



Bitdefender®

Bitdefender Email Security

USER GUIDE

Bitdefender GravityZone User Guide

Publication date 2020.01.23

Copyright© 2020 Bitdefender

Legal Notice

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without written permission from an authorized representative of Bitdefender. The inclusion of brief quotations in reviews may be possible only with the mention of the quoted source. The content can not be modified in any way.

Warning and Disclaimer. This product and its documentation are protected by copyright. The information in this document is provided on an "as is" basis, without warranty. Although every precaution has been taken in the preparation of this document, the authors will not have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in this work.

This book contains links to third-party Websites that are not under the control of Bitdefender, therefore Bitdefender is not responsible for the content of any linked site. If you access a third-party website listed in this document, you will do so at your own risk. Bitdefender provides these links only as a convenience, and the inclusion of the link does not imply that Bitdefender endorses or accepts any responsibility for the content of the third-party site.

Trademarks. Trademark names may appear in this book. All registered and unregistered trademarks in this document are the sole property of their respective owners, and are respectfully acknowledged.



Table of Contents

- 1. Product Information 6
 - 1.1. More Information 6
 - 1.1.1. Documentation 6
 - 1.1.2. Support Center 6
 - 1.1.3. Customer Care 6
 - 1.2. Email Security Overview 6
 - 1.3. Supported Languages 7
- 2. Setup and Installation 8
 - 2.1. Product Requirements 8
 - 2.1.1. Solution Requirements 8
 - 2.1.2. Licensing 8
 - 2.1.3. Provision Email Security Accounts (Bitdefender Partners only) 9
 - 2.2. Configure Email Security 9
 - 2.2.1. Add Domains 9
 - 2.2.2. Configure Email Service 10
 - 2.2.3. Add Mailboxes 27
 - 2.3. Usage Scenarios 27
- 3. Understanding Mail Flow 28
- 4. Message Rules 29
 - 4.1. Message Rule Overview 29
 - 4.2. Message Rule Priority 29
 - 4.2.1. Changing Message Rule Order 29
 - 4.2.2. Managing Active/Inactive Message Rules 29
 - 4.3. Message Rule Direction 30
 - 4.4. Managing Message Rules 30
 - 4.4.1. Adding Message Rules 30
 - 4.4.2. Editing Message Rules 31
 - 4.4.3. Deleting Message Rules 31
 - 4.5. Message Rule Cards 32
 - 4.5.1. Conditions 32
 - 4.5.2. Actions 36
 - 4.5.3. Final Actions 38
 - 4.6. System Message Rules 39
- 5. Connection Rules 41
 - 5.1. Connection Rules Overview 41
 - 5.2. Connection Rule Priority 41
 - 5.2.1. Changing Connection Rule Order 41
 - 5.2.2. Managing Active/Inactive Connection Rules 41
 - 5.3. Connection Rule Direction 42
 - 5.4. Managing Connection Rules 42
 - 5.4.1. Adding Connection Rules 42
 - 5.4.2. Editing Connection Rules 43
 - 5.4.3. Deleting Connection Rule 43



- 5.5. Connection Rule Cards 44
 - 5.5.1. Conditions 44
 - 5.5.2. Final Actions 45
- 5.6. System Connection Rules 45
- 6. Custom Rule Data 47
 - 6.1. Custom Rule Data Overview 47
 - 6.2. Managing Rule Data 47
 - 6.2.1. Adding Rule Data 47
 - 6.2.2. Editing Rule Data 48
 - 6.2.3. Deleting Rule Data 48
- 7. Global Quarantine 49
 - 7.1. Global Quarantine 49
 - 7.1.1. Running Quarantine Reports 50
 - 7.1.2. Viewing Quarantine Messages 50
 - 7.1.3. Taking Actions 50
- 8. Global Deny List 51
 - 8.1. Global Deny List Overview 51
 - 8.2. Viewing Global Deny List 51
 - 8.3. Managing Global Deny List 51
 - 8.3.1. Adding Entries 53
 - 8.3.2. Editing Entries 53
 - 8.3.3. Deleting Entries 54
- 9. Global Safe List 53
 - 9.1. Global Safe List Overview 53
 - 9.2. Viewing Global Safe List 53
 - 9.3. Managing Global Safe List 53
 - 9.3.1. Adding Entries 53
 - 9.3.2. Editing Entries 53
 - 9.3.3. Deleting Entries 54
- 10. Mailboxes 55
 - 10.1. Adding Mailboxes 55
 - 10.2. Importing Mailboxes from Exchange Online 55
 - 10.3. Editing Mailboxes 56
 - 10.4. Deleting Mailboxes 56
- 11. Product Configuration 57
 - 11.1. Product Configuration Overview 57
 - 11.2. Domains 57
 - 11.2.1. Adding Domains 57
 - 11.2.2. Editing Domains 58
 - 11.2.3. Deleting Domains 58
 - 11.3. Inbound Mail 58
 - 11.3.1. Adding Inbound Routes 58
 - 11.3.2. Editing Inbound Routes 59
 - 11.3.3. Deleting Inbound Routes 59



- 11.4. Outbound Mail 59
 - 11.4.1. Adding Outbound Routes 59
 - 11.4.2. Editing Outbound Routes 60
 - 11.4.3. Deleting Outbound Routes 60
- 11.5. Disclaimer 60
- 11.6. Custom Quarantine 61
 - 11.6.1. Custom Quarantine Overview 61
 - 11.6.2. Managing Custom Quarantine 61
- 12. Active Directory 63
 - 12.1. Active Directory Overview 63
 - 12.2. Adding Azure Active Directory 63
- 13. Group Management 65
 - 13.1. Group Management Overview 65
 - 13.2. Managing Groups 65
 - 13.2.1. Adding Groups 65
 - 13.2.2. Editing Groups 65
 - 13.2.3. Deleting Groups 65
- 14. Analytics 66
 - 14.1. Analytics Overview 66
 - 14.2. Reports 66
 - 14.2.1. Reports Overview 66
 - 14.2.2. Managing Reports 66
 - 14.2.3. Report Types 67
 - 14.3. Charts 68
 - 14.3.1. Chart Reports Overview 68
 - 14.3.2. Managing Chart Reports 68
 - 14.3.3. Chart Report Types 69
- 15. Scheduled Reports 71
 - 15.1. Scheduled Reports Overview 71
 - 15.2. Creating Scheduled Reports 71
 - 15.3. Managing Scheduled Reports 72
- 16. Log Archives 73
 - 16.1. Log Archives Overview 73
 - 16.2. Managing Log Archives 73

1. PRODUCT INFORMATION

- [More Information](#)
- [Email Security Overview](#)
- [Supported Languages](#)

1.1. More Information

1.1.1. Documentation

Bitdefender provides the following resources to learn more about your GravityZone products.

- [GravityZone Business \(Cloud-Based\) Documentation](#)

1.1.2. Support Center

[Bitdefender Support Center](#) is the place where you will find all the assistance you need with your Bitdefender product.

1.1.3. Customer Care

[Contact Customer Care](#) to get technical assistance.

1.2. Email Security Overview

The Bitdefender Email Security includes the following features:

- **Policy Engine** is an out of the box system to control email delivery and filter messages through a comprehensive rule builder.
- **Connection Rules** monitors connection attempt to and from mailboxes.
- **Email Authentication** supports SPF, DKIM, and DMARC.
- **User Synchronization** manages Active Directory users and groups.
- **Mailbox Synchronization** synchronizes Microsoft Azure Active Directory.
- **Antispam** technologies detect spam and sophisticated targeted phishing attacks.
- **Antimalware** uses security content and behaviour to detect malware.
- **Quarantine** uses a company-wide policy.



- **Safe and Deny Lists** configures individual and company-wide lists.
- **Executive Tracking List** detects users' real names within the header and envelope address fields to protect against impersonation attacks.
- **Disclaimer** adds an HTML text disclaimer to outbound emails.
- **Reports and Charts** provide detailed visibility of mail flow, triggered rules, and taken actions.
- **Scheduled Reports** link reports to schedules and sends alerts to recipients.

1.3. Supported Languages

Bitdefender Email Security is available in the following languages:

- English

2. SETUP AND INSTALLATION

- [Product Requirements](#)
- [Configure Email Security](#)
- [Usage Scenarios](#)

2.1. Product Requirements

- [Solution Requirements](#)
- [Licensing](#)
- [Provision Email Security Accounts \(Bitdefender Partners only\)](#)

2.1.1. Solution Requirements

To prepare for Email Security configuration, meet the following requirements:

- **Access to GravityZone Control Center**

If you do not have a Bitdefender account, you can find more information in the following resources:

- [Bitdefender Business Solutions](#)
- [Bitdefender Cloud Security for MSP](#)

- **Email Security add-on license key**

For more information, [Contact Business Sales](#).

- **Gather setup information:**

- Organizational mailboxes
- Routing information for inbound/outbound mail delivery

2.1.2. Licensing

Now that you have access to GravityZone Control Center, use the following procedure to enable Email Security.

1. Log in to Control Center.
2. Click your username at the upper-right corner and choose **My Company**.
3. Under **License** enter your Email Security key and click **Add**.

The add-on details appears.

4. Click **Save**.
5. Log out and log back in to Control Center to enable Email Security.

The **Email Security** page is now available only for users with **Manage Network** rights.

2.1.3. Provision Email Security Accounts (Bitdefender Partners only)

1. Log in to Control Center.
2. Go to the **Email Security** page.
3. Choose a managed company and click **Create Account** under the **Action** column.
A Email Security is created for the selected company.



Note

An error is returned when:

- The account creation failed
- An API returned an error

To open a Email Security console associated to a managed company, click **Open console** under the **Action** column.

2.2. Configure Email Security

To configure Email Security with your email service you need to follow these procedures:

1. [Add Domains](#)
2. [Configure Email Service](#)
3. [Add Mailboxes](#)

2.2.1. Add Domains

Add a domain to point to your mail server.

1. Navigate to **Products > Email Security > Product Configuration**.

2. Go to **Domains**.
3. Click **Add**.
4. Under **Domain** enter your domain name.
5. Under **Deliver To** enter the full hostname or IP address of your mail server.

**Note**

You can add additional [Inbound Mail](#) routes later.

6. Click **Add**

This enables a DKIM for your domain.

Find your domain in the list and click  to view the DKIM public key.

2.2.2. Configure Email Service

Use one of the following procedures to integrate your email service with Email Security.

1. [Microsoft Office 365](#)
2. [Microsoft Exchange](#)
3. [G Suite Gmail](#)

Microsoft Office 365

Follow these procedure to integrate Email Security with Microsoft Office 365, for inbound and outbound email delivery.

1. [Configure Email Security Inbound Mail](#)
2. [Configure Email Security Outbound Mail](#)
3. [Change MX Records](#)
4. [Configure Office 365 Inbound Mail](#)
5. [Configure Office 365 Outbound Mail](#)

Configure Email Security Inbound Mail

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Inbound Mail**.

3. Click **Add** to add a new delivery route.
4. Select your **Domain** from the drop-down list.
5. Under **Cost** set route priority.

The cost defines route priority for multiple routes. The lower the number, the higher the priority.

6. Under **Route** enter the following:

```
domain_name.mail.protection.outlook.com
```

7. **Update** to save changes.

Configure Email Security Outbound Mail

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Outbound Mail**.
3. Click **Add**.
4. Under **Hostname** enter the following hostname:

```
spf://spf.protection.outlook.com
```

5. **Update** to save changes.

Change MX Records

Change the MX Records of your domain, based on your region.

- For US and ROW:

```
mail1.us.scanscope.net  
mail2.us.scanscope.net
```

- For EU:

```
mta01.scanscope.net  
mail1.scanscope.net  
mail2.scanscope.net  
mail3.scanscope.net
```

**Note**

Wait at least an hour for the changes to come into effect in the DNS Servers.

Configure Office 365 Inbound Mail

Configure Office 365 to reject emails with an address source outside of Email Security.

1. Log in to your Office 365 Admin Center.
2. Navigate to **Admin Centers > Exchange**.
3. In the left pane, go to **Mail Flow > Rules**.
4. Click **+** and select **Create a new rule**.
5. Enter a name for your rule.
6. Click **More Options** at the bottom of the rule window.
7. From the **Apply this rule if** drop-down menu, select the following conditions:
The Sender > Is External/Internal > Outside the organization.
8. From the **Do the following** drop-down menu, select the following conditions:
Block the message > Reject the message with the Explanation.
9. Enter the message you want to include in the Non-Delivery-Report.
For example, you can use this message to notify the email sender: IP restricted, not using MX record. Please ensure your DNS is up-to-date and try sending this message again.
10. Click **Add exception**.
11. In **Sender > Sender's IP address is in the range or exactly matches** enter the following IPs based on your region.

- For US and ROW:

```
104.214.75.142
52.200.11.158
104.214.75.99
52.200.119.29
```

- For EU:

```
51.140.50.9
23.97.185.122
52.28.195.233
104.40.205.111
52.28.207.52
46.137.91.239
46.51.191.66
46.51.184.151
52.29.103.252
40.115.45.200
40.115.43.250
```

12. Click **+** to add the IP entries.
13. Click **OK** to confirm changes.
14. Click **Add exception**.
15. Go to the rule property and under **Match sender address in message**, select **Header or Envelope**.
Office 365 now rejects emails with an address source outside of Email Security.

Configure Office 365 Outbound Mail

Configure Office 365 to send emails only through Email Security.

1. Log in to your Office 365 Admin Center.
2. Navigate to **Admin Centers > Exchange**.
3. In the left pane, go to **Mail Flow > Connectors**.
4. Click **+** to add a new connector.
5. In the **From:** field select **Office 365**.
6. In the **To:** field select **Partner Organization**.
7. Enter a name for your connector.
8. Click **Next**.
9. Under **When do you want to use this connector?** select **Only when email messages are sent to these domains** then click **+** and enter *****.
10. Click **Next**.

11. Under **How do you want to route email messages** select **Route email through these smart hosts** and add the following hosts based on your region.

- For US and ROW:

```
smtp1.us.scanscope.net  
smtp2.us.scanscope.net
```

- For EU:

```
smtp1.scanscope.net  
smtp2.scanscope.net
```

12. Click **Next** and confirm changes.

Office 365 now sends emails only through Email Security. To add your mailboxes, refer to [Add Mailboxes](#).

Microsoft Exchange

Follow these procedures to integrate Email Security with Microsoft Exchange, for inbound and outbound email delivery.

1. [Configure Exchange Inbound Mail](#)
2. [Configure Exchange Outbound Mail](#)
3. [Update SPF Records \(Optional\)](#)
4. [Test Product Configuration](#)

Configure Exchange Inbound Mail

For inbound configuration, change the MX records and allow IP addresses for Email Security based on your region. To check for your account's cluster contact your MSP (if applicable).

Related Topics

- [US and ROW Cluster](#)
- [EU Cluster](#)

US and ROW Cluster

Configure the following:

- [MX Records \(Inbound\)](#)
- [IP Addresses](#)

MX Records (Inbound)

Change the MX records as follows:

```
mail1.us.scanscope.net  
mail2.us.scanscope.net
```

IP Addresses

The email delivery service operates using the SMTP port 25. Configure firewall rules to allow the following IP addresses:

```
104.214.75.142  
52.200.11.158  
104.214.75.99  
2.200.119.29
```



Important

Use actual IP addresses in your firewall, instead of hostnames.

EU Cluster

Configure the following:

- [MX Records \(Inbound\)](#)
- [IP Addresses](#)

MX Records (Inbound)

Change the MX records as follows:

```
mta01.scanscope.net  
mail1.scanscope.net  
mail2.scanscope.net  
mail3.scanscope.net
```

IP Addresses

The email delivery service operates using the SMTP port 25. Configure firewall rules to allow the following IP addresses:

```
51.140.50.9
23.97.185.122
52.28.195.233
104.40.205.111
52.28.207.52
46.137.91.239
46.51.191.66
46.51.184.151
52.29.103.252
40.115.45.200
40.115.43.250
```



Important

Use actual IP addresses in your firewall, instead of hostnames.

Configure Exchange Outbound Mail

Configure outbound mail (smart host) through the Exchange MailSafe connector. Set up the connector according to your Exchange version.

- [Exchange 2007/2010](#)
- [Exchange 2016](#)

Exchange 2007/2010

1. Log in to your Microsoft Exchange Server as an administrator.
2. Open Exchange Management Console.
3. In the left pane, expand and navigate to **Microsoft Exchange > Organization Configuration**.
4. Select **Hub Transport**.
5. In the middle pane, select the **Send Connectors** tab.
6. Delete any Send Connectors that are destined for the internet.
7. Create connectors for each sending host according to your cluster.

- For US and ROW open ports 25 and 587 and add the following hosts:

```
smtp1.us.scanscope.net (cost 10)
smtp2.us.scanscope.net (cost 10)
```

- For EU open ports 25 and 587 and add the following hosts:

```
smtp1.scanscope.net (cost 10)
smtp2.scanscope.net (cost 10)
```

8. In the right pane, select the **New Send Connector** link.
9. Enter the name according to your cluster, and select **Intended use as Internet**.
10. Select **Next**.
11. On the **Address Space** page, select the **Add** button to add an SMTP Address Space.
12. Enter the following values:
 - **Address Space** = *
 - **Cost** = 10
13. Click **OK** to create the connector.
14. Click **Next** to continue.
15. On the **Network Settings** page, select **Route Mail Through the following Smart Hosts**.
16. Click **Add** to add a smart host.
17. When prompted, select **Fully Qualified Domain Name** and the first hostname according to your cluster.
18. Click **Next**.
19. On the **Configure Smart Host Authentication settings** page, select **None**.
20. Click **Next**.

21. On the **Source Server** page, add any other Exchange Servers that should be able to send email to this connector. If there is only one server, it will already be added.
22. Click **Next**.
23. On the final page, click **New** to create the connector then **Finish**.

Exchange 2016

1. Log in to your Microsoft Exchange Server as an administrator.
2. Go to <https://your-exchange-servers-hostname/ecp> to open Exchange Admin Center.
3. In the left pane, select **mail flow > Connectors**.
4. Select the **+** icon to create a new send connector.
5. Enter an identifiable name for your connector such as "Email Security Mail Relay".
6. Set the type to **Custom**.
7. Select **Next**.
8. Specify the mail to be relayed by the option **Route mail through smart hosts**.
9. Select the **+** icon to create a new smart host.
10. Create connectors for each sending host according to your cluster.
 - For US and ROW open ports 25 and 587 and add the following hosts:

```
smtp1.us.scanscope.net (cost 10)
smtp2.us.scanscope.net (cost 10)
```

- For EU open ports 25 and 587 and add the following hosts:

```
smtp1.scanscope.net (cost 10)
smtp2.scanscope.net (cost 10)
```

11. Select **Next**.

12. Set **Smart Host Authentication** to **None**.
13. In the **Address space** select the **+** button to add a domain.
14. Enter the following values:
 - **Type** = SMTP
 - **Fully Qualified Domain Name** = *
 - **Cost** = 10
15. Click **Save**.
16. Select **Next**.
17. Select **Next**.
18. On the **Source Server** page, add any other Exchange Servers that should be able to send email to this connector by pressing the **+** button.
If there is only one server, it will already be added.
19. Click **Next**.
20. Click **Finish**.

Update SPF Records (Optional)

If you use an SPF record for your domain, update it as follows:

```
include: scanscope.net
```



Important

Enable outbound email only after the Time to Live (TTL) for the SPF has passed. Using `-all` in your SPF record causes the remote domain to reject your email if the TTL has not expired.

Test Product Configuration

To test the product configuration, you can use the following outbound connectivity tests.

For US and ROW Cluster

```
telnet smtp1.us.scanscope.net 25
telnet smtp2.us.scanscope.net 25
```

For EU Cluster

```
telnet smtp1.scanscope.net 25
telnet smtp2.scanscope.net 25
```

To add your mailboxes, refer to [Add Mailboxes](#).

G Suite Gmail

Follow these procedure to integrate Email Security with G Suite Gmail, for inbound and outbound email delivery.

1. [Configure Email Security Inbound Mail](#)
2. [Configure Email Security Outbound Mail](#)
3. [Configure G Suite Gmail Inbound Mail](#)
4. [Configure G Suite Gmail Outbound Mail](#)

Configure Email Security Inbound Mail

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Inbound Mail**.
3. Click **Add** to add a new delivery route.
4. Select your **Domain** from the drop-down list.
5. Under **Cost** set route priority to 5.

The cost defines route priority for multiple routes. The lower the number, the higher the priority.

6. Under **Route** enter the following: `ASPMX.L.GOOGLE.COM`
7. **Update** to save changes.
8. Repeat steps 3 to 7 to add the following routes and associated costs:

`ALT1.ASPMX.L.GOOGLE.COM` with the cost of 10

`ALT2.ASPMX.L.GOOGLE.COM` with the cost of 15

`ALT3.ASPMX.L.GOOGLE.COM` with the cost of 20

`ALT4.ASPMX.L.GOOGLE.COM` with the cost of 25

The final routes should look similar to the ones in the screenshot below.

gmaildomain.com	5	ASPMX.L.GOOGLE.COM
gmaildomain.com	10	ALT1.ASPMX.L.GOOGLE.COM
gmaildomain.com	15	ALT2.ASPMX.L.GOOGLE.COM
gmaildomain.com	20	ALT3.ASPMX.L.GOOGLE.COM
gmaildomain.com	25	ALT4.ASPMX.L.GOOGLE.COM

Configure Email Security Outbound Mail

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Outbound Mail**.
3. Click **Add**.
4. Under **Hostname** enter the following hostname:
`spf://_spf.google.com`
5. **Update** to save changes.

Configure G Suite Gmail Inbound Mail

Configure G Suite to reject emails with an address source outside of Email Security. Follow these procedures to configure G Suite Gmail Inbound Mail.

1. [Configure Inbound Gateways](#)
2. [Change MX Records](#)
3. [Reject Mail Sent from Outside of the Gateway](#)
4. [Configure Whitelist IP Addresses](#)

Configure Inbound Gateways

Configure the inbound gateway setting to identify the gateway's range of addresses. Add the Email Security IP addresses to the inbound gateway before changing the MX Records. This will prevent the messages from being quarantined.

**Note**

If you have inbound gateway entries listed in G Suite, add the Email Security entries from the following procedure. Remove existing entries, after you change the MX Records.

To configure inbound gateways:

1. Login to your G Suite Admin Console with an administrator account.
2. Navigate to **Apps > G Suite Core Services**.
3. Go to **Gmail > Settings**.
4. At the bottom of the page, click **Advanced Settings**.
5. Go to **Spam, phishing, and malware** to edit Inbound Gateways.
6. Enter a **Name** for the this configuration, such as Email Security.
7. Add the following Email Security IPs based on your region.

- For US and ROW:

```
104.214.75.142
52.200.11.158
104.214.75.99
2.200.119.29
```

- For EU:

```
51.140.50.9
23.97.185.122
52.28.195.233
104.40.205.111
52.28.207.52
46.137.91.239
46.51.191.66
46.51.184.151
52.29.103.252
40.115.45.200
40.115.43.250
```

8. Uncheck **Reject all mail not from gateway IPs**.

9. Ensure that this configuration is replicated to G Suite before changing any MX records.

**Note**

Inbound Gateway changes in G Suite can take up to one hour to come into effect. You can track changes in the [Admin console audit log](#).

Change MX Records

Change the MX Records of your domain, based on your region.

- For US and ROW:

```
mail1.us.scanscope.net  
mail2.us.scanscope.net
```

- For EU:

```
mta01.scanscope.net  
mail1.scanscope.net  
mail2.scanscope.net  
mail3.scanscope.net
```

**Note**

Wait at least an hour for the changes to come into effect in the DNS Servers.

To verify MX record change in G Suite:

1. Login to your G Suite Admin Console with an administrator account.
2. Navigate to **Apps > G Suite Core Services**.
3. Go to **Gmail > Settings**.
4. At the bottom of the page, click **Advanced Settings**.
5. Go to **MX Records** and verify the MX Records.

You should have a match with the Email Security records.

Reject Mail Sent from Outside of the Gateway

Configure inbound gateways to reject mail that was not sent from the gateway.

1. Login to your G Suite Admin Console with an administrator account.
2. Navigate to **Apps > G Suite Core Services**.
3. Go to **Gmail > Settings**.
4. At the bottom of the page, click **Advanced Settings**.
5. Go to **Spam, phishing, and malware** to edit Inbound Gateways.
6. Select the **Reject all mail not from gateway IPs** checkbox and click **Save**.
7. At the bottom of the **Advanced Settings** page, click **Save** to apply changes.

Configure Whitelist IP Addresses

Configure Whitelist IP addresses to ensure that messages received from specific sending IP addresses do not get quarantined.

1. Login to your G Suite Admin Console with an administrator account.
2. Navigate to **Apps > G Suite Core Services**.
3. Go to **Gmail > Settings**.
4. At the bottom of the page, click **Advanced Settings**.
5. Go to **Spam, phishing, and malware** to edit Inbound Gateways.
6. Under **Email whitelist** add the following Email Security service IP addresses:

```
51.140.50.9
46.137.91.239
104.40.205.111
23.97.185.122
52.28.207.52
52.28.195.233
```

7. At the bottom of the **Advanced Settings** page, click **Save** to apply changes.

Configure G Suite Gmail Outbound Mail

Configure G Suite to send emails only through Email Security. You will need to add a mail route and configure rules.

1. Login to your G Suite Admin Console with an administrator account.
2. Navigate to **Apps > G Suite Core Services**.



3. Go to **Gmail > Settings**.
4. At the bottom of the page, click **Advanced Settings**.
5. Go to **Hosts > Add Route**.
6. Enter a **Name** for the route, such as Email Security Outbound.
7. In the **Specify email server** select **Multiple hosts**.
8. Add a primary entry for each of the outbound servers based on your region.
 - For US and ROW open ports 25 and 587 and add the following hosts:

```
smtp1.us.scanscope.net  
smtp2.us.scanscope.net
```

- For EU open ports 25 and 587 and add the following hosts:

```
smtp1.scanscope.net  
smtp2.scanscope.net
```

Add mail route ✕

Cloud EMS Outbound Help

1. Specify email server

Multiple hosts ▾

Primary		Load %	ADD
smtp1.scanscope.net	: 25 ?	50	Delete
smtp2.scanscope.net	: 25 ?	50	Delete

Secondary		Load %	ADD
smtp2.scanscope.net	: 25 ?	50	Delete
smtp1.scanscope.net	: 25 ?	50	Delete

2. Options

Require secure transport (TLS)

Require CA signed certificate

CANCEL SAVE

9. Click **Save**.

10. Navigate back to **General settings > Routing > Routing** section.

11. Click **Configure for routing**.

The **Add settings** option appears.

12. Enter a **Name** for the rule, such as Email Security Outbound Rule.

13. Under **Messages to affect**(section 1), select **Outbound**.

14. Under **For the above types of messages, do the following**(section 3), select **Change route**.

15. Change **Normal routing** to Email Security Outbound Rule, created above.

16. (Optional) Under **Encryption (onward delivery only)**, select **Require Secure Transport (TLS)**.
17. Click **Add Settings** or **Save** if you are editing an existing configuration.
18. At the bottom of the **Advanced Settings** page, click **Save** to apply changes.

**Note**

It can take up to one hour for your settings to come into effect. You can track changes in the [Admin console audit log](#).

2.2.3. Add Mailboxes

Add your user mailboxes to Email Security. Each mailbox is associated to a user. You can choose to manually add user mailboxes for Microsoft Office 365, Exchange and G Suite Gmail. For Office 365, you can add your user mailboxes through Azure Active Directory. For more information, refer to [Adding Azure Active Directory](#).

1. Navigate to **Products > Email Security > Mailboxes**.
2. Click **Add** and enter a mailbox.
3. (Optional) Add a real name for better tracking.
4. Configure the following settings:
 - **Exec Tracking** to mark the mailbox as company executive and prevent CEO impersonation fraud.
 - **Manage Variants** to add multiple user names.
 - **Groups** to add or remove from specific Active Directory groups.
5. Press **Enter** to add the mailbox.

**Note**

For mailboxes without a valid domain refer to [Product Configuration](#) to add new domains.

2.3. Usage Scenarios

Follow these procedures to set up a typical Email Security configuration in your environment.

- [Configuring DKIM](#)

3. UNDERSTANDING MAIL FLOW

Email Security uses MX record redirect and outbound “Smart Host” configuration to control the mail flow.

The following diagram shows the relationships among the Email Security components.

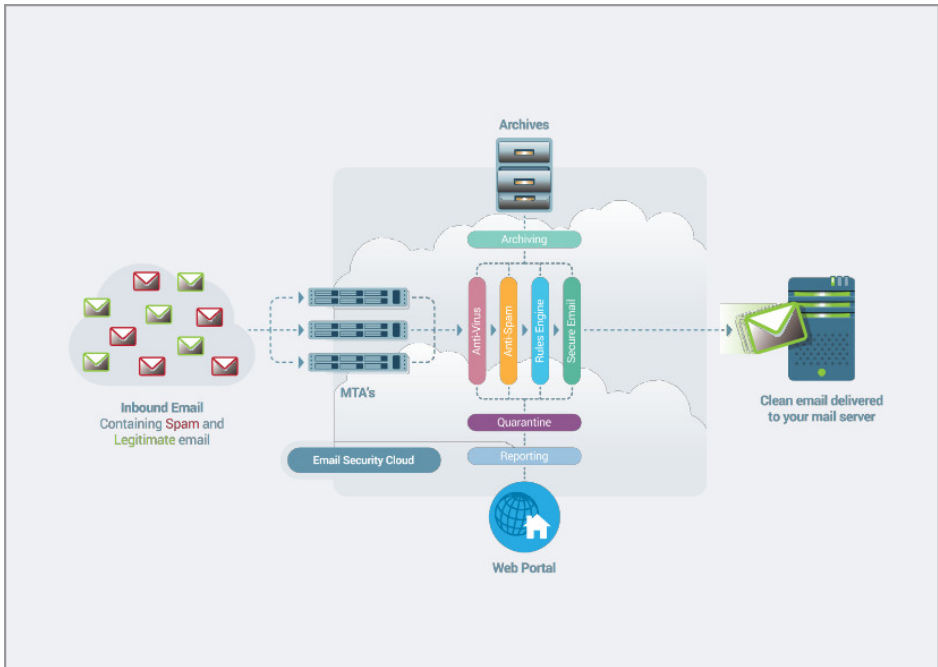


Figure 3-1 Mail Flow

4. MESSAGE RULES

- [Message Rule Overview](#)
- [Message Rule Priority](#)
- [Message Rule Direction](#)
- [Managing Message Rules](#)
- [Message Rule Cards](#)
- [System Message Rules](#)

4.1. Message Rule Overview

Message rules use a rule builder to control email traffic to and from your domains. The Rule Builder works by selecting conditions and applying actions to your emails.

4.2. Message Rule Priority

Message rules are processed in priority order. A lower priority number indicates a lower priority rule, whereas a higher priority number indicates a higher priority rule, and it is processed before the former.

Related Topics

- [Changing Message Rule Order](#)
- [Managing Active/Inactive Message Rules](#)

4.2.1. Changing Message Rule Order

1. Navigate to **Email Security > Message Rules**.
2. Select a rule and drag it to a new position within the list.



Note

System Rules cannot be reordered or edited.




4.2.2. Managing Active/Inactive Message Rules

1. Navigate to **Email Security > Message Rules**.
2. Select a message rule to open Rule Builder.

3. Set Active settings by toggling the **On/Off** button.
4. **Save** changes.

4.3. Message Rule Direction

Message rules are processed according to a predefined direction. The following table lists the direction for which the message rules are processed.

Direction	Description
	Message rule processed for incoming emails.
	Message rule processed for outgoing emails.
	Message rule processed for incoming and outgoing emails.

4.4. Managing Message Rules

The Rule Builder applies conditions and actions to a message, followed by a final action, after which the processing stops.

Related Topics

- [Adding Message Rules](#)
- [Editing Message Rules](#)
- [Deleting Message Rules](#)

4.4.1. Adding Message Rules

1. Navigate to **Product > Email Security > Message Rules**.
2. Select [icon] **Add Rule** at the upper-right corner.
A list of default rules appears.
3. Enter a name and select [icon] **Add**.
The Rule Builder appears.
4. Set Active settings by toggling the **On/Off** button.
5. Add a description to the message rule.
6. In the **Conditions** panel, select one or multiple cards then drag and drop them in the **Selected Conditions** column.

- Create specific conditions and avoid ambiguities.
7. Click [icon] **Configure** within the selected Condition card.
The configuration window appears.
 8. Configure settings and **Save** changes.
For more information, refer to [Conditions](#).
 9. In the **Actions** panel, select one or multiple cards then drag and drop them in the **Selected Actions** column.
The configuration window appears.
 10. **Configure** the Action card and **Save** changes.
For more information, refer to [Actions](#).
 11. In the **Final Actions** panel, select one or multiple cards then drag and drop them in the **Final Actions** column, if needed.
The configuration window appears.
 12. **Configure** the Final Action card and **Save** changes.
For more information, refer to [Final Actions](#).

**Note**

You can only add one Final Action.

13. Click **Save** at the upper-right corner of the window.
The message rule is saved and activated.
- Click **X** at the upper-right corner to close Rule Builder.

4.4.2. Editing Message Rules

1. Navigate to **Email Security > Message Rules**.
2. Select a message rule to open Rule Builder.
3. Configure settings and **Save** changes.

4.4.3. Deleting Message Rules

1. Navigate to **Email Security > Message Rules**.
2. Click **X** next to a message rule and select **Yes** to confirm changes.

4.5. Message Rule Cards

Message Rule Cards sorts components into conditions, actions and final actions.

Related Topics


- [Conditions](#)
- [Actions](#)
- [Final Actions](#)

4.5.1. Conditions


Conditions define matching criteria and values. You can select up to 8 conditions for each rule. The following table lists available conditions.

Condition	Description
Attachment Name	<p>Configure this condition to match email attachments.</p> <p>Select the Match Type and choose a Condition Value. You can choose between default values (Double extension, Office macro extensions) and your Custom Rule Data.</p>
Body	<p>Configure this condition to match the body of the email message.</p> <p>Select the Match Type and choose a Condition Value. You can choose between default values (Homophobic Content, Sexually Explicit) and your Custom Rule Data.</p>
Body or Subject	<p>Configure this condition to match the body or the subject of the email message.</p> <p>Select the Match Type and choose a Condition Value. You can choose between default values (Racist Content, Redirect Spam URLs) and your Custom Rule Data.</p>
Connection IP	<p>Configure this condition to match the remove server connection IP.</p> <p>Select the Match Type and choose a Condition Value. You can choose between default values (LocalHost) and your Custom Rule Data.</p>


Condition	Description
Core Service	<p>Configure this condition to match the email reputation as determined by the core anti-spam service.</p> <p>Select the Match Type and choose a Condition Value. You can choose between default values (CoreService Spam) and your Custom Rule Data.</p>
Direction	<p>Configure this condition to match the direction of the mail flow.</p> <p>Select the Inbound or Outbound as a Condition Value. To process both inbound and outbound, do not use the Direction card.</p>
DKIM Enabled	<p>Configure this condition to determine if DKIM is enabled for your account.</p> <p>Select the Match Type and choose a Boolean Condition Value.</p>
DKIM Signature	<p>Configure this condition to match the DKIM signature result.</p> <p>Select the Match Type and choose a Condition Value.</p>
DMARC Failure	<p>Configure this condition to match the failed action to carry out from the remote DNS record.</p> <p>Select the Match Type and choose a Condition Value.</p>
DMARC Policy	<p>Configure this condition to match the DMARC policy result.</p> <p>Select the Match Type and choose a Condition Value.</p>
Domain Threat Level	<p>Configure this condition to match high-risk domains.</p> <p>Select the Match Type and choose a Condition Value.</p>
E-mail Size	<p>Configure this condition to match the size of the email.</p> <p>Select the Match Type and choose a Condition Value.</p>
E-mail Sandbox - Level 1	<p>Configure this condition to send email attachments to the Level 1 Sandbox.</p> <p>Select the Match Type and choose a Condition Value.</p>
Executive Tracking	<p>Configure this condition to match CEO impersonation fraud.</p> <p>Select the Match Type and choose a Condition Value.</p>
Fake Sender Headers	<p>Configure this condition to match spoofing emails.</p> <p>Select the Match Type and choose a Boolean Condition Value.</p>

Condition	Description
File Type	Configure this condition to match email attachment file types. Select the Match Type and choose a Condition Value .
Group Membership	Configure this condition to match synchronized Active Directory group types. Select the Match Type and choose a Condition Value .
Image Analyser	Configure this condition to match NSFW image content within email attachments and Office documents. Select the Match Type and choose a Condition Value .
IP Reputation	Configure this condition to match the sender's IP reputation. Select the Match Type and choose a Condition Value .
Mailbox Exists	Configure this condition to match existing mailboxes. Select the Match Type and choose a Condition Value .
Message Security	Configure this condition to match encrypted and digitally signed messages. Select the Match Type and choose a Condition Value .
MX Record	Configure this condition to match the hostname responding to SMTP requests. Select the Match Type and choose a Boolean Condition Value .
Nearby Domains	Configure this condition to match nearby domains. Select the Match Type and choose a Condition Value between 1 and 10 . The value is based on the number of your domain's characters. Longer domain names require a higher value, whereas shorter ones require lower values.  Note Set the Condition Value to 3 as a starting point and increase, if necessary. Consider using this condition with the Add to Spam Score action and set a score of 108 for the latter.
Own Domain	Configure this condition to match a sender configured as a domain for your account.



Condition	Description
	Select the Match Type and choose a Boolean Condition Value .
Protected Attachment	Configure this condition to match password-protected email attachments. Select the Match Type and choose a Boolean Condition Value .
Recipient	Configure this condition to match the recipient of the email message. Select the Match Type and choose a Condition Value . You can choose between (AD Export) and your Custom Rule Data .
Recipient Count	Configure this condition to match the number of recipients. Select the Match Type and choose a Condition Value .
Sender	Configure this condition to match email sender. Select the Match Type and choose a Condition Value . You can choose from your Regex Rules .
Sender in List	Configure this condition to match sender lookup. Select the Match Type and choose a Condition Value .
Sending Domain MX	Configure this condition to match invalid sending domain MX Records. Select the Match Type and choose a Condition Value .
Spam Score	Configure this condition to match the Email Security spam score. Select the Match Type and choose a Condition Value . <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Note To adjust the score, consider using this condition with Add to Spam Score, Set Spam Score, or Subtract from Spam Score Subtract from Spam Score actions.</p> </div> </div>
SPF	Configure this condition to match domain SPF status. Select the Match Type and choose a Condition Value .
Subject	Configure this condition to match the subject of the email message.





Condition	Description
	Select the Match Type and choose a Condition Value . You can choose between default values (Homophobic Content , Sexually Explicit) and your Custom Rule Data .
URL Scanner	Configure this condition to match URL scanning. Select the Match Type and choose a Condition Value .
Virus Ruleset	Configure this condition to match malware presence in macros, VBA scripts, and Office documents. Select the Match Type and choose a Condition Value .
Virus Score	Configure this condition to match the virus score. Select the Match Type and choose a Condition Value . <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;">  </div> <div> <p>Note To adjust the score, consider using this condition with Add to Virus Score, Set Virus Score or Subtract from Virus Score actions.</p> </div> </div>

4.5.2. Actions

Actions start processing emails based on matching conditions. You can select up to 8 actions for each rule. The following table lists available actions.

Action	Description
Add Message Header	Configure this action to add a custom header to the email. You can add any value, such as nametags.
Add to Global Quarantine	Configure this action to save a copy of the email message in the Global Quarantine. Select the Value from the dropdown list.
Add to Spam Score	Configure this action to increase the spam score. Enter the amount in the Value field.
Add to Virus Score	Configure this action to increase the virus score. Enter the amount in the Value field.



Action	Description
Append HTML	Configure this action to add an HTML snippet to the email body.
Append Text	Configure this action to add a plain text to the email body.
Append to Subject	Configure this action to add a plain text to the email subject.
DKIM Signing	Configure this action to add DKIM signature.
DKIM Verification Required	Configure this action to configure the type of DMARC verification required to pass. Select the Value from the dropdown list.
Linkscan	Configure this action to apply on-demand link scanning to URLs in the email body. Select the Value from the dropdown list.
Notify Recipient	Configure this action to send a customized message to the email recipient. Configure sender and recipient addresses, and create the customized message. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>Note This action requires the Direction condition set to Inbound.</p> </div> </div> Select the Value from the dropdown list.
Notify Sender	Configure this action to send a customized message to the email sender. Configure sender and recipient addresses, and create the customized message. Select the Value from the dropdown list. <div style="display: flex; align-items: flex-start;"> <div style="margin-right: 10px;"></div> <div> <p>Note This action requires the Direction condition set to Outbound.</p> </div> </div>
Prefix HTML	Configure this action to add a prefix HTML snippet to the email body. Use Prefix Text for email clients that do not display HTML.

Action	Description
Prefix Text	Configure this action to add a prefix plain text to the email body.
Prefix to Subject	Configure this action to add a prefix plain text to the email subject.
Re-Route to	Configure this action to re-route to a specific mail server.
Save Copy in Quarantine	Configure this action to save a copy in Quarantine. Select the Value from the dropdown list.
Save Copy to	Configure this action to send a copy to another recipient. Select the Value from the dropdown list.
Set Spam Score	Configure this action to set a Spam Score value. Enter the amount in the Value field.
Set Virus Score	Configure this action to set a Virus Score value. Enter the amount in the Value field.
Strip & Replace	Configure this action to strip attachments with text files if any threat is found.
Subtract from Spam Score	Configure this action to decrease the Spam Score. Enter the amount in the Value field.
Subtract from Virus Score	Configure this action to decrease the Virus Score. Enter the amount in the Value field.

4.5.3. Final Actions

Final Actions end email processing after selecting the last step. You can select only one final action. The following table lists available final actions.

Final Action	Description
Quarantine	Configure this final action to place the email in the selected quarantine area. Select the Value from the dropdown list.
Quarantine - Company	Configure this final action to place the email in the company quarantine area.

Final Action	Description
	Select the Value from the dropdown list.
Delete	Select this final action to delete the email.
Deliver	Select this final action to deliver the email to the specified destination server.

4.6. System Message Rules

System Message Rules provide an initial set to your email security and protects you from most threats. You can override system message rules with your own rules but cannot reorder or edit them.

Examine System Rules to explore the email security engine and get insights on how to create rules based on your organization's needs. The following table lists available default message rules.

System Message Rule	Description
(Default) Apply DKIM Signing Subtract from Virus Score	Applies a DKIM entry to outbound emails.
(Default) Bitdefender AV	Scans email messages and attachments using Bitdefender. Adds 110 to virus score if malware is found.
(Default) Blog Spam	Scans emails for known blog spam entries and adds 110 to spam score if it finds any.
(Default) CoreService Malware	Scans and tags emails as Malware detected. Adds to virus score based on heuristic detections.
(Default) CoreService Phishing	Scans and tags emails as Phishing attempts. Adds to spam score based on heuristic analysis.
(Default) CoreService Spam	Scans and tags emails as known Spam. Adds to spam score.
(Default) DMARC Fail	Scans inbound emails for failed DMARC. Emails with failed DMARC results are quarantined.
(Default) Domain Tools Threat Intelligence	Scans for known threat domains and adds 110 to spam score if it finds any.



System Message Rule	Description
(Default) Invalid Sending Domain	Checks connectivity to the sender domain's MX record and host. Adds 110 to spam score if the validation is not triggered.
(Default) Password Protected Attachment	Adds a message header to password protected attachments.
(Default) Signature Verification	Adds a message header with verification results (pass/fail).
(Default) SWL Safe List	Runs an RBL lookup on the Global Safe List to check for whitelist matches. For any matching entry, it subtracts 100 from the spam score.
(Default) URL Scanner	Applies on-demand link scanning to URLs in the email body.

5. CONNECTION RULES

- [Connection Rules Overview](#)
- [Connection Rule Priority](#)
- [Connection Rule Direction](#)
- [Managing Connection Rules](#)
- [Connection Rule Cards](#)
- [System Connection Rules](#)

5.1. Connection Rules Overview

Connection rules use a rule builder to control connection attempts to and from your mailboxes. The Rule Builder works by selecting conditions and applying actions to your emails.

5.2. Connection Rule Priority

Message rules are processed in priority order. A lower priority number indicates a lower priority rule, whereas a higher priority number indicates a higher priority rule, and it is processed before the former.

Related Topics

- [Changing Connection Rule Order](#)
- [Managing Active/Inactive Connection Rules](#)

5.2.1. Changing Connection Rule Order

1. Navigate to **Email Security > Connection Rules**.
2. Select a rule and drag it to a new position within the list.



Note

System Rules cannot be reordered or edited.




5.2.2. Managing Active/Inactive Connection Rules

1. Navigate to **Email Security > Connection Rules**.

2. Select a message rule to open Rule Builder.
3. Set Active settings by toggling the **On/Off** button.
4. **Save** changes.

5.3. Connection Rule Direction

Connection rules are processed according to a predefined direction. The following table lists the direction for which the message rules are processed.

Direction	Description
	Rule processed for incoming connections.
	Rule processed for outgoing connections.
	Rule processed for incoming and outgoing emails.

5.4. Managing Connection Rules

Related Topics

- [Adding Connection Rules](#)
- [Editing Connection Rules](#)
- [Deleting Connection Rules](#)

5.4.1. Adding Connection Rules

1. Navigate to **Products Email > Security > Connection Rules**.
2. Select [icon] **Add Rule** at the upper-right corner.
A list of default rules appears.
3. Enter a name and select [icon] **Add**.
The Rule Builder appears.
4. Set Active settings by toggling the **On/Off** button.
5. Add a description to the connection rule.
6. In the **Conditions** panel, select one or multiple cards then drag and drop them in the **Selected Conditions** column.

- Create specific conditions and avoid ambiguities.
7. Click [icon] **Configure** within the selected Condition card.
The configuration window appears.
 8. Configure settings and **Save** changes.
For more information, refer to [Conditions](#).
 9. In the **Actions** panel, select one or multiple cards then drag and drop them in the **Selected Actions** column.
The configuration window appears.
 10. **Configure** the Action card and **Save** changes.
For more information, refer to [Actions](#).
 11. In the **Final Actions** panel, select one or multiple cards then drag and drop them in the **Final Actions** column, if needed.
The configuration window appears.
 12. **Configure** the Final Action card and **Save** changes.
For more information, refer to [Final Actions](#).

**Note**

You can only add one Final Action.

13. Click **Save** at the upper-right corner of the window.
The message rule is saved and activated.
- Click **X** at the upper-right corner to close Rule Builder.

5.4.2. Editing Connection Rules

1. Navigate to **Email Security > Connection Rules**.
2. Select a message rule to open Rule Builder.
3. Configure settings and **Save** changes.

5.4.3. Deleting Connection Rule

1. Navigate to **Email Security > Connection Rules**.
2. Click **X** next to a message rule and select **Yes** to confirm changes.

5.5. Connection Rule Cards

Connection Rules Cards sorts components into conditions and final actions.

Related Topics

- [Conditions](#)
- [Final Actions](#)

5.5.1. Conditions

Conditions define matching criteria and values. You can select up to 8 conditions for each rule. The following table lists available conditions.

Condition	Description
Connection IP	<p>Configure this condition to match the remove server connection IP.</p> <p>Select the Match Type and choose a Condition Value. You can choose between default values (LocalHost) and your Custom Rule Data.</p>
Direction	<p>Configure this condition to match the direction of the mail flow.</p> <p>Select the Inbound or Outbound as a Condition Value. To process both inbound and outbound, do not use the Direction card.</p>
E-mail Size	<p>Configure this condition to match the size of the email.</p> <p>Select the Match Type and choose a Condition Value.</p>
IP Reputation	<p>Configure this condition to match the sender's IP reputation.</p> <p>Select the Match Type and choose a Condition Value.</p>
Mailbox Exists	<p>Configure this condition to match existing mailboxes.</p> <p>Select the Match Type and choose a Condition Value.</p>
Recipient	<p>Configure this condition to match the recipient of the email message.</p> <p>Select the Match Type and choose a Condition Value. You can choose between (AD Export) and your Custom Rule Data.</p>

Condition	Description
Sender	Configure this condition to match email sender. Select the Match Type and choose a Condition Value . You can choose from your Regex Rules .
Sender in List	Configure this condition to match sender lookup. Select the Match Type and choose a Condition Value .
Sender IP Geolocation	Configure this condition to match a specific country. Select the Match Type and choose a Country

5.5.2. Final Actions

Final Actions end email processing after selecting the last step. You can select only one final action. The following table lists available final actions.

Final Action	Description
Permanent Reject	Configure this final action to permanently reject a message and provide a status code. Select the status code from the Value drop-down.
Accept	Use this final action to accept a message and continue processing with Message Rules.

5.6. System Connection Rules

System Connection Rules provide an initial set to your mailbox connections. You can override system message rules with your own rules but cannot reorder or edit them.

Examine System Rules to get insights on how to create rules based on your organization's needs. The following table lists available default message rules.

System Connection Rules	Description
(Locked) DHA	Rejects emails for non-existing mailboxes.
Default) Spamhaus	Rejects emails based on IP blacklist.
(Default) Spam RBL	Rejects emails based on crows sourced and community supported IP blacklist.



System Connection Rules	Description
(Default) Invalid MX Record	Rejects emails if the MX record is invalid.

6. CUSTOM RULE DATA

- [Custom Rule Data Overview](#)
- [Managing Rule Data](#)

6.1. Custom Rule Data Overview

Custom Rule Data adds customized information and specific entries to enhance [Message Rules](#) and [Connection Rules](#).

6.2. Managing Rule Data

- [Adding Rule Data](#)
- [Editing Rule Data](#)
- [Deleting Rule Data](#)

6.2.1. Adding Rule Data

1. Navigate to **Products > Email Security > Custom Rule Data**.
2. Click **New** at the bottom of the **Custom Rule Data** column.
3. Select:
 - **Rule Data** to define matching text values.
 - **Rule RegEx** to define matching patterns.
4. Enter a name and click **Update**.
5. Under Value, add:
 - For **Rule Data**: text values
 - For **Rule RegEx**: symbols, groups and ranges, assertions

**Note**

Keep each value as a separate line.
For RegEx use /n to add a new line.

6. Click **Save**.

The rule data is ready to be used in custom message and connection rules.



6.2.2. Editing Rule Data

1. Navigate to **Products > Email Security > Custom Rule Data**.
2. Select an item under the **Custom Rule Data** column.
3. Configure settings and **Save** changes.

6.2.3. Deleting Rule Data

1. Navigate to **Products > Email Security > Custom Rule Data**.
2. Select an item under the **Custom Rule Data** column.
3. Click **Delete** and select **Yes** to confirm changes.

7. GLOBAL QUARANTINE

Global Quarantine holds quarantined items tagged as Virus or Spam.


7.1. Global Quarantine

1. [Running Quarantine Reports](#)
2. [Viewing Quarantine Messages](#)
3. [Taking Actions](#)

7.1.1. Running Quarantine Reports

1. Navigate to **Products Email > Security > Global Quarantine**.
2. Select a timespan from the drop-down list or specify your own period.
3. Choose **Quarantine** tag.
4. Set the following **Filters**:
 - a. **Connection**
Choose email **Direction** (Incoming/Outgoing).
 - b. **Rules**
Choose a **Message Rule** Message Rule from the drop-down list.
 - c. **Content**
Enter **Sender/Recipient** and **Subject**.
5. **Run Report** to view the messages.

7.1.2. Viewing Quarantine Messages

1. Navigate to **Products Email > Security > Global Quarantine**.
2. Click  next to the message.
The **Message Details** windows appears.
3. Navigate through the following tabs:
 - **General** for email summary and activity reports.
 - **Actions** for matching rule actions.

- **Header** for detailed breakdown of all message headers.
You can export headers to CSV or Excel supported file formats.
 - **Server Log** for detailed server interaction.
You can export server logs to CSV or Excel supported file formats.
4. Click **X** to close the window.
 5. Click the email subject to preview the message content.


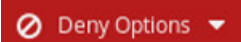
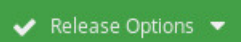


Note

To add or remove columns in the table, select the column header filter button and check/uncheck sections.

7.1.3. Taking Actions

The following table lists available actions for quarantined messages.

Action	Description
Delete	Click  Delete to remove a message from Global Quarantine.
Deny	Click  Deny Options and select from the following options: <ul style="list-style-type: none"> ● Deny Sender to block existing and upcoming email delivery from the sender. ● Deny Domain to block existing and upcoming email delivery from the domain.
Release	Click  Release Options and select from the following options: <ul style="list-style-type: none"> ● Release to dismiss the email from the quarantine. ● Safe Sender to dismiss the email from the quarantine and add the sender to the Global Safe List. ● Safe Domain to dismiss the email from the quarantine and add the domain sender to the Global Safe List.

8. GLOBAL DENY LIST

- [Global Deny List Overview](#)
- [Viewing Global Deny List](#)
- [Managing Global Deny List](#)

8.1. Global Deny List Overview

Global Deny List holds rejected mailboxes, domains and IP addresses as list entries. Its behavior is subject to **Message Rules** and **Connection Rules**.

8.2. Viewing Global Deny List

1. Navigate to **Products > Email Security > Global Deny List**.
2. Use the search bar at the top or scroll through the list.

8.3. Managing Global Deny List

- [Adding Entries](#)
- [Editing Entries](#)
- [Deleting Entries](#)

8.3.1. Adding Entries

1. Navigate to **Products > Email Security > Global Deny List**.
2. Click **Add** and enter an entry.



Note

You can add full specific mailboxes, domains or IP addresses.
To add domains associated to the Email Security account, use the IP addresses.

3. Click **Update** to save changes.


8.3.2. Editing Entries

1. Navigate to **Products > Email Security > Global Deny List**.
2. Double click an entry to edit



3. Click **Update** to save changes.

8.3.3. Deleting Entries

1. Navigate to **Products > Email Security > Global Deny List**.
2. Select individual or multiple entries.
To select all, click the column header checkbox.
3. Click  **Remove** and select **Yes** to confirm changes.

9. GLOBAL SAFE LIST

- [Global Safe List Overview](#)
- [Viewing Global Safe List](#)
- [Managing Global Safe List](#)

9.1. Global Safe List Overview

Global Safe List holds rejected mailboxes, domains and IP addresses as list entries. Its behavior is subject to **Message Rules** and **Connection Rules**.

9.2. Viewing Global Safe List

1. Navigate to **Products > Email Security > Global Safe List**.
2. Use the search bar at the top or scroll through the list.

9.3. Managing Global Safe List

- [Adding Entries](#)
- [Editing Entries](#)
- [Deleting Entries](#)

9.3.1. Adding Entries

1. Navigate to **Products > Email Security > Global Safe List**.
2. Click **Add** and enter an entry.

**Note**

You can add full specific mailboxes, domains or IP addresses.
To add domains associated to the Email Security account, use the IP addresses.

3. Click **Update** to save changes.


9.3.2. Editing Entries

1. Navigate to **Products > Email Security > Global Safe List**.
2. Double click an entry to edit



3. Click **Update** to save changes.

9.3.3. Deleting Entries

1. Navigate to **Products > Email Security > Global Safe List**.
2. Select individual or multiple entries.
To select all, click the column header checkbox.
3. Click  **Remove** and select **Yes** to confirm changes.

10. MAILBOXES

- [Adding Mailboxes](#)
- [Importing Mailboxes from Exchange Online](#)
- [Editing Mailboxes](#)
- [Deleting Mailboxes](#)

10.1. Adding Mailboxes

1. Navigate to **Products > Email Security > Mailboxes**.
2. Click **Add** and enter a mailbox.
3. (Optional) Add a real name for better tracking.
4. Configure the following settings:
 - **Exec Tracking** to mark the mailbox as company executive and prevent CEO impersonation fraud.
 - **Manage Variants** to add multiple user names.
 - **Groups** to add or remove from specific Active Directory groups.
5. Press **Enter** to add the mailbox.



Note

For mailboxes without a valid domain refer to [Product Configuration](#) to add new domains.

10.2. Importing Mailboxes from Exchange Online

1. Open your Exchange Online Admin Center and go to **Mailboxes**.
2. Select **Export data to a CSV file**.

To include aliases in the CSV file, check the **Email Address** field when you select the columns of data you would like to export.
3. Click **Export**.
4. Navigate to **Products > Email Security > Mailboxes**.

5. Click **Import** and select the CSV file you downloaded from the Exchange Online Admin Center.
6. Confirm your action by clicking **Import**.



Important

If the email addresses you import are not part of a domain that Email Security is already tracking, the new mailboxes will fail to import. You can add new domains by visiting [Product Configuration](#). Mailboxes will also fail to import if they already exist.



Note


To create your own CSV file, you need to add EMAIL ADDRESSES as the header line and individual email addresses for each line, as follows:

```
"EMAIL ADDRESS"  
"email@domain.com"
```

10.3. Editing Mailboxes

1. Navigate to **Products > Email Security > Mailboxes**.
2. Double click an mailbox to edit
3. Click **Update** to save changes.

10.4. Deleting Mailboxes

1. Navigate to **Products > Email Security > Mailboxes**.
2. Select individual or multiple mailboxes.
To select all, click the column header checkbox.
3. Click  **Remove** and select **Yes** to confirm changes.



Note

Deleting mailboxes only ends mailbox synchronization for the selected email addresses.

11. PRODUCT CONFIGURATION

- [Product Configuration Overview](#)
- [Domains](#)
- [Inbound Mail](#)
- [Outbound Mail](#)
- [Disclaimer](#)
- [Custom Quarantine](#)

11.1. Product Configuration Overview

Product Configuration allows you to further set up Email Security.

11.2. Domains

- [Adding Domains](#)
- [Editing Domains](#)
- [Deleting Domains](#)

11.2.1. Adding Domains

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Domains**.
3. Click **Add**.
4. Under **Domain** enter a domain name.
5. Under **Deliver To** enter the full hostname or IP address of your mail server.



Note

You can add additional [Inbound Mail](#) routes later.

6. Click **Add**

This enables a DKIM for your domain.


Find your domain in the list and click  to view the DKIM public key.

11.2.2. Editing Domains

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Domains**.
3. Double click a domain to edit.
4. Click **Update** to save changes.

Domain name change results in modified DKIM public key.

11.2.3. Deleting Domains

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Domains**.
3. Find your domain in the list.
4. Click  **Remove** and select **Yes** to confirm changes.



Note

Domain removal disrupts mail flow. Update MX records for removed domains.

11.3. Inbound Mail

- [Adding Inbound Routes](#)
- [Editing Inbound Routes](#)
- [Deleting Inbound Routes](#)

11.3.1. Adding Inbound Routes

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Inbound Mail**.
3. Click **Add**.
4. Select **Domain** from the drop-down list.
5. Under **Cost** set route priority.

The lower the number, the higher the priority.

**Note**


The cost defines route priority for multiple routes.

6. Under **Route** enter a full hostname or IP address as new route.
7. **Update** to save changes.

11.3.2. Editing Inbound Routes

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Inbound Mail**.
3. Double click a domain to edit.
4. Click **Update** to save changes.

11.3.3. Deleting Inbound Routes

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Inbound Mail**.
3. Find your domain in the list.
4. Click  **Remove** and select **Yes** to confirm changes.

**Note**

Route removal disrupts mail flow.

11.4. Outbound Mail

- [Adding Outbound Routes](#)
- [Editing Outbound Routes](#)
- [Deleting Outbound Routes](#)

11.4.1. Adding Outbound Routes


1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Outbound Mail**.
3. Click **Add**.

4. Under **Hostname** enter a full hostname or IP address as new route.
5. **Update** to save changes.

11.4.2. Editing Outbound Routes

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Outbound Mail**.
3. Double click a domain to edit.
4. Click **Update** to save changes.

11.4.3. Deleting Outbound Routes

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Outbound Mail**.
3. Find your domain in the list.
4. Click  **Remove** and select **Yes** to confirm changes.



Note

Route removal disrupts mail flow.

11.5. Disclaimer

Use the following procedure to set up an HTML disclaimer message for outbound emails.

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Disclaimer**.
3. Select the **Domain** from the drop-down list.
4. Enter your message in the text box.
5. (Optional) Use the editing toolbars at the top of the text box.
6. Select the **Activate this disclaimer** checkbox.
7. Select **Apply Changes**.

11.6. Custom Quarantine

[Custom Quarantine Overview](#)

[Managing Custom Quarantine](#)

11.6.1. Custom Quarantine Overview

The [Global Quarantine](#) holds quarantined items tagged as Virus or Spam but you can add custom tags.

11.6.2. Managing Custom Quarantine

- [Adding Quarantine Tags](#)
- [Editing Quarantine Tags](#)
- [Deleting Quarantine Tags](#)

Adding Quarantine Tags

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Custom Quarantine**.
3. Click **Add**.
4. Select **Permit User Access**.
5. **Update** to save changes.

Editing Quarantine Tags

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Custom Quarantine**.
3. Double click a quarantine tag to edit.
4. Click **Update** to save changes.

Deleting Quarantine Tags

1. Navigate to **Products > Email Security > Product Configuration**.
2. Go to **Custom Quarantine**.
3. Find your quarantine tag in the list.



4. Click  **Remove** and select **Yes** to confirm changes.

12. ACTIVE DIRECTORY

- [Active Directory Overview](#)
- [Adding Azure Active Directory](#)

12.1. Active Directory Overview

Active Directory allows you to configure mailbox synchronizations for Microsoft Office 365 configurations. Follow this procedure to synchronize your Office 365 mailboxes through Azure Active Directory.

12.2. Adding Azure Active Directory

1. Navigate to **Products > Settings > Active Directory**.
2. Click [icon] **Add Domain** at the upper-right corner and choose **Azure Active Directory**

The Azure Active Directory Domain configuration window appears.

3. Configure the following Azure Active Directory settings:
 - **Domain** to enter a name of your choice.
 - **Source name/IP** to enter your Azure tenant name (name.onmicrosoft.com).
 - **Email addresses** to exclude mailbox synchronization.
 - **Default Prefix** to specify default phone prefix.
 - **Phone numbers** to exclude phone number synchronization.
 - **Only synchronize users with this attribute set** to specify a [User Property from the Graph API](#).
 - **name** = officeLocation
 - **value** = London;Paris



Note

To specify multiple strings, use a semicolon ;

4. Click **Add Domain**.



You are redirected to the Microsoft login page associated to the Azure tenant name

5. Sign in to Microsoft and **Accept** the permissions requested by Email Security. Mailbox synchronization with Azure Active Directory can take up to 15 minutes.

**Note**

To correctly sync from Active Directory, a user must have a matching domain and associated first name, last name, email address, and phone number. If the user object cannot be synchronized, a triangle icon appears next to the user name.

13. GROUP MANAGEMENT

Group Management Overview

Managing Groups

13.1. Group Management Overview

Group Management allows you to view and apply Exec Tracking on Active Directory groups.

13.2. Managing Groups

- [Adding Groups](#)
- [Editing Groups](#)
- [Deleting Groups](#)


13.2.1. Adding Groups

1. Navigate to **Products > Email Security > Group Management**.
2. Click **Add** and enter a name.
3. Select **Exec Tracking** to mark the group as company executives and prevent CEO impersonation fraud.
4. Hit **Enter** to add the group.

13.2.2. Editing Groups

1. Navigate to **Products > Email Security > Group Management**.
2. Double click a group to edit.
3. Hit **Enter** to save changes.

13.2.3. Deleting Groups

1. Navigate to **Products > Email Security > Group Management**.
2. Find your group in the list.
3. Click  **Remove** and select **Yes** to confirm changes.

14. ANALYTICS

- [Analytics Overview](#)
- [Reports](#)
- [Charts](#)

14.1. Analytics Overview

Analytics provide insights to email activity through reports and charts.

14.2. Reports

- [Reports Overview](#)
- [Managing Reports](#)
- [Report Types](#)

14.2.1. Reports Overview

Generate customized reports to view email activity.

14.2.2. Managing Reports

- [Generating Reports](#)
- [Viewing Saved Reports](#)
- [Deleting Reports](#)

Generating Reports

1. Navigate to **Products > Analytics**.
2. Under **Reports & Charts**, select a report to open a tab on the right side.
3. Configure the **Filter** settings available for your [report type](#).
4. **Run Report** to view results.
5. (Optional) Save the report to [Saved Reports](#):
 - a. Click the menu button at the upper-right side of the table and select **Save**.
 - b. Enter a report title and **Save** changes.

You can use this report to create [Scheduled Reports](#).


**Note**

Select **Favourite** to add it to the Favourite list.

Viewing Saved Reports

1. Navigate to **Products > Analytics**.
2. Go to **Saved**.
3. Click a saved report to view results.
4. (Optional) Select the **Favourite** checkbox to add it to the Favourite list.

Deleting Reports


1. Navigate to **Products > Analytics**.
2. Go to **Saved**.
3. Find your report in the list.
4. Click  **Delete** and confirm changes.

**Note**

Deleting a report removes any associated schedules.

14.2.3. Report Types

The following table lists available report types.

Report	Description
Email Activity	<p>The results provide a list of primary mailboxes that have sent or received at least one email during the specified period.</p> <p> Note To filter by content, run the report individually for senders or for recipients.</p>

14.3. Charts

- [Chart Reports Overview](#)
- [Managing Chart Reports](#)
- [Chart Report Types](#)

14.3.1. Chart Reports Overview

Generate customized reports to view email activity.

14.3.2. Managing Chart Reports

- [Generating Chart Reports](#)
- [Viewing Chart Reports](#)
- [Merging Chart Reports](#)
- [Deleting Chart Reports](#)

Generating Chart Reports

1. Navigate to **Products > Analytics**.
2. Under **Reports & Charts**, select a chart report to open a tab on the right side.
3. Configure the **Filter** settings available for your [chart report type](#).
4. **Run Report** to view results.
5. (Optional) Save the report to [Saved Reports](#):
 - a. Click the menu button at the upper-right side of the table and select **Save**.
Alternatively, you can choose to download the chart in one of the available file format, or to print it.
 - b. Enter a report title and **Save** changes.
You can use this report to create [Scheduled Reports](#).



Note

Select **Favourite** to add it to the Favourite list.


Viewing Chart Reports

1. Navigate to **Products > Analytics**.
2. Go to **Saved**.
3. Click a saved chart report to view results.
Alternatively, you can view favourite reports in the Favourite list.

Merging Chart Reports

1. Navigate to **Products > Analytics**.
2. Click the menu button right next to the search bar to open the dropdown menu.
3. Select **Combine charts**.
4. Enter a chart report name.
5. Check your chart reports.
6. (Optional) Check **Make favourite** to add it to the Favourite list.
7. Select **Combine**.

Deleting Chart Reports

1. Navigate to **Products > Analytics**.
2. Go to **Saved**.
3. Find your chart report in the list.
4. Click  **Delete** and confirm changes.



Note

Deleting a chart report removes any associated schedules.

14.3.3. Chart Report Types

The following table lists available report types.



Report	Description
Email Activity	The results provide a list of primary mailboxes that have sent or received at least one email during the specified period.
Inbound Email Activity	The results provide the number of inbound messages tagged as delivered, rejected, spam or virus.
Top Email Actions	The results provide the top email actions triggered by inbound messages.
Top Email Rules	The results provide the top email rules triggered by inbound messages.
Top Final Rules	The results provide the top email final actions triggered by inbound messages.
Top Recipients	The results provide the top recipients that have received inbound messages.
Top Senders	The results provide the top email message senders.
Top Spam Recipients	The results provide the top recipients of spam messages.
Top Virus Recipients	The results provide the top recipients of messages containing virus or malware.

15. SCHEDULED REPORTS

1. [Scheduled Reports Overview](#)
2. [Creating Scheduled Reports](#)
3. [Managing Scheduled Reports](#)

15.1. Scheduled Reports Overview

Scheduled Reports allows you to attach saved reports to a regular schedule and send them to by email to one or more recipients.

You can also generate the [Email Security] Monthly License Usage Report through Control Center. For more information, refer to the GravityZone Administrator's Guide.

15.2. Creating Scheduled Reports



1. Navigate to **Products > Analytics**.
2. Click the menu button right next to the search bar to open the dropdown menu.
3. Select **Schedules**.
4. Click the **+** button to add a schedule.
5. Configure the following settings:
 - **Start date** to select the date and time for the first run of the report.
You need to set a future date.
 - **Frequency** to set the schedule interval.
 - **Report** to select from available saved reports.
 - **Format** to set the output format.
 - **Recipient** to add from available email addresses.
Recipients receive an email containing a download link for the report.
 - **Email empty report** to receive notifications for reports with no results.
Leave this option unchecked to schedule as an alert.
6. Click **Add** to place it to the queue.

**Note**

You can only schedule saved reports that have the flowing timespan: **Last Hour**, **Last Day**, and **Last Month**.

15.3. Managing Scheduled Reports

1. Navigate to **Products > Analytics**.
2. Click the menu button right next to the search bar to open the dropdown menu.
3. Select Schedules.
4. Select the table icon at the upper-right side to change between modes.

Calendar Mode	List Mode
Use this mode to edit format, recipient and report content.	Use this mode to set running/pause status and remove schedules.
<ul style="list-style-type: none">• Select a schedule to edit and Update changes.	<ul style="list-style-type: none">• Toggle the   icons to set Running/Pause status• Click Delete and confirm changes



16. LOG ARCHIVES

- [Log Archives Overview](#)
- [Managing Log Archives](#)

16.1. Log Archives Overview

Log Archives provide access to scheduled report.

16.2. Managing Log Archives

1. Navigate to **Products > Analytics**.
2. Click the menu button right next to the search bar to open the dropdown menu.
3. Select **Log Archives**.
4. Select your log from the list or use the date filter.