



FREQUENTLY ASKED QUESTIONS

MailMarshal Blended Threat Module

Table of Contents

1 What is a Blended Threat? 2

2 What is the Blended Threat Module? 2

3 How Does the BTM Work? 2

4 How Does URL Validation Work? 3

5 How Do I Enable the BTM? 3

 5.1 MailMarshal Cloud 3

 5.2 MailMarshal (SEG) Premises 4

6 What URLs Does the BTM Rewrite and Check? 5

7 What Do End Users See? 5

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

 8.1 MailMarshal Cloud 8

 8.2 MailMarshal (SEG) Premises 9

9 What Reporting on BTM is Available? 10

10 Can I Report Wrong Classifications? 10

About LevelBlue 11

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?

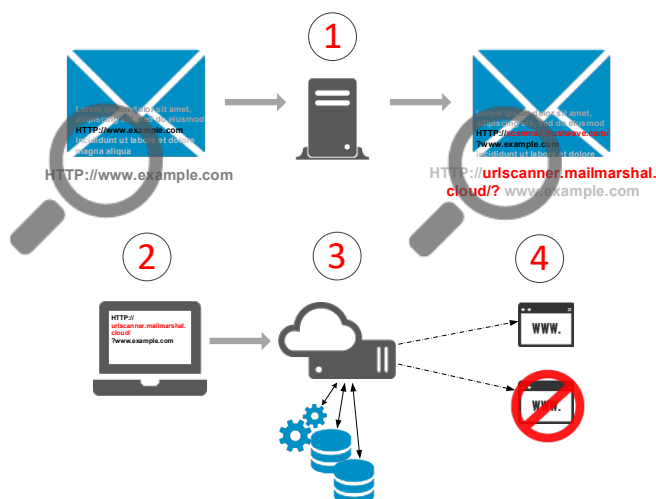
The MailMarshal Blended Threat Module uses a number of validation methods, including real-time behavioral analysis and content inspection as well as information from a number of industry standard sources, to identify and block sites that serve suspicious or malicious code.

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.



4 How Does URL Validation Work?

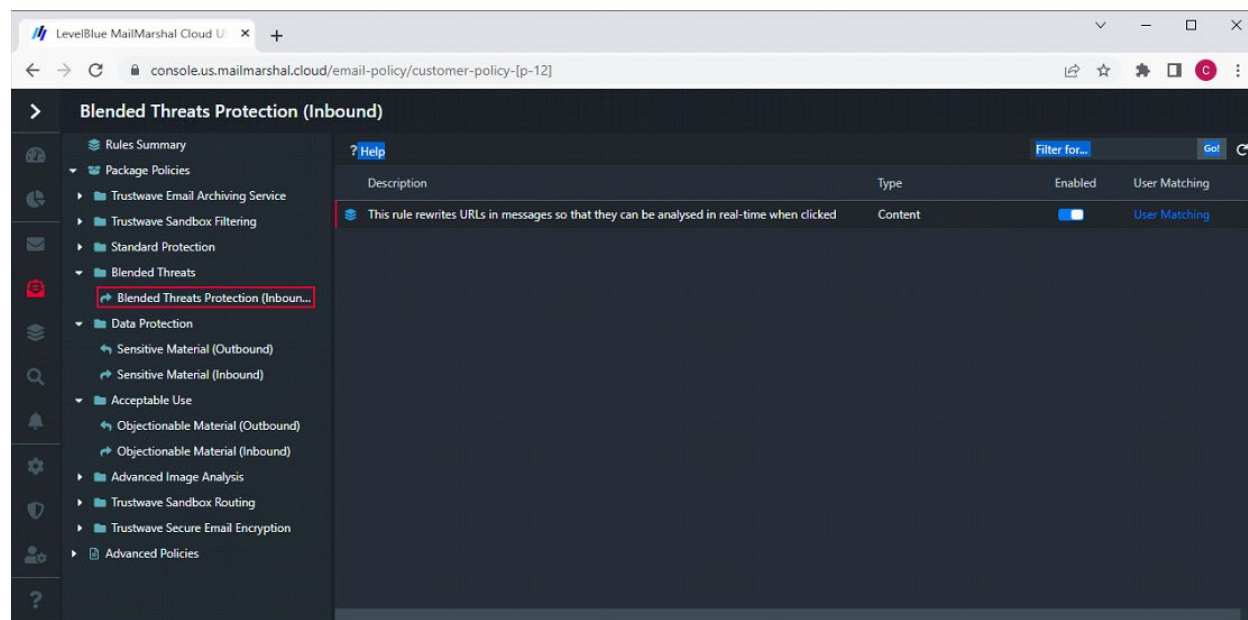
URLs are loaded, followed if they contain redirects, and subjected to a range of different URL validation services. These include various URL reputation services that check whether the URL has been associated with phishing or other malicious activity. URLs are also subject to real-time checking of page 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.



5.2 MailMarshal (SEG) Premises

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

- <https://mailmarshal.licensing.marshall.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.

The screenshot shows the MailMarshal web interface. The left sidebar contains navigation links: Administrator, Overview (Dashboard, Status), Management (Mail Servers, Folders, Message History, Rejected Messages, Quarantine Audit, Alert History, Event History, Audit History, User Account Audit), and Configuration (System Configuration, **Email Policy**, Policy Elements, Advanced Settings, Authorized Users). The main content area is titled 'Blended Threats'. It includes a table of rules with columns: Name, Enabled, Created Time, and Last Modified Time. Two rules are listed: 'Block Suspect URLs' and 'Rewrite URLs for Blended Threat Scanning', both with 'Enabled' checked. The 'Rewrite URLs for Blended Threat Scanning' rule is expanded, showing its configuration details in a table below.

Name	Enabled	Created Time	Last Modified Time
Block Suspect URLs	✓	11/11/2024 12:07:45 PM	11/11/2024 12:07:45 PM
Rewrite URLs for Blended Threat Scanning	✓	11/11/2024 12:07:45 PM	7/29/2026 7:49:07 PM

Rewrite URLs for Blended Threat Scanning			
Update Type	Updated	Updated By	admin
IP Address	127.0.0.1	Update Time	Wednesday, July 29, 2026 7:49:07 PM
Commit Set	19		



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.

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](#).

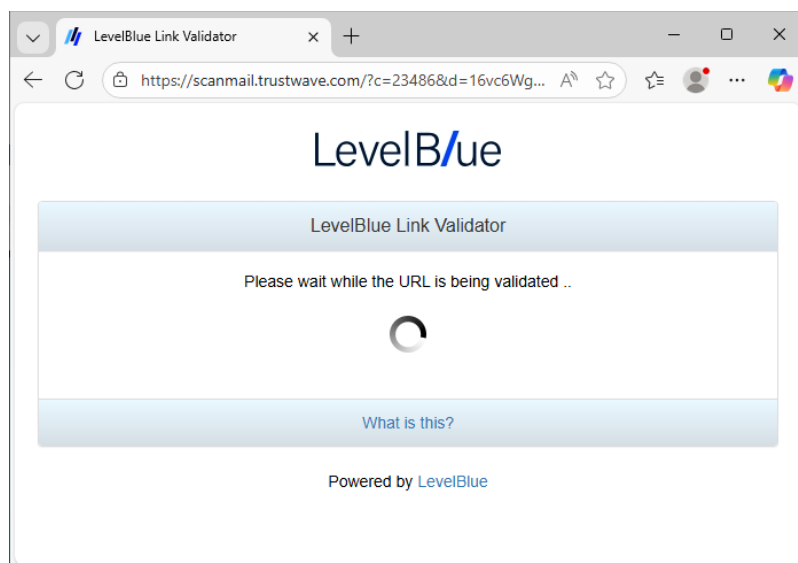
7 What Do End Users See?

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.

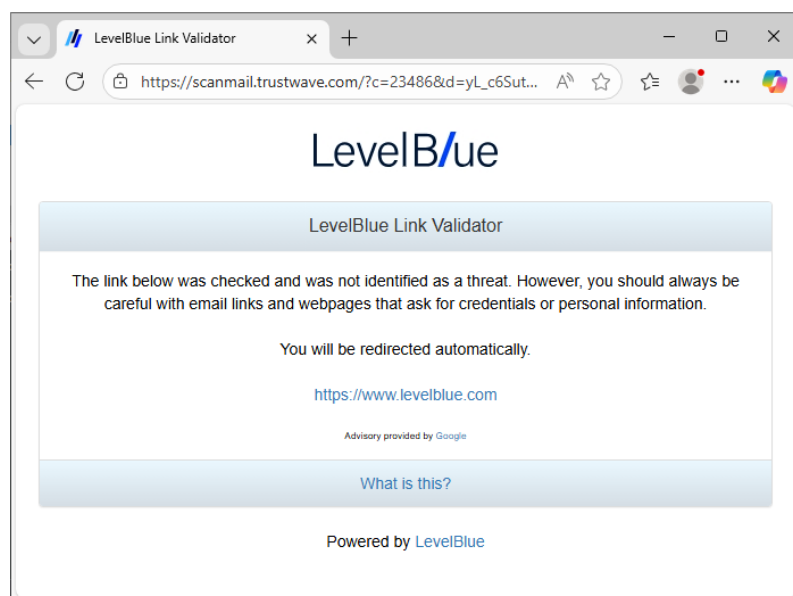
The URL of the Link Validator cloud service accessed by the email clients is:

<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.



When a result is available it is reported.

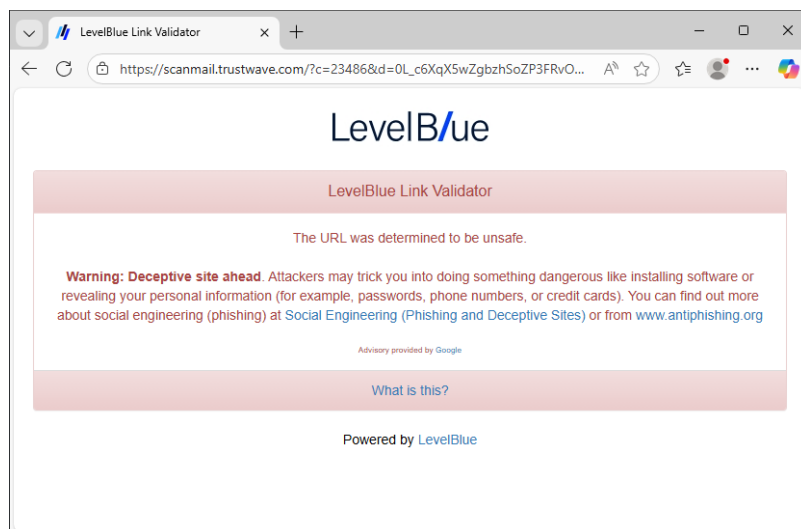


If the result is "not identified as a threat", the user is automatically redirected to the original URL.

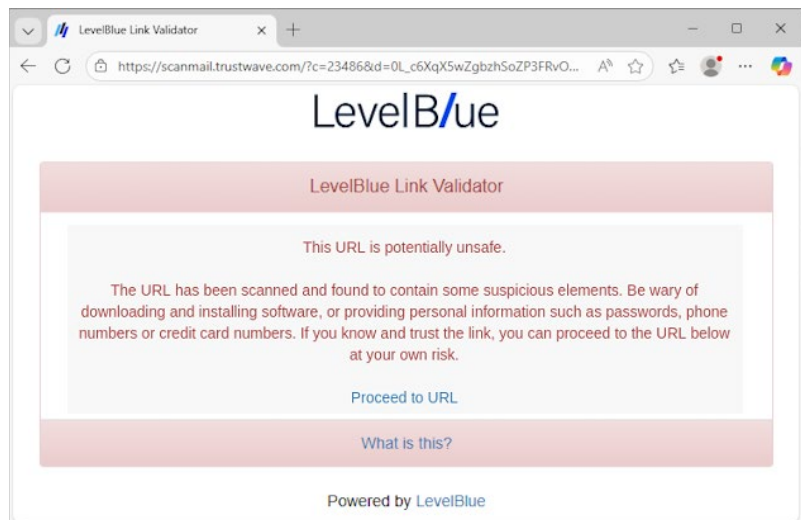


Caution: Even if a site is not determined to be a threat, users should always take due care, particularly if the site requests credentials or personal information.

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.



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.



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?

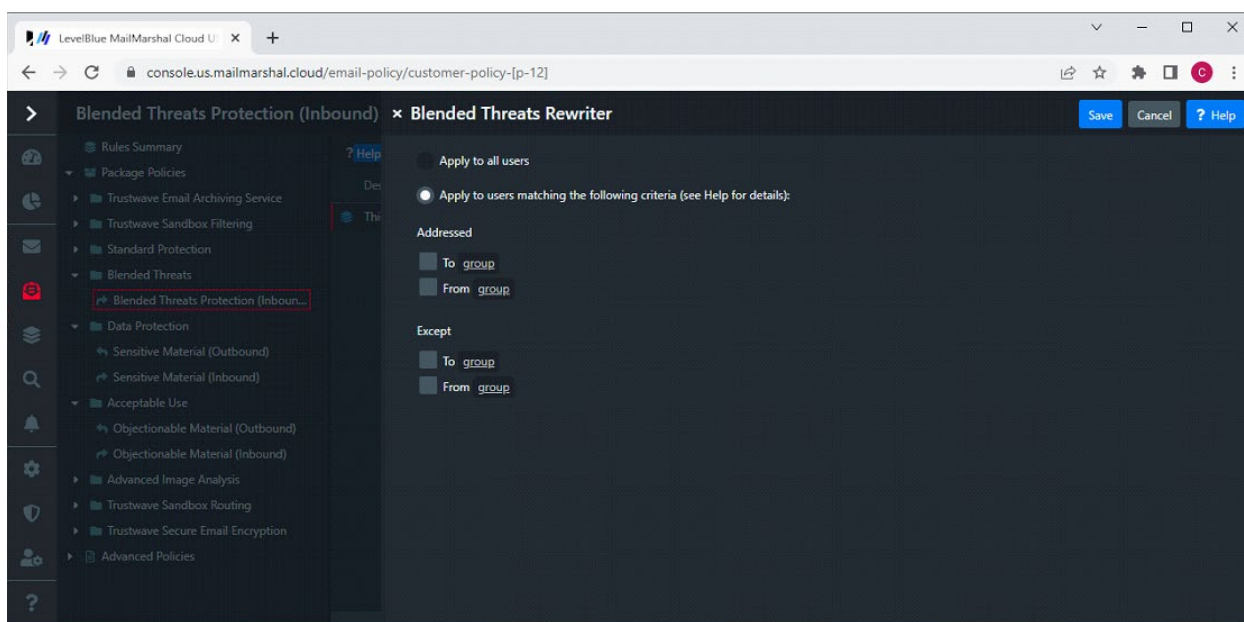
You can configure BTM to not rewrite some URLs, or not rewrite content for some users.



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

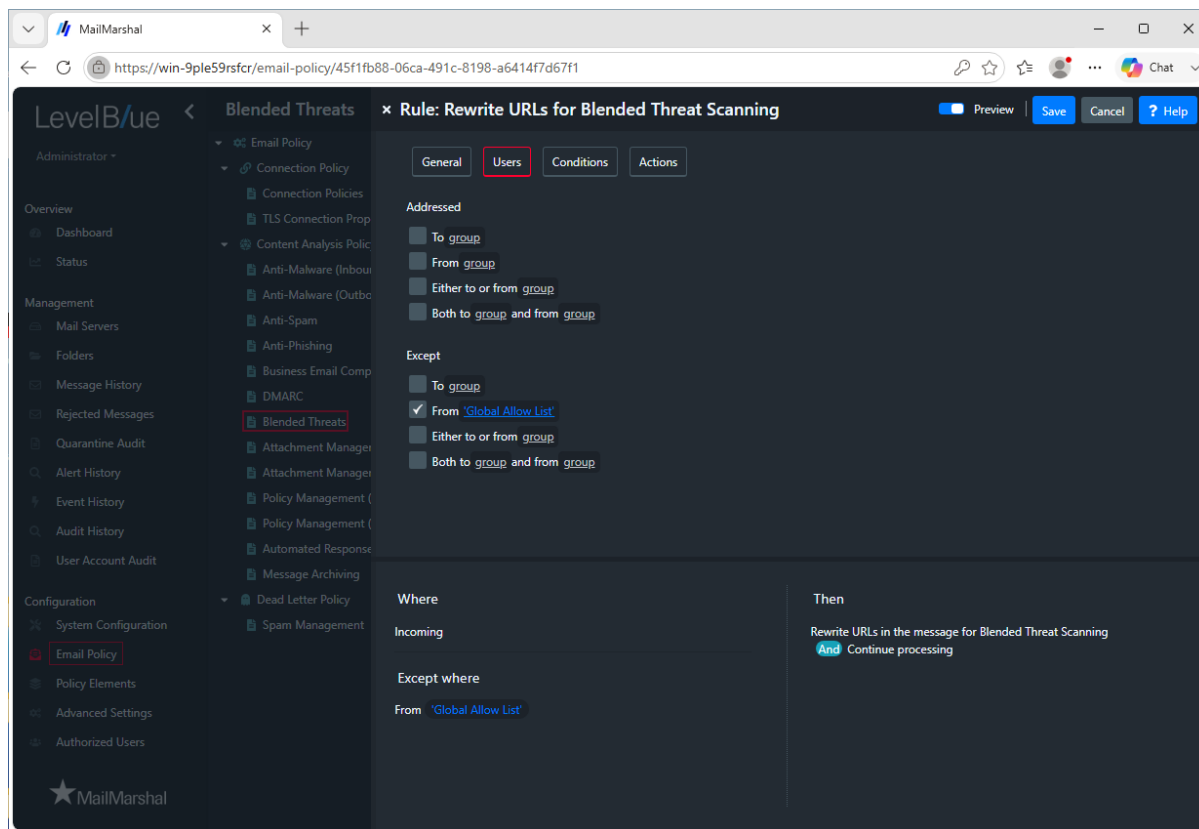
To bypass BTM rewriting, configure User Matching on the Blended Threats Rewriter Rule. You can choose to bypass rewriting for messages that are addressed to certain internal users, or from certain external addresses. For testing purposes only, you can choose only to rewrite messages addressed to, or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



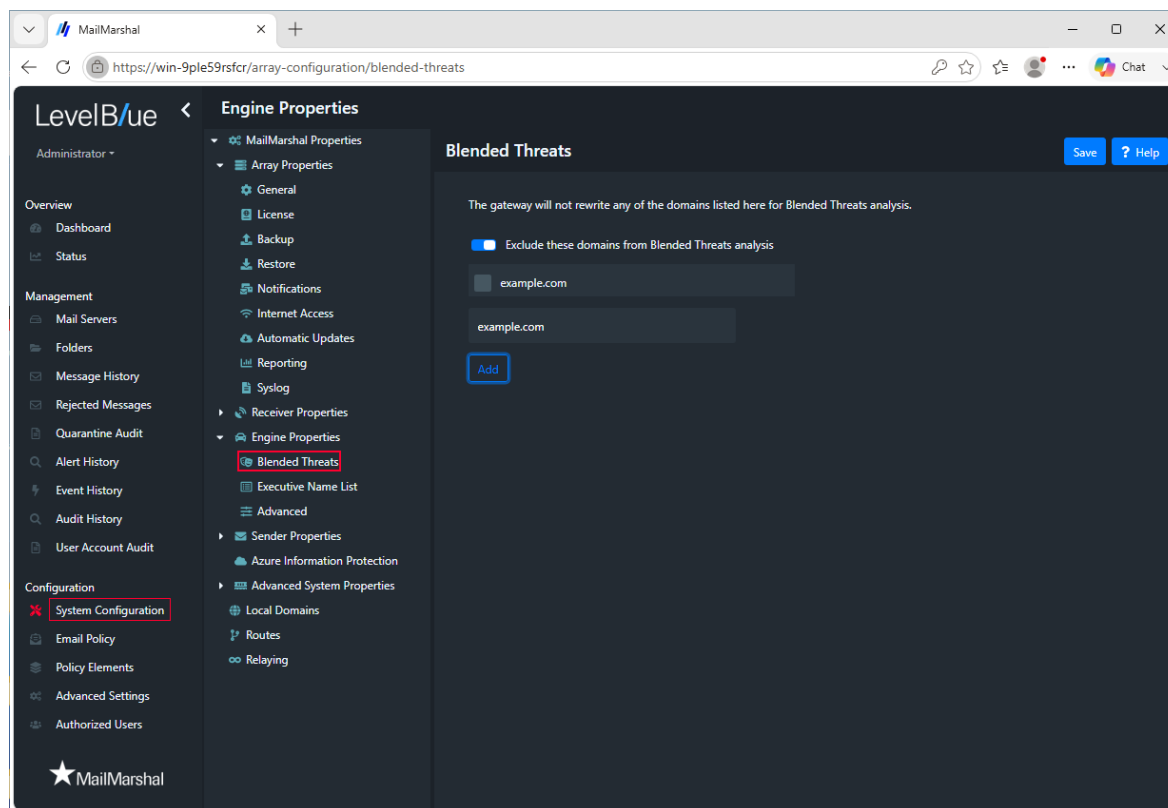
For more information about User Matching, see Help for this page of the Customer Console.

8.2 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.



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.

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.