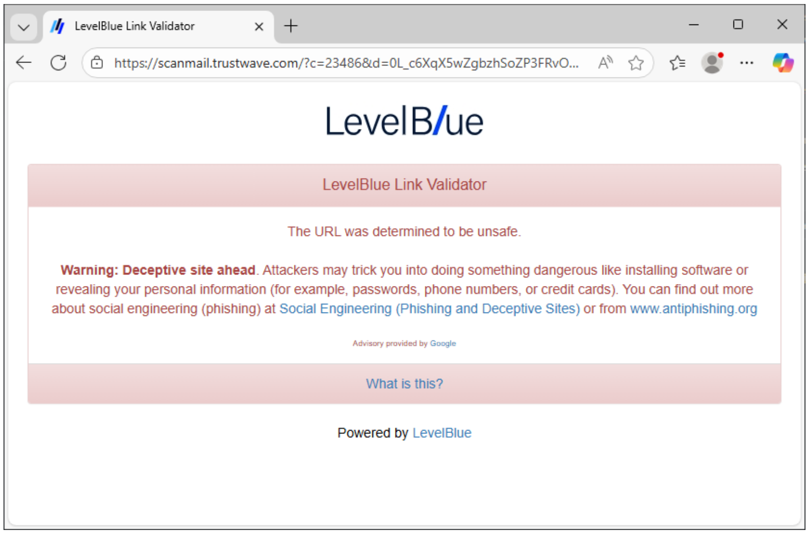
What is this?

Powered by LevelBlue

If the result is "not identified as a threat", the user is automatically redirected to the original URL.

Caution: Even if a site is not determined to be a threat, users should always take due care, particularly if the site requests credentials or personal information.

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


LevelBlue Link Validator
https://scanmail.trustwave.com/?c=23486&d=0L_c6XqX5wZgbzhSoZP3FRvO...
LevelBlue

LevelBlue Link Validator

The URL was determined to be unsafe.

Warning: Deceptive site ahead. Attackers may trick you into doing something dangerous like installing software or revealing your personal information (for example, passwords, phone numbers, or credit cards). You can find out more about social engineering (phishing) at Social Engineering (Phishing and Deceptive Sites) or from www.antiphishing.org

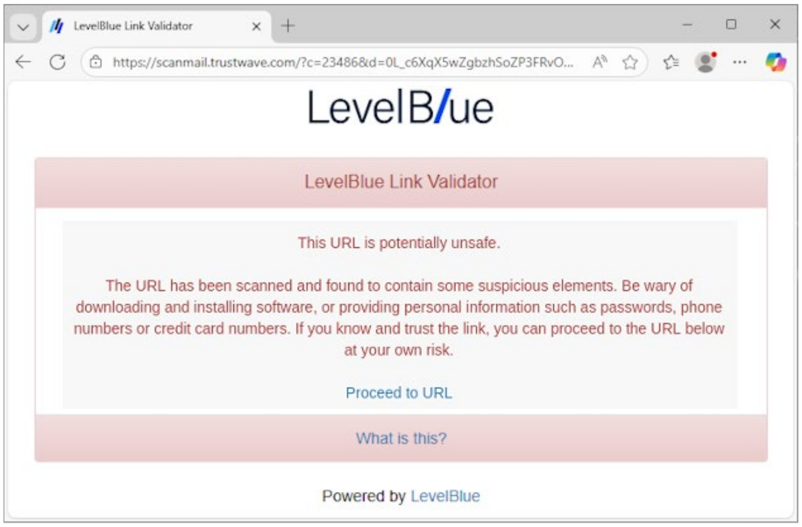
Advisory provided by Google

What is this?

Powered by LevelBlue

In some cases the scan notes a page as suspicious, but with lower confidence. In these cases the validator page presents a warning, but allows click-through to the original site.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.



LevelBlue Link Validator
https://scanmail.trustwave.com/?c=23486&d=0L_c6XqX5wZgbzhSoZP3FRvO...
LevelBlue

LevelBlue Link Validator

This URL is potentially unsafe.

The URL has been scanned and found to contain some suspicious elements. Be wary of downloading and installing software, or providing personal information such as passwords, phone numbers or credit card numbers. If you know and trust the link, you can proceed to the URL below at your own risk.

Proceed to URL

What is this?

Powered by LevelBlue

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

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

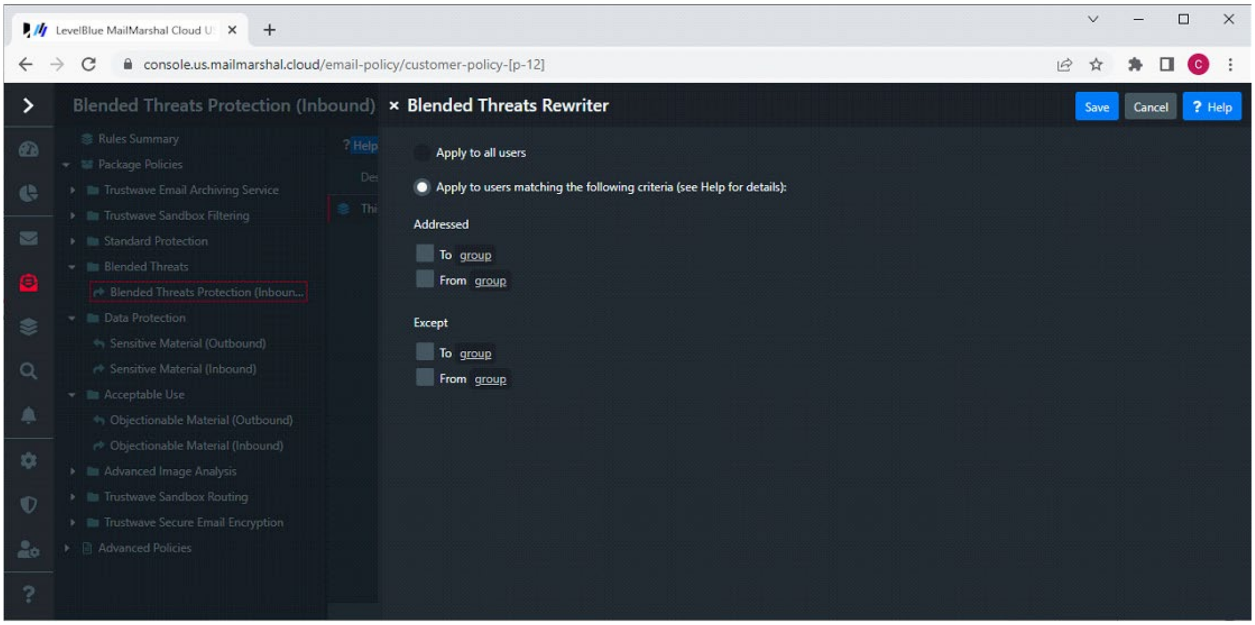
You can configure BTM to not rewrite some URLs, or not rewrite content for some users.

⚠ **Caution**: As best practice for security, do not bypass rewriting if at all possible. "Trusted" sites and "busy executive" users are among the highest risks for Blended Threats.

8.1 MailMarshal Cloud

To bypass BTM rewriting, configure User Matching on the Blended Threats Rewriter 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.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.


LevelBlue MailMarshal Cloud U
console.us.mailmarshal.cloud/email-policy/customer-policy-[p-12]
Blended Threats Protection (Inbound)
Rules Summary
Package Policies
Trustwave Email Archiving Service
Trustwave Sandbox Filtering
Standard Protection
Blended Threats
Blended Threats Protection (Inboun...
Data Protection
Sensitive Material (Outbound)
Sensitive Material (Inbound)
Acceptable Use
Objectionable Material (Outbound)
Objectionable Material (Inbound)
Advanced Image Analysis
Trustwave Sandbox Routing
Trustwave Secure Email Encryption
Advanced Policies
Save
Cancel
? Help

× Blended Threats Rewriter

○ Apply to all users

● Apply to users matching the following criteria (see Help for details):

Addressed

☐ To group

☐ From group

Except

☐ To group

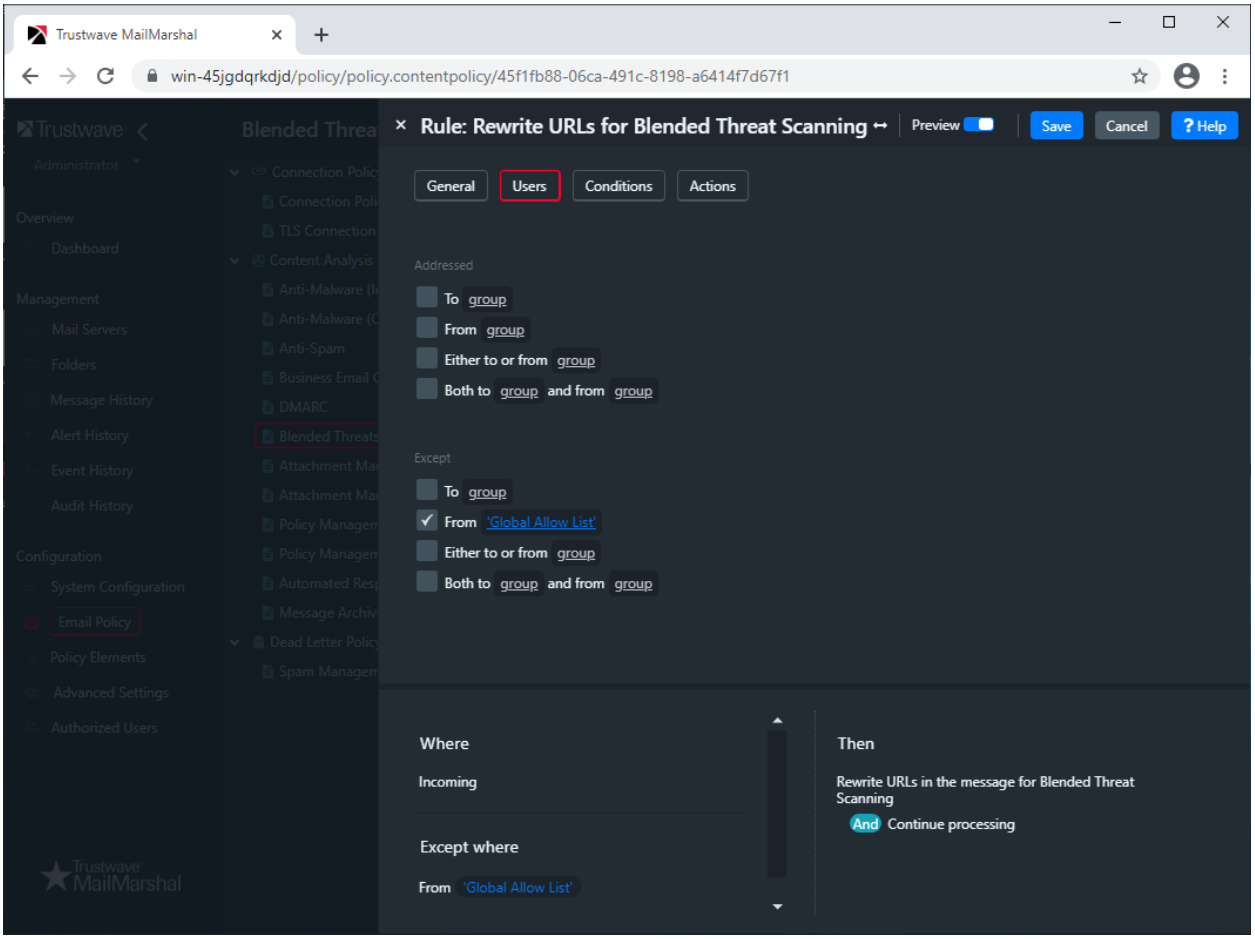
☐ From group

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

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

8.2 MailMarshal (SEG) Premises

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



Rule: Rewrite URLs for Blended Threat Scanning

Addressed

□ To group

□ From group

□ Either to or from group

□ Both to group and from group

Except

□ To group

☑ From 'Global Allow List'

□ Either to or from group

□ Both to group and from group

Where

Incoming

Except where

From 'Global Allow List'

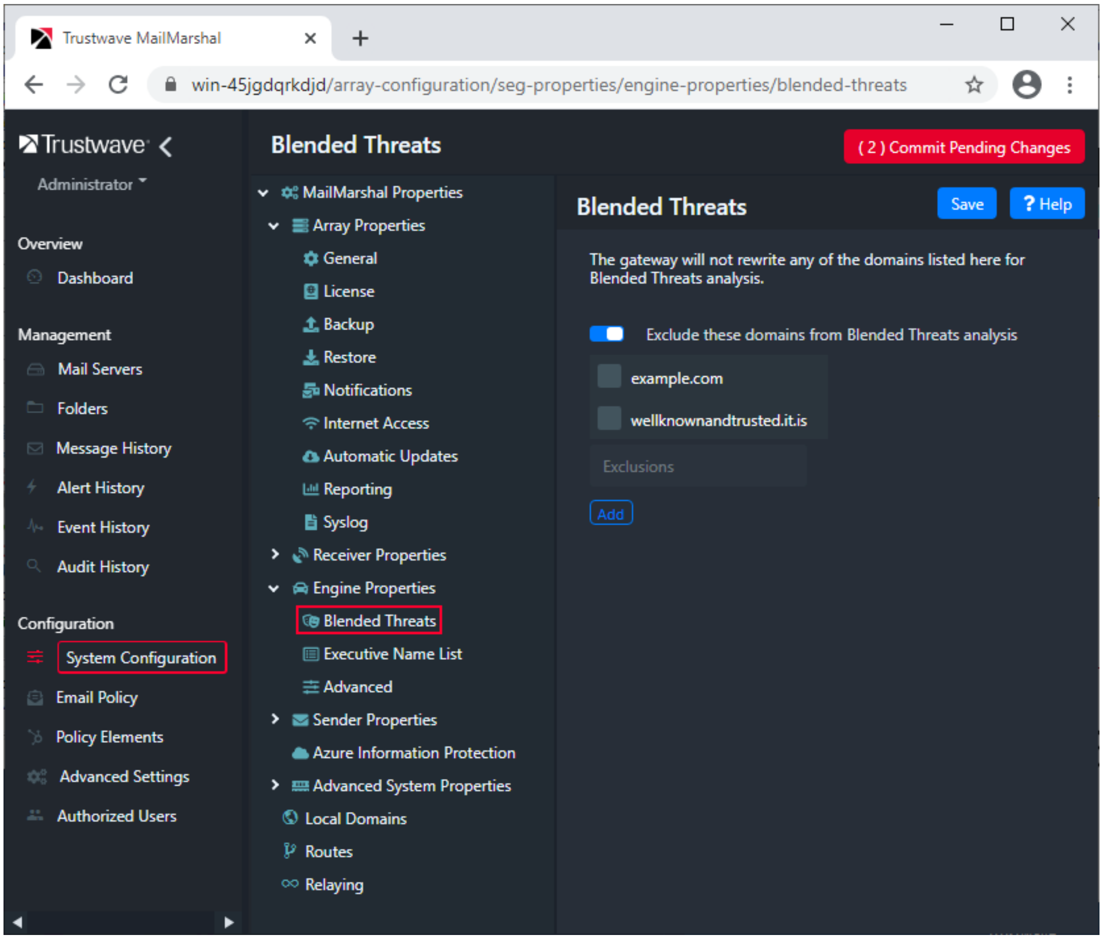
Then

Rewrite URLs in the message for Blended Threat Scanning

And Continue processing

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

You can also exclude specific domains from rewriting. In the Management Console, navigate to MailMarshal Properties > Engine Properties > Blended Threats.



The gateway will not rewrite any of the domains listed here for Blended Threats analysis.

● Exclude these domains from Blended Threats analysis

□ example.com

□ wellknownandtrusted.it.is

9 What Reporting on BTM is Available?

Statistics of URLS rewritten, permitted ("safe") clicks, and "unsafe" clicks display on the MailMarshal Premises Console Dashboard and the MailMarshal Cloud Customer Console Dashboard.

10 Can I Report Wrong Classifications?

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

Use this form to report URLs that should be blocked by BTM, or blocked URLs that you believe are legitimate and not malicious.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks and service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners.

About LevelBlue

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