MetaDefender Email Gateway Security 4.7.4
# Table of Contents

## About This Guide

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About MetaDefender Email Gateway Security</td>
<td>10</td>
</tr>
<tr>
<td>Second Layer of Defense for Your Email Security Gateway</td>
<td>10</td>
</tr>
<tr>
<td>Key Features</td>
<td>10</td>
</tr>
<tr>
<td>Deployment Options</td>
<td>10</td>
</tr>
<tr>
<td>Mail Proxy Deployment (Generic)</td>
<td>10</td>
</tr>
<tr>
<td>Cloud Deployment</td>
<td>11</td>
</tr>
<tr>
<td>Onsite Microsoft Exchange Deployment</td>
<td>11</td>
</tr>
<tr>
<td>MetaDefender Email Gateway Security as mail proxy</td>
<td>12</td>
</tr>
</tbody>
</table>

## 1 Quick start with MetaDefender Email Gateway Security

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Installation</td>
<td>13</td>
</tr>
<tr>
<td>Installing MetaDefender Email Gateway Security on Windows</td>
<td>13</td>
</tr>
<tr>
<td>1.1.1 Basic configuration wizard</td>
<td>14</td>
</tr>
<tr>
<td>1.2 License activation</td>
<td>24</td>
</tr>
<tr>
<td>1.3 Creating MetaDefender Core server profile</td>
<td>25</td>
</tr>
<tr>
<td>Creating Core server profile</td>
<td>25</td>
</tr>
<tr>
<td>1.4 Creating relay and notification SMTP server profile</td>
<td>27</td>
</tr>
<tr>
<td>Creating SMTP profile</td>
<td>27</td>
</tr>
<tr>
<td>Assigning notification SMTP server</td>
<td>28</td>
</tr>
<tr>
<td>1.5 Basic security rules</td>
<td>29</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>29</td>
</tr>
<tr>
<td>Configuration</td>
<td>30</td>
</tr>
<tr>
<td>1.6 Email traffic redirection</td>
<td>32</td>
</tr>
</tbody>
</table>

## 2 Installing or upgrading MetaDefender Email Gateway Security

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1 Before installation</td>
<td>33</td>
</tr>
<tr>
<td>Notes</td>
<td>136</td>
</tr>
<tr>
<td>3.3.1 Change user password</td>
<td>137</td>
</tr>
<tr>
<td>3.3.2 Active Directory attributes</td>
<td>138</td>
</tr>
<tr>
<td>3.3.3 LDAP attributes</td>
<td>141</td>
</tr>
<tr>
<td>3.4 General settings</td>
<td>148</td>
</tr>
<tr>
<td>Global settings</td>
<td>149</td>
</tr>
<tr>
<td>Data retention</td>
<td>155</td>
</tr>
<tr>
<td>3.5 Logging &amp; alerts</td>
<td>157</td>
</tr>
<tr>
<td>3.5.1 Configuration</td>
<td>157</td>
</tr>
<tr>
<td>3.5.2 Debug logging</td>
<td>160</td>
</tr>
<tr>
<td>3.5.3 Web Management Console logs</td>
<td>162</td>
</tr>
<tr>
<td>3.6 Quarantine configuration</td>
<td>162</td>
</tr>
<tr>
<td>Quarantining emails</td>
<td>162</td>
</tr>
<tr>
<td>Quarantine reports</td>
<td>164</td>
</tr>
<tr>
<td>3.6.1 Quarantine emails on another mail server</td>
<td>166</td>
</tr>
<tr>
<td>3.7 Server profiles</td>
<td>170</td>
</tr>
<tr>
<td>Properties</td>
<td>171</td>
</tr>
<tr>
<td>Property validation</td>
<td>175</td>
</tr>
<tr>
<td>Testing the configuration</td>
<td>176</td>
</tr>
<tr>
<td>3.7.1 MetaDefender Core specific inventory properties</td>
<td>177</td>
</tr>
<tr>
<td>3.8 Mail proxy deployment configuration</td>
<td>182</td>
</tr>
<tr>
<td>3.8.1 Configuring incoming threat protection</td>
<td>183</td>
</tr>
<tr>
<td>3.8.2 Configuring outgoing threat protection</td>
<td>187</td>
</tr>
<tr>
<td>3.9 Cloud deployment configuration</td>
<td>191</td>
</tr>
<tr>
<td>Overview</td>
<td>191</td>
</tr>
<tr>
<td>Steps overview</td>
<td>192</td>
</tr>
<tr>
<td>Limitation</td>
<td>192</td>
</tr>
<tr>
<td>3.9.1 AppRiver integration</td>
<td>192</td>
</tr>
<tr>
<td>3.9.2 Google Apps integration</td>
<td>197</td>
</tr>
<tr>
<td>3.9.3 Microsoft Office 365 Integration</td>
<td>204</td>
</tr>
<tr>
<td>3.10 Onsite Microsoft Exchange deployment</td>
<td>212</td>
</tr>
<tr>
<td>Installation</td>
<td>212</td>
</tr>
<tr>
<td>Exchange Server message expiration timeout</td>
<td>212</td>
</tr>
<tr>
<td>How To Verify</td>
<td>213</td>
</tr>
<tr>
<td>3.11 Customization of notification emails</td>
<td>214</td>
</tr>
<tr>
<td>Customizing blocked notifications</td>
<td>215</td>
</tr>
</tbody>
</table>
4 Operating MetaDefender Email Gateway Security

4.1 Dashboard
  Statistics details

4.2 Security rules
  Security rules overview
  Security Rule Management
  Unavailable MetaDefender Core rules
  4.2.1 Disclaimer variables

4.3 Quarantine
  Quarantine
  Quarantining conditions
  Quarantine operations
  Quarantine reports
  4.3.1 Sanitize before release

4.4 Email history
  Email history
  Operations
  Failed emails

4.5 Refused emails
  Refused emails
  Conditions of refusal

4.6 Specific email headers
  Identification header
  Scan information headers
  External quarantine header
  Sender policy framework lookup header
  Custom headers

4.7 Support for password protected attachments
  Problem
  Solution
  Software requirements
  Limitations
4.8 Support for signed emails
   Modification rules for signed emails
   Adding extra headers to the email
4.9 Integration with MetaDefender Vault
   About MetaDefender Vault
   Example use cases
   Prerequisites and limitations
   Configuring Security Rules
   Browsing email attachments in MetaDefender Vault
   Upload information in Processing history
   Troubleshooting
4.10 Search
   Filtering columns
   Value only search
   Full text search (FTS)
4.11 Config history
   Config history

5 Troubleshooting MetaDefender Email Gateway Security

5.1 How to create support package
   Content of the created package
5.2 How to read the MetaDefender Email Gateway Security log
5.3 Inaccessible Web Management Console
   Connection refused or browser is waiting
5.4 Understanding email processing statuses
   Workflow statuses
   Temporary failure statuses
   Permanent failure statuses
   Other statuses
5.5 Whitelisting recipients of encrypted files
5.6 Proof-of-concept scenarios
   5.6.1 Stand-alone PoC environment
   5.6.2 High availability
5.7 Can't view scan details
6 Release Notes

6.1 Changelog
   Version 4.7.4
   Version 4.7.3
   Version 4.7.1
   Version 4.7.0
   Version 4.6.2
   Version 4.6.1
   Version 4.6.0
   Version 4.5.3
   Version 4.5.2
   Version 4.5.1
   Version 4.5.0
   Version 4.4.1
   Version 4.4.0
   Version 4.3.3
   Version 4.3.2
   Version 4.3.1
   Version 4.3.0
   Version 4.2.1
   Version 4.2.0
   Version 4.1.3
   Version 4.1.2
   Version 4.1.1
   Version 4.1.0
   Version 4.0.0

6.2 Archived release notes
   6.2.1 Version 4.4.1
   6.2.2 Version 4.5.0
   6.2.3 Version 4.5.1
   6.2.4 Version 4.5.2
   6.2.5 Version 4.5.3
   6.2.6 Version 4.6.0
   6.2.7 Version 4.6.1
7. Legal

Copyright 409
DISCLAIMER OF WARRANTY 409
COPYRIGHT NOTICE 409
MetaDefender Export Classification 409

8. Knowledge Base Articles 411

Emails released or forwarded from Quarantine and retried from Failed emails, fail permanently on Exchange Server 411

How do I perform a clean re-install of MetaDefender Email Security v4? 411
   Overview 412
   Details 412

How long is the support life cycle for a specific version/release of MetaDefender Email Security v4? 417

Manually registering MetaDefender Email Security in Exchange server 418

What is the difference between MetaDefender Email Security 3.X vs 4.X? 422
About This Guide

This guide is intended to provide the information you need to:

- Install, configure, and manage MetaDefender Email Gateway Security v4.x.

⚠️ MetaDefender Email v3 users

When using MetaDefender Email v3, refer to MetaDefender Email v3 user guide. In case of migrating from MetaDefender Email v3 to MetaDefender Email Gateway Security v4 see 2.5 Migrating from MetaDefender Email v3.

- Learn about new and updated features, and bug fixes on each MetaDefender Email Gateway Security release (i.e. each product version's release notes).
- Learn about frequently asked questions and additional concepts through our library of knowledge base articles.

While we offer the option to download this guide to a PDF file, it is optimized for online browser viewing. OPSWAT updates the online version of the guide regularly on an "as needed" basis. By viewing the document online, you are assured that you are always seeing the most recent and most comprehensive version of the guide.
About MetaDefender Email Gateway Security

Second Layer of Defense for Your Email Security Gateway

Email security gateways, although offering tremendous protection, are not perfect. MetaDefender Email Gateway Security enhances existing email security gateways by offering additional protection with more than 30 anti-malware engines (leveraging both heuristics and signature-based detection) and Deep Content Disarm and Reconstruction (Deep CDR) to combat increasingly popular document-based or image-based attacks.

Key Features

- Prevent with email sanitization using Deep Content Disarm and Reconstruction (Deep CDR)
- Detect and prevent more threats by scanning with more than 30 leading anti-malware engines
- Leverage heuristic analysis to detect more unknown and targeted attacks
- Decrease detection time of outbreaks
- Easily integrate with existing email security layer
- Real-time monitoring threats
- Real-time alert and monitoring
- Schedule report
- High performance
- Quarantine infected and sanitized email

Deployment Options

Mail Proxy Deployment (Generic)

In this traditional setup MetaDefender Email Gateway Security acts as an anti-malware email proxy between the email gateway (anti-spam) and the mail server.
**Cloud Deployment**

For hosted solutions such as Office 365 or G Suite Gmail.

**Onsite Microsoft Exchange Deployment**

This is the standard setup with Microsoft Exchange Server.
MetaDefender Email Gateway Security as mail proxy

MetaDefender does not incorporate or include the following functionalities:

- Replace email gateway
  - for spam filtering
  - for NDR based on email validation although we can validate syntactically and mark failed to deliver.
- Replace mail server
  - user-based quarantine
  - user authentication based on email address (e.g., active directory)
# 1 Quick start with MetaDefender Email Gateway Security

This guide describes the basic steps for installing and using MetaDefender Email Gateway Security.

This quick guide assumes that the deployment server has working internet connection.

- **1.1 Installation**
- **1.2 License activation**
- **1.3 Creating MetaDefender Core server profile**
- **1.4 Creating relay and notification SMTP server profile**
- **1.5 Basic security rules**
- **1.6 Email traffic redirection**

## 1.1 Installation

Before starting the installation please make sure your server computer or virtual machine meets the **minimum hardware and software requirements**.

### Installing MetaDefender Email Gateway Security on Windows

1. **Download**
   a. MetaDefender Email Gateway Security stand-alone Windows installer ([mdemailsecurity-<version>-1-x64.msi](#), for example [mdemailsecurity-4.0.0-1-x64.msi](#)) from the OPSWAT Portal
   - If you already have a MetaDefender Core installed or wish to scan using MetaDefender Core on a separate server select the stand-alone installer (a).
   - If you want to install MetaDefender Email Gateway Security & MetaDefender Core on a single server, select bundle (b).

2. Copy the installation package to your server computers
3. Install the product by executing the installer

4. Open a web browser and point to:

   http://<server name or IP>:8058

   <server name or IP> is the DNS name or IP address of your server

1. Follow the steps in 1.1.1 Basic configuration wizard

For more information on Installation procedures see 2.2 Installing MetaDefender Gateway Email Security.

1.1.1 Basic configuration wizard

- Introduction
- Basic configuration steps
  - End-User License Agreement
  - Admin User Setup
  - License activation
  - Deployment mode
  - Create Core Server Profile
  - Configure inbound SMTP settings
  - Automatically configure Email Gateway Security
  - SMTP relay
  - Wizard completion
- Transport Layer Security

Introduction

When trying to access the Web Management Console for the first time, you are to complete a basic configuration wizard in order to be able to use the product. The Web Management Console will be available only after you have successfully finished this wizard.
To start the wizard click CONTINUE.

⚠️ **Sensitive information**

This wizard may transfer sensitive information over an unencrypted connection. Always use this wizard on a secure, closed network or localhost, and with care!

**Basic configuration steps**

**End-User License Agreement**

In the first page you can find the End-User License Agreement. You have to accept the terms before moving on. Please read through the EULA carefully and if you agree with it, check I ACCEPT THE TERMS IN THE LICENSE AGREEMENT and click NEXT to continue.
Admin User Setup

The next step is to set up an administrator account. This account will be the first one being able to access the Web Management Console and to create accounts for other users. You have to fill all fields in this page to be able to move forward. When you are done, click NEXT to continue.

**User directory**

The administrator account, that is created via the basic configuration wizard, is always added to the LOCAL user directory as a member.

The following information is required for the administrator account:

<table>
<thead>
<tr>
<th>ACCOUNT NAME</th>
<th>The unique name of the account that is used at the time of login and in log messages for accountability.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACCOUNT DISPLAY NAME</td>
<td>Name of the person bound to this account. This name (appended to the name of the account's user directory) is displayed in the top right corner of the Web Management Console.</td>
</tr>
<tr>
<td>PASSWORD</td>
<td>Password of the user bound to this account that is used at the time of login.</td>
</tr>
</tbody>
</table>

**Passwords sent clear-text**

As long as TLS is not configured for the basic configuration wizard, passwords are sent clear-text over the network and may be disclosed to unauthorized parties.

As a mitigation action:

1. Either use the wizard on localhost or on a direct network connection, or
2. Enable TLS as soon as possible and change the password immediately if it has already been set.

| EMAIL | Email address of the person bound to this account. |
License activation

For license activation details see 2.4.1 Activating MetaDefender Email Gateway Security licenses.

Deployment mode

In this step you will decide in what mode you wish to deploy MetaDefender Email Gateway Security. If you are installing MetaDefender Email Gateway Security into a production environment, select 'PROTECTION MODE'.
<table>
<thead>
<tr>
<th>PROTECTION MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diagram</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OUT-OF-BAND MONITORING MODE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Diagram</strong></td>
</tr>
</tbody>
</table>
You can also change the deployment mode after installing MetaDefender Email Gateway Security. Refer to the following section: 3.4 General settings

Create Core Server Profile

This step is not displayed when installing MetaDefender Email Gateway Security bundled with MetaDefender Core
In this step you can create a basic Core server profile which will be used for connecting to a MetaDefender Core instance so your emails can be scanned and sanitized. You should give a name for the profile (e.g. "My MetaDefender Core"), set the address of your MetaDefender Core instance and choose a rule from the list. In order to go to the next step the wizard will check if a connection can be made to the address provided. If the connection seems fine a NEXT button will appear in the place of the TEST button and you can continue the configuration process by clicking on it.

By skipping this step the wizard won’t be able to create a security rule later however you will still be able to create a Core server profile and a security rule in the product after the wizard is finished. You will also have the chance to modify the profile created in the wizard with more advanced configuration possibilities later. For more information on server profiles please see 3.7 Server profiles.

Configure inbound SMTP settings
In this step you can configure to which SMTP port MetaDefender Email Gateway Security should listen for inbound traffic.

**Automatically configure Email Gateway Security**

This wizard can help you configure default policies in MetaDefender Email Security. You can skip this option if you want to configure MetaDefender Email Security manually.

- YES, HELP ME CREATE A DEFAULT POLICY
- NO, I WILL MANUALLY CONFIGURE POLICIES

In this step you can decide if you want help to create a default security rule in MetaDefender Email Gateway Security. If you are already familiar with MetaDefender Email Gateway Security you can decide to manually configure server profiles & security rules.

**Security rule**

- STANDARD PROTECTION
  This rule type will prioritize mail flow. If unforeseen events occur during scanning and/or sanitization, then email will be delivered with a warning informing the recipient of the issue.
MAXIMUM PROTECTION
This rule type ensures maximum protection and will quarantine any email that could potentially contain a threat.

ENABLE DATA SANITIZATION (CDR) FOR ALL EMAILS
This option will enable Data Sanitization (CDR) for all emails and sanitize content using OPSWAT Data Sanitization technology.

SMTP relay

Exchange mode
This step is not available when the product was installed in Exchange mode.

On this page you will create a basic SMTP server profile which will be used as a destination for the emails processed by MetaDefender Email Gateway Security and for sending notification emails. You can also select what transport level encryption to use and you can set authentication information if your SMTP server requires it. In order to go to the next step the wizard will check if a connection can be made to the address provided. If the connection seems fine a NEXT button will appear in the place of the TEST button and you can continue the configuration process by clicking on it.

For more information on server profiles please see 3.7 Server profiles

Click NEXT to continue the configuration process.
Wizard completion

After you have completed every steps you are ready to finish the wizard and start using the product. Click the FINISH button to complete the wizard.

⚠️ The product's service will be restarted and the browser will be redirected to the Web Management Console. This could take several seconds.

You can login to the Web Management Console with the administrator user that have just been created in the previous steps.

Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol that provides communications security over a computer network. Websites, like the Web Management Console, are able to use TLS to secure all communications between their servers and web browsers.

The TLS protocol aims primarily to provide confidentiality (privacy) and data integrity between two communicating computer applications.

⚠️ No TLS for the wizard

By default, TLS is not enabled for the basic configuration wizard. As a consequence sessions between the wizard's backend and the browser may be insecure.
Performing the same steps as for the Web Management Console, it is possible to set up TLS for the basic configuration wizard. Remember completing the TLS setup before launching the wizard.

For instructions to set up TLS see 3.2 Configuring TLS.

1.2 License activation

To activate your installation go to the **Settings > License** menu in the Web Management Console. If you haven't yet activated the product, you will only see your installation's Deployment ID. You will also see a warning in the Web Management Console header.

Perform the following steps:

1. Press the ACTIVATE button to bring up the Activation menu, where you should choose from the available modes:
   - Online: the product will contact the OPSWAT license server online, and acquire its license based on your Activation key and Deployment ID.
   - Offline: you can upload a manually acquired license file.
• Request trial key online: if you want to try out the product first, you can receive a trial Activation key via email.

2. Select the desired option
3. Follow the on-screen instructions
4. Finally press the SEND button

⚠️ When your hardware information changes, for example if your mac address changes because the product runs in a virtual machine, the license gets automatically reactivated on the first update attempt.

After successful activation the web management console will be available with all its functionality.

For detailed license activation instructions see 2.4 MetaDefender Email Gateway Security licensing.

1.3 Creating MetaDefender Core server profile

After installation and successful license activation MetaDefender Email Gateway Security user interface is ready to be used with full functionality.

For emails to be scanned MetaDefender Email Gateway Security needs, however, to be connected to MetaDefender Core.

Establishing this connection requires two steps:

1. Creating a MetaDefender Core type server profile
2. Assigning this server profile to Email Gateway Security (see 1.5 Basic security rules)

Creating Core server profile

Go to Inventory > Server profiles and click ADD NEW PROFILE. In the SERVER PROFILE TYPE drop-down list select MetaDefender Core and specify the details of your MetaDefender Core instance(s).

⚠️ Properties not listed in the table below may be left on their default values or blank, or filled according to the organizational policies.
### Server Profiles

<table>
<thead>
<tr>
<th>Server profile type</th>
<th>Profile name</th>
<th>Server specifications (URI)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Value</strong></td>
<td>MetaDefender Core</td>
<td>Core servers URI</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td>MetaDefender Core</td>
<td>Core</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>URI example</th>
<th>Transport level encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://10.0.0.10:8008">http://10.0.0.10:8008</a></td>
<td>None</td>
</tr>
<tr>
<td><a href="https://10.0.0.10:8008">https://10.0.0.10:8008</a></td>
<td>TLS</td>
</tr>
</tbody>
</table>

For further details about server profiles see 3.7 Server profiles.
1.4 Creating relay and notification SMTP server profile

Creating SMTP profile

Go to **Inventory > Server profiles** click ADD NEW PROFILE. In the SERVER PROFILE TYPE drop-down list select **SMTP** and configure the relay SMTP servers to where the processed email messages will be forwarded.

⚠️ Properties not listed in the table below may be left on their default values or blank, or filled according to the organizational policies (e.g. TRANSPORT LEVEL ENCRYPTION).

<table>
<thead>
<tr>
<th>Value</th>
<th>Server profile type</th>
<th>Profile name</th>
<th>Server specifications (URI)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>SMTP</td>
<td>Unique name</td>
<td>SMTP relay servers URI</td>
</tr>
</tbody>
</table>

### Examples

<table>
<thead>
<tr>
<th>URI example</th>
<th>Typical transport level encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtp://10.0.0.10:25</td>
<td>None</td>
</tr>
<tr>
<td>smtp://10.0.10:25</td>
<td>StartTLS (STARTTLS optional or STARTTLS required)</td>
</tr>
<tr>
<td>smtps://10.0.0.10:587</td>
<td>TLS</td>
</tr>
</tbody>
</table>
For further server profile details see 3.7 Server profiles.

**Assigning notification SMTP server**

Go to **Settings > Global settings / Notification and report settings / SMTP SERVER** and in the drop-down list select the SMTP server profile that has been created above.
1.5 Basic security rules

- Prerequisites
- Configuration
  - Inbound
  - Outbound

After installation, successful license activation and basic configuration MetaDefender Email Gateway Security is ready to be used.

However, MetaDefender Email Gateway Security blocks all emails by default. To allow both inbound and outbound email traffic some basic security rule configuration is needed.

⚠️ The basic security rules created in this chapter may be too permissive and may not be suitable for production deployments.

**Prerequisites**

The following information is needed to create the basic security rules:
1. SMTP type server profile containing the email gateway (see 1.4 Creating relay and notification SMTP server profile)

2. SMTP type server profile containing the mail server (see 1.4 Creating relay and notification SMTP server profile)

3. MetaDefender Core type server profile containing the Core (see 1.3 Creating MetaDefender Core server profile)

4. Internal email addresses (email address or QRegExp pattern; may be restricted to organization internal addresses only, or allow any email address)

5. External email addresses (email address or QRegExp pattern)

**Configuration**

To allow both inbound and outbound email traffic go to **Policy > Security rules** and create the following two basic security rules.

---

In the examples below we assume that

- The email gateway IP address is 10.0.0.1 and the SMTP type server profile `GateWayRelayProfile` contains it,
- The mail server IP address is 10.0.0.9 and the SMTP type server profile `MailServerRelayProfile` contains it,
- Both are on the same /24 subnet.
- The Core server is configured in the MetaDefender Core type server profile `CoreProfile`.

---

**Inbound**

Properties not listed in the table below may be left on their default values (if they have, e.g. settings on ACTIONS or ADVANCED tabs) or filled according to the organizational policies (e.g. USE TLS).

<table>
<thead>
<tr>
<th>Tab</th>
<th>FILTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>DIRECTION</td>
</tr>
</tbody>
</table>

---
<table>
<thead>
<tr>
<th>Tab</th>
<th>FILTER</th>
<th>Value INBOUND</th>
<th>Examples INBOUND</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Email gateway IP address</td>
<td>External email addresses, Internal email addresses</td>
<td>1. 10.0.0.1 2. 10.0.0.0/24 1. <a href="mailto:+@example.com">+@example.com</a> (example.com emails only) 2. <a href="mailto:test@example.com">test@example.com</a> (this single sender only)</td>
</tr>
<tr>
<td></td>
<td>INBOUND</td>
<td></td>
<td>1. .+@.+ (any email recipient) 2. <a href="mailto:+@opswat.com">+@opswat.com</a> (opswat.com email only) 3. <a href="mailto:mengineer@opswat.com">mengineer@opswat.com</a> (this single recipient only)</td>
</tr>
</tbody>
</table>

**Outbound**

Properties not listed in the table below may be left on their default values (if they have, e.g. settings on ACTIONS or ADVANCED tabs) or filled according to the organizational policies (e.g. USE TLS).

<table>
<thead>
<tr>
<th>Tab</th>
<th>FILTER</th>
<th>Field OUTBOUND</th>
<th>Example OUTBOUND</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SCAN</td>
<td>DIRECTION, SENDER IP ADDRESS, SENDER DOMAIN OR ADDRESS, RECIPIENT DOMAIN OR ADDRESS, METADEFENDER CORE</td>
<td>1. 10.0.0.9 1. .+@.+ (any email recipient)</td>
</tr>
<tr>
<td></td>
<td>SCAN</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1.6 Email traffic redirection

As a final step—when all the previous steps in this chapter are done—the email traffic must be redirected to flow through MetaDefender Email Gateway Security.

MetaDefender Email Gateway Security's email relay SMTP service is listening on port 10025 by default.

For further details about the configuration see 3.4 General settings.

Depending on the deployment type:

1. In case of mail proxy deployment:
   a. Configure the email gateway to redirect inbound emails,
   b. Configure the mail server to redirect outbound emails.

2. In case of cloud deployment configure the MX record to point to MetaDefender Email Gateway Security.
2 Installing or upgrading MetaDefender Email Gateway Security

- 2.1 Before installation
- 2.2 Installing MetaDefender Email Gateway Security
- 2.3 Upgrading MetaDefender Email Gateway Security
- 2.4 MetaDefender Email Gateway Security licensing
- 2.5 Migrating from MetaDefender Email v3

2.1 Before installation

MetaDefender Email Gateway Security provides multiple deployment options as described in this documentation. If you need additional information on selecting the optimal deployment option, OPSWAT Technical Support is available to assist.

MetaDefender Email Gateway Security's performance and capacity vary depending on the specifications of the system hosting MetaDefender Email Gateway Security. Increasing the resources available to the MetaDefender Email Gateway Security system will likely increase the performance of the MetaDefender Email Gateway Security system, however this is not guaranteed.

- 2.1.1 Increase capacity and resiliency
- 2.1.2 System requirements
- 2.1.3 Testing tool

2.1.1 Increase capacity and resiliency

Single server capacity

⚠️ Please note that in the capacity measurement below MetaDefender Core and MetaDefender Email Gateway Security were deployed to the same physical machine.
<table>
<thead>
<tr>
<th>System profile</th>
<th>Email consists of</th>
<th>Throughput</th>
<th>CPU usage</th>
</tr>
</thead>
</table>
| • 4 Core Processor  
• 16 GB RAM  
• 64 bit OS  
• MetaDefender Core 20 engines | • 30% of emails with no attachment  
• 40% of emails with single attachment (sanitization is not enabled)  
• 12.5% of emails have PDF¹ attachment (sanitization is enabled)  
• 12.5% of emails have DOCX¹ attachment (sanitization is enabled)  
• 5% of emails have JPG¹ attachment (sanitization is enabled) | 300 emails / minute | 50-100% |

**Load balancing MetaDefender Email Gateway Security**

For *mail proxy* and *hosted* deployment, this is desired configuration to increase the resilience and performance.

In order to achieve this, the following options should be considered.

- Using load balancer (e.g., elastic load balancer, barracuda load balancer)
- Using SMTP failover mechanism on your email gateway (configuration varies depending on the email gateway solution).

**Sizing examples**

The following displays two examples in real production environment. This will provide reference to sizing of the hardware hosting MetaDefender Email Gateway Security. Neither of the two setups in the examples experienced latency (more than 100 emails pending for process).

⚠️ Please note that in the examples below MetaDefender Core and MetaDefender Email Gateway Security were deployed to separate physical machines.
Common parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Windows Server 2012 R2 Standard 64</td>
</tr>
<tr>
<td>Instances</td>
<td>2 (HA)</td>
</tr>
<tr>
<td>Core version</td>
<td>MetaDefender Core 4.7.2</td>
</tr>
<tr>
<td>Email Security version</td>
<td>MetaDefender Email Gateway Security 4.0.0</td>
</tr>
</tbody>
</table>

Hardware profile

<table>
<thead>
<tr>
<th>Organization</th>
<th>Emails / hour</th>
<th>Hardware Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>organization A</td>
<td>10,000</td>
<td>8 CPU cores, 16 GB RAM, 140 GB HDD</td>
</tr>
<tr>
<td>organization B</td>
<td>1000</td>
<td>2 CPU cores, 8 GB, 100 GB HDD</td>
</tr>
</tbody>
</table>

Footnotes

1 Files that we used for testing have the following sizes:
   - PDF: 8 KB
   - DOCX: 220 KB
   - JPG: 650 KB

The result may vary depending on data set you select. We strongly recommend to conduct testing based on your organization’s email traffic statistics. If you need assistance on the tools for testing, contact OPSWAT support.

2.1.2 System requirements

- Minimum hardware requirements
- Software requirements
  - MetaDefender Core
    - Version compatibility matrix
• Scan engines
• Security rules
• Additional installation of 3rd party framework or components
• Additional installation of Windows services
• Ports that must be available
• Browser requirements
• Directories

⚠ The following requirements do not include the system requirements for MetaDefender Core if installed on the same system.

## Minimum hardware requirements

<table>
<thead>
<tr>
<th>Hardware property</th>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>4 GB</td>
<td></td>
</tr>
<tr>
<td>Free SSD space</td>
<td>16 GB</td>
<td>⚠ Space details</td>
</tr>
</tbody>
</table>

⚠ Space details

Please note that this hard disk space is only enough for installing MetaDefender Email Gateway Security and for very limited operation.

Quarantine and permanently failing emails (especially with large attachments) may consume huge disk volumes.

⚠ Performance concerns

For performance reasons it is not recommended to use HDD instead of SSD.
## Software requirements

<table>
<thead>
<tr>
<th>Software property</th>
<th>Requirement</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution</td>
<td>Version(s)</td>
<td>Bitness</td>
</tr>
<tr>
<td>Operating system</td>
<td>Microsoft Windows</td>
<td>64 bit</td>
</tr>
<tr>
<td></td>
<td>7 / 8 / 8.1 / 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Microsoft Windows Server</td>
<td>64 bit</td>
</tr>
<tr>
<td></td>
<td>2008 R2 / 2012 / 2012 R2 / 2016 / 2019</td>
<td></td>
</tr>
<tr>
<td>TLS toolkit</td>
<td>OpenSSL</td>
<td>32 bit</td>
</tr>
<tr>
<td></td>
<td>latest</td>
<td>Optional, it is needed only if TLS is utilized.</td>
</tr>
</tbody>
</table>

## MetaDefender Core

### Version compatibility matrix

<table>
<thead>
<tr>
<th>MetaDefender Email Gateway Security</th>
<th>MetaDefender Core</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>4.7.0+</td>
</tr>
<tr>
<td>4.1.0 - 4.2.0</td>
<td>4.8.2+</td>
</tr>
</tbody>
</table>

## Scan engines

The following scan engines must be active:

<table>
<thead>
<tr>
<th>Scan engine</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data sanitization</td>
<td>5.0.2-6 +</td>
</tr>
<tr>
<td><strong>At least one of the available anti-malware engines</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
Security rules

Under **Policy > Security rules** on Core, security rules—that are used by MetaDefender Email Gateway Security's security rules—

1. SHOULD enable the following **Visibility of scan result**:

<table>
<thead>
<tr>
<th>Role</th>
<th>Visibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Everybody</td>
<td>FULL DETAILS</td>
</tr>
</tbody>
</table>

⚠️ Without this visibility Email Gateway Security can still work, but certain details may not be provided on the UI.

Additional installation of 3rd party framework or components

<table>
<thead>
<tr>
<th>Name</th>
<th>Version</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET Framework</td>
<td>4.5</td>
<td>REQUIRED</td>
</tr>
</tbody>
</table>

Additional installation of Windows services

<table>
<thead>
<tr>
<th>Name</th>
<th>Service Name</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSWAT MetaDefender Email Gateway Security</td>
<td>mdemailsecurity</td>
<td>REQUIRED</td>
</tr>
</tbody>
</table>

Ports that must be available

<table>
<thead>
<tr>
<th>Direction</th>
<th>Component / Service</th>
<th>Port</th>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>MetaDefender Email Gateway Security</td>
<td>SMTP service</td>
<td>10025</td>
</tr>
<tr>
<td>Inbound</td>
<td></td>
<td>8058</td>
<td></td>
</tr>
</tbody>
</table>
## Browser requirements

One of the following desktop browsers is required to use the Web Management Console:

- Latest two Chrome versions
- Latest two Firefox versions
- Latest two Safari versions
- Latest two Microsoft Edge versions
- Internet Explorer 11

⚠️ Mobile layouts are not supported yet.

## Directories

This section contains references to directories used by Email Gateway Security.

In further sections of this user guide the *directory reference* is used instead of the actual directory to refer to locations on the system disk.

Everything, except logs, is placed under the installation folder that can be customized during the installation.

<table>
<thead>
<tr>
<th>Directory reference</th>
<th>Directory path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation folder</td>
<td><code>C:\Program Files\OPSWAT\Metadefender Email Security</code></td>
</tr>
</tbody>
</table>
Directory reference | Directory path
--- | ---
Event log files | C:\Windows\System32\WinEvt\Logs
Log file | N log file is written by default. For details see 3.1 MetaDefender Email Gateway Security configuration.

**Certified component versions**

MetaDefender Email Gateway Security team will continuously test and monitor various component (engine and database) versions to ensure that they integrate well with the product and provide the highest reliability and performance.

⚠️ **Potential adverse impact**

MetaDefender Email Gateway Security will accept other, preferably newer component versions; stability and performance of the product may, however, be adversely impacted.

**Certified component versions**

Any components *not listed* below are always expected to work correctly with MetaDefender Email Gateway Security.

The components *listed* below were tested and certified to work correctly on their versions below to work correctly.

⚠️ **Potential adverse impact**

Any other versions may have an adverse impact on stability and/or performance.

<table>
<thead>
<tr>
<th>Component</th>
<th>Certified version</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender</td>
<td>4.14.0</td>
</tr>
<tr>
<td>Archive engine</td>
<td>5.1.7-359</td>
</tr>
<tr>
<td>Archive database</td>
<td>5.1.7-359</td>
</tr>
</tbody>
</table>
Microsoft Exchange Server supportability matrix

Overview
This page describes the supported operating systems and Microsoft Exchange version for installing MetaDefender Email Gateway Security for 3.10 Onsite Microsoft Exchange deployment.

The matrix is built considering the MetaDefender Core System Requirements and Microsoft Exchange Server Supportability Matrix.

Supported Environments
The following table identifies supported environments for installing MetaDefender Email Gateway Security on an operating system running Microsoft Exchange Server. Supported environments are marked with ✅.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Server 2013 CU17</td>
<td>✗ (error)</td>
<td>✅ (tick)</td>
<td>✅ (tick)</td>
<td>✅ (tick)</td>
<td>✗ (error)</td>
</tr>
<tr>
<td>• Enterprise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Service Pack 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Standard Edition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Component | Certified version
---|------------------
Deep CDR engine | 5.3.2-1484
Deep CDR database | 5.1.1
Proactive DLP engine | 1.0.2-121
Proactive DLP database | 1.0.2-160
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Exchange Server 2016</strong></td>
<td>✗ (error)</td>
<td>✓ (tick)</td>
<td>✓ (tick)</td>
<td>✓ (tick)</td>
<td>✓ (tick)</td>
</tr>
<tr>
<td>• Enterprise Edition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Standard Edition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.1.3 Testing tool

**Bulwarx email tester client**

The tool provides a simple UI to send email for the purpose of testing setup rather than using telnet.

**How To**

1. Download the tool from this link.
2. Unpack the downloaded zip file and run Bulwarx Tester Client.exe.
3. Put IP of MetaDefender Email Gateway Security and port (10025 by default).
4. Fill out sender and recipient email address along with subject.
5. Choose either HTML or Plain text for message format.
   a. If you choose HTML: MailTemplate.html will be loaded to email.
   b. If you choose Plain text: MailTemplate.txt will be loaded to email.
   c. If you choose Combined, both MailTemplate.txt and MailTemplate.html will be loaded to email.
6. Add files as email attachments.
7. Click Send to send email.
Area To Test

- If email is delivered to mail box when attachment is clean.
- If email is blocked and quarantined on MetaDefender Email Gateway Security when attachment is blocked by MetaDefender Core.
- If email is sanitized and original copy of email is quarantined on MetaDefender Email Gateway Security if email is sanitized.
- Administrators and users are getting quarantine reports.

Who are Bulwarx?

Bulwarx Ltd. – Founded in 2013 – Is an independent and innovative new force in the Israeli cyber security market. We are striving to serve as a knowledge center in the cyber security field by developing an expertise in the application of leading technological solutions against cyber attacks, providing a comprehensive service which assists in dealing cyber threats and efficient use of all tools and techniques, providing fast response to cyber attacks (or suspicion of such) incidents. Bulwarx uniqueness and one of our greatest strength beyond the ability to provide high quality support, is the proficiency to leverage the capabilities and flexibility of existing
solutions by providing development of 3rd party solution to existing or new implementations. In Bulwarx products list you will be able to find the most high-end security vendors in the market including CyberArk, OPSWAT, Forcepoint (formerly Websense), and more.

2.1.5 Sizing guide
The following information can be used as a guideline when deploying MataDefender Email Gateway Security in your organization. Since there are many factors that may affect performance, these test results should not be viewed as performance guarantees.

Factors that may affect performance
- Package and configuration
  - set of engines (which and how many)
  - configuration (e.g. CDR is enabled)
- System environment
  - profile (CPU, RAM, Storage)
- Traffic characteristics
  - average attachment number/size/type

Test results
Performance is measured by the number of processed emails in one hour interval. In the test scenarios below, the traffic was generated by using real-world attachment number/attachment size/attachment type distributions. In all cases, MetaDefender Email Gateway Security was deployed as an SMTP Proxy. For test cases with CDR enabled, CDR was allowed for all possible file types.

Results

<table>
<thead>
<tr>
<th>CPU cores</th>
<th>Memory (GB)</th>
<th>OS</th>
<th>Engine package</th>
<th>Duration</th>
<th>Processed emails</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>4 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>6 000</td>
</tr>
<tr>
<td>8 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>4 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>8 000</td>
</tr>
<tr>
<td>CPU cores</td>
<td>Memory (GB)</td>
<td>OS</td>
<td>Engine package</td>
<td>Duration</td>
<td>Processed emails</td>
</tr>
<tr>
<td>-----------</td>
<td>------------</td>
<td>---------------------</td>
<td>------------------------------------------------</td>
<td>----------</td>
<td>------------------</td>
</tr>
<tr>
<td>16 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>4 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>8 000</td>
</tr>
<tr>
<td>8 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>4 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>9 000</td>
</tr>
<tr>
<td>16 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>4 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>11 500</td>
</tr>
<tr>
<td>8 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>8 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>6 500</td>
</tr>
<tr>
<td>16 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>8 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>8 000</td>
</tr>
<tr>
<td>8 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>8 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>7 500</td>
</tr>
<tr>
<td>16 @2.1 GHz</td>
<td>16</td>
<td>Windows Server 2016</td>
<td>8 engine package + Data sanitization + DLP + Yara</td>
<td>1h</td>
<td>12 000</td>
</tr>
</tbody>
</table>

⚠️ **On-site Exchange deployment**

In case of on-site Exchange deployment scenarios the resource needs of the Microsoft Exchange Server must also be taken into consideration.

### 2.2 Installing MetaDefender Email Gateway Security

**Installation overview**

The following steps are needed to be executed to install MetaDefender Email Gateway Security:

1. Download the package of your choice from the [OPSWAT portal](https://www.opswat.com/metascan/).
2. Install the package on your computer.
3. Open a web browser and point to:
Installation

Two options are available to install MetaDefender Email Gateway Security:

- 148573850
- 148573850

GUI installation

As usual with Windows installers, you may click through the installer steps to install the product. Following are the detailed installation steps for MetaDefender Email Gateway Security:

<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image" alt="Welcome message" /></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="MetaDefender Email Gateway Security Setup" /></td>
</tr>
</tbody>
</table>

4. Follow the steps in 1.1.1 Basic configuration wizard
<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
</table>
| 1. Accept the license agreement | ![Screenshot](image1.png) | **End-User License Agreement**

This Server End User License Agreement ("EULA"), version 10 Jan 2019, is a legal and enforceable agreement between you, a natural person or legal entity, acting by and through its officers, employees, and third-party agents to:

- I accept the terms in the License Agreement
- I do not accept the terms in the License Agreement

2. Select setup type | ![Screenshot](image2.png) |

**Choose Setup Type**

Choose the setup type that best suits your needs

- **Simple**
  - Installs the most common program features. Recommended for most users.

- **Custom**
  - Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.
<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
</table>
| 4    | ![MetaDefender Email Gateway Security Setup](image)  
**Custom Setup**  
To change default installation directory click on browse button below.  
Location: C:\Program Files\OPSWAT\MetaDefender Email Security|  
| 5    | ![MetaDefender Email Gateway Security Setup](image)  
**MetaDefender Email Gateway Security server setup**  
The setup wizard setup the MetaDefender Email Gateway Security  
Please enter MetaDefender Email Gateway Security web server and REST server IP address and port.  
Users can access MetaDefender Email Gateway Security web server and REST services over this IP and port address.  
To make the service available on any IP of this computer set *, otherwise specify accordingly.  
REST Address:  
REST Port: 8058  
Microsoft Exchange Server (2013/2016) mode |
<table>
<thead>
<tr>
<th>Step</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Commit installation</td>
</tr>
<tr>
<td>Step</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>7</td>
<td><em>Installation in progress</em></td>
</tr>
<tr>
<td>8</td>
<td><em>Finish installation</em></td>
</tr>
</tbody>
</table>

**Screenshot:**

![MetsDefender Email Gateway Security Setup](Image)

**Ready to Install**
The setup wizard is ready to begin the Typical installation.

Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
Command line installation

- **2.2.1 Installing MetaDefender Email Gateway Security using the command line**

2.2.1 Installing MetaDefender Email Gateway Security using the command line

⚠️ The instruction below apply when installing the stand-alone version of MetaDefender Email Gateway Security.

Perform the following steps to install MetaDefender Email Gateway Security using the command line:

1. Download MetaDefender Email Gateway Security installation package from the [OPSWAT Portal](https://www.opswat.com). Make sure that you download the applicable package for your operating system version
2. Copy the installation package to your server
3. Install the product with the following command (<filename> is the MetaDefender Email Gateway Security package you downloaded from our portal):

```
> msiexec /i <filename> <option key>=<option value>
```

The possible option keys and their default option values are the following:

<table>
<thead>
<tr>
<th>Key</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESTADDRESS</td>
<td>0.0.0.0</td>
<td>REST interface binding address</td>
</tr>
<tr>
<td>RESTPORT</td>
<td>8058</td>
<td>REST interface binding port</td>
</tr>
</tbody>
</table>

For details on using `msiexec` please consult Windows installer documentation.

2.3 Upgrading MetaDefender Email Gateway Security

Notes for upgrading from MetaDefender Email v3

⚠️ It is not possible to directly upgrade MetaDefender Email v3 to MetaDefender Email Gateway Security v4. MetaDefender Email v3 comes built into MetaDefender Core v3. Uninstall MetaDefender Core v3 first, then start a fresh installation.

❗️ There is no support for importing MetaDefender Email v3 configuration into MetaDefender Email Gateway Security v4. The configuration must be migrated manually.

Upgrading from MetaDefender Email Gateway Security v4

To upgrade from a former version of MetaDefender Email Gateway Security v4 a simple installation of the latest version is enough.

⚠️ When upgrading, ensure to use the same edition of MetaDefender Email Gateway Security as originally installed (stand-alone or bundle version respectively)
All existing MetaDefender Email Gateway Security configuration and data will be kept during the upgrade.

**Changing between on-site SMTP and on-site Exchange mode during an upgrade**

Security rules of an on-site SMTP deployment and an on-site Exchange Server deployment are not compatible.

- In case of on-site SMTP deployments each security rule must have an SMTP relay configured where emails are sent forward at the end of processing.
- In case of on-site Exchange Server deployments there is, however, no need for explicit relay configuration (it is disabled). Emails are sent back to Exchange Server automatically at the end of processing.

For further details see [4.2 Security rules](#) and [3.7 Server profiles](#).

- As a consequence of rule incompatibility:
  - processing emails won't work as expected and
  - security rules require manual adjustments after changing between on-site SMTP and on-site Exchange mode.

### 2.4 MetaDefender Email Gateway Security licensing

In order to use MetaDefender Email Gateway Security you need to activate the product.

- If you already purchased email protection together with MetaDefender Core v3 then please contact OPSWAT sales for your activation key.

  - [2.4.1 Activating MetaDefender Email Gateway Security licenses](#)
  - [2.4.2 Checking MetaDefender Email Gateway Security license](#)

#### 2.4.1 Activating MetaDefender Email Gateway Security licenses

- Initial steps
- Online activation
- Offline activation
Initial steps

1. To activate your installation go to the **Settings > License** menu in the Web Management Console. If you have no valid license, you will only see your installation's Deployment ID. You will also see a warning in the Web Management Console header.

2. Press the **ACTIVATE** button to bring up the Activation menu. The following modes are available:
   a. Online
   b. Offline
   c. Request trial key online
Online activation
With internet connection on the server, the MetaDefender Email Gateway Security instance may be activated directly using the Activation key received at the time of purchasing the product.

Offline activation
With no internet connection on the server the MetaDefender Email Gateway Security instance may be activated indirectly from a different machine, that has internet connection. The Deployment ID of the MetaDefender Email Gateway Security instance and the Activation key received at the time of purchasing the product will be required. Follow the steps on the screen to activate the product offline.
Activation

**ACTIVATION MODE**

- [ ] ONLINE
- [x] OFFLINE
- [ ] REQUEST TRIAL KEY ONLINE

Offline activation steps:

1. Copy down your Deployment ID: MDEMAILONYMCJT2jRxErMq0y36rVRsuV1s7KoNUX
2. Go to OPSWAT portal: [https://portal.opswat.com/activation](https://portal.opswat.com/activation)
3. Activate and download your license file (you will need your Activation key and the Deployment ID of this instance)
4. Upload the license file here
5. Check license details in the license menu

**ACTIVATION FILE**

(Select a file)

SEND  CANCEL
## Offline activation details

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log on to <a href="https://portal.opswat.com/activation">https://portal.opswat.com/activation</a></td>
</tr>
<tr>
<td>2</td>
<td>Select MetaDefender Email Gateway Security as MetaDefender Package</td>
</tr>
<tr>
<td>3</td>
<td>Fill in the requested information about your deployment</td>
</tr>
</tbody>
</table>
Click the Request Unlock Key button.
The Download Unlock Key link appears.

Metadefender Package

Metadefender Email Security

Activation Key *

Password: [Redacted]

Number Of Recipient Addresses

100

Deployment ID *

MDEMAILGNYMCT2jRxBMqGv36rVRsuV1s7KoNUX

Optional Description

This helps you to identify this deployment OPSWAT License portal

Request Unlock Key

Please click this link to download license file.

Download Unlock Key
Click the **Download Unlock Key** link and save the activation file.

Go back to MetaDefender Email Gateway Security's Web Management Console. Browse for the activation file and click the **SEND** button.
Request trial key online

An evaluation license may be acquired for 14 days. To obtain a trial key register on the OPSWAT Portal first.
Activation

ACTIVATION MODE

○ ONLINE  ○ OFFLINE  ○ REQUEST TRIAL KEY ONLINE

Activation key required to use this installation. You can receive a trial key valid for 14 days via email. Please provide the email address you registered with on OPSWAT Portal. Trial key is valid for up to 3 scan nodes. If you would like to test our product with more than 3 scan nodes please contact our sales via oswat.com

EMAIL ADDRESS

Email address

SEND  CANCEL
### Trial key request details

1. Provide your e-mail address (that was registered on the OPSWAT portal) in the *EMAIL ADDRESS* field and click the *SEND* button.

2. An e-mail response will arrive from [sales@opswat.com](mailto:sales@opswat.com) containing your trial activation key and activation instructions.

   ![image]

   Wed 2017-04-19 14:24
   sales@opswat.com
   [OPSWAT] Metadefender Core v4 Evaluation Key
   To 
   
   Thank you for requesting evaluation key for a Metadefender product!
   
   We registered a trial key request from your email address: <br>
   
   Your activation key is 1fOC-g5U2-XpVe-ABWm-VMP3-4Nyb-nRCH-zLjB
   
   This key is valid for the following products:
   
   Metadefender iCAP Server - Evaluation
   
   To activate your Metadefender product installation, please follow the follow<br>
   
   1. Access the web management console from a web browser.

3. Using the received activation key continue with an 148578732 or 148578732 activation.

### Notes

⚠️ If you activated your installation, but your license becomes invalid or expired, you will see a *RE-ACTIVATE* button. After clicking it, the product tries to activate the license with the formerly entered activation information.
2.4.2 Checking MetaDefender Email Gateway Security license

User menu pane

Basic license information is always visible in the user menu pane on the lower left side of the screen. The following information is available:

- Product version
- License expiration: last day of license validity

License

For more license details and activating your installation go to Settings > License menu on the Web Management Console:

- Product ID: product identification as on your order
- Product name: product name as on your order
- Expiration: last day of license validity
- Accounts: number of licenses committed / number of licenses allowed
- Deployment ID: identification of this installation
2.5 Migrating from MetaDefender Email v3

- Precautions
  - MetaDefender Core compatibility
  - System requirements
    - Standalone deployment
    - Combined Core & Email Gateway Security deployment
- Migrating configuration
  - Configuration map
- Migrating data
  - Migration window
    - Waiting for workflows-in-progress to settle
  - Potential data loss
  - Migrated data
No backward compatibility

MetaDefender Email Gateway Security v4 is not backwards compatible with MetaDefender Email v3.
As a consequence configuration and databases of Email v3 must be migrated manually to Email Gateway Security v4.

Precautions

MetaDefender Core compatibility
MetaDefender Email v3 is bundled into MetaDefender Core v3. MetaDefender Email v3 is not compatible with MetaDefender Core v4.
MetaDefender Email Gateway Security v4 is a standalone product. MetaDefender Email Gateway Security v4 is not compatible with MetaDefender Core v3.
For MetaDefender Email Gateway Security v4 requirements on MetaDefender Core see 2.1.2 System requirements.

System requirements
For MetaDefender Email Gateway Security v4 requirements on hardware, OS and other software, see 2.1.2 System requirements.

Standalone deployment
When MetaDefender Email Gateway Security v4 is deployed in standalone mode (to a separate machine from MetaDefender Core) then it is expected to require a less powerful hardware than a MetaDefender Email v3 (and a combined MetaDefender Core v3) deployment.

Combined Core & Email Gateway Security deployment
When MetaDefender Email Gateway Security v4 is deployed in combined mode (to the same machine as MetaDefender Core) then it is expected to require approximately the same hardware performance than a MetaDefender Email v3 (and a combined MetaDefender Core v3) deployment.
Migrating configuration

Configuration map

<table>
<thead>
<tr>
<th>MetaDefender Email v3 configuration topic</th>
<th>v3 documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configuring Incoming Threat Protection</strong></td>
<td>Configuring Incoming Threat Protection</td>
</tr>
<tr>
<td><strong>Configuring Outgoing Threat Protection</strong></td>
<td>Configuring Outgoing Threat Protection</td>
</tr>
</tbody>
</table>

1. Sources > Metadefender Email > Setup / Instances / Setup
2. Email Relay Server
<table>
<thead>
<tr>
<th>MetaDefender Email v3 configuration topic</th>
<th>v3 documentation</th>
</tr>
</thead>
</table>
| 1. **Sources > Metadefender Email > Setup / Instances / Setup**  
   2. Email Direction |                  |

**Configuring Recipient Verification**

C:\Program Files (x86)\OPSWAT\Metadefender Core\<engine count>\Metadefender Mail Agent\Metadefender.Email.Engine.Generic.Agent.dll.config / EmailRelayInLocalDomains
<table>
<thead>
<tr>
<th>MetaDefender Email v3 configuration topic</th>
<th>v3 documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS support (Incoming/Outgoing emails)</td>
<td>TLS support (Incoming/Outgoing emails)</td>
</tr>
<tr>
<td>Cloud Deployment</td>
<td>3. Cloud Deployment</td>
</tr>
<tr>
<td>Onsite Microsoft Exchange Deployment</td>
<td>4. Onsite Microsoft Exchange Deployment</td>
</tr>
</tbody>
</table>
## Notification and Report

Sources > Metadefender Email > Settings / E-Mail Settings For Notifications

### Error Email Notification

### Infection Email Notification

### Quarantine Reports
<table>
<thead>
<tr>
<th>MetaDefender Email v3 configuration topic</th>
<th>v3 documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine &gt; Configure Quarantine Reports / SMTP Configuration Settings</td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>Quarantine &gt; Configure Quarantine Reports / Schedule Quarantine Reports</td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>Configuration From Config File</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--</td>
</tr>
<tr>
<td><strong>MetaDefender</strong></td>
<td></td>
</tr>
<tr>
<td><strong>.Common.dll.config</strong></td>
<td></td>
</tr>
<tr>
<td><strong>InstallationFolder</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LogsFolder</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LogMaxSize</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LogFormat</strong></td>
<td></td>
</tr>
<tr>
<td><strong>LogLevel</strong></td>
<td></td>
</tr>
<tr>
<td><strong>RestClientTimeoutMs</strong></td>
<td></td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>Metadefender.Email.Engine. Generic .Agent.dll.config</strong></td>
<td></td>
</tr>
<tr>
<td>WorkExtension</td>
<td></td>
</tr>
<tr>
<td>BadExtension</td>
<td></td>
</tr>
<tr>
<td>AgentGuid</td>
<td>Agent Guid. Should be unique.</td>
</tr>
<tr>
<td>AgentStatusCheckInterval</td>
<td>Durations between agent status checks</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol to use when sending process requests. Possible values are REST</td>
</tr>
<tr>
<td>StartRestServer</td>
<td>Start the REST server</td>
</tr>
<tr>
<td>RestoreWorkItemsOnStartup</td>
<td>Rename any items with a work extension (.work) to .eml service startup</td>
</tr>
<tr>
<td>EmailProcessedHeaderName</td>
<td>MIME Header name for emails processed by Mail Agent order to avoid duplicates</td>
</tr>
<tr>
<td>EmailRelayInProcessName</td>
<td>Process name for emailrelay.exe application</td>
</tr>
<tr>
<td>EmailRelayOutProcessName</td>
<td>Process name for emaillayout.exe application</td>
</tr>
<tr>
<td>EmailRelayInStart</td>
<td>Start Email relay process on service startup. (To monitor incoming SMTP traffic)</td>
</tr>
<tr>
<td>EmailRelayInPort</td>
<td>10025</td>
</tr>
</tbody>
</table>

4.7.4
<table>
<thead>
<tr>
<th>MetaDefender Email v3 configuration topic</th>
<th>v3 documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailRelayInParameters</td>
<td>Parameters that are passed to email relay application</td>
</tr>
<tr>
<td></td>
<td>--no-daemon --remote-clients --hidden --as-server --port 25 --spool-dir &quot;&lt;dir&gt;&quot;</td>
</tr>
<tr>
<td>EmailRelayOutStart</td>
<td>Start Email relay process on service startup. (To monitor outgoing email and forward via SMTP)</td>
</tr>
<tr>
<td>EmailRelayOutHosts</td>
<td>List of Name (or IP adress) and port of server(s) to forward email to. Multiple servers are separated with a comma (,). For example: server1:25,server2:25</td>
</tr>
<tr>
<td></td>
<td>Note: Ensure that when the setting is updated the config doesn't contain settings called 'EmailRelayOutServer' or 'EmailRelayOutPort' (delete them if they exist).</td>
</tr>
<tr>
<td>EmailRelayOutParameters</td>
<td>Parameters that are passed to email relay application</td>
</tr>
<tr>
<td>EmailRelayInDirection</td>
<td>Determine the direction of emails. Possible values:</td>
</tr>
<tr>
<td></td>
<td>0 = Incoming</td>
</tr>
<tr>
<td></td>
<td>1 = Outgoing</td>
</tr>
<tr>
<td></td>
<td>2 = Determine email direction using the local domain list parameter EmailRelayInLocalDomains</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>(If sender's email domain exists in parameter <code>EmailRelayInLocalDomains</code> direction is outgoing, or else incoming)</td>
<td></td>
</tr>
<tr>
<td>EmailRelayInLocalDomains</td>
<td>List of local domains. Separate multiple domains with a <code>;</code>. For example opswat.com;mycompany.com. Used to perform recipient verification (any recipient with domain different than the specified domain(s) will be rejected at the SMTP protocol level). Also used when <code>EmailRelayInDirection</code> is set to 2 in order to determine direction.</td>
</tr>
<tr>
<td>EmailRelayInQueueThreshold</td>
<td>Maximum inbound email queue size (exceeding this value will generate an email alert)</td>
</tr>
<tr>
<td>EmailRelayOutQueueThreshold</td>
<td>Maximum outbound email queue size (exceeding this value will generate an email alert)</td>
</tr>
<tr>
<td>EmailRelayOutRetryStart</td>
<td>Start the retry monitor thread (for emails that failed submission)</td>
</tr>
<tr>
<td>EmailRelayOutRetryInterval</td>
<td>Duration between submit retries (increasing with retry count)</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>EmailRelayOutRetryMaxInterval</td>
<td>Maximum duration between retries.</td>
</tr>
<tr>
<td>EmailRelayOutRetryCount</td>
<td>Maximum number of submit retries before email is moved permanent failure</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>EmailRelayOutQueue BadThreshold</td>
<td>Maximum number of .bad files in email queue (exceeding this value cause email alert to be generated)</td>
</tr>
<tr>
<td>EmailRelayOutPermanent FailureThreshold</td>
<td>Maximum number of items in permanent failure (exceeding this value cause email alert to be generated)</td>
</tr>
<tr>
<td>EmailRelayOutMaxConnections</td>
<td>Maximum number of simultaneous SMTP connections when forwarding emails to remote server.</td>
</tr>
<tr>
<td>EmailRelayInRetryStart</td>
<td>Start the retry monitor thread (for emails that failed processing)</td>
</tr>
<tr>
<td>EmailRelayInRetryInterval</td>
<td>Minimum duration between process retries</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>EmailRelayInRetryCount</td>
<td>Maximum number of process retries before email is moved to process failure</td>
</tr>
<tr>
<td>MaxMonitorProcessThreads</td>
<td>Maximum number of emails processed simultaneously</td>
</tr>
<tr>
<td>FastNoAttachment ProcessingEnabled</td>
<td>Avoid sending emails without attachments for processing (improved performance)</td>
</tr>
<tr>
<td>LowPriorityMinSize</td>
<td>Minimum size (in MB) for emails that will be processed on low priority threads</td>
</tr>
<tr>
<td>HighPriorityMaxSize</td>
<td>Maximum size (in MB) for emails that will be processed on the high priority threads</td>
</tr>
<tr>
<td>UseAdjustingThreads</td>
<td>Specifies if monitoring threads for incoming emails should adjust thread count dynamically or have fixed count</td>
</tr>
<tr>
<td>AddressValidation</td>
<td>Specifies if Mail Agent should perform address validation for the incoming emails to detect invalid address (e.g. root@smth, ..@stop, inv/valid)</td>
</tr>
<tr>
<td>EmailRelayInUseTls</td>
<td>Enable TLS for incoming SMTP connections</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>EmailRelayInForceTls</td>
<td>Force all incoming SMTP connections to use TLS (only if EmailRelayInUseTls is true)</td>
</tr>
<tr>
<td>EmailRelayOutUseTls</td>
<td>Enable TLS for outgoing SMTP connections</td>
</tr>
<tr>
<td><strong>MetaDefender Email v3 configuration topic</strong></td>
<td><strong>v3 documentation</strong></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>EmailRelayInTlsCertificate</td>
<td>TLS certificate for incoming SMTP connections (only use when EmailRelayInUseTls is true) Example: <code>-----BEGIN CERTIFICATE-----MIIFYDCCA0igAwIBAgIJALmTg-----END CERTIFICATE-----</code></td>
</tr>
<tr>
<td>EmailRelayInTlsKey</td>
<td>TLS certificate private key for incoming SMTP connections (only used when EmailRelayInUseTls is true) Example: <code>-----BEGIN PRIVATE KEY-----MIIJQgIBADANBgkqhkiG9w0BA....-----END PRIVATE KEY-----</code></td>
</tr>
<tr>
<td>EmailRelayOutClientCertificate</td>
<td>Client certificate for outgoing SMTP connections (used when server requests a client certificate) Example: <code>-----BEGIN CERTIFICATE-----MIIJQgIBADANBgkqhkiG9w0BA....-----END CERTIFICATE-----</code></td>
</tr>
<tr>
<td><strong>Metadefender.Quarantine.Mail.dll.config</strong></td>
<td></td>
</tr>
<tr>
<td>StartRestServer</td>
<td>Start the REST server (SmtpConfiguration)</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>SubmitCommandTimeout</td>
<td>Timeout for SMTP commands</td>
</tr>
<tr>
<td>EmailSubmission RequestExpireSpan</td>
<td>TTL (Time To Live) for an SMTP submit request. If email not been submitted within this timespan the request is lo:</td>
</tr>
</tbody>
</table>

## MetaDefender.Engine .History.dll.config

<table>
<thead>
<tr>
<th>HistoryEntryExpireSpan</th>
<th>Duration to keep history entries in the database</th>
</tr>
</thead>
</table>

## StartRestServer

| StartRestServer                        | Start the REST server (History) |

## MetaDefender.Email.Engine .Processor.dll.config

<table>
<thead>
<tr>
<th>StartRestServer</th>
<th>Start the REST server (Processor)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConvertTnefMessagesToSmtp</td>
<td>Convert TNEF encoded emails to MIME format</td>
</tr>
<tr>
<td>MonitorMode</td>
<td>Enables a monitoring mode of the Mail Agent. When set, emails will be sanitized or quarantined (even when infect etc.)</td>
</tr>
<tr>
<td>AddXHeadersToOutgoingEmail</td>
<td>Force Mail Agent to add x-headers (Custom Email Headers) to outgoing emails</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>EmailProcessedHeaderName</strong></td>
<td>MIME Header name for emails processed by Mail Agent order to avoid duplicates</td>
</tr>
<tr>
<td><strong>EmailAddCustomXHeaders</strong></td>
<td>Add custom x-headers to each email processed by Mail Agent. See <a href="#">Custom Email Headers</a> for more information.</td>
</tr>
<tr>
<td><strong>EmailBlockedQuarantineMode</strong></td>
<td>Option to move blocked emails to MD Core quarantine or submit them via SMTP for quarantine by other service. Possible values are REST (MD Core Quarantine) or SMTP</td>
</tr>
<tr>
<td><strong>EmailSanitizedQuarantineMode</strong></td>
<td>Option to move original copy of sanitized emails to MD Core quarantine or submit them via SMTP for quarantine by other service. Possible values are REST (MD Core Quarantine) or SMTP</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>EmailQuarantineHeaderName</td>
<td>The name of the X-Header that will be added to emails when <code>EmailBlockedQuarantineMode</code> or <code>EmailSanitizedQuarantineMode</code> is set to SMTP. Header value will always be 'True'.</td>
</tr>
<tr>
<td>DoSpfCheck</td>
<td>Enables SPF (Sender Policy Framework) lookups in Mail Agent. Result is placed in a header.</td>
</tr>
<tr>
<td>SpfCheckHeaderName</td>
<td>The name of the X-Header where to store the SPF lookup result</td>
</tr>
<tr>
<td>SpfCheckReasonName</td>
<td>The name of the X-Header where to store a reason for a skipped SPF lookup</td>
</tr>
<tr>
<td>Metadefender.Scanner.dll.config</td>
<td></td>
</tr>
<tr>
<td>MetascanMode</td>
<td>Possible values are <code>COM</code>, <code>RESTv1</code> and <code>RESTv2</code></td>
</tr>
<tr>
<td>MetascanScanTimeout</td>
<td>Scanning timeout</td>
</tr>
<tr>
<td>MetascanScanQueueTimeout</td>
<td>Metadefender Core In Queue timeout</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>MetascanScanProgressPauseMS</td>
<td>Used in RESTv2 mode. Pause (in ms) between progress request calls</td>
</tr>
<tr>
<td>MaxMetadefenderCore InQueueThreshold</td>
<td>If this limit is exceeded an alert will be sent saying that Metadefender Core is unresponsive and email delivery n be slower</td>
</tr>
<tr>
<td>MetadefenderUnavailableRetrySpan</td>
<td>Minimum pause for retry after a Metadefender Core goes down (only applicable if multiple scanners are configurec</td>
</tr>
<tr>
<td>MetadefenderAverageScanTimeSpan</td>
<td>Span for for scan times when calculating average scan ti (when using multiple MD Cores)</td>
</tr>
<tr>
<td>UrlPrioritzationMethod</td>
<td>Metadefender Core Url prioritization method. Possible ve RoundRobin, Circular, ScanTime</td>
</tr>
<tr>
<td>LogAllRequests</td>
<td></td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Increased logging. When set to true it will log all GET requests for getting scan settings and email disclaimers</td>
<td></td>
</tr>
</tbody>
</table>

**MetaDefender.Quarantine.dll.config**

- **MaintenanceInterval**: Interval between checking folder actions & auto-deliver
- **RunAutoActionThread**: Start the thread checking folder actions & auto-deliver
- **CompressionMode**: Quarantine item compression mode. Possible values are None, Zip
- **MonitoringFolderId**: Predefined Quarantined folder id
- **QuarantineReportId**: Predefined Quarantine Report id
- **StartRestServer**: Start the REST server (Quarantine)
- **ReportUidExpireSpan**: Expiry time for entries used to record which quarantine items were included in Quarantine Reports
- **MaxQuarantineItemSize**: Maximum buffer size when accepting quarantine items via REST
- **EmailAlertExpireSpan**: The minimum interval between unique email alerts (error). This is used to prevent too many alerts being sent during continuous errors

**MetaDefender.Email.Engine.Service.exe.config**

- **LogName**: Log name
- **LogFilename**: Log file name
<table>
<thead>
<tr>
<th>MetaDefender Email v3 configuration topic</th>
<th>v3 documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>ComponentList</td>
<td>List of component loaded by service at startup</td>
</tr>
<tr>
<td>RestBaseUrl</td>
<td>REST server base URL</td>
</tr>
<tr>
<td>QuarantineBaseUrl</td>
<td>Metadefender Core Quarantine server base URL</td>
</tr>
<tr>
<td>MetascanUrl</td>
<td>Metadefender Core REST URL</td>
</tr>
<tr>
<td>MetascanApiKey</td>
<td>Metascan API key (encrypted)</td>
</tr>
<tr>
<td>StatusCheckInterval</td>
<td>Interval between component status checks (for error aler</td>
</tr>
<tr>
<td>UsePerformanceCounters</td>
<td>Creates a performance counter category (Metadefender Generic Mail Agent) for monitoring and recording proces data</td>
</tr>
<tr>
<td>ScanEmailBody</td>
<td>Specifies if Mail Agent should scan the body of the email</td>
</tr>
<tr>
<td>MaxRetries</td>
<td>Maximum number of retries before quit trying to connect Metadefender Core</td>
</tr>
<tr>
<td>TimeBetweenRetries</td>
<td>Number of milliseconds before attempting to connect to Metadefender Core</td>
</tr>
<tr>
<td>UpdateUrlsOnStartup</td>
<td></td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td>Specifies if the service should attempt to update config URLs at startup.</td>
</tr>
<tr>
<td></td>
<td>Note: If MD Core load balancing is configured (multiple MetascanUrl's) no URL update will be performed for that setting, regardless of this value.</td>
</tr>
<tr>
<td>MetadefenderCoreIsLocal</td>
<td>Specifies if Metadefender Core is installed locally</td>
</tr>
<tr>
<td>ConnectionCheckOnStartup</td>
<td>Specifies if Mail Agent should do a connection + valid license test on service startup. If enabled Mail Agent will not intercept emails before MD Core is responding.</td>
</tr>
</tbody>
</table>

**Metadefender.Quarantine .Service.exe.config**

<table>
<thead>
<tr>
<th>Key</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MongoDbUrl</td>
<td>Mongo DB URL</td>
</tr>
<tr>
<td>MongoDbUrlEncryptionMode</td>
<td>MongoDb Url value encryption mode. Possible values are None, Encrypted</td>
</tr>
<tr>
<td>MongoDbName</td>
<td>MongoDB database name</td>
</tr>
<tr>
<td>MongoDBStartupTimeout</td>
<td>Timeout to wait for MongoDB to respond</td>
</tr>
<tr>
<td>LogName</td>
<td>Log name</td>
</tr>
<tr>
<td>LogFilename</td>
<td>Log file name</td>
</tr>
<tr>
<td>ComponentList</td>
<td>List of component loaded by service at startup</td>
</tr>
<tr>
<td>RestBaseUrl</td>
<td>REST server base URL</td>
</tr>
<tr>
<td>QuarantineBaseUrl</td>
<td>Metadefender Core Quarantine server base URL</td>
</tr>
<tr>
<td>MetascanUrl</td>
<td>Metadefender Core REST URL</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>MetascanApiKey</td>
<td>Metadefender API key (encrypted)</td>
</tr>
<tr>
<td>WebBaseUrl</td>
<td>Metadefender Web Site base URL</td>
</tr>
<tr>
<td>UpdateUrlsOnStartup</td>
<td>Specifies if the service should attempt to update config URLs at startup</td>
</tr>
<tr>
<td>MetadefenderCoreIsLocal</td>
<td>Specifies if Metadefender Core is installed locally</td>
</tr>
<tr>
<td><strong>Metadefender.Engine</strong>.Statistics.dll.config</td>
<td></td>
</tr>
<tr>
<td><strong>Metadefender.Engine</strong>.Events.dll.config</td>
<td></td>
</tr>
<tr>
<td>Custom Email Headers</td>
<td>Custom Email Headers</td>
</tr>
<tr>
<td>Enable Sender Policy Framework (SPF) Lookup</td>
<td>Enable Sender Policy Framework (SPF) Lookup</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Log collection (collectLogs.exe)</td>
<td>Log collection (collectLogs.exe)</td>
</tr>
<tr>
<td>Log options</td>
<td>Log options</td>
</tr>
<tr>
<td>Multiple Metadefender Core Instances Configuration</td>
<td>Multiple Metadefender Core Instances Configuration</td>
</tr>
<tr>
<td>MetaDefender Email v3 configuration topic</td>
<td>v3 documentation</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>------------------</td>
</tr>
</tbody>
</table>

**Email Processing Workflow (Metadefender Core)**

Sources > Metadefender Email > Workflows

**Configuration > Workflows**

**Quarantine Email**

**Quarantine Email**
<table>
<thead>
<tr>
<th>MetaDefender Email v3 configuration topic</th>
<th>v3 documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources &gt; Metadefender Email &gt; Settings / Quarantine any e-mails that are blocked</td>
<td>Quarantine Email</td>
</tr>
<tr>
<td>Quarantine Email On Another Mail Server</td>
<td>Quarantine Email On Another Mail Server</td>
</tr>
</tbody>
</table>

### Migrating data

⚠️ Currently there is no automation supporting migration from v3 to v4.

In case MetaDefender Email v3 data wanted to be migrated to MetaDefender Email Gateway Security v4, OPSWAT customer support must be contacted.

The description in this section is given for information only.

### Migration window

Migrating data from MetaDefender Email v3 to MetaDefender Email Gateway Security v4 takes time.

During the time of the migration processing will be most probably down (otherwise the migration would potentially be a never ending procedure). For this reason the time window for migration must be planned with care in advance.

The length of the migration procedure depends on the amount of data to be migrated.
Waiting for workflows-in-progress to settle

It is advised to wait all emails in progress to finish processing (either to be completed, quarantined or fail permanently) so that the migration procedure can happen on a stable state of the system.

Potential data loss

Emails (and related information) in processing may be lost during the migration.

Migrated data

During the migration the following data will be migrated:

1. Email history
2. Emails in quarantine
3. Emails in permanent failure status
3 Configuring MetaDefender Email Gateway Security

- 3.1 MetaDefender Email Gateway Security configuration
- 3.2 Configuring TLS
- 3.3 User management
- 3.4 General settings
- 3.5 Logging & alerts
- 3.6 Quarantine configuration
- 3.7 Server profiles
- 3.8 Mail proxy deployment configuration
- 3.9 Cloud deployment configuration
- 3.10 Onsite Microsoft Exchange deployment
- 3.11 Customization of notification emails

3.1 MetaDefender Email Gateway Security configuration

The MetaDefender Email Gateway Security configuration is separated into two parts. The basic server configurations are stored in the configuration files. Other configuration values can be set via the Web Management Console.

- 3.1.1 Web Management Console
- 3.1.2 Windows Registry configuration

3.1.1 Web Management Console

The Web Management Console is available at (<server name or IP> is the DNS name or IP address of your test server):

http://<server name or IP>:8058

⚠️ As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. To set up TLS see 3.2 Configuring TLS.
Every change made in MetaDefender Email Gateway Security configuration via the Web Management Console is applied when you select **Save settings** or **OK**, except if the change cannot be applied.

Typical issues related to the Web Management Console:

- **5.3 Inaccessible Web Management Console**

### 3.1.2 Windows Registry configuration

- `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security`
- `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security\global`
- `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security\logger`

Some configuration options of the server are available in Windows Registry.

⚠️ **After modifying the server configuration entries in the Windows Registry, you must restart the Metadefender Email Gateway Security service in order for the changes to take effect.**

Default logging target is Windows Event Log with default level of **info** (see below).
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExchangeMode</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td><img src="https://example.com" alt="Important Note" /> Do not change this value manually!</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This value is set when Email Gateway Security is installed in Exchange plugin mode (for details see 3.10 Onsite Microsoft Exchange deployment).</td>
</tr>
<tr>
<td>external_quarantine_block</td>
<td>dword</td>
<td>optional</td>
<td></td>
<td>Enable quarantining the original copy of blocked emails on another mail server. For details see 3.6.1 Quarantine emails on another mail server.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If the parameter does not exist or if it is 0, then the internal quarantine will be used in case of blocked emails.</td>
</tr>
<tr>
<td>external_quarantine_sanitize</td>
<td>dword</td>
<td>optional</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Parameter</td>
<td>Default value</td>
<td>Type</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------</td>
<td>------------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enable quarantining the original copy of sanitized emails on an other mail server. For details see 3.6.1 Quarantine emails on another mail server. If the parameter does not exist or if it is 0, then the internal quarantine will be used in case of sanitized emails.</td>
<td>None</td>
<td>string</td>
<td>optional</td>
<td></td>
</tr>
<tr>
<td>sender_helo_domain</td>
<td>string value</td>
<td>string</td>
<td>optional</td>
<td>The fully qualified domain name (FQDN) that Email Gateway Security will send in HELO/EHLO commands to relay SMTP servers. Besides this FQDN the external IP address of Email Security will also be sent. For details see section Opening and closing in RFC 821. If the parameter does not exist or if it is empty then the computer name of Email Gateway Security is sent in HELO/EHLO. Error rendering macro 'drawio' : null</td>
</tr>
<tr>
<td>receiver_helo_domain</td>
<td>string value</td>
<td>string</td>
<td>optional</td>
<td>The fully qualified domain name (FQDN) that Email Gateway Security will send in HELO/EHLO</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default value</td>
<td>Type</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>---------------</td>
<td>--------</td>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>commands to SMTP clients. For details see section <em>Opening and closing</em> in RFC 821. If the parameter does not exist or if it is empty then the computer name of Email Gateway Security is sent in the response to a HELO/EHLO. Error rendering macro 'drawio': null</td>
</tr>
<tr>
<td>exchange_exclude_probe_emails</td>
<td>dword</td>
<td>optional</td>
<td></td>
<td>Microsoft Exchange Server sends probe email messages to monitor the health status of the email processing components. This probe messages can, however, fill Audit &gt; Email History. Setting this parameter to 0 will enable listing Exchange probe messages in Audit &gt; Email History. If the parameter does not exist or if it is 1, then Exchange probe messages are not listed in Audit &gt; Email History.</td>
</tr>
</tbody>
</table>
There is no need to restart any services for this setting to take effect, because the transport agent reads and applies this registry setting for each email.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>processing_threshold</td>
<td></td>
<td>dword</td>
<td>optional</td>
<td>This parameter limits the number of emails with &quot;Processing&quot; status at the same time. If this parameter is not present then this number is 150 by default. Setting this value lower can reduce the processing load on both Email Gateway Security and Core. If the parameter is 0 then the throttling is disabled.</td>
</tr>
</tbody>
</table>

HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security\global

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restaddress</td>
<td>0.0.0.0</td>
<td>string</td>
<td>required</td>
<td>One of the IP addresses of the computer that runs the product to serve REST API and web user interface (0.0.0.0 means all interface)</td>
</tr>
</tbody>
</table>
### restport

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>restport</td>
<td>8058</td>
<td>string value</td>
<td>required</td>
<td>Designated port number for the web and REST interface</td>
</tr>
</tbody>
</table>

### HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security\logger

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>logfile</td>
<td></td>
<td>string value</td>
<td>optional</td>
<td>Location of a log file to write log messages to. If the parameter does not exist, then no logs are written to any logfile.</td>
</tr>
<tr>
<td>loglevel</td>
<td></td>
<td>string value</td>
<td>optional</td>
<td>Level of logging. Supported values are: debug, info, warning, error.</td>
</tr>
<tr>
<td>wineventlog_level</td>
<td>info</td>
<td>string value</td>
<td>optional</td>
<td>Level of logging. Supported values are: debug, info, warning, error. If the parameter does not exist, then no logs are written to the Windows Logs.</td>
</tr>
<tr>
<td>syslog</td>
<td></td>
<td>string value</td>
<td>optional</td>
<td>Value can only be in form of udp://&lt;hostname&gt;:&lt;port&gt;. If the parameter does not exist, then no logs are written to syslog.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default value</td>
<td>Type</td>
<td>Required</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------</td>
<td>----------</td>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(Multiple server can be specified separated with comma)</td>
</tr>
<tr>
<td>syslog_level</td>
<td></td>
<td>string</td>
<td>optional</td>
<td>Level of logging. Supported values are: debug, info, warning, error.</td>
</tr>
<tr>
<td>override</td>
<td></td>
<td>string</td>
<td>optional</td>
<td>Override specific log ids to display them on another level e.g.: &quot;1723: error,663:info&quot;. Note: when displaying these log ids their original level will remain the same. Empty string is allowed as a value.</td>
</tr>
<tr>
<td>cef</td>
<td>false</td>
<td>string</td>
<td>optional</td>
<td>If true, the log format is Common Event Format.</td>
</tr>
<tr>
<td>local_timezone</td>
<td>false</td>
<td>string</td>
<td>optional</td>
<td>If true, the times sent in syslog messages will be in the server's local timezone. This does not effect entries in the log file/Windows event log. When syslog is used with cef and local_timezone enabled the timezone name can vary based on the underlying system and it's settings.</td>
</tr>
</tbody>
</table>

Examples
- Syslog
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Type</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nginx_logfile</td>
<td>[installdir] \nginx\nginx.log</td>
<td>string</td>
<td>optional</td>
<td>File name and path to store the NGINX logs. (Rotation of this log has not yet been solved on Windows systems)</td>
</tr>
</tbody>
</table>

You must set both of `syslog` and `syslog_level` or none of them, and you must set both of `logfile` and `loglevel` or none of them.

### 3.2 Configuring TLS

- **Digital ID**
  - Key and certificate files
- **Inbound connections**
• Web Management Console
• Inbound SMTP service
• Outbound connections
  • Connection to Core
  • Outbound SMTP
    • StartTLS
      • Optional StartTLS
      • Mandatory StartTLS
    • SMTPS

⚠️ For production MetaDefender Email Gateway Security deployments a more sophisticated TLS configuration is recommended than what is described below. Please consult the nginx documentation on Configuring HTTPS servers for further details.

⚠️ It is not recommended to use self-signed certificates in production environments. If you do not have a suitable certificate, you can apply to a Certificate Authority to obtain one.

Digital ID
To keep the solution simple, MetaDefender Email Gateway Security uses a single private/public key pair as its digital identifier.

⚠️ This digital ID –the same certificate– is used when MetaDefender Email Gateway Security acts either as a server or as a client.

⚠️ Key and certificate files must be in PEM format.

Key and certificate files
The following files of the digital ID must be placed on the following paths in the server’s file system:
### Inbound connections

#### Web Management Console

MetaDefender Email Gateway Security supports accessing Web Management Console via HTTPS. This feature is, however, not enabled by default. To enable the TLS/HTTPS you should modify MetaDefender Email Gateway Security configuration by following the next steps.

Let us assume that MetaDefender Email Gateway Security is installed in:

```
C:\Path\To\Metadefender Email Security
```

To simply enable TLS:

1. **Create file ssl.conf in the directory** `C:\Path\To\MetaDefender Email Security\nginx`
2. **Add the following lines:**

<table>
<thead>
<tr>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private key</td>
</tr>
<tr>
<td>Certificate</td>
</tr>
<tr>
<td>Private key and certificate</td>
</tr>
</tbody>
</table>
Inbound SMTP service

MetaDefender Email Gateway Security's SMTP service can be configured to use TLS encryption for increased security. For details see 3.2.1 Inbound TLS support.

Outbound connections

TLS for outbound connections can be set up at the appropriate server profile. For details see 3.7 Server profiles.

⚠️ In case of outbound connections the servers certificate must always be trusted by the client.

In practice it means that either the CA certificate –that was used for signing the server's certificate–, or the server's certificate itself must be installed in the Email Gateway Security's operating system's trusted certificate store.

Connection to Core

To connect to a Core server over TLS perform the following steps:

1. Configure the Core server to listen on HTTPS. For details see 3.8. Configuring TLS/SSL,
2. Add this Core to your server profiles using https scheme. For details see 3.7 Server profiles.

Outbound SMTP

To connect to an SMTP server over TLS first you need to decide which favour to use: StartTLS (TLS over SMTP) or SMTPS (SMTP over TLS).

✅ Due to security considerations always prefer SMTPS to StartTLS whenever possible.
StartTLS

In case of StartTLS you still need to decide whether using StartTLS is just an option or it is mandatory.

Optional StartTLS

If StartTLS is optional then the client will try to establish the TLS connection, and if it fails, then the connection will fail over to a clear text connection.

To connect to an SMTP server using optional StartTLS perform the following steps:

1. Configure the SMTP server to either
   a. Support StartTLS – in this case clear text SMTP connections will be upgraded to TLS; or
   b. Not support StartTLS – in this case SMTP connections will be fall back to clear text.
2. Add this SMTP server to your server profiles
   a. Using smtp scheme, with
   b. TRANSPORT LEVEL ENCRYPTION set to STARTTLS optional.
   c. For details see 3.7 Server profiles.

Mandatory StartTLS

If StartTLS is mandatory then the client will try to establish the TLS connection, and if it fails, then the connection will fail.

To connect to an SMTP server using mandatory StartTLS perform the following steps:

1. Configure the SMTP server to Support StartTLS;
2. Add this SMTP server to your server profiles
   a. Using smtp scheme, with
   b. TRANSPORT LEVEL ENCRYPTION set to STARTTLS required.
   c. For details see 3.7 Server profiles.

SMTPS

In case of SMTPS, the TLS handshake comes first, and if (and only if) it succeeds, then the SMTP connection is established over the TLS.

To connect to an SMTP server over TLS perform the following steps:
Configure the SMTP server to listen on SMTPS.

Add this SMTP server to your server profiles using smtps scheme. For details see 3.7 Server profiles.

3.2.1 Inbound TLS support
MetaDefender Email Gateway Security's SMTP service can be configured to use TLS encryption for increased security. Refer to the sections below how to import/generate a TLS certificate for inbound SMTP traffic.

Prerequisite
- OpenSSL 32-bit

Incoming TLS support
Follow the instructions below if you want to enable TLS encryption for incoming emails.

I have a pkcs#12 certificate:
For these steps you will need a pkcs#12 certificate file (.pfx).

⚠️ If you don't have a certificate .pfx file, refer to 148381589 for instructions how to export a certificate to a .pfx file.

1. Ensure that OpenSSL is installed. If you do not have OpenSSL installed, it can be downloaded from here: https://slproweb.com/products/Win32OpenSSL.html (unofficial distribution)
   Note: MetaDefender Email Gateway Security requires that the OPENSSL_CONF system environment variable is set (normally this is done automatically when installing OpenSSL)

2. Open an administrator command prompt and navigate to the MetaDefender Email Gateway Security mailagenthost folder (default: C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost)

3. Type the following command:

   ```
   tlsutil.exe -b "<path to .pfx>" -j "<certificate password>"
   ```

   (Replace <path to .pfx> with the path to your .pfx certificate file. -j parameter can be omitted if the certificate is not password protected)
4. The certificate is imported and a tls.pem file is created.

C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost>tlsutil.exe -b "<path to .pfx>" -j "<certificate password>"
Private key & certificate written to C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost\tls.pem

5. Go to Settings > Global Settings and enable TLS selecting STARTTLS optional or STARTTLS required as ENCRYPTION.

I have a pkcs#8 certificate:
For these steps you will need a certificate file and a private key file (pkcs#8).

1. Ensure that OpenSSL is installed. If you do not have OpenSSL installed, it can be downloaded from here: https://slproweb.com/products/Win32OpenSSL.html (unofficial distribution)
   
   Note: MetaDefender Email Gateway Security requires that the OPENSSL_CONF system environment variable is set (normally this is done automatically when installing OpenSSL)

2. Open an administrator command prompt and navigate to the MetaDefender Email Gateway Security mailagenthost folder (default: C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost)

3. Type the following command:

   tlsutil.exe -y "<path to certificate file>" -z "<path to private key file>"

   (Replace <path to certificate file> with the path to your certificate file and <path to private key file> with the path to your private key file)

4. The certificate is imported and a tls.pem file is created.

C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost>tlsutil.exe -y "<path to certificate file>" -z "<path to private key file>"
Private key & certificate written to C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost\tls.pem

5. Go to Settings > Global Settings and enable TLS selecting STARTTLS optional or STARTTLS required as ENCRYPTION.
I want to use a self-signed certificate:

Follow these steps if you wish to use a self-signed certificate.

1. Ensure that OpenSSL is installed. If you do not have OpenSSL installed, it can be downloaded from here: https://slproweb.com/products/Win32OpenSSL.html (unofficial distribution)
   
   Note: MetaDefender Email Gateway Security requires that the OPENSSL_CONF system environment variable is set (normally this is done automatically when installing OpenSSL)

2. Open an administrator command prompt and navigate to the MetaDefender Email Gateway Security mailagenthost folder (default: C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost)

3. Type the following command:

   ```
   tlsutil.exe -e -d 365 -c US -s "California" -l "San Francisco" -o "Company"
   ```

   Replace any of the following parameters with desired values:
   
   - `-d` = Number of days the certificate is valid
   - `-c` = Country code (2 letter ISO)
   - `-s` = State/District
   - `-l` = City
   - `-o` = Company name

4. The certificate is imported and a tls.pem file is created.

   ```
   C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost>tlsutil.exe -e -d 365 -c US -s "California" -l "San Francisco" -o "Company"
   Generating a 4096 bit RSA private key
   ................++
   ..............................................................
   ................++
   writing new private key to 'tls_key.pem'
   ----- Private key & certificate written to C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost\tls.pem
   ```

5. Go to **Settings > Global Settings** and enable TLS selecting **STARTTLS optional** or **STARTTLS required** as ENCRYPTION.
**TLS settings for incoming connections**

Starting with v.4.3.0 Email Gateway Security uses Window's Schannel for incoming secure connections by default. This makes possible to configure the accepted SSL/TLS versions, ciphers, cipher suites etc. via Windows registry settings. You can find information about how to configure specific settings here: [https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings](https://docs.microsoft.com/en-us/windows-server/security/tls/tls-registry-settings)

**Example: How to disable SSL3 support**

Let's check first if SSL 3.0 is supported. For that you should run this command:

```plaintext
Check SSL 3.0 support
openssl.exe s_client -ssl3 -connect localhost:10025 -starttls smtp
```

If SSL 3.0 is supported you will have an output like this:

![SSL 3.0 output example](image)

Let's disable it following these steps:

1. Open the registry editor (regedit)
2. Go to HKLM
   - SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
3. Add a new key called "SSL 3.0"
4. Add a new subkey to "SSL 3.0" called "Server"
5. Create an Enabled entry under the "Server" key as a DWORD and set it's value to 0
6. Restart MetaDefender Email Gateway Security service
The registry should look like this:

![Registry Editor Screenshot]

Run the command again to check the SSL 3.0 support now.

```
C:\openssl\openssl.exe s_client -ssl3 -connect localhost:10025 -starttls smtp
```

```
CONNECTED(00000003)
4294966072:error:140900E0:SSL routines:ssl3_write_bytes:ssl handshake failure:s3_pkt.c:659:
---
No peer certificate available
---
SSL handshake has read 114 bytes and written 0 bytes
---
New (NONE) Cipher is (NONE)
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
  Protocol : SSLv3
  Cipher : 0000
  Session-ID: 619252d4f11e11d
  Session-ID-ctx: Master-Key:
    Key-Arg : None
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    Start Time: 1529576568
    Timeout : 7200 (sec)
    Verify return code: 0 (ok)
```

In the image above it can be seen that the SSL 3.0 is not supported after the changes.

**Export a certificate**

If you have an existing certificate in your certificate store that you want to use with MetaDefender Email Gateway Security to enable incoming TLS it will first have to be exported into a .pfx file. Follow the instructions below to export the certificate.
1. Run Microsoft Management Console (mmc.exe).

2. Add the Certificates Snap-In:
   a. Select File > Add/Remove Snap in...
   b. Select 'Certificates' and click 'Add >'.
   c. Select the account for whom the certificate is installed (usually this is 'Computer account'), then click 'Next >'.
   d. Select 'Local Computer' if the certificate is installed this computer, then click 'Finish'.
   e. Click 'OK' to close the 'Add or Remove Snap-ins' dialog.

   ![Microsoft Management Console](image1.png)

   f. Navigate to the certificate you wish to export, then right-click and select 'All Tasks > Export...'.

   g. Click 'Next >' in the 'Certificate Export Wizard' welcome step.

   ![Certificate Export Wizard](image2.png)
h. Select 'Yes, export the private key' and click 'Next >'.

![Certificate Export Wizard]

Note: The certificate must include the private key, so if this option is unavailable the certificate cannot be used with MetaDefender Email Gateway Security.

i. Select 'Personal Information Exchange - PKCS #12 (.PFX)' and click 'Next >'.

![Certificate Export Wizard]

j. Specify a certificate password and click 'Next >'.

![Certificate Export Wizard]
k. Specify a file name for the exported certificate and click 'Next >'.

l. Click 'Finish' to complete the export.
4.7.4

m. A dialog will display that export was successful.

![Certificate Export Wizard]

The export was successful.

Once the export is complete, refer to 3.2.1 Inbound TLS support for instructions how to install the certificate in MetaDefender Email Gateway Security.

3.3 User management

- Users and groups tab
  - Legacy default user
  - Functions
    - Add new user from a Local type user directory
    - API keys
    - Add new users from an LDAP type or Active Directory type user directory
    - Add new group from an LDAP type or Active Directory type user directory
    - Assign roles to a user, LDAP group or Active Directory group
    - Delete user
  - Special user accounts
    - SYSTEM/management account
- Roles tab
  - Default roles
  - Permissions
    - Effective right
  - Functions
    - Modify role
- User directories tab
Default user directories
Local type user directories
Active Directory type user directories
LDAP type user directories

Functions
- Add new Local type user directory
- Add new LDAP type or Active Directory type user directory
  - Differences between LDAP and Active Directory type user directories
- Delete user directory
- Enable or disable user directory
- Unlock locked accounts

- Transport Layer Security
- LDAP attributes
- Active Directory attributes
- Notes

To manage the users of the product, go to the Settings > User Management menu in the Web Management Console.

**Users and groups tab**

The USERS AND GROUPS tab lists the existing users, LDAP groups and Active Directory groups in the system.
Legacy default user

Previous versions of the product created a default user during the installation with the following credentials and parameters. This default user may still exist if the product was upgraded from previous versions.

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Name</th>
<th>Email</th>
<th>Roles</th>
<th>User directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>admin</td>
<td>Administrator</td>
<td>admin@localhost</td>
<td>Administrators</td>
<td>LOCAL</td>
</tr>
</tbody>
</table>

Functions

Besides listing existing users, LDAP and AD groups, the USERS AND GROUPS tab provides the following functions:

- Add new user, LDAP or AD group
- Modify (and view) existing user’s, LDAP or AD group’s properties
- Delete existing user, LDAP or AD group
Add new user from a Local type user directory

To add a new user from a Local type user directory click the ADD NEW USER button and select a Local type user directory in the USER DIRECTORY drop down list.

The field ASSIGN TO ROLES lists all the roles that are assigned to this user. See section Assign roles to a user, LDAP group or Active Directory group for details about role assignment.

⚠️ As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. For details see Transport Layer Security.

⚠️ If enhanced password policy is enabled for the user directory this user belongs to then the new password must fulfill the password complexity requirements listed at the Local type user directories section.

API keys

The APIKEY value provides access to the product’s REST API for the user under editing with no authentication. If no such functionality is needed for the user then this field can be left blank.

There are two methods to create an APIKEY for a user:

1. Generate the APIKEY by using Generate link next to the APIKEY field,
2. Manually enter the APIKEY value; it must matches the following criteria:

-APIKEY validation criteria

- The length of the API key must be exactly 36 characters.
- It must contain numeric and lower case a, b, c, d, e and f letter characters only (e.g. "1x2y3z..." is invalid because of the x, y and z characters).
- It must contain at least 10 lower case a, b, c, d, e or f letter characters.
- It must contain at least 10 numeric characters.
- It is allowed to contain at most 3 consecutive lower case letter characters (e.g. "abcd1a2b3c..." is invalid because of the four consecutive letters).
- It is allowed to contain at most 3 consecutive numeric characters (e.g. "1234a1b2c3..." is invalid because of the four consecutive numeric characters).
Add new users from an LDAP type or Active Directory type user directory

To add a new user from an LDAP type or Active Directory type user directory click the ADD NEW USER button and select an LDAP type or Active Directory type user directory in the USER DIRECTORY drop down list. Select USER as the ACCOUNT TYPE.

Provide the name of the account in the ACCOUNT NAME field and click the FIND ACCOUNT button to look up the account in the LDAP or Active Directory. If the lookup succeeds then the ACCOUNT DISPLAY NAME and the DISTINGUISHED NAME fields are filled automatically.

⚠️ Do provide the account name precisely. There is no functionality to look up similar names or partial matches.

The field ASSIGN TO ROLES lists all the roles that are assigned to this user. See section Assign roles to a user, LDAP group or Active Directory group for details about role assignment.
Add new group from an LDAP type or Active Directory type user directory

The purpose of adding an LDAP or Active Directory group to the product is to assign role(s) to all the users in that LDAP or Active Directory group. The users of the LDAP or Active Directory group can authenticate with their LDAP or Active Directory credentials in the product's Web Management Console and will be assigned with the roles assigned to the group.

To add a new group from an LDAP type or Active Directory type user directory click the ADD NEW USER button and select an LDAP type or Active Directory type user directory in the USER DIRECTORY drop down list.

Select GROUP as the ACCOUNT TYPE.

Provide the name of the group in the ACCOUNT NAME field and click the FIND ACCOUNT button to look up the group in the LDAP or Active Directory. If the lookup succeeds then the ACCOUNT DISPLAY NAME and the DISTINGUISHED NAME fields are filled automatically.
Do provide the group name precisely. There is no functionality to look up similar names or partial matches.

The field ASSIGN TO ROLES lists all the roles that are assigned to all users of the selected group. See section Assign roles to a user, LDAP group or Active Directory group for details about role assignment.

**Assign roles to a user, LDAP group or Active Directory group**

Role(s) must be assigned to users, LDAP groups and Active Directory groups in order they can use the Web Management Console. The roles assigned to a certain user determine what pages that user can access in the Web Management Console and whether she can only read, or modify as well values on a page.

The field ASSIGN TO ROLES in the Add/assign new user(s) and Modify user dialogs lists all the roles that are assigned to the user.

The following is the role assignment policy:

1. At least one role must be assigned to a user, LDAP group or Active Directory group
2. Optionally multiple different roles can be assigned
   a. In this case the most permissive available right applies to each function.

For details about the permissiveness of roles see the Roles tab section.

Example:

<table>
<thead>
<tr>
<th>Roles assigned</th>
<th>Effective permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Read only permission</td>
</tr>
<tr>
<td></td>
<td>Config history, Global settings</td>
</tr>
<tr>
<td>security_auditor</td>
<td>Config history, Global settings</td>
</tr>
<tr>
<td>help_desk</td>
<td>Global settings</td>
</tr>
<tr>
<td>security_admin AND security_auditor</td>
<td>Config history, Global settings</td>
</tr>
</tbody>
</table>
Delete user

⚠️ Active sessions of the deleted user will be aborted at the time of the next interaction with the server.

Special user accounts

Some user accounts are reserved in the product for system internal usage. These accounts are documented in this section.

⚠️ The special accounts documented in this section are for internal usage. Do not directly modify these accounts through the user management functions cause it may give unexpected results.

SYSTEM/management account

The SYSTEM/management account is reserved for Central Management.

When the product is connected to Central Management as a managed instance, then this account is automatically created by Central Management at the first successful connection with the following parameters:

<table>
<thead>
<tr>
<th>Username</th>
<th>Password</th>
<th>Name</th>
<th>Email</th>
<th>Roles</th>
<th>User directory</th>
</tr>
</thead>
<tbody>
<tr>
<td>management</td>
<td>N/A</td>
<td>Metadefender Central Management</td>
<td>management@localhost</td>
<td>Administrators</td>
<td>SYSTEM</td>
</tr>
</tbody>
</table>

All consecutive connection attempts are performed by Central Management using the SYSTEM/management account.

Roles tab

Roles can be assigned to users. This simplifies controlling permissions. The Roles tab lists the existing roles in the system.
Default roles

After installation the following default roles are created with the following parameters:

<table>
<thead>
<tr>
<th>Rolename</th>
<th>Display name</th>
<th>Default member username</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Administrators</td>
<td>admin</td>
<td>Full on all functions</td>
</tr>
<tr>
<td>security_admin</td>
<td>Security administrators</td>
<td></td>
<td>Full on Email History, Quarantine, Failed Emails, Refused Emails, Security rules, Server profiles, Quarantine reports and Global settings functions</td>
</tr>
<tr>
<td>security_auditor</td>
<td>Security auditor</td>
<td></td>
<td>Read-only on all functions</td>
</tr>
<tr>
<td>help_desk</td>
<td>Help desk</td>
<td></td>
<td>Read-only on Email History, Security rules, Server profiles and Global settings functions</td>
</tr>
</tbody>
</table>
Permissions

Each role has a set of rights associated to it. Each of these rights represent the level of access to the appropriate function of the MetaDefender product’s Web Management Console. A right can be set to one of three different values:

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NONE</td>
<td>Users with this effective right have no right to access the given function of the MetaDefender product’s Web Management Console. The menu belonging to the function is not displayed.</td>
</tr>
<tr>
<td>READ-ONLY</td>
<td>Users with this effective right are granted to access the given function for observation purposes only. Users of this role can, however, not effectuate any modifications or any change to the function.</td>
</tr>
<tr>
<td>FULL</td>
<td>Users with this effective right have full access to the given function, including viewing any data belonging to it and modifying its configuration.</td>
</tr>
</tbody>
</table>

Effective right

A single user may have multiple roles assigned to it. There may be cases, when one of the assigned roles of the user would prohibit, while the other assigned role of the user would permit a certain function. In this case the more permissive right will be effective.

<table>
<thead>
<tr>
<th>Right</th>
<th>More permissive</th>
<th>More restrictive</th>
</tr>
</thead>
<tbody>
<tr>
<td>FULL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>READ-ONLY</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NONE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See section Assign roles to a user, LDAP group or Active Directory group for details about assigning multiple roles to a single user.

Functions

Besides listing existing roles the Roles tab provides the following functions:

- Add new role
- Modify (and view) existing role
- Delete existing role
The default role *Administrators* can not be deleted or modified.

**Modify role**

The users' permissions won't be modified during the session, even if one of their roles are modified in the meantime.

For example:

1. A user is assigned to the role *security_admin* and has Full permissions on *Config history*
2. She can see *Config history* changes
3. During her session the *Config history* permissions are set to *None* for the *security_admin* role.
4. The logged in user can still select the *Config history* menu and can see the configuration changes there.

Then new permissions will be effective only after a logout and new login.

**Delete role**

A role can not be deleted as long as it is assigned to any user.

As a consequence deleting a role can not affect active sessions of users.

**User directories tab**

Users can be organized into separate user directories. User directories help to enforce the following login policies:

1. Lockout after a number of consecutive failed login attempts
2. Disable logins for all users of the user directory

The Users tab lists the existing user directories in the system.
Default user directories

After installation two default user directories are created with the following parameters:

<table>
<thead>
<tr>
<th>User directory type</th>
<th>Name</th>
<th>Number of failed logins before lockout</th>
<th>Lockout time [minutes]</th>
<th>Enable enhanced password policy</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local</td>
<td>LOCAL</td>
<td>3</td>
<td>5</td>
<td>False</td>
<td>This user directory can be used to add local user accounts to the system.</td>
</tr>
<tr>
<td>Local</td>
<td>SYSTEM</td>
<td>0</td>
<td>0</td>
<td>False</td>
<td>This user directory is used to add special, (e.g. machine-to-machine) user accounts to the system.</td>
</tr>
</tbody>
</table>
## Local type user directories

Local type user directories allow creating users that locally exist on the MetaDefender product.

To protect user accounts of a local user directory against brute force password breaking attacks, the following policy settings may be applied to each local type user directory:

- **NUMBER OF FAILED LOGINS BEFORE LOCKOUT**: After this number of consecutive failed login attempts the account gets locked.
- **LOCKOUT TIME [MINUTES]**: The account remains locked for the given minutes.
  - When the lockout time elapses, the account lock gets released automatically.
  - Users with appropriate permission may release the account lock earlier using the **RELEASE LOCKOUT** button.
- **ENABLE ENHANCED PASSWORD POLICY**: If enabled, then the following policy is enforced for new passwords:

### Enhanced password complexity policy

- The password must be at least 8 characters long;
- The password must contain at least one of each
  - Upper case Latin letter character ([A-Z]),

---

<table>
<thead>
<tr>
<th>User directory type</th>
<th>Name</th>
<th>Number of failed logins before lockout</th>
<th>Lockout time [minutes]</th>
<th>Enable enhanced password policy</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>This user directory is for system internal use, do not modify (delete, assign users, etc.) it manually.</td>
</tr>
</tbody>
</table>
Active Directory type user directories

Active Directory type user directories allow users defined in an Active Directory to access the MetaDefender product.

Active Directory type user directories do not provide the possibility to define login policies; these policies may be defined in the Active Directory directly.

LDAP type user directories

LDAP type user directories allow users defined in an LDAP directory to access the MetaDefender product.

LDAP type user directories do not provide the possibility to define login policies; these policies may be defined in the LDAP directory directly.

Functions

Besides listing existing user directories the USER DIRECTORIES tab provides the following functions:

- Add new user directory
- Modify (and view) existing user directory
- Delete existing user directory
- Enable or disable existing user directory
- Unlock locked accounts

Add new Local type user directory

Click the ADD NEW USER DIRECTORY button and select Local in the USERDIRECTORY TYPE drop down list.

For explanation of the NUMBER OF FAILED LOGINS BEFORE LOCKOUT and LOCKOUT TIME [MINUTES] fields read the Local type user directories section.
Add new LDAP type or Active Directory type user directory

1. Click the ADD NEW USER DIRECTORY button and select LDAP or Active Directory in the USERDIRECTORY TYPE drop down list respectively. Learn more about the differences between LDAP and Active Directory type user directories.

2. Multiple LDAP or Active Directory servers can be configured to provide high availability of the directory services.

   a. Server preference:

      i. The configured servers are taken for a connection attempt in a top-bottom fashion.

      ![Diagram of LDAP/AD Server 1 to Server n]

   b. Failover conditions

      i. If the connection to a certain LDAP or AD server fails (for a reason other then authentication error) then
ii. The next server in the preference order is attempted.

![Flowchart diagram]

**c. Server properties**

The following properties must be specified for each LDAP or AD server:

i. **SERVER HOST**: IP address or FQDN of the server

ii. **SERVER PORT**: The TCP port on which the directory service is listening

iii. **ENCRYPTION**: What kind of encryption to use when establishing the connection

   1. **None**: No encryption, communication on a clear-text channel

   As long as ENCRYPTION field is set to *None* there is no encryption used between the MetaDefender product and the LDAP or Active Directory server. All passwords and other information are sent clear-text over the network.

   Use *StartTLS* or *SSL* as ENCRYPTION whenever possible.
2. StartTLS: The connection is established on a clear-text channel, then upgraded to TLS (TLS over LDAP)

3. SSL: The connection is established on a TLS encrypted channel (LDAP over TLS)

For StartTLS and SSL type encrypted connections the LDAP or Active Directory server must authenticate itself with a certificate that's validity can be verified by the MetaDefender product. This can happen in basically two ways:

a. Trusted certificate: the certificate's root certificate is issued by a trusted certificate authority (e.g. Comodo, Symantec, GoDaddy, GlobalSign, IdenTrust, DigiCert, StartCom, Entrust, Trustwave, Verizon, etc.) These root certificates are usually pre-installed in modern operating systems and as a result can be verified by the MetaDefender product.

b. Self-signed certificate: the certificate (or it's root certificate) is added to the system as a trusted root certificate. For details about adding a certificate as a trusted root certificate, see the manuals of the operating system of your MetaDefender product. For your convenience here are the necessary commands for Windows and some Linux distributions (the path to the self signed certificate file is C:\Path\To\certificate.crt or /path/to/certificate.crt on Windows or Linux respectively):

   **Windows**

   ```
   > certutil -addstore -f "ROOT" C:\Path\To\certificate.crt
   ```

3. Select whether to authenticate or not at the time of the bind request. Authentication at the time of the bind request is an additional security control for directory services like host based authentication at SSH. It may or may not be required by the server.
4. Selecting the ANONYMOUS BIND option will try to attempt to bind to the directory service with no username and password.

If the ANONYMOUS BIND option is selected, then the values specified for BIND USERNAME and BIND PASSWORD are ignored, their text fields are disabled.

Some LDAP and Active Directory servers may be configured to not permit anonymous bind requests.

b. Specify the BIND USERNAME and BIND PASSWORD values. These values must be the name as DN (distinguished name) and password of a user who has permissions to do searches in the directory.

As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. For details see Transport Layer Security.

4. The USER BASE DN and the GROUP BASE DN values should provide the entries in the LDAP or Active Directory tree where user and group entity lookups should be started.

For further LDAP specific property details see LDAP attributes.

For further Active Directory specific property details see Active Directory attributes.

5. Click the TEST button to test the LDAP or Active Directory settings. If the test succeeds then the user directory can be added to the list with the ADD button.
Add user directory

USER DIRECTORY TYPE

Active Directory

NAME

NAME

ACTIVE DIRECTORY SETTINGS

SERVER HOST

SERVER PORT

ENCRYPTION

Delete

Add Server

[ ] ANONYMOUS BIND

BIND USERNAME

USERNAME

BIND PASSWORD

PASSWORD

USER BASE DN

USER BASE DN

GROUP BASE DN

GROUP BASE DN

ADD CANCEL TEST
Add user directory

USER DIRECTORY TYPE
LDAP

NAME
NAME

LDAP SETTINGS

SERVER HOST
SERVER PORT
ENCRIPTION
Delete

Add Server

Anonymous BIND

BIND USERNAME
USERNAME

BIND PASSWORD
PASSWORD

USER BASE DN
USER BASE DN

GROUP BASE DN
GROUP BASE DN

LDAP USER SCHEMA SETTINGS

USER OBJECT CLASS
USER OBJECT CLASS

USER ACCOUNT ATTRIBUTE
USER ACCOUNT ATTRIBUTE

USER EMAIL ATTRIBUTE
USER EMAIL ATTRIBUTE
Differences between LDAP and Active Directory type user directories

From MetaDefender products' perspective LDAP directories are supersets of Active Directory directories. In other words, an Active Directory configuration can be specified using LDAP user directory type, setting certain properties to predefined values.

The following properties must be set to the following values to implement an Active Directory type user directory with LDAP type user directory
<table>
<thead>
<tr>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER OBJECT CLASS</td>
<td>user</td>
</tr>
<tr>
<td>USER ACCOUNT ATTRIBUTE</td>
<td>samaccountname</td>
</tr>
<tr>
<td>USER EMAIL ATTRIBUTE</td>
<td>mail</td>
</tr>
<tr>
<td>USER DISPLAY NAME ATTRIBUTE</td>
<td>cn</td>
</tr>
<tr>
<td>GROUP OBJECT CLASS</td>
<td>group</td>
</tr>
<tr>
<td>GROUP ACCOUNT ATTRIBUTE</td>
<td>samaccountname</td>
</tr>
<tr>
<td>GROUP DISPLAY NAME ATTRIBUTE</td>
<td>cn</td>
</tr>
</tbody>
</table>

**Delete user directory**

⚠️ Users of the deleted user directory will be deleted as well. As a consequence: active sessions of the users of the deleted user directory will be aborted at the time of the next interaction with the server (for details see Delete user).

**Enable or disable user directory**

To disable a user directory hover over the user directory's entry in the list and click the Disable user directory icon.

![Disable user directory icon](image)

When disabling a user directory, all users that are assigned to it will be blocked from logging in.

⚠️ Active sessions of users of the disabled user directory will not be aborted. The user will be blocked at the time of the next login.
When a user directory is disabled then the user directory's entry in the list displays the x mark. To enable the user directory click the *Enable user directory* icon.

Unlock locked accounts

All the locked user accounts that belong to a Local type user directory, can be released clicking the RELEASE LOCKOUT button.

Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol that provides communications security over a computer network. Websites, like the Web Management Console, are able to use TLS to secure all communications between their servers and web browsers.

The TLS protocol aims primarily to provide confidentiality (privacy) and data integrity between two communicating computer applications.

For instructions to set up TLS see 3.2 Configuring TLS.

LDAP attributes

For further details see 3.3.3 LDAP attributes

Active Directory attributes

For further details see 3.3.2 Active Directory attributes

Notes

The currently logged on user can not disable the user directory to which her account is assigned to. For example the *admin* user can not disable the LOCAL user directory.

The currently logged on user can not delete the following:

- Her own user account. For example the *admin* user can not delete the *admin* user account.
- The user directory to which her account is assigned to. For example the *admin* user can not delete the LOCAL user directory.
3.3.1 Change user password

The current user can change her password under **Settings > Password**.

The password change option is only available for users of *Local* type user directories.

Changing passwords in LDAP or Active Directory services is not supported.

- **Important notes**
  - If enhanced password policy is enabled for the user directory this user belongs to then the new password must fulfill the password complexity requirements listed at the *Local type user directories* section.

- **Important notes**
  - As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. To set up TLS see *3.2 Configuring TLS*. 
3.3.2 Active Directory attributes

- Bind username
- User base and group base DN

This page contains tips on how to obtain the BIND USERNAME, the USER BASE DN and GROUP BASE DN attributes when creating an Active Directory type user directory.

⚠️ Normally a domain administrator should provide these values.

✔️ All three attributes must be expressed using a valid LDAP syntax.
Bind username

Normally a domain administrator should provide these values, however there is a way to get the BIND USERNAME as an LDAP DN, that is needed for the product to do searches in the directory information tree, and it is as follows:
1. Log on to a Windows server machine that has connectivity to the Active Directory
2. Choose a user that is intended for this purpose (ie: has rights to do searches in the tree)
3. Open a Command window with elevated rights (Run as Administrator)
4. Assuming example.com as domain and John Smith with account name john.smith as the user, type the following:

```
> dsquery user domainroot -samid john.smith
```

or

```
> dsquery user domainroot -name John Smith
```

The commands above will return the correct DN for the user in question. The DN should look something like this:

```
CN=John Smith,OU=People,OU=Engineering,DC=example,DC=com
```

Please note, the actual user DN will not look exactly like the above example, but will depend on the structure of the underlying directory information tree in the Active Directory server.

On non-server Windows machines the dsquery command can be obtained with installing the Remote Server Administration Tools (RSAT).

**User base and group base DN**

Once the bind user DN is obtained, an easy way to get the DNs for the user and group searches is by taking all the DC parts of the user DN and leaving the rest out, which results in the following DN:

```
DC=example,DC=com
```
Please note that using only DC components for the user/group DNs may result in searches to be executed from the top of the directory information tree and potentially slow down AD server responses a lot and thus have an impact on the MetaDefender product's password validation. The rule of thumb here is that the more specific the user/group DN the faster the server response.

Taking the above example into consideration: a user search DN of "OU=People,OU=Engineering,DC=example,DC=com" could potentially result in much faster server response than "DC=example,DC=com" and should be preferred assuming all users reside under "OU=People,OU=Engineering,DC=example,DC=com" in the directory information tree.

Please also note that users and groups may reside in different parts of the directory information tree, as a consequence applying the same, more specific DN both as USER BASE DN and GROUP BASE DN may cause the MetaDefender product to not find group accounts in the directory information tree. So these DNs should be chosen carefully.

3.3.3 LDAP attributes

- Bind username
- User base and group base DN
- LDAP user schema settings
  - Example
- LDAP group schema settings

This page contains tips on how to obtain the BIND USERNAME, the USER BASE DN and GROUP BASE DN attributes, the LDAP USER SCHEMA SETTINGS and the LDAP GROUP SCHEMA SETTINGS when creating an LDAP type user directory.

Normally a domain administrator should provide these values.
The BIND USERNAME, the USER BASE DN and GROUP BASE DN attributes must be expressed using a valid LDAP syntax.
## Add user directory

### User Directory Type
- LDAP

### Name
- NAME

### LDAP Settings
- **Server Host**: SERVER HOST
- **Server Port**: PORT
- **Encryption**: Dropdown

### Add Server
- **Anonymous Bind**: Checkbox

### Bind Username
- **Username**: USERNAME

### Bind Password
- **Password**: PASSWORD

### User Base DN
- **User Base DN**: USER BASE DN

### Group Base DN
- **Group Base DN**: GROUP BASE DN

### LDAP User Schema Settings
- **User Object Class**: USER OBJECT CLASS
- **User Account Attribute**: USER ACCOUNT ATTRIBUTE
- **User Email Attribute**: USER EMAIL ATTRIBUTE
Bind username

Normally an LDAP administrator should provide these values, however there is a way to get the BIND USERNAME as an LDAP DN, that is needed for the product to do searches in the directory information tree. To get this information, there is, however, some information about the LDAP tree, that must be known in advance:

<table>
<thead>
<tr>
<th>LDAP property</th>
<th>Notes</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>DN of the LDAP tree node that has the bind user as a child.</td>
<td>This will be the base for the search. If selected improperly then the search may be very slow or won't find the appropriate user.</td>
<td>ou=users,dc=test</td>
</tr>
<tr>
<td>Attributes and their values that uniquely identify the bind user account.</td>
<td>These will be used as filter conditions to find the proper user.</td>
<td>uid=bind</td>
</tr>
</tbody>
</table>

To find the bind user, perform the following steps:

1. Log on to a Windows machine that has connectivity to the LDAP server
2. Choose a user that is intended for this purpose (i.e., has rights to do searches in the tree)
3. Open the LDP.exe tool with elevated rights (Run as Administrator)
4. Assuming the example properties above are correct, do the following search:

![Search dialog box]

The search above will return the attributes for the user in question:

![Search results]

The DN should look something like this:

```
cn=bind, ou=users, dc=test
```
Please note, the actual user DN will most probably look completely different than the above example, as it depends on the structure of the underlying directory information tree in the LDAP server.

On non-server Windows machines the `LDP.exe` tool can be obtained with installing the [Remote Server Administration Tools (RSAT)](https://docs.microsoft.com/en-us/windows-server/system-services/remote-server-administration-tools).

**User base and group base DN**

Once the bind user DN is obtained, an easy way to get the DNs for the user and group searches is by taking all the DC parts of the user DN and leaving the rest out. Using the examples above the result DN will be the following:

```plaintext
dc=test
```

Please note that using only DC components for the user/group DNs may result in searches to be executed from the top of the directory information tree and potentially slow down the LDAP server responses a lot and thus have an impact on the MetaDefender product's password validation. The rule of thumb here is that the more specific the user/group DN, the faster the server response is.

Please also note that users and groups may reside in different parts of the directory information tree, as a consequence applying the same, more specific DN both as USER BASE DN and GROUP BASE DN may cause the MetaDefender product to not find group accounts in the directory information tree. So these DNs should be chosen carefully.

**LDAP user schema settings**

Similarly to the search in **Bind username**, we can search for users and determine the appropriate values.
Example

1. Let's assume the following search is executed:

2. That gives the following result:

3. The LDAP USER SCHEMA SETTINGS may be the following:

<table>
<thead>
<tr>
<th>User schema setting</th>
<th>LDAP attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER OBJECT CLASS</td>
<td>user</td>
</tr>
<tr>
<td>User schema setting</td>
<td>LDAP attribute</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>USER ACCOUNT ATTRIBUTE</td>
<td>uid or samaccountname</td>
</tr>
<tr>
<td>USER EMAIL ATTRIBUTE</td>
<td>mail</td>
</tr>
<tr>
<td>USER DISPLAY NAME ATTRIBUTE</td>
<td>cn</td>
</tr>
</tbody>
</table>

**LDAP group schema settings**

Similarly to the search in LDAP user schema settings, we can search for users and determine the appropriate values.

### 3.4 General settings

- **Global settings**
  - Notification and report settings
  - Inbound SMTP settings
  - Sender Policy Framework lookup
    - SPF results
    - SPF related headers
  - DKIM signature verification
    - DKIM results
  - Resend settings
  - Deployment mode
- **Data retention**
Global settings

Notification and report settings

The following properties can be set:

1. SMTP SERVER: defines what SMTP servers MetaDefender Email Gateway Security should use to send notification and report emails. This value is an SMTP type server profile. For details about server profiles see 3.7 Server profiles.
   The following functions, notifications and reports use this setting:
   a. Quarantine reports (4.3 Quarantine)
   b. Quarantine forward (4.3 Quarantine)
   c. Quarantine release (4.3 Quarantine)
   d. Notification emails

2. PUBLIC SERVER ADDRESS: this is the IP or DNS address that will be used in notifications and reports to identify this server. When left empty there won't be any links in the notification and reports to this instance.
When setting this property please be aware that this address may be sent for recipients outside of your company (e.g. in a notification about password protected document).

3. RESCAN LINK AVAILABILITY: the time window (in hours) while the link is allowed to be used to initiate rescanning an email.

4. USE THE SERVER'S LOCAL TIMEZONE INSTEAD OF UTC: instead of using UTC in dates in notifications/disclaimers MetaDefender Email Gateway Security will use the server's timezone where it is installed.

### Inbound SMTP settings

In this sections properties of MetaDefender Email Gateway Security's SMTP service can be set. MetaDefender Email Gateway Security receives emails on this interface from any kind of its mail sources (email gateway, mail server, etc., see 1.6 Email traffic redirection).

The following properties can be set:

- **SMTP PORT**: TCP port of the SMTP service
- **ENCRYPTION**
  - None: no encryption is used for communication with SMTP service,
  - StartTLS optional: StartTLS may be used if the client chooses to use it,
  - StartTLS required: using StartTLS is mandatory.

> StartTLS optional and StartTLS required are applicable only if TLS is configured.

For details see 3.2 Configuring TLS.

### Sender Policy Framework lookup

Sender Policy Framework (SPF) is a mechanism defined by RFC 7208 which can help determine if incoming mails are sent from a host authorized by the domain's administrators. Usually a domain administrator will publish a TXT record in the Domain Name System (DNS) in order to specify a list of authorized hosts that can send emails from that domain. Enabling SPF is an anti-spam technique that will instruct MetaDefender Email Gateway Security to perform SPF checks on the "FROM" address(es) and add a header to the email with the SPF result.
For further details see Sender Policy Framework (SPF) for Authorizing Use of Domains in Email.

The following option is available:

1. PERFORM SPF LOOKUP ON EXTERNAL IP ADDRESSES: perform the SPF lookup on external IP addresses from which emails were submitted

**SPF results**

After the SPF check is performed the X-Metadefender-Spf-Result header will be added to the email and the value will be one of the following:

<table>
<thead>
<tr>
<th>Header value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass</td>
<td>A pass result is an explicit statement that the client is authorized to inject mail with the given identity.</td>
</tr>
<tr>
<td>NoRecord</td>
<td>A result of norecord means either</td>
</tr>
<tr>
<td></td>
<td>1. No syntactically valid DNS domain name was extracted from the SMTP session that could be used as the one to be authorized, or</td>
</tr>
<tr>
<td></td>
<td>2. No SPF records were retrieved from the DNS.</td>
</tr>
<tr>
<td>SoftFail</td>
<td>A softfail result is a weak statement by the publishing ADMD that the host is probably not authorized. It has not published a stronger, more definitive policy that results in a hardfail.</td>
</tr>
<tr>
<td>HardFail</td>
<td>A hardfail result is an explicit statement that the client is not authorized to use the domain in the given identity.</td>
</tr>
<tr>
<td>Error</td>
<td>An error result means the SPF verifier encountered a transient (generally DNS) error while performing the check. A later retry may succeed without further DNS operator action.</td>
</tr>
<tr>
<td>Neutral</td>
<td>A neutral result means the ADMD has explicitly stated that it is not asserting whether the IP address is authorized.</td>
</tr>
<tr>
<td>Unknown</td>
<td></td>
</tr>
</tbody>
</table>
An *unknown* result means the domain's published records could not be correctly interpreted. This signals an error condition that definitely requires DNS operator intervention to be resolved.

**UnknownMechanism**

An *unknownmechanism* result means that the ADMD uses a mechanism not recognized by this client.

### SPF related headers

<table>
<thead>
<tr>
<th>Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Metadefender-Spf-Result</td>
<td>Result of SPF lookup. See the <a href="#">148569283</a> section.</td>
</tr>
<tr>
<td>X-Metadefender-Spf-Sender</td>
<td>Sender email used for SPF lookup.</td>
</tr>
<tr>
<td>X-Metadefender-Spf-Ip</td>
<td>IP address used in SPF lookup.</td>
</tr>
<tr>
<td>X-Metadefender-Spf-Reason</td>
<td>Description of the reason, when SPF lookup failed for a reason.</td>
</tr>
</tbody>
</table>

### DKIM signature verification

> DomainKeys Identified Mail (DKIM) is a mechanism defined by [RFC6376](#). It is an email authentication method designed to detect forged sender addresses in emails (email spoofing), a technique often used in phishing and email spam.

The following option is available:

1. **VERIFY DKIM SIGNATURES** verify DKIM signatures for processed emails

### DKIM results

After the DKIM check is performed the *X-Metadefender-Dkim-Result* header will be added to the email and the value will be one of the following:
<table>
<thead>
<tr>
<th>Header value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid</td>
<td>Signature verification was successful and email has not been modified since submission.</td>
</tr>
<tr>
<td>Invalid</td>
<td>Signature verification was NOT successful and this email could be forged /modified during its transit.</td>
</tr>
<tr>
<td>Empty</td>
<td>No DKIM signature header was found in the email.</td>
</tr>
<tr>
<td>Error</td>
<td>An unexpected error occurred while attempting to verify the DKIM signature.</td>
</tr>
</tbody>
</table>

**Resend settings**

If MetaDefender Email Gateway Security fails to connect Core or the relay SMTP servers during the processing of an email, then the connection attempt will be retried according to the settings below.

Resend settings under Settings > Global settings apply to reconnection attempts to both Core and the configured SMTP servers.

If the connection succeeds to the Core after a certain number of attempts (but before it is exhausted), then the RETRY COUNT counter is reset for the retry attempts connecting to the SMTP servers.

The following properties can be set:

- **RETRY COUNT**: how many times to try to resend the email –in case of failure– to all the relays (see 4.2 Security rules) before giving up
- **RETRY INTERVAL**: base factor (in seconds) to wait before next resend attempt

**Deployment mode**

Deployment mode options are used to evaluate/test MetaDefender Email Gateway Security without necessarily affecting your existing email traffic. The following deployment modes are available:
PROTECTION MODE

Diagram

OUT-OF-BAND MONITORING MODE

Diagram
Data retention

Data retention settings may be configured under Settings > Data retention.

The following properties are available for configuration:

1. Email history clean up: audit records under Dashboard > Email history will be retained for the time configured here.
   a. OFF: Switch off automatic clean up.
   b. 1 HOUR .. 12 MONTHS: history records are automatically deleted after reaching the age specified by the configuration value.
Only records with permanent, non-failure statuses (*Completed* and *Deleted*) are cleaned-up.

2. Refused email history clean up: history records under **Dashboard > Refused emails** will be retained for the time configured here.
   a. OFF: Switch off automatic clean up.
   b. 1 HOUR .. 12 MONTHS: records are automatically deleted after reaching the age specified by the configuration value.

3. Quarantine clean up: quarantine items under **Dashboard > Quarantine** will be retained for the time configured here (except pinned items which are not affected by the automatic clean up).
   a. OFF: Switch off automatic clean up.
   b. 1 HOUR .. 12 MONTHS: items are automatically deleted after reaching the age specified by the configuration value.

4. Audit records clean up: audit records under **Dashboard > Config history** will be retained for the time configured here.
   a. OFF: Switch off automatic clean up.
   b. 1 HOUR .. 12 MONTHS: audit records are automatically deleted after reaching the age specified by the configuration value.
3.5 Logging & alerts

MetaDefender Email Security has wide variety of options to configure logging. Log settings are in the Windows Registry. To see more details about log configuration see the following pages:

- 3.5.1 Configuration
- 3.5.2 Debug logging
- 3.5.3 Web Management Console logs

3.5.1 Configuration

- Logging configuration
- Email alerts
  - Alert email settings
  - Alert types

Logging configuration

To configure the log outputs and levels see 3.1.2 Windows Registry configuration.
Email alerts

Email alerts can be configured so that certain users can instantly be notified about the occurrence of certain system events.

**Alert email settings**

<table>
<thead>
<tr>
<th><strong>SENDER ADDRESS</strong></th>
<th>Email address from whom alert emails are sent</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RECIPIENTS</strong></td>
<td>Recipient(s) of the alert email</td>
</tr>
</tbody>
</table>
## Alert types

<table>
<thead>
<tr>
<th>Alert Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SENDER ADDRESS</strong></td>
<td>Email address from whom alert emails are sent</td>
</tr>
<tr>
<td><strong>RECIPIENTS</strong></td>
<td>Recipient(s) of the email alert</td>
</tr>
<tr>
<td><strong>SMTP SERVER NOT RESPONDING</strong></td>
<td>An alert is sent if the inbound SMTP server is not responding as expected</td>
</tr>
<tr>
<td><strong>SMTP RELAY NOT RESPONDING</strong></td>
<td>An alert is sent if an SMTP relay configured in a server profile is not responding as expected</td>
</tr>
<tr>
<td><strong>METADEFENDER CORE NOT RESPONDING</strong></td>
<td>An alert is sent if a MetaDefender Core server configured in a server profile is not responding as expected</td>
</tr>
<tr>
<td><strong>METADEFENDER VAULT NOT RESPONDING</strong></td>
<td>A notification will be sent if a MetaDefender Vault server configured in a server profile is not responding as expected</td>
</tr>
<tr>
<td><strong>SCAN FAILURE</strong></td>
<td>An alert is sent if a scan failure occurs during the processing of an email</td>
</tr>
<tr>
<td><strong>SANITIZATION FAILURE</strong></td>
<td>An alert is sent if a sanitization failure occurs during the processing of an email</td>
</tr>
<tr>
<td><strong>EMAIL REFUSED</strong></td>
<td>An alert is sent when an email is refused by MetaDefender Email Gateway Security.</td>
</tr>
<tr>
<td><strong>EMAIL FAILED</strong></td>
<td>An alert is sent when an email fails processing and is moved to Failed.</td>
</tr>
<tr>
<td><strong>EMAIL BYPASSED</strong></td>
<td>A notification will be sent if Email Gateway Security bypassed scanning an email.</td>
</tr>
</tbody>
</table>

⚠️ **For every bypassed email**

This alert will be sent for every bypassed email occurrence.
* For persistent failures a notification email will be sent once an hour.

Every change made is applied when you select **Save settings** or **OK**, except if the change cannot be applied.

### 3.5.2 Debug logging

Debug logging can be used to identify issues with connections. It provides debug level details for each connection as well as the time each step took (e.g. parsing time, scan time, response time). It also tracks the number of active connections.

- **Important notes**
- **Step-by-step guide**
  - **Enable debug logging**
  - **Disable debug logging**

**Important notes**

⚠️ Debug logging is not designed to be constantly enabled. It should only be used for investigating issues for short periods of time.

Keeping it enabled permanently may impact performances. If running for too long, the log file can become huge and significantly reduce the available disk space.

⚠️ In each case below, both of `logfile` and `loglevel` must be set or none of them.

**Step-by-step guide**

**Enable debug logging**

Perform the following steps to enable debug logging:

1. Make sure MetaDefender Email Gateway Security is stopped

   
   ```
   > net stop mdemailsecurity
   ```
2. Open the Windows Registry with `regedit`. Go to the
   HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email
   Security\logger entry

3. Add or modify the following entries with the following values:
   a. loglevel: debug
   b. logfile: Path to the logfile, for example 
      C:\Program Files\OPSWAT\Metadefender Email
      Security\data\mdemailsecurity.log
   
   Please note that the directory path must exist, logs are not written if the
   directory is not present.

4. Close the registry editor

5. Start MetaDefender Email Gateway Security

   > net start mdemailsecurity

**Disable debug logging**

Perform the following steps to disable debug logging:

1. Make sure MetaDefender Email Gateway Security is stopped

   > net stop mdemailsecurity

2. Open the Windows Registry with `regedit`. Go to the
   HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email
   Security\logger entry

3. Delete the following entries:
   a. loglevel
   b. logfile

4. Close the registry editor

5. Start MetaDefender Email Gateway Security
The log level debug can also be set for the wineventlog_level entry. Sending debug logs to the Windows Events would, however, flood the Event Viewer and as so it is not recommended.

3.5.3 Web Management Console logs

The MetaDefender Email Gateway Security Web Management Console and REST interface is hosted by the nginx web server. Web Management Console and REST interface logs are written by nginx.

Windows

Let us assume that MetaDefender Email Gateway Security is installed in:

C:\Path\To\Metadefender Email Security

In this case on Windows nginx logs to the following file:

C:\Path\To\Metadefender Email Security\nginx\nginx_error.log

3.6 Quarantine configuration

- Quarantining emails
  - Blocked emails
  - Sanitized emails
- Quarantine reports

Quarantining emails

Quarantining rules may be set at security rules. For details about security rules see 4.2 Security rules.

For general information about quarantine and information about operating quarantine see 4.3 Quarantine.
**Blocked emails**

Create or modify a security rule under **Policy > Security rules**. On the ACTIONS tab in the IF CONTENT IS BLOCKED section select QUARANTINE ORIGINAL EMAIL to quarantine blocked emails.

⚠ Emails can only be blocked—and as so quarantined—if scanning is enabled for the appropriate security rule when creating or modifying a security rule under **Policy > Security rules** on the SCAN tab.

**Sanitized emails**

Create or modify a security rule under **Policy > Security rules**. On the ACTIONS tab in the IF CONTENT IS SANITIZED section select QUARANTINE ORIGINAL EMAIL to quarantine sanitized emails.

⚠ Emails can only be sanitized—and as so quarantined—if scanning is enabled for the appropriate security rule when creating or modifying a security rule under **Policy > Security rules** on the SCAN tab.
Quarantine reports

MetaDefender Email Gateway Security can be configured to periodically send reports about the quarantine status.

Under **Settings > Quarantine reports** the following properties can be configured:

1. **SCHEDULE**: the frequency of the reports

   - **OFF**: no reports are sent
   - **HOURLY**: a report is sent at every o'clock
   - **DAILY**: a report is sent every day, at midday
   - **WEEKLY**: a report is sent every Monday, at midday
   - **MONTHLY**: a report is sent on the first day of every month, at midday

2. **SENDER ADDRESS**: the email address from which the report is sent
3. **RECIPIENTS**: email address of recipients to whom the report is sent

   *Time and date values below are calculated in the MetaDefender Email Gateway Security server's time.*
4. SUBJECT: subject of the report email

5. RULES: the digest email may be restricted to inbound or outbound quarantined items only
   a. ALL: all quarantined emails are reported
   b. INBOUND: only inbound quarantined emails are reported (emails that were matched by a rule set as INBOUND)
   c. OUTBOUND: only outbound quarantined emails are reported (emails that were matched by a rule set as OUTBOUND)

6. ONLY INCLUDE QUARANTINED EMAILS THAT WERE BLOCKED: when this option is enabled emails which got quarantined because they were sanitized will not be listed in the quarantine report

⚠️ Quarantine report limitation

Quarantine report will not contain more than 1000 entries. If there were more than 1000 new quarantined entries since the last quarantine report you will have to check the actual quarantine for more information. If you set a restriction for reporting only blocked emails and/or reporting only inbound/outbound emails the numbers and entries in the quarantine report will reflect those options.
Currently the same settings (e.g. schedule) apply for all the quarantine report recipients.

### 3.6.1 Quarantine emails on another mail server

- External quarantine summary
- Quarantine mode
  - Default
  - External quarantining design
  - Configuration
MetaDefender Email Gateway Security does not provide access to quarantined files for each email users other than access to administrator for all the quarantined emails. If your email server (either hosted or on-site mail server) has quarantine management capability for each user, it is recommended to quarantine email on your email server. By default, MetaDefender Email Gateway Security will quarantine emails in its own quarantine but you can change this behaviour.

### External quarantine summary

<table>
<thead>
<tr>
<th>Key</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registry key name</td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security</td>
</tr>
<tr>
<td>Registry value name (blocked emails)</td>
<td>external_quarantine_block</td>
</tr>
<tr>
<td>Registry value name (allowed-and-sanitized emails)</td>
<td>external_quarantine_sanitize</td>
</tr>
<tr>
<td>Email header</td>
<td>X-Metadefender-To-Quarantine</td>
</tr>
</tbody>
</table>

### Quarantine mode

MetaDefender Email Gateway Security supports two quarantine modes for each of blocked, and allowed-and-sanitized emails independently, in an exclusive fashion (there is an exclusive or relation between the two: either this, or that):

1. Internal
2. External

Changing quarantine mode will allow you to quarantine emails—that are detected as blocked or allowed-and-sanitized by MetaDefender Email Gateway Security—on a different email server.
When `external_quarantine_block` is set to 1 the original copy of any blocked emails will be delivered with the `X-Metadefender-To-Quarantine` header added. When `external_quarantine_sanitize` is set to 1 the original copy of any allowed-and-sanitized emails will be delivered with the `X-Metadefender-To-Quarantine` header added.

**Default**

By default MetaDefender Email Gateway Security uses the internal quarantine mode for both blocked and allowed-and-sanitized emails (neither the value `external_quarantine_block` nor the `external_quarantine_sanitize` exist under the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security`; see the 152677101 section).

**External quarantining design**

The external quarantine support is designed in the following way:

1. A header is appended to the original (potentially harmful) email,

<table>
<thead>
<tr>
<th>Header</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Metadefender-To-Quarantine</td>
<td>True</td>
</tr>
</tbody>
</table>

2. The (potentially harmful) email gets delivered to the original recipient,
3. The receiving email server is configured to quarantine emails that contain this header.

**Configuration**

**Prerequisites**

1. Quarantine must be enabled for blocked and/or allowed-and-sanitized emails (see 3.6 Quarantine configuration) for emails to be quarantined at all

**Setup**

1. Stop MetaDefender Email Gateway Security service

   ```
   > net stop mdemailsecurity
   ```
2. Enable or disable external quarantine support for blocked emails:
   
a. Enable external quarantine (and disable internal quarantine) support for blocked emails by setting the value `external_quarantine_block` under the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security (DWORD)` to 1

   ```
   > reg add "HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security" /v external_quarantine_block /t REG_DWORD /d 1
   ```

   b. Disable external quarantine (and enable internal quarantine) support for blocked emails by deleting the value `external_quarantine_block` under the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security`

   ```
   > reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security" /v external_quarantine_block
   ```

3. Enable or disable external quarantine support for allowed-and-sanitized emails:
   
a. Enable external quarantine (and disable internal quarantine) support for allowed-and-sanitized emails by setting the value `external_quarantine_sanitized` under the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security (DWORD)` to 1

   ```
   > reg add "HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security" /v external_quarantine_sanitize /t REG_DWORD /d 1
   ```

   b. Disable external quarantine (and enable internal quarantine) support for allowed-and-sanitized emails by deleting the value `external_quarantine_sanitized` under the registry key `HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security`

   ```
   > reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\Metadefender Email Security" /v external_quarantine_sanitize
   ```
4.7.4

Example

The following screenshot shows the source of an email delivered for external quarantining. Please note the position of the X-Metadefender-To-Quarantine header added to the email.

```
Return-Path: two@other
Received: from [127.0.0.1] (HUWLO01.us.opswat.com [127.0.0.1])
    by HUWL001 with ESMTP
    Thu, 21 Sep 2017 15:47:29 +0200
Message-ID: <AFE90018-D4F0-478G-9F1C-F6451AD51AF6@HUWL001>
Received: from localhost.localdomain ([127.0.0.1]) by HUWL001.us.opswat.com
    with ESMTP ; Thu, 21 Sep 2017 15:47:00 +0200
To: two@other
From: two@other
Subject: 47 test bulk email
Date: Thu, 21 Sep 2017 15:46:57 +0200
X-Metadefender-To-Quarantine: True
X-MD-Email-Security-ID: c0262788c0364d228cd5a47a94c4839

This is my message: XSO1PX%AP[4a\PIX4a(P')7CC7]$EICAR-STD-ANTI-VIRUS-
TEST-FILE!$H+H*
```

3.7 Server profiles

Server profiles under `Inventory > Server profiles` help to organize services of one or more servers based on the service type.

For example in case of security rules one or more SMTP servers are needed to forward the emails after processing. For this purpose a server inventory may be created collecting all relay SMTP servers. Then at the rule itself only this server profile needs to be selected.
Currently MetaDefender Email Gateway Security uses and allows SMTP and MetaDefender Core type server profiles only.

### Properties

<table>
<thead>
<tr>
<th>Property</th>
<th>Server profile type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Server profile type</strong></td>
<td>N/A</td>
<td>Service type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported service types are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. SMTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. MetaDefender Core</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. MetaDefender Vault</td>
</tr>
<tr>
<td><strong>Profile name</strong></td>
<td>All</td>
<td>Unique identifier of the server profile</td>
</tr>
<tr>
<td><strong>Server specifications (URI)</strong></td>
<td>All</td>
<td>Service specifications in URI syntax. Multiple server specifications may be added to an SMTP or MetaDefender Core type server profile. At least one server specification must exist in a server profile. Only the following URI components are used:</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>URI component</th>
<th>Supporting server profile type</th>
<th>Example</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>scheme</td>
<td>All</td>
<td><a href="http://10.0.0.10:25">http://10.0.0.10:25</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>/vault_rest</td>
<td></td>
</tr>
<tr>
<td>host</td>
<td>All</td>
<td><a href="http://10.0.0.10:25">http://10.0.0.10:25</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>/vault_rest</td>
<td>N/A</td>
</tr>
</tbody>
</table>
### Server profile examples

The following list contains examples for each server profile type with reasonable defaults (all use 127.0.0.1 as host).

<table>
<thead>
<tr>
<th>Server profile type</th>
<th>URI</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP</td>
<td>smtp://127.0.0.1:25</td>
</tr>
<tr>
<td>MetaDefender Core</td>
<td><a href="http://127.0.0.1:8008">http://127.0.0.1:8008</a></td>
</tr>
<tr>
<td>MetaDefender Vault</td>
<td><a href="http://127.0.0.1:8010/vault_rest">http://127.0.0.1:8010/vault_rest</a></td>
</tr>
<tr>
<td>Property</td>
<td>Server profile type</td>
</tr>
<tr>
<td>----------</td>
<td>---------------------</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Server preference
- **1. SMTP**
- **2. MetaDefender Core**

Preference order in which servers are addressed for services:

1. **FAILOVER**: high availability order; first successfully addressed server in the list will do the service
   - Always start with the first server URL in list.
   - Fail over to the next server in the list, if the server fails.
   - Possible values:
     - Core 1
     - Core n

2. **ROUND ROBIN**: load balancing order; next successfully addressed server in the list will do the service
   - Do a Round Robin selection of the Core URLs defined in the Core inventory.
<table>
<thead>
<tr>
<th>Property</th>
<th>Server profile type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>a. For the first scan request use Core</td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. If previous scan request used Core</td>
<td></td>
</tr>
<tr>
<td></td>
<td>c. ...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>d. If previous scan request used Core</td>
<td></td>
</tr>
<tr>
<td></td>
<td>e. ...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>f. If previous scan request used Core</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Core 1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Core n</td>
<td></td>
</tr>
</tbody>
</table>

Instead of a real Round Robin selection, the initial server is selected in a random fashion currently:

Do a random selection of the Core URLs defined in the Core inventory.

Fail over to the next Core in the list if the actual Core fails. Start over the selection at the end of the list and continue until the starting entry is reached.

<table>
<thead>
<tr>
<th>Start</th>
<th>Core k (random)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Core n, Core 1</td>
</tr>
<tr>
<td>Last</td>
<td>Core k-1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Start</th>
<th>Core k</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Core n, Core 1</td>
</tr>
<tr>
<td>Last</td>
<td>Core k-1</td>
</tr>
</tbody>
</table>
### Property validation

Some of the server profile properties have cross-dependencies and as so must match.

<table>
<thead>
<tr>
<th>Property</th>
<th>Server profile type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transport level encryption</td>
<td>1. SMTP</td>
<td>Configure whether the destination server requires transport level security. Possible values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1. None: no transport level security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. StartTLS: transport level encryption using SMTP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. TLS: transport level security using SMTPS protocol</td>
</tr>
<tr>
<td>Username and password</td>
<td>1. SMTP</td>
<td>If the destination server requires (machine-to-machine) user based authentication, then the credentials can be specified here.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>⚠️ As long as TLS is not configured for the Web Management Console, passwords are sent clear-text over the network. To set up TLS:</strong></td>
</tr>
<tr>
<td>Certificate based client authentication</td>
<td>1. SMTP</td>
<td>If the destination server requires certificate based client host authentication then this checkbox must be marked. MetaDefender Email Gateway Security will use the actual deployment's digital ID, for details see 3.2 Configuring TLS.</td>
</tr>
<tr>
<td></td>
<td>2. MetaDefender Core</td>
<td></td>
</tr>
<tr>
<td>API key</td>
<td>1. MetaDefender Vault</td>
<td>The destination Vault server will require the authorization token specified here for Email Gateway Security to be able to upload files. For details see MetaDefender Vault's user guides.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property validation</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Server profile type</td>
<td>Server specifications (URI) allowed schemes</td>
<td></td>
</tr>
<tr>
<td>SMTP</td>
<td>smtp, smtps</td>
<td></td>
</tr>
<tr>
<td>MetaDefender Core</td>
<td>http</td>
<td></td>
</tr>
</tbody>
</table>
### Server profile type

<table>
<thead>
<tr>
<th></th>
<th>Server specifications (URI) allowed schemes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>https</td>
</tr>
<tr>
<td>MetaDefender Vault</td>
<td>http</td>
</tr>
<tr>
<td></td>
<td>https</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server specifications (URI) scheme</th>
<th>Transport level encryption allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>smtp</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td>StartTLS optional</td>
</tr>
<tr>
<td></td>
<td>StartTLS required</td>
</tr>
<tr>
<td>smtps</td>
<td>Irrelevant</td>
</tr>
<tr>
<td>http</td>
<td>N/A</td>
</tr>
<tr>
<td>https</td>
<td>N/A</td>
</tr>
</tbody>
</table>

If `smtps` scheme is specified then the SMTP connection is established over TLS irrelevant of the setting of TRANSPORT LEVEL ENCRYPTION.

If https scheme is specified then the HTTP connection is established over TLS.

### Testing the configuration

Clicking the *TEST* button will test the configuration. The test consists of two steps:

1. Syntactical validation of the values
2. Connection test

⚠️ If the test fails, then the server profile can not be added.

Syntactical validation
The correctness of the provided values is validated:

1. PROFILE NAME must be unique
2. The SERVER SPECIFICATIONS (URI) values must conform with the URI syntax with the restriction that only the scheme, host and port values are allowed
3. Cross dependencies must match (see the 149718360 section)

Connection test
If the syntactical validation pass, then each server specification is tested for a successful connection.

Limitations

⚠️ Currently the connection is tested without using TLS (when configured at all).

3.7.1 MetaDefender Core specific inventory properties

Query parameters
Addresses specified in CORE URI ADDRESS may contain optional query parameters for specific use cases.

Syntax
With the optional query parameters the Core URI is formatted as follows:

```
URI schema with query parameter
```
```
scheme://host:port[?query]
```

Valid parameters
<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Use case</th>
<th>Example</th>
</tr>
</thead>
</table>
| apikey| 32 characters long API key of an account that belongs to the role the Core side rule is restricted to. | Core side rules may be restricted to roles (for details see 3.6.4. Security rule configuration in MetaDefender Core v4 documentation). ICAP Server can use these rules if:  
   1. A user is created on Core,  
      a. That belongs to the role the Core side rule is restricted to;  
      b. And the user has an API key generated.  
   2. In ICAP Server the Core is added to a server profile  
      a. And the API key above is specified in the Core URI. | **URI example with query parameter**  
https://127.0.0.1:8058?apikey=24a586f3023b4309b65a1974198d6c6 |

**Rule**

Right after the CORE URI ADDRESS has been specified, and is valid (connection can be established) the RULE drop-down list is populated with the available rules on the corresponding MetaDefender Core instance.
The desired security rule may be selected from the configured Core's available rules. Default is Automatic.

⚠️ Please note that if the security rules on the configured MetaDefender Core under Policy > Security rules are limited to a specific user agent other than mdemailsecurity or restricted to specific roles, then those security rules will not be available in MetaDefender Email Gateway Security.

MetaDefender Email Gateway Security identifies itself on MetaDefender Core with the user agent mdemailsecurity.
Prior to version 4.2.0: Please note that *Enable archive handling* must be enabled and the Archive engine must be active on Core so that MetaDefender Email Gateway Security can work properly. For further details see 2.1.2 System requirements.
From version 4.2.0 MetaDefender Email Gateway Security uses batch scanning instead of archives so enabling archive handling is not necessary anymore.
On the example below the Core rule *Kiosk* is not listed on Email Gateway Security as that rule is restricted to user agent *kiosk*.

Otherwise all unrestricted core rules are in the list.

3.8 Mail proxy deployment configuration

In this traditional setup MetaDefender Email Gateway Security acts as an anti-malware email proxy between the email gateway (anti-spam) and the mail server.
3.8.1 Configuring incoming threat protection

3.8.2 Configuring outgoing threat protection

3.8.1 Configuring incoming threat protection

- Routing configuration
  - Server profile
  - Security rules
- Verify Settings

In order to and configure MetaDefender Email Gateway Security incoming threat protection, you must configure the routing of the *inbound* security rules.
For the examples below let us assume that the following is configured:

<table>
<thead>
<tr>
<th>Asset</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email gateway</td>
<td>IP</td>
<td>192.168.0.10</td>
</tr>
<tr>
<td>Mail server</td>
<td>IP</td>
<td>192.168.0.20</td>
</tr>
<tr>
<td>Corporate domain (domain in inbound emails)</td>
<td>domain name</td>
<td>example.com</td>
</tr>
</tbody>
</table>

**Routing configuration**

**Server profile**

Under Inventory > Server profiles create an SMTP type server profile that contains the mail server(s).

Set the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER PROFILE TYPE</td>
<td>SMTP</td>
<td>SMTP</td>
</tr>
</tbody>
</table>
### Server Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE NAME</td>
<td>Unique name for this profile</td>
<td>Mail server</td>
</tr>
<tr>
<td>SERVER SPECIFICATIONS</td>
<td>Specification of the mail server(s) in URI syntax</td>
<td>smtp://192.168.0.20:25</td>
</tr>
</tbody>
</table>

For further details about server profiles see 3.7 Server profiles.

### Security rules

Under **Policy > Security rules** add or modify *inbound* security rules.

Set the following:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Field</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILTER</td>
<td>SENDER IP ADDRESS</td>
<td>IP address of email gateway(s)</td>
<td>192.168.0.10</td>
</tr>
<tr>
<td>Tab</td>
<td>Field</td>
<td>Value</td>
<td>Example</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td><strong>RECIPIENT DOMAIn OR ADDRESs</strong></td>
<td></td>
<td>Email address(es) of potential organization internal recipients (QRegExp syntax may be used)</td>
<td><a href="mailto:.+@example.com">.+@example.com</a></td>
</tr>
<tr>
<td><strong>RELAY</strong></td>
<td>FORWARD PROCESSED EMAILS TO</td>
<td>Server profile containing the mail server(s)</td>
<td>Mail server</td>
</tr>
</tbody>
</table>

For further details about security rules see 4.2 Security rules.
Verify Settings

Send an email to MetaDefender Email Gateway Security's SMTP service (port 10025 by default) with a recipient with the corporate internal domain and check whether the email was handled by the proper rule and delivered to the mail server(s).

### 3.8.2 Configuring outgoing threat protection

- Routing configuration
  - Server profile
  - Security rules
- Verify Settings

In order to and configure MetaDefender Email Gateway Security incoming threat protection, you must configure the routing of the *outbound* security rules.
For the examples below let us assume that the following is configured:

<table>
<thead>
<tr>
<th>Asset</th>
<th>Property</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email gateway</td>
<td>IP</td>
<td>192.168.0.10</td>
</tr>
<tr>
<td>Mail server</td>
<td>IP</td>
<td>192.168.0.20</td>
</tr>
<tr>
<td>Corporate domain (domain in inbound emails)</td>
<td>domain name</td>
<td>example.com</td>
</tr>
</tbody>
</table>

Routing configuration

Server profile

Under **Inventory > Server profiles** create an SMTP type server profile that contains the email gateway(s).

Set the following:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>SERVER PROFILE TYPE</td>
<td>SMTP</td>
<td>SMTP</td>
</tr>
</tbody>
</table>
### Server Profiles

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>PROFILE NAME</td>
<td>Unique name for this profile</td>
<td>Email gateway</td>
</tr>
<tr>
<td>SERVER SPECIFICATIONS</td>
<td>Specification of the email gateway(s) in URI syntax</td>
<td>smtp://192.168.0.10:25</td>
</tr>
</tbody>
</table>

For further details about server profiles see 3.7 Server profiles.

---

### Security rules

Under **Policy > Security rules** add or modify *outbound* security rules.

Set the following:

<table>
<thead>
<tr>
<th>Tab</th>
<th>Field</th>
<th>Value</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>FILTER</td>
<td>SENDER IP ADDRESS</td>
<td>IP address of mail server(s)</td>
<td>192.168.0.20</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.+@.+</td>
</tr>
<tr>
<td>Tab</td>
<td>Field</td>
<td>Value</td>
<td>Example</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>RECIPIENT DOMAIN OR ADDRESS</strong></td>
<td></td>
<td>Email address(es) of external recipients (QRegExp syntax may be used)</td>
<td></td>
</tr>
<tr>
<td><strong>RELAY</strong></td>
<td>FORWARD PROCESSED EMAILS TO</td>
<td>Server profile containing the email gateway(s)</td>
<td>Email gateway</td>
</tr>
</tbody>
</table>

For further details about security rules see [4.2 Security rules](#).
Verify Settings

Send an email to MetaDefender Email Gateway Security's SMTP service (port 10025 by default) with a recipient not with the corporate internal domain, and check whether the email was handled by the proper rule and delivered to the email gateway(s).

3.9 Cloud deployment configuration

Overview

For hosted solutions such as Office 365 or G Suite Gmail.
Steps overview

1. Configure the hosted email server to accept email from MetaDefender Email Gateway Security.
2. Configure MetaDefender Email Gateway Security to relay out to hosted email server.
3. Update MX record to point to MetaDefender Email Gateway Security.

Limitation

- SPF enforcement will be skipped on the hosted email server
- 3.9.1 AppRiver integration
- 3.9.2 Google Apps integration
- 3.9.3 Microsoft Office 365 Integration

3.9.1 AppRiver integration

Overview

1. Configure the hosted email server to accept email from MetaDefender Email Gateway Security server.
2. Configure MetaDefender Email Gateway Security to relay out to hosted email server.
3. Update MX record to point to MetaDefender Email Gateway Security server.
### Detailed Steps

<table>
<thead>
<tr>
<th>Steps</th>
<th>Why and How To Verify</th>
<th>Details</th>
</tr>
</thead>
</table>
| Disable SPF rules (soft/hard)              | WHY: This is to allow email to come from MD email  
How to verify: send email from the server where MD email will be setup and confirm email reach to AppRiver                                                                                                                                                                                                                               | ![SpamLab Settings](image)

#### SPF HARDFAIL
- Hard fail during Sender Policy Framework verification

#### SPF SOFTFAIL
- Soft fail during Sender Policy Framework verification

| Add custom header for quarantine (X-MetaDefender-To-Quarantine) | WHY: To quarantine email on AppRiver instead of on MetaDefender.  
HOW TO VERIFY: send custom email with this header and be sure rule is set to if Header "contains" and not "equals" | ![SpamLab Settings](image)

#### X-MetaDefender-To-Quarantine
- To change the order in which the rules are evaluated, just drag the rules. These rules are applied one after another, meaning that each rule is evaluated against the email after the previous one.

We do not recommend using regex tests or any rules to filter spam messages.
<table>
<thead>
<tr>
<th>Steps</th>
<th>Why and How To Verify</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>confirm email is quarantined even though email is clean.</td>
<td>1 Quick start with MetaDefender Email Gateway Security</td>
</tr>
<tr>
<td></td>
<td>HOW TO VERIFY: Use telnet and send email to MetaDefender Email Gateway Security (on SMTP port 10025) and confirm email history on Web Management Console</td>
<td>❗️ Remember to configure relays to match your original MX record Security rules .</td>
</tr>
<tr>
<td>Install MetaDefender Email Gateway Security and configure</td>
<td>WHY: By default SMTP traffic use port 25 and when we redirect MX record we must use port 25 (not 10025)</td>
<td></td>
</tr>
<tr>
<td>Steps</td>
<td>Why and How To Verify</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Restart MetaDefender Email Gateway Security service | WHY: To apply SMTP port changes in the previous step  
HOW TO VERIFY: Use telnet and send email to MetaDefender Email Gateway Security (on SMTP port 25) and confirm | Restart the 'OPSWAT MetaDefender Email Gateway Security' service. net stop mdemailsecurity net start mdemailsecurity |
### Steps | Why and How To Verify | Details
--- | --- | ---
Email arriving in AppRiver hosted mailbox. |  |  
Redirect your MX record to MetaDefender Email Gateway Security | WHY: To ensure emails pass through MetaDefender Email Gateway Security before reaching AppRiver  
HOW TO VERIFY: Using your regular mail client send email to an AppRiver hosted mailbox and confirm delivery | Refer to your Internet domain registrar for details how to change MetaDefender Email Gateway Security IP address. Configure relays to match your original MX record; for details  
⚠️ Make sure that your MX record changes have propagated

### Concurrent SMTP connection limits
Some hosted scenarios may implement SMTP connection limitations, such as a maximum number of concurrent SMTP connections from a single IP address, to prevent abuse of their SMTP service. This will require some configuration changes in MetaDefender Email Gateway Security to prevent delays in email delivery, or worse, the not being delivered and put in Permanent failure.

### Known concurrent SMTP connection limits
Below is a list of known SMTP connection limits from providers
<table>
<thead>
<tr>
<th>Provider</th>
<th>Max concurrent SMTP connections</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SendGrid</td>
<td>10</td>
<td>See <a href="https://sendgrid.com/docs/Classroom/Basics/Email_Infrastructure/recommended_smtp_settings.html">https://sendgrid.com/docs/Classroom/Basics/Email_Infrastructure/recommended_smtp_settings.html</a></td>
</tr>
</tbody>
</table>
| AppRiver | 1                               | By default AppRiver only allows 1 concurrent SMTP connection. AppRiver can adjust this on request. 

*Note: For OPSWAT MetaDefender Email Gateway Security integration this has been adjusted to allow 10 concurrent SMTP connections*

Handling in MetaDefender Email Gateway Security

As opposed to MetaDefender Email v3 it is not possible to restrict concurrent SMTP connections in MetaDefender Email Gateway Security v4.

To mitigate this issue MetaDefender Email Gateway Security v4 has a mature retry mechanism that most probably avoids the risk of limited concurrent SMTP connections.

3.9.2 Google Apps integration

Overview

1. Configure the hosted email server to accept email from MetaDefender Email Gateway Security server.
2. Configure MetaDefender Email Gateway Security to relay out to hosted email server.
3. Update MX record to point to MetaDefender Email Gateway Security server.

Detailed Steps

<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Go to <a href="https://admin.google.com">https://admin.google.com</a> and</td>
</tr>
<tr>
<td>Steps</td>
<td>Details</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------</td>
</tr>
<tr>
<td>login to your Google Apps subscription</td>
<td>Click 'MORE CONTROLS'</td>
</tr>
<tr>
<td>Click 'MORE CONTROLS'</td>
<td><img src="image" alt="Admin console" /></td>
</tr>
<tr>
<td>Click 'Apps'</td>
<td></td>
</tr>
<tr>
<td>Steps</td>
<td>Details</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>4.7.4</td>
<td><strong>Click 'Google Apps'</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Google Apps" /></td>
</tr>
<tr>
<td></td>
<td><strong>Click 'Gmail'</strong></td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Gmail" /></td>
</tr>
<tr>
<td>Steps</td>
<td>Details</td>
</tr>
<tr>
<td>---------------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td><strong>Click 'Advanced settings'</strong></td>
</tr>
</tbody>
</table>

- **Gmail**
  - Get a fresh start with email that has less spam.
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scroll down to the ‘Inbound gateway’ section and click ‘CONFIGURE’</td>
<td>![Image of Google Apps settings for Email]</td>
</tr>
<tr>
<td>Specify a gateway name (e.g. <em>Metadefender Email Relay</em>) and the IP address of the MetaDefender Email Gateway Security server; check 'Automatically detect external IP (recommended)', 'Reject all mail not from gateway IPs', and 'Require</td>
<td>![Image of Add setting for Inbound gateway]</td>
</tr>
</tbody>
</table>
| | **MetaDefender Email Relay**  
1. Gateway IPs  
| IP addresses / ranges | ADD |  
| 31.14.16.148 |  
| **Automatically detect external IP (recommended)**  
| **Reject all mail not from gateway IPs**  
| **Require TLS for connections from the email gateways listed above**  
| 2. Message Tagging  
| Message is considered spam if the following header regexp matches | **CANCEL**  
<p>| <strong>ADD SETTING</strong> |</p>
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7.4</td>
<td><strong>TLS connection from the email gateways listed above</strong>'</td>
</tr>
<tr>
<td></td>
<td>Click ‘SAVE’ at the bottom right of the screen to save the changes.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Install MetaDefender Email Gateway Security and configure; for instruction see</strong> <a href="#">Quick start with MetaDefender Email Gateway Security</a></td>
</tr>
</tbody>
</table>

*Remember to configure relays to match your original MX record.*
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Configure MetaDefender Email Gateway Security to listen on port 25</strong></td>
<td><img src="image" alt="Configure MetaDefender Email Gateway Security" /></td>
</tr>
<tr>
<td><strong>Verify routing settings by sending an email to a Google Apps recipient directly to the MetaDefender Email Gateway Security server and verify that it arrives correctly in the recipient inbox</strong></td>
<td></td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Refer to your Internet domain registrar for</td>
</tr>
<tr>
<td></td>
<td><strong>Configure relays to match your original MX record; for details see 4.2 Security rules</strong></td>
</tr>
</tbody>
</table>

*Make sure that your MX record changes have propagated before verifying.*
### 3.9.3 Microsoft Office 365 Integration

#### Overview

1. Configure the hosted email server to accept email from MetaDefender Email Gateway Security server.
2. Configure MetaDefender Email Gateway Security to relay out to hosted email server.
3. Update MX record to point to MetaDefender Email Gateway Security server.

#### Detailed Steps

<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Goto <a href="https://portal.office.com">https://portal.office.com</a> and login with your Office365 credentials</td>
</tr>
</tbody>
</table>

### Additional notes

- **Quarantine:** Google Apps always does a malware check on all incoming emails, so releasing an infected item from quarantine will be rejected by Google Apps. As a workaround for this, configure quarantine to deliver emails to an alternative SMTP server that can accept infected emails.
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go to Office 365 Portal &gt; Admin &gt; Admin Centers &gt; Exchange. Once the Exchange Admin has opened, go to mail flow &gt; connectors and click + to add a new connector.</td>
<td>Select From: Partner organization and To: Office 365, then click Next.</td>
</tr>
<tr>
<td>Specify a name for the connector (e.g. Metadefender Email) and ensure that the option 'Turn it on' is checked. Then click Next.</td>
<td></td>
</tr>
<tr>
<td>Steps</td>
<td>Details</td>
</tr>
<tr>
<td>-------</td>
<td>---------</td>
</tr>
<tr>
<td></td>
<td>Select 'Use the sender's domain' and click Next</td>
</tr>
</tbody>
</table>

This connector enforces routing and security restrictions for email messages sent from your partner organization or service provider to Office 365.

*Note:
Metafilter Email

What do you want to do after connector is saved?
- Turn it on

New connector

How do you want to identify the partner organization?

Specify whether you want to use a domain or IP address to identify the partner organization:
- Use the partner's domain
- Use the sender's domain

Select this option to apply this connector to email messages that come from your partner's domains.
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Click on the +</td>
<td><img src="image.png" alt="Image of New Connector" /></td>
</tr>
<tr>
<td></td>
<td>Enter * as domain and click OK; then click Next</td>
</tr>
</tbody>
</table>

New connector

What sender domain do you want to use to identify your partner?

Specify one or more sender domains.

Back  Next  Cancel
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Select 'Reject email messages if they aren't sent over TLS' and 'Reject email messages if they aren't sent from within this IP address range', then click +</td>
</tr>
<tr>
<td>Steps</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------</td>
</tr>
<tr>
<td>Specify your public IP address (e.g. 213.149.186.214) and click OK; then click Next.</td>
<td><img src="https://outlook.office365.com/ecp/Connectors/InboundPartnerConnector.aspx" alt="Image" /></td>
</tr>
</tbody>
</table>

Verify connector properties and click Save to save the connector.
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td><strong>Steps</strong>&lt;br&gt;Obtain your MX record address by going to <a href="https://portal.office.com">https://portal.office.com</a> &gt; Admin &gt; Settings &gt; Domain and click on your domain; copy the MX Record value to the clipboard.</td>
</tr>
<tr>
<td>2.</td>
<td>Connect to MetaDefender Email Gateway Security Web Management console</td>
</tr>
</tbody>
</table>

**Details**

New connector

Confirm your settings.<br>Before using, make sure these are the settings you want to configure.

Mail flow scenario<br>From: Partner organization<br>To: Office 365

Name<br>MetaDefender Email

Description<br>None

Status<br>Turn it on after saving

How to identify your partner organization<br>Identify the partner organization by verifying that messages are coming from these domain(s).

Security restrictions<br>Reject messages if they aren’t encrypted using Transport Layer Security (TLS).<br>Reject messages if they don’t come from within these IP address ranges: 213.146.81.214.
<table>
<thead>
<tr>
<th>Steps</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Configure relays to match your original MX record; for details see 4.2 Security rules</td>
</tr>
<tr>
<td>2.</td>
<td>Configure MetaDefender Email Gateway Security to listen on port 25</td>
</tr>
<tr>
<td></td>
<td>Verify routing settings by sending an email to a Office365 recipient directly to the MetaDefender Email Gateway Security server and verify that it arrives correctly in the recipient inbox</td>
</tr>
<tr>
<td>3</td>
<td>Refer to your Internet domain registrar for the details how to change MX record to point to Make sure that your MX record changes have propagated routing.</td>
</tr>
<tr>
<td>Steps</td>
<td>Details</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>MetaDefender Email Gateway Security IP address; verify email routing by sending an email to a Office365 recipient</strong></td>
</tr>
</tbody>
</table>

3.10 Onsite Microsoft Exchange deployment

This is the standard setup with Microsoft Exchange Server.

⚠️ MetaDefender Email Gateway Security can only be installed on Hub or Edge role Exchange Servers (2013 or 2016).

**Installation**

See 2.2 Installing MetaDefender Email Gateway Security.
Exchange Server message expiration timeout

The MessageExpirationTimeout parameter of Microsoft Exchange Server specifies the maximum time that a particular message can remain in a queue.

If a message remains in the queue for longer than the MessageExpirationTimeout period of time, the message is returned to the sender as a permanent failure.

As a consequence this parameter is likely to affect the delivery of emails released or forwarded from Quarantine (see 4.3 Quarantine) or emails retried from Audit > Email History (see 4.4 Email history).

The default value of MessageExpirationTimeout is 2 days. It means that if an email spends more than 2 days in Quarantine or in Audit > Email History then releasing or forwarding and retrying (accordingly) after 2 days will fail.

MessageExpirationTimeout can be extended to the maximum of 90 days.

Reference and further reading


How To Verify

To verify that the Exchange Transport Agent has been installed successfully, open the Exchange Management Shell and type 'Get-TransportAgent' [ENTER]

Ensure that MetaDefender Email Security Smtp Agent and MetaDefender Email Security Routing Agent are listed and their Enabled statuses are True.

<table>
<thead>
<tr>
<th>Identity</th>
<th>Enabled</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>--------</td>
<td>----------</td>
</tr>
</tbody>
</table>
Transport Rule Agent                        True      1
DLP Policy Agent                            True      2
Malware Agent                               False     3
Text Messaging Routing Agent                True      4
Text Messaging Delivery Agent               True      5
System Probe Drop Smtp Agent                True      6
System Probe Drop Routing Agent             True      7
Metadefender Email Security Smtp Agent       True      8
Metadefender Email Security Routing Agent   True      9

3.11 Customization of notification emails

- Customizing blocked notifications
  - Example
    - Replacing the logo
    - Using different colors
    - Changing texts
- Customizing quarantine reports
- Notes
  - Removing xslt elements

Currently there are two types of notification emails: one for quarantine reports and one for blocked contents. By default these notification emails are written in English and have an OPSWAT related style (colors, logos, texts). If you would like to change the texts or the style of the email you can do it by modifying our email templates. These templates can be found under `<MetaDefender Email Gateway Security installation path>\mailagenthost\xslt` (C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost\xslt by default).

⚠️ Persistency of template changes

Please note that when upgrading your MetaDefender Email Gateway Security the customized templates could be overwritten by the installer. If you want to keep your modifications please make a copy of your templates before upgrading the product and copy them back after the upgrade is finished.
Customizing blocked notifications

The template for blocked notifications can be found in the `blockednotification.xsl` file. It is an XSLT file which contains HTML, CSS and XSLT elements. By modifying the HTML and CSS elements you can get a different look or language for your notifications. XSLT elements **should not be modified** as we use them to fill the email with actual data.

**Example**

Let's try to give a different look for our blocked notification email. The email looks like this by default:

![Blocked Notification Email Example](image)

We will replace the logo, change the colors and we will also have some text related changes.
Replacing the logo

In order to replace the logo you should find and modify the current part in the blockednotification.xsl file:

```
Logo

<a href="https://www.opswat.com/products/metadefender/email-security">
    <img src="img/logo.png" />
</a>
```

Let's assume that we have a `newlogo.png` image in the `img` folder. In this case we should modify this part to look like this:

```
Modified logo

<a href="https://www.opswat.com">
    <img src="img/newlogo.png" />
</a>
```

By modifying the `href` part the new logo will point to `http://www.opswat.com` instead of `https://www.opswat.com/products/metadefender/email-security`.

After these modifications the notification email will look like this:
Using different colors

Let's say we would like to modify the colors for our table containing the information related to the blocked email. In this case we should modify this part:

Table colors

```
// Table colors

// Primary header color
table.email-details .table-header { background: #2672FB; color: #FFFFFF; }
// Primary header text color
//table.email-details .table-header p { font-weight: 700; white-space: nowrap; }
// Alternate row background color
//table.email-details tr.alt td { background: #EAEFF2; }
// Alternate row header background color
//table.email-details tr.alt .table-header { background: #2672FB; }
```

Modifying the background color values we could have a style like this:

Modified table colors

---

4.7.4
The following changes would make our notification to look like this:

![Example Company](Image)

**MetaDefender Email Security** has found problems in the following email:

<table>
<thead>
<tr>
<th>Date:</th>
<th>2018-04-09 09:18:53 UTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>From:</td>
<td><a href="mailto:test1@test.com">test1@test.com</a></td>
</tr>
<tr>
<td>To:</td>
<td><a href="mailto:test2@test.com">test2@test.com</a></td>
</tr>
<tr>
<td>Subject:</td>
<td>[1] Test blocked</td>
</tr>
<tr>
<td>Result:</td>
<td>Infected (EICAR_Test_file, Eicar-Test-Signature, Eicar-Test-Signature, Eicar test file)</td>
</tr>
<tr>
<td>Scan result:</td>
<td>[Click here to view scan result]</td>
</tr>
</tbody>
</table>

The original – potentially harmful – email was put into quarantine. If you think that this email was erroneously blocked, contact your administrator to release it.

Best regards,
MetaDefender Email Security

**Changing texts**

If we would like to have different texts in the notification we could just simply change or remove the text literals in the template. Let's change **MetaDefender Email Gateway Security** to **Example Company**. For this we should modify these two lines:

```text
```
MetaDefender Email Gateway Security has found problems in the following email:

Best regards,

MetaDefender Email Gateway Security

After the changes we have:

Example Company has found problems in the following email:

Best regards,

Example Company

The result will look like this:

We can also change the text direction to right-to-left by adding dir="rtl" to the html element:
Customizing quarantine reports

The template for quarantine reports can be found in the qreport.xsl file. Here we have the same rules for the modifications as in the case of customizing blocked notifications.

Notes

Removing xslt elements

However the modification of xslt elements are not recommended since it can result in missing or incorrect data, you can remove them if not having some data is your actual goal.

For example if you don't want to include the Scan result link in the notification you could remove this part from the blockednotification.xsl:
After removing these elements the email won't have the *Scan result* row:
4.1 Dashboard

- Statistics details

MetaDefender Email Gateway Security's Dashboard gives an overview about the email processing status.

ℹ️ Refresh rate

The default refresh rate of the displayed information is 30 seconds.
The Overview page shows information about:

- **MALICIOUS ATTACK PREVENTION**: status of the data sanitization feature.
- **ADVANCED THREAT DETECTION**: status of the multi-scanning (anti-malware) feature.
- **DATA LOSS PREVENTION**: status of the data loss / leak prevention feature.
- **IN QUEUE**: status of email processing queues:
  - Pending (waiting for processing),
  - Processing actively, and
  - Retrying after incomplete processing.
- **QUARANTINE**: Number of emails in quarantine (for details see the Actions for emails with blocked contents and Actions for emails with sanitized contents sections in 4.2 Security rules)
- **FAILED**: Number of refused emails (for details see 4.4 Email history)
- **REFUSED**: Number of refused emails (for details see 4.5 Refused emails)

**Statistics details**

The Dashboard can show additional statistics information for certain widgets. When additional statistics are supported, then a Show details link is present in the bottom of the widget.
In case of INBOUND EMAILS and OUTBOUND EMAILS, the bars represent the share between the BLOCKED and ALLOWED emails. The number shows the total (blocked and allowed) number of emails of that email address.

In case of INBOUND EMAILS and OUTBOUND EMAILS, the information is split by recipients and senders. Clicking the title, the appropriate data is displayed.
In case of MALICIOUS ATTACKS PREVENTION, ADVANCED THREAT DETECTION and DATA LOSS PREVENTION, the bars represent each entry's share from the total.
The following widgets can show detailed statistics:

- MALICIOUS ATTACKS PREVENTION
- ADVANCED THREAT DETECTION
- DATA LOSS PREVENTION
- INBOUND EMAILS
- OUTBOUND EMAILS

4.2 Security rules

Security rules in MetaDefender Email Gateway Security can be configured under **Policy > Security rules**.

- Security rules overview
  - General information
  - Email filter
    - Filter parts
      - Sender IP address conditions
In traditional configurations MetaDefender Email Gateway Security is wedged between the organization's email gateway and mail server (see the image below). In case of inbound email directions it receives the email from the email gateway and sends it towards the mail server. In case of outbound directions it receives the email from the mail server and sends it towards the email gateway.
Metadefender Email Security traditional setup

Security rules overview

Security rules help to assign security policies to specific email messages.

A security rule consists of four parts:

- General information
- Email filter
- Security policy definition
- Rule order

General information

The following properties may be configured:

1. NAME: unique name of the rule
2. DESCRIPTION: optional, detailed description
3. DIRECTION: direction of the email messages this rule is intended to match.

⚠️ From an email message it is hard—in some cases not even possible at all—to tell whether it was inbound or outbound. That is the reason why this setting only records what the administrator's intention was with the rule and it serves statistical purposes only.
There is no guarantee for example that an inbound rule will match inbound messages only.

On the 4.1 Dashboard page, however, MetaDefender Email Gateway Security will categorize an email as *inbound* or *outbound* based on the direction setting the matching rule has.

a. **INBOUND**: default, messages that are coming in to the organization

b. **OUTBOUND**: messages that are going out from the organization

**Email filter**

Based on the source(s), sender(s) and recipient(s), email filters select messages on which the assigned security policy will be applied. Email filters can be set up on the **Filter** tab while creating or editing a security rule.

**Filter parts**

A filter may consist of three parts:

1. Sender IP address conditions
2. Sender domain or email address conditions
3. Recipient domain or email address conditions

There is **AND** relation among the above parts of the filter.

**Sender IP address conditions**

Sender IP addresses are the addresses of infrastructure elements in the deployment, from which MetaDefender Email Gateway Security is allowed to receive emails according to this rule.

In case of a traditional setup, for example, sender is the email gateway for inbound messages and the mail server for outbound messages.

<table>
<thead>
<tr>
<th>Type</th>
<th>IP address or subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match type</td>
<td><strong>EQUALS</strong></td>
</tr>
<tr>
<td>Examples</td>
<td>IP</td>
</tr>
<tr>
<td></td>
<td>10.0.0.1</td>
</tr>
<tr>
<td></td>
<td><strong>Subnet</strong></td>
</tr>
<tr>
<td></td>
<td>10.0.0.0/24</td>
</tr>
</tbody>
</table>

There is **OR** relation among entries in sender IP address conditions.

**Sender domain or email address conditions**

Sender filter makes possible to apply security rule based on who sent the email. The value comes from the email envelope’s MAIL FROM part.

**Spoofing**

When using this filter please be very aware of the fact that spoofing the sender of the email is a very easy task. A more secure way to use this filter would be for OUTBOUND emails only along with filtering to the sender IP.
Type | QRegExp
---|---
**Match type** | regular expression match

**Examples**
- .+@opswat.com
- somespecificuser@opswat.com
- opswat.com (treated as .+@opswat.com)

**Note**
Please note that the "." (dot) in a regular expression matches any character. This means .+@opswat.com can match test@opswat1.com. If you want to match explicitly for a dot you should escape it like this: .+@opswat\.com

⚠️ There is **OR** relation among the sender domain or email address conditions.

**Recipient domain or email address conditions**
Recipient conditions help to restrict email recipients allowed by the rule.

- Recipient domain or email address conditions can also help to counter emails sent to invalid recipients; that do not even exist at an organization or among the partners, for example.
  - This kind of defense may protect against unnecessary overloads or even against malicious attacks.

In case of inbound directions rules usually allow organization internal e-mail addresses only. In case of outbound directions all e-mail addresses may be allowed.

<table>
<thead>
<tr>
<th>Type</th>
<th>QRegExp</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Match type</strong></td>
<td>regular expression match</td>
</tr>
<tr>
<td><strong>Examples</strong></td>
<td></td>
</tr>
</tbody>
</table>
- .+@opswat.com  
- somespecificuser@opswat.com |
4.7.4

- opswat.com (treated as .+@opswat.com)

**Note**

Please note that the "." (dot) in a regular expression matches any character. This means .+@opswat.com can match test@opswat1com. If you want to match explicitly for a dot you should escape it like this: .+@opswat\..com

**Warning**

There is OR relation among the recipient domain or email address conditions.

**Security policy**

A security policy consists of the SCAN settings and the ACTIONS.

**Scan settings**

The scan policy can be set up on the SCAN tab while creating or editing a security rule.

The following options are available:

1. ALLOW SCAN: enable or disable scanning of requests. Default is enabled.
   a. METADEFENDER CORE: MetaDefender Core type server profile to which emails are sent for scanning. Default is None.
   b. SCAN TIMEOUT [IN SECONDS]: If a scan result is not available from the MetaDefender Core within this timeframe the scan will be cancelled. Default is 300 secs.
   c. SCAN EMAIL BODY: Whether to scan the email body or not. Default is to enable scanning the body.

   - The attachments of the email will be scanned indifferent of this setting.
   d. SCAN EMAIL HEADERS: Whether to scan the email headers or not. Default is to enable scanning the headers.

   - This function can help—for example—to prevent leaking sensitive information in email subjects.
When the header contains infection or sensitive data and if scanning email headers is enabled and the header is removed due to be blocked or sensitive (Policy > Security Rules / add/modify/ ACTIONS / HANDLING OF THE EMAIL is set to DELETE BLOCKED CONTENTS) then the email may be rendered with no sender, recipient, subject, etc. in the email client (as all this metadata is in headers):

1. When scanning is disabled, all matching emails will be accepted.

2. Referenced Core rules may be changed or even deleted while they are still used by MetaDefender Email Gateway Security. For symptoms and solutions of such cases see section 148433311.

**Actions**

The actions policy define what should happen to a matching email message based on the scan outcome. Actions can be set up on the ACTIONS tab while creating or editing a security rule. Scanning may have three kinds of outcome. The email message may either be
1. Blocked, or
2. Sanitized, or
3. Allowed.

An email message is blocked when any content in it is blocked by MetaDefender Core due to malware infection for example.

An email message is sanitized, when any attachment in it is sanitized by MetaDefender Core due to potentially harmful content for example.

An email message is allowed when there was no actual or potential problem found in it.

Description of the existing actions are the following:

1. DELETE BLOCKED ATTACHMENTS: all attachments blocked by MetaDefender Core are irreversibly deleted.

2. QUARANTINE ORIGINAL EMAIL: the whole email is blocked from further processing and sent to a specific container called quarantine. Messages can be recovered from the quarantine, for details see 4.3 Quarantine.

3. ADD DISCLAIMER: add the specified content to the end of the email message.
   a. DISCLAIMER POSITION: Disclaimer can be added before or after the original content of an email
   b. DISCLAIMER STYLE: A disclaimer style can be applied to emphasize content to the user (HTML only)
   c. HTML: If the email is formatted as HTML then the content specified here will be appended. A HTML markup may be specified (e.g. HTML link, inline CSS) and it will be rendered properly in the resulting email message.

---

**Example**


---

⚠️ Internal and external CSS
Using internal style sheets (defined by using the `<style>` tag within the `<head>` area of the HTML document) or external CSS (a file that contains only CSS code and is saved usually with a `.css` file extension, then this CSS file is referenced in the `<head>` area of the document using the `<link>` (instead of `<style>`) may give unexpected results.

d. PLAIN TEXT: If the email is plain text or formatted as Rich Text Format (RTF) then the text specified here will be appended with no formatting.

4. ADD THE FOLLOWING HEADERS: the specified headers will be added to the internet headers section of the email message. Click the ADD ROW button to add a new header to the list.

**Actions for emails with blocked contents**

The following actions are available for emails with blocked contents:

<table>
<thead>
<tr>
<th>Action</th>
<th>QUARANTINE ORIGINAL EMAIL</th>
<th>HANDLING OF THE EMAIL</th>
<th>ADD DISCLAIMER</th>
<th>DISCLAIMER POSITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>ON</td>
<td>BLOCK EMAIL</td>
<td>ON</td>
<td>AFTER CONTENT</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NOTIFY RECIPIENTS IF EMAIL IS BLOCKED</td>
<td>OFF</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FROM</td>
<td>Blank</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUBJECT</td>
<td>Email Gateway Security notification: Email blocked</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>CUSTOMIZE NOTIFICATION RECIPIENTS</td>
<td>OFF</td>
<td></td>
</tr>
</tbody>
</table>

MetaDefender Email Gateway Security blocked this email due to malicious embedded objects. For more information on MetaDefender Email Gateway Security, please visit [https://www.opswat.com/products/metadefender/email/](https://www.opswat.com/products/metadefender/email/).
<table>
<thead>
<tr>
<th>Action</th>
<th>QUARANTINE ORIGINAL EMAIL</th>
<th>HANDLING OF THE EMAIL</th>
<th>ADD DISCLAIMER</th>
<th>DISCLAIMER POSITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notes</td>
<td></td>
<td>1. BLOCK EMAIL: do not deliver the email</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2. DELETE BLOCKED CONTENTS: deliver the email without blocked (infected) contents</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3. DELIVER BLOCKED CONTENTS: deliver the email keeping blocked (infected) contents</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Customizing notifications

**Restricting blocked emails causing notifications**

You can customize what range of blocked emails to produce notification emails.

**Default**

By default Email Gateway Security will send a notification for each blocked email.

To configure what range of blocked emails to cause a notification email to be sent, go to **Policy > Security Rules** / add/modify / ACTIONS / NOTIFY RECIPIENTS IF EMAIL IS BLOCKED / SEND NOTIFICATION FOR and from the drop down list select your preference.

The following options are currently available:
1. **ALL BLOCKED EMAILS**: Email Gateway Security will send a notification email for each blocked email (including emails with password protected attachments).

2. **ONLY EMAILS WITH PASSWORD PROTECTED ATTACHMENTS**: notification emails are sent for emails with password protected attachments only.

### Customizing notification recipients

You can customize the recipients of notification emails. To enable the customization the `CUSTOMIZE NOTIFICATION RECIPIENTS` should be enabled.

- **SEND NOTIFICATION FOR ORIGINAL SENDER**: When this option is enabled, the sender of the original email will receive the notification email.

---

**Example**

Enabling this option will allow the sender to provide the password (for a password protected document or archive) so that she can have the email scanned before it is sent out the organization.
• **SEND NOTIFICATION FOR ORIGINAL RECIPIENTS:** When this option is enabled every recipient of the original email will receive the notification email. If disabled only the additional recipients will receive the notification email.

• **ADDITIONAL RECIPIENTS:** You can add additional recipients who should also receive the notification emails. This could be an administrator or a notification email parser system for example.

There is at least one recipient is needed for the notification emails, so disabling the notification sending for original recipients without an additional recipient is not allowed.

Options for emails with blocked contents if the blocked content is a password protected attachments

<table>
<thead>
<tr>
<th>Option</th>
<th>ADD DISCLAIMER FOR ENCRYPTED ATTACHMENTS</th>
<th>DISCLAIMER POSITION</th>
<th>HTML</th>
<th>PLAIN TEXT</th>
<th>SE</th>
<th>UP</th>
<th>RE</th>
<th>LI</th>
<th>EV</th>
<th>RE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default</td>
<td>OFF</td>
<td>AFTER CONTENT</td>
<td>&lt;p&gt;MetaDefender Email Gateway Security has removed &lt;strong&gt;password protected attachment(s)&lt;/strong&gt; in this email.  Please click &lt;strong&gt;&lt;a href=&quot;%[ ]%rescan_link_url [:]%&quot; here&lt;/a&gt;&gt;&lt;/p&gt; to rescan the email and deliver all contents. For more information on MetaDefender Email Gateway Security, please</td>
<td>MetaDefender Email Gateway Security has removed password protected attachment(s) in this email. Please click %[]rescan_link_url [Your administrator did not set a public server address for rescan]% to rescan the email and deliver all contents. For more information</td>
<td>Of</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Option</td>
<td>ADD DISCLAIMER FOR ENCRYPTED ATTACHMENTS</td>
<td>DISCLAIMER POSITION</td>
<td>HTML</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------------------------------</td>
<td>---------------------</td>
<td>------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| Notes | %\[
rescan_link_expiry []\% and %\[
rescan_link_url[]\% will be replaced by the RESCAN LINK AVAILABILITY and PUBLIC SERVER ADDRESS values from 3.4 General settings. If the PUBLIC SERVER ADDRESS is not set then the "Your administrator did not set a public server address for rescan" text will be displayed instead. |      | %\[
rescan_link_expiry []\% and %\[
rescan_link_url[]\% will be replaced by the RESCAN LINK AVAILABILITY and PUBLIC SERVER ADDRESS values from 3.4 General settings. If the PUBLIC SERVER ADDRESS is not set then the "Your administrator did not set a public server address for rescan" text will be displayed instead. |
### Actions for emails with sanitized contents

The following actions are available for emails with sanitized contents:
<table>
<thead>
<tr>
<th>Action</th>
<th>QUARANTINE ORIGINAL EMAIL</th>
<th>ADD DISCLAIMER</th>
<th>DISCLAIMER POSITION</th>
<th>HTML</th>
<th>PLAIN TEXT</th>
</tr>
</thead>
</table>

**Actions for allowed emails**

The following actions are available for allowed emails:
<table>
<thead>
<tr>
<th>Action</th>
<th>ADD DISCLAIMER</th>
<th>DISCLAIMER POSITION</th>
<th>HTML</th>
<th>PLAIN TEXT</th>
<th>ADD THE FOLLOWING HEADER</th>
</tr>
</thead>
</table>

**Relay**

⚠️ Exchange Server mode
Relay is not available in case of on-site Exchange Server deployments. The reason is that in case of Exchange mode emails are sent back to the Exchange Server at the end of processing.

Relay specifies where to send next an e-mail message when it is not blocked (it is not scanned; it is allowed, sanitized, released or forwarded). As a closing act of processing the email message it is tried to be forwarded to the SMTP servers specified by the relay.

Relay can be set up on the Relay tab while creating or editing a security rule.

Relay itself is an SMTP type server profile. For details about server profiles see 3.7 Server profiles.

In case of a traditional setup, for example, relay is the email gateway for outbound messages and the mail server for inbound messages.

Resending

If the email is failed to be sent to any of the SMTP server defined by the relay server profile, then sending is retried according to the settings documented in 3.4 General settings.

If sending the email keeps failing even after the retries, then MetaDefender Email Gateway Security gives up.

In case of permanent failure the email message remains in the queue, it will not be deleted. As a consequence permanently failing messages may accumulate on the MetaDefender Email Gateway Security server consuming disk space.

Vault

MetaDefender Email Gateway Security can be integrated with MetaDefender Vault which makes possible to upload attachments to MetaDefender Vault during processing emails on a security rule basis. For more details and possibilities please check 4.9 Integration with MetaDefender Vault.

Advanced scan settings

The advanced scan settings policy define certain exceptions from the default behavior. Advanced scan settings can be set up on the ADVANCED tab while creating or editing a security rule.

The following options are available:
1. OVERRIDE SMTP RESULTS allows overriding default behavior in the following cases
   a. SMTP SERVER NOT RESPONDING: SMTP server is not reachable or some other connection error occurred when trying to reach it; default: Retry
   b. SMTP PERMANENT FAILURE: SMTP server responded with 5xx error code (e.g. 550 mailbox unavailable); default: Retry

2. OVERRIDE SANITIZATION BEHAVIOR allows overriding default behavior in the following cases
   a. SKIP PARTIAL SANITIZATIONS: Do not replace partially sanitized archives in email attachments, handle them as if there was no sanitization at all for the archive file.

⚠️ Core 4.15.1 required

This feature requires MetaDefender Core version 4.15.1.

For this feature to work, Policies > Workflow rules / add/modify / DATA SANITIZATION / INCLUDE ALLOWED ORIGINAL FILE INTO SANITIZED ARCHIVE FILE REGARDLESS must be disabled for the Core side rule, that is in use in the Email Gateway Security side rule.
b. SEND SANITIZED VERSION OF BLOCKED FILES: when this option is enabled and the 148433311 is set to "DELETE BLOCKED CONTENTS" then instead of deleting the blocked file Email Gateway Security will send the sanitized version of that file if available. If the sanitized version of the blocked file is not available the file will be deleted.

c. SEND ORIGINAL FILE IF THE SANITIZATION FAILED FOR makes possible to receive the original file if the sanitization fails for the given cases
   i. NONE: Emails with sanitization failure will be blocked or the files whose sanitization failed will be deleted for every type of file; this is the default behavior
   ii. PASSWORD PROTECTED DOCUMENTS: Emails with sanitization failure will be allowed or the files whose sanitization failed won't be deleted if the original file was identified as a "Password Protected Document". The email will still be blocked if there is an other issue like an infected file or a sanitization failure for a non "Password Protected Document".
   iii. EVERY ALLOWED FILE: Emails with sanitization failure will be allowed or the files whose sanitization failed won't be deleted if the original file was not blocked by Core. The email will still be blocked if there is an other issue like an infected file.

d. ADD SANITIZATION FAILURE DISCLAIMER: Add this disclaimer to the email if there is a sanitization failure.

3. DO NOT MODIFY S/MIME AND PGP SIGNED EMAILS allows skipping the modification of emails which are signed; default: Enabled. With this option enabled the digital signature of the email can remain valid. For more information check 4.8 Support for signed emails.

4. OVERRIDE ERROR HANDLING BEHAVIOR allows overriding default error handling behavior in the following cases
   a. CORE UNREACHABLE: no network connection to Core; default: Retry
   b. CORE BUSY: Core actively refuses scanning due to overload; default: Retry
   c. SCAN TIMEOUT: scanning timeouts on Core; default: Retry
   d. CORE PROCESSING FAILED: Core fails to scan; default: Fail immediately

5. BYPASS HEADERS: the specified headers will be added to the internet headers section of the email messages that bypassed scanning (Bypass if all retry fail). Click the ADD ROW button to add a new header to the list.

6. BYPASS DISCLAIMER
a. DISCLAIMER POSITION: the position of the disclaimer; default: BEFORE CONTENT

b. DISCLAIMER STYLE: A disclaimer style can be applied to emphasize content to the user (HTML only)

c. HTML: the specified disclaimer will be added to the HTML formatted email messages that bypassed scanning (Bypass if all retry fail).

d. PLAIN TEXT: the specified disclaimer will be added to the plain text and RTF formatted email messages that bypassed scanning (Bypass if all retry fail).

Rule order

Several security rules can be created that may target different messages from different sources going to different recipients. However, care must be taken how these rules are set up and ordered, as there is a 148433311 and a 148433311.

Specific rules should come first while generic rules should go at last.

First match policy

If there are more matching rules in the system, then the email message will be accepted or rejected according to the security policy of the first matching rule in the list.

No match policy

If there is no matching rule in the system (or no rule at all), then the email message will be rejected.

⚠️ There are no default security rules in MetaDefender Email Gateway Security. As a consequence all email messages are blocked by default.

⚠️ Deleting all security rules from the system results all email messages being blocked.
Security Rule Management

The Security Rule Management screen lists the existing security rules in the system.

Functions

Besides listing existing security rules the Security Rule Management screen provides the following functions:

- Add new security rule
- Clone an existing security rule
- Modify (and view) existing security rule's properties
- Delete existing security rule
- Reorder existing security rule
Unavailable MetaDefender Core rules

There is a loose coupling between security rules in MetaDefender Core and security rules in MetaDefender Email Gateway Security. This means that Core won't check whether its rules are in use in Email Gateway Security. Core will allow the rules to be modified or deleted even if these rules are in use in Email Gateway Security.

To resolve this situation, MetaDefender Email Gateway Security periodically checks whether the applied rules still exist on the coupled MetaDefender Cores and notifies the user about unavailable Core rules.

⚠️ Core rules are fetched in every 30 seconds. Changes on Cores—mentioned below to mitigate unavailable Core rules issues—need 30 seconds to be reflected in MetaDefender Email Gateway Security. If the applied changes can not be seen then wait some seconds and try again by refreshing the Web Management Console page in your browser.

⚠️ There is also a 30 seconds connection timeout for reaching MetaDefender Core, so if the connection can not be established in that timeframe, the scan rules won't be available.

Security rules which have ALLOW SCAN disabled are not affected by this issue.

⚠️ Using unavailable Core rules for scanning may lead to failing scans.

Symptoms
The following symptoms show that there are rules defined under Policy > Security rules that are configured with Core profiles havin unavailable rules:

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>There are one or more active alerts in the UI</td>
<td>👁️</td>
</tr>
<tr>
<td>Symptom</td>
<td>Screenshot</td>
</tr>
<tr>
<td>---------</td>
<td>-----------</td>
</tr>
<tr>
<td>One of the notifications is about unavailable Core rules</td>
<td><img src="image" alt="Notification" /></td>
</tr>
<tr>
<td>One or more items in the list of the CORE URI ADDRESS and RULE print the <em>(Unavailable)</em> postfix in the appropriate server profile under <strong>Inventory &gt; Server profiles</strong></td>
<td><img src="image" alt="Core URI Address" /></td>
</tr>
</tbody>
</table>

**Possible reasons**

The following reasons may lead to unavailable Core rules:

- Under **Inventory > Server profiles** the CORE URI ADDRESS point to a MetaDefender Core that is unavailable
- Under **Inventory > Server profiles** the RULE got renamed on MetaDefender Core after it was set in the server profile on MetaDefender Email Gateway Security
- Under **Inventory > Server profiles** the RULE became visible for some specific agents only on MetaDefender Core and therefore MetaDefender Email Gateway Security cannot see it anymore

The unavailable security rule(s) can be found under **Inventory > Server profiles** by checking all the MetaDefender Core type server profiles looking for the *(Unavailable)* postfix among the configured RULE entries:
Resolution

The following steps may eliminate unavailable Core rules:

- Check if MetaDefender Cores set under **Inventory > Server profiles** are available
- Check whether the unavailable rules got renamed on MetaDefender Cores
- Check whether there are any limitations for the given Core rules which would make them unavailable for MetaDefender Email Gateway Security

4.2.1 Disclaimer variables

- Variable format
- Available variables
  - Generally available variables
  - Specific variables
    - Emails with encrypted attachments
- Example disclaimer with variables

Starting from version 4.4.0 you can add some predefined variables to the disclaimers to show additional email specific information there.

Variable format

The common format of a variable looks like this: %[<prefix>]<variable_name>[<placeholder>]%

A variable contains three parts:

- **prefix**: this text will be displayed before the value of the variable if the value is not empty or there is a placeholder defined
- **variable_name**: the name of the variable
- **placeholder**: this text will be displayed if the value of the variable is empty

Examples:
<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
<th>Output in disclaimer</th>
</tr>
</thead>
<tbody>
<tr>
<td>%[]email_subject[]%</td>
<td>Test subject</td>
<td>Test subject</td>
</tr>
<tr>
<td>%[]email_subject[]%</td>
<td>***</td>
<td>***</td>
</tr>
<tr>
<td>%[Subject: ]email_subject[]%</td>
<td>Test subject</td>
<td>Subject: Test subject</td>
</tr>
<tr>
<td>%[Subject: ]email_subject[]%</td>
<td>***</td>
<td>***</td>
</tr>
<tr>
<td>%[Subject: ]email_subject[No subject]%</td>
<td>***</td>
<td>Subject: No subject</td>
</tr>
<tr>
<td>%[]email_subject[No subject]%</td>
<td>***</td>
<td>No subject</td>
</tr>
<tr>
<td>%[]email_subject[No subject]%</td>
<td>Test subject</td>
<td>Test subject</td>
</tr>
</tbody>
</table>

**Available variables**

**Generally available variables**

The following variables are available for any disclaimer:

- `email_date`
- `email_sender`
- `email_recipients`
- `email_subject`
- `email_message_id`
- `origin_ip`
- `scan_verdicts`

**Specific variables**

**Emails with encrypted attachments**

The following variables are available for disclaimers to emails with encrypted attachments only:
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rescan_link_url</td>
<td>Replaced by the Settings &gt; Global Settings / PUBLIC SERVER ADDRESS value. If the PUBLIC SERVER ADDRESS is not set then the &quot;Your administrator did not set a public server address for rescan&quot; text will be displayed instead.</td>
</tr>
<tr>
<td>rescan_link_expiry</td>
<td>Replaced by the Settings &gt; Global Settings / RESCAN LINK AVAILABILITY value.</td>
</tr>
<tr>
<td>rescan_link_expiry_time</td>
<td>Replaced by the date and time value calculated using the Settings &gt; Global Settings / RESCAN LINK AVAILABILITY value.</td>
</tr>
</tbody>
</table>

**Calculation method**

The date and time value is calculated as:

(Time of email arrival to Email Gateway Security) + (Settings > Global Settings / RESCAN LINK AVAILABILITY)

**UTC or server local time**

The value of Settings > Global Settings / USE THE SERVER'S LOCAL TIME INSTEAD OF UTC affects the format of this value.

Server local time
<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UTC</td>
<td></td>
</tr>
<tr>
<td>Variable</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>

---

Example disclaimer with variables

Here is an example disclaimer for blocked contents:

---

MetaDefender Email Gateway Security has removed one or more attachments in this email because it contained potentially malicious embedded objects. For more information on MetaDefender Email Gateway Security, please visit https://www.opswat.com/products/metadefender/email-security.

`@[Date: ]email_date[]%
@[Sender: ]email_sender[]%
@[Recipients: ]email_recipients[]%
@[Subject: ]email_subject[]%
@[Message ID: ]email_message_id[]%`
And an example result after sending an infected attachment:

---
MetaDefender Email Gateway Security has removed one or more attachments in this email because it contained potentially malicious embedded objects. For more information on MetaDefender Email Gateway Security, please visit https://www.opswat.com/products/metadefender/email-security.

Date: 2018-08-15 13:07:51 UTC
Sender: test1@test.com
Recipients: test2@test.com
Subject: Eicar attachment
Message ID: 90b5cc66-cf5d-9ef5-9ac8-4f9dcce083aa@test.com
Origin IP: 127.0.0.1
Scan verdicts: Eicar attachment/eicar.com: Infected

4.3 Quarantine

- Quarantine
  - Safety
- Quarantining conditions
  - Blocked emails
  - Sanitized emails
- Quarantine operations
  - Bulk operations
    - Download
      - File naming
    - Release
  - Forward
  - Pin
  - Delete
  - Rescan
    - Select alternative rule for the rescan
• Provide password for encrypted attachments
• View details
• Quarantine reports

Quarantine is the safe storage for emails which were blocked or sanitized by MetaDefender Email Gateway Security.

For details about quarantine configuration see 3.6 Quarantine configuration.

ℹ️ The machine hosting the quarantine is safe from infections as long as items in the quarantine are not opened or executed.

**Quarantine**

The quarantine can be accessed under **Quarantine** in the Web Management Console.

⚠️ **Quarantine moved**

Starting with MetaDefender Email Gateway Security version 4.7.0, the former **Dashboard > Quarantine** entry has been moved to the root level **Quarantine** menu entry.
Safety

Unless the malicious contents are opened or executed, the quarantine does not expose the hosting machine to risk.

Care must be taken when granting access to the quarantine as releasing or forwarding the items from the quarantine might cause harm.

Quarantining conditions

Blocked emails

If

1. the email's body and/or any of its attachments is blocked by MetaDefender Core and
2. the email matched by a security rule on MetaDefender Email Gateway Security that marks blocked emails to be quarantined,

then the original message is kept in the quarantine.
Sanitized emails

If

1. the email's body and/or any of its attachments is sanitized by MetaDefender Core and
2. the email is matched by a security rule on MetaDefender Email Gateway Security that marks sanitized items to be quarantined,

then the original message is kept in the quarantine.

Quarantine operations

Once an email is in quarantine, the following operations can be executed on it:

1. Download
2. Release
3. Forward
4. Pin
5. Delete
6. View details

Bulk operations

Use the checkbox in front of each row to select elements (or use the checkbox in the header row to select all visible items).
Only visible elements can be selected. Elements that are not visible (due to pagination, search or filtering) are not selected even by the select all checkbox.

Download

Download the selected original emails from the quarantine to the local hard drive.
The format of the downloaded emails is zipped MIME (.eml).
File naming

<table>
<thead>
<tr>
<th>Component</th>
<th>File name</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive package</td>
<td>EmailSecurity-Quarantine-&lt;year&gt;-&lt;month&gt;-&lt;day&gt;-&lt;hour&gt;-&lt;minute&gt;-&lt;second&gt;</td>
<td>.zip</td>
</tr>
<tr>
<td>Email file</td>
<td>&lt;subject&gt;_&lt;unique ID&gt;</td>
<td>.eml</td>
</tr>
</tbody>
</table>

Release

Release the selected original emails from the quarantine and send them to the original recipients. The original emails are removed from the quarantine.

⚠️ The recipients will receive the (potentially) malicious contents.

⚠️ For this function to work correctly SMTP SERVER must be set under Notification and report settings on the Settings > Global settings tab. For details see 3.4 General settings.
Quarantining puts the original email into the quarantine and sends a notification or a disinfected/sanitized copy to the original recipient. As a result, releasing from the quarantine virtually duplicates the history entry for the quarantined email.

These duplicates are marked with a 🎥 (paper plane) icon in front of the RECIPIENT (S) in Audit > Email history: 

Forward

Send the selected original emails to additional recipient(s) (for investigation purposes, for example). The original emails remain in the quarantine.

⚠️ The recipient(s) will receive the (potentially) malicious contents.

⚠️ For this function to work correctly SMTP SERVER must be set under Notification and report settings on the Settings > Global settings tab. For details see 3.4 General settings.
Quarantining puts the original email into the quarantine and sends a notification or a disinfected/sanitized copy to the original recipient. As a result, forwarding from the quarantine virtually duplicates the history entry for the quarantined email.

These duplicates are marked with a (forward) icon in front of the RECIPIENT(S) in Audit > Email history:

Pin

Pinning prevents cleaning up an email from the quarantine by the manual or automatic clean-up mechanism. For details about automatic clean-up see the Data retention section in 3.4 General settings.

You can pin multiple emails simultaneously however unpinning an email is possible only per email. For unpinning you should click on the email and uncheck the checkbox next to Pinned.
Delete

Delete the original email from the quarantine.

⚠️ Deleted emails can not be recovered.

Rescan

MetaDefender Email Gateway Security provides the capability to rescan emails that were previously blocked and ended up in the quarantine. After a rescan the email may be allowed and delivered normally. Some of the reasons why emails may be rescanned:

- To process the email with updated scan engines that may not block the contents,
- To process the email with an alternative rule that may give different results,
  - To sanitize a blocked email before releasing
- To provide password for encrypted attachments and process the decrypted contents.
Select alternative rule for the rescan

Rescan email

Are you sure you want to rescan this email: QR?

PROCESS EMAIL USING THIS RULE:

rule

Rescan email

Provide password for encrypted attachments

For further details see 4.7 Support for password protected attachments.

Provide passwords for the following attachments:

CMAKE-3.1.3-WIN32-X86.RAR

Password

Rescan email

CANCEL
View details

Display:

1. The same details about the email as in Audit > Email history / Email details (see 4.4 Email history),

2. The raw email contents:
   a. Email headers
   b. Attachments
      i. Content-Type
      ii. Filename
   c. Raw email body

Quarantine reports

MetaDefender Email Gateway Security can be configured to periodically send report emails about the quarantine status.

To set up quarantine reports see 3.6 Quarantine configuration.
For this function to work correctly SMTP SERVER must be set under Notification and report settings on the Settings > Global settings tab. For details see 3.4 General settings.

A quarantine report email looks like the one below.

4.3.1 Sanitize before release
• Preparations
• Release

It is a potential use case to sanitize emails before releasing them. This feature is not supported by the regular Release function but can be achieved using Rescan. For details about rescanning see the Rescan section in 4.3 Quarantine.

Preparations

1. On Core servers create a rule that does not scan, but applies the desired sanitization.
   a. It is necessary to allow the not scanned results for the Core rule (in Core under Policy > Workflow rules / Add/Modify Rule / ADVANCED / OVERRIDE SCAN RESULTS CLASSIFIED AS ALLOWED / NOT SCANNED)

   ![Rescan screenshot]

   To allow password protected archives to be processed, the encrypted archive results must be disabled (in Core under Policy > Workflow rules / Add/Modify Rule / ADVANCED / OVERRIDE SCAN RESULTS CLASSIFIED AS ALLOWED / ENCRYPTED ARCHIVE)

2. On Email Security create a MetaDefender Core type server profile having the Core servers and rules created in the previous step.
3. On Email Security, under **Policy > Security rules** create a rule using the server profile created in the previous step.
   a. ⚠ Optionally set 0.0.0.0 as SENDER IP ADDRESS for this rule to not match any regular incoming emails or
   b. Set the priority of this rule accordingly if it is expected to process regular incoming emails.

**Release**

1. ⚠ Instead of using the *Release* function use the *Rescan* function.
2. In the confirmation dialog select the rule created in the previous section:

   ![Rescan email dialog](image)

   3. The email will be re-processed using the newly selected rule.
      a. If the new rule allows the email, then it gets delivered normally.

**4.4 Email history**

- Email history
  - Differentiating forked emails
    - Example
  - Operations
    - Force retry
    - View email details
- Processing history
- Failed emails
  - Failure conditions
  - Operations
  - Bulk operations
    - Operations on all failed items
      - Retry Failed
    - Operations on selected items
      - Selecting entries
      - Retry
      - Delete
      - Download
    - File naming

⚠️ Email history and Failed emails merged

Starting with MetaDefender Email Gateway Security version 4.7.0, the former Dashboard > Email history and Dashboard > Failed emails pages are merged into the Audit > Email History page.

Email history

Audit > Email History shows information about email events in the system.

On the Email history page you can search for RECEIVED DATE, SCAN VERDICT, STATUS, SENDER, RECIPIENT(S), EMAIL RULE, DIRECTION and SUBJECT (DIRECTION and EMAIL RULE are not displayed in the list).

⚠️ No auto refresh

Due to usability reasons the Email history list is not updated automatically. Click the Refresh icon to update.

ℹ️ N/A values

The SCAN VERDICT value N/A means that MetaDefender Core was not involved in the processing of this entry.
Such cases are:
- Notifications for blocked emails
- Released from quarantine
- Forwarded from quarantine
- Delivered for external quarantining

**Differentiating forked emails**

In some cases there are seemingly duplicate entries in Email history. Such cases are when an email is:
- Released from quarantine,
- Forwarded from quarantine,
- Delivered for external quarantining.

These cases are marked in Email history with the following icons in front of the RECIPIENT(S) value:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Fork case</th>
</tr>
</thead>
<tbody>
<tr>
<td>🔄</td>
<td>Released from quarantine</td>
</tr>
<tr>
<td>🔖</td>
<td>Forwarded from quarantine</td>
</tr>
<tr>
<td>⚠️</td>
<td>Delivered for external quarantining</td>
</tr>
</tbody>
</table>

**Example**

In the example below the quarantined (down) and the released-from-quarantine (over) email can be observed.
Operations

Force retry

If one of your emails entered into a Resending state due to some errors (5.4 Understanding email processing statuses) and you don't want to wait until the next scheduled retry then you have the option to trigger a forced retry. For doing this you should move your mouse over the email and click on the Force retry icon ( ).
View email details

Display details about the email and its processing history.

Clicking an Email history entry displays public details (that do not require authentication on MetaDefender Core) about the scan.
The View scan details link points to the scan details on the MetaDefender Core instance where the actual scanning took place.

⚠ Broken scan details links

The View scan details link utilizes the Core address as specified under Inventory > Server profiles. If Core is specified with an address that is not reachable on the machine where the actual browsing of the Web Management Console happens, then the browser will report error.

Example: Core and Email Gateway Security are installed on the same machine and Core is referenced with the URI http://127.0.0.1:8008 on Email Gateway Security. If Email Gateway Security's Web Management Console is browsed from any other machine, then (most probably) the View scan details link will be broken.

See also 3.7 Server profiles.

⚠ View scan details availability

The View scan details link works with MetaDefender Core version 4.7.0 (or later) only. For MetaDefender Core versions earlier than 4.7.0 the Dashboard is opened.
From MetaDefender Email Gateway Security 4.2.0 you will need a logged in session to the MetaDefender Core to see the scan details.

**Absolute scan details links**

To generate the View scan details links, MetaDefender Email Gateway Security stores the actual Core IP where the current request's files were scanned.

As a result the View scan details links continue to work properly even after a new Core is configured instead the old one (given that the old Core is still available).

**Breaking scan details links**

View scan details links stop working after the referenced Core is uninstalled or migrated to a new address.

**Processing history**

The processing history section of the email details contains information about the processing of the email. The following type of entries are listed:

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>StatusChange</td>
<td>Added when a status change occurs. If the status change was manually initiated, the message contains the name of the user that executed the REST call.</td>
<td>LOCAL/admin changed status from Failed to Pending</td>
</tr>
<tr>
<td>ScanFailed</td>
<td>Added when a scan failure occurs.</td>
<td>Scan failed on url <a href="https://localhost:8008">https://localhost:8008</a> (Reason: Core unavailable)</td>
</tr>
<tr>
<td>SendDetails</td>
<td>Added when sending an email</td>
<td>Sending email to smtp://127.0.0.1:25</td>
</tr>
<tr>
<td>SendSucceeded</td>
<td>Added when sending an email succeeded</td>
<td>SMTP send succeeded to smtp://127.0.0.1:25</td>
</tr>
<tr>
<td>Type</td>
<td>Description</td>
<td>Example</td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
<tr>
<td>SendFailed</td>
<td>Added when a send failure occurs.</td>
<td>SMTP send failed to smtps://localhost:587 (Response: No connection could be made because the target machine actively refused it 127.0.0.1:587)</td>
</tr>
<tr>
<td>ModifyFailed</td>
<td>Added when an email cannot be modified/sanitized (e.g. parsing error).</td>
<td></td>
</tr>
<tr>
<td>ForkEmail</td>
<td>Occurs when an email is forked (e.g. different policy rules apply to different recipients, partial send failure for certain recipients).</td>
<td></td>
</tr>
<tr>
<td>DuplicateEmail</td>
<td>Occurs when email content is duplicated (e.g. original copy is moved to quarantine, quarantined original copy is forwarded).</td>
<td></td>
</tr>
<tr>
<td>ScanVerdict</td>
<td>Added when we receive a scan verdict for a file related to the email.</td>
<td>email/[body].txt: No Threat Detected</td>
</tr>
<tr>
<td>VaultUpload</td>
<td>Added when uploading an attachment to MetaDefender Vault</td>
<td>Attachment 'LargeAttachment' was uploaded to Vault</td>
</tr>
</tbody>
</table>

**Failed emails**

⚠️ **Email history and Failed emails merged**

Starting with MetaDefender Email Gateway Security version 4.7.0, the former Dashboard > Email history and Dashboard > Failed emails pages are merged into the Audit > Email History page.
Failure conditions

To understand in what conditions an email fails permanently, see section *Permanent failure statuses* in 5.4 Understanding email processing statuses.

Operations

⚠️ **Only for failed emails**

The functions in this section are available for failed emails only.

If there are other than failed emails in the selection, then the function will execute for the failed selected entries only. For the rest of the entries, a notification is displayed.

The following operations are available on entries in the Email history:

1. Retry Failed
2. Retry
3. Delete
4. Download

Bulk operations

Operations on all failed items

Retry Failed

This function will call the 198213880 for all (visible and not visible) failed entries in the Email history.

Operations on selected items

Selecting entries

Use the checkbox in front of each row to select entries (or use the checkbox in the header row to select all visible items).
Retry

Retry processing the email from the point where it failed and send it to the original recipient(s). The email is removed from the permanent failures queue.

Delete

Delete the email from the permanent failures queue without trying to reprocess it.

Download

Download the selected original emails from the failed emails to the local hard drive. The format of the downloaded emails is zipped MIME (.eml).

File naming
### Component File name Extension

<table>
<thead>
<tr>
<th>Component</th>
<th>File name</th>
<th>Extension</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive package</td>
<td>EmailSecurity-Failed-&lt;year&gt;-&lt;month&gt;-&lt;day&gt;-&lt;hour&gt;-&lt;minute&gt;-&lt;second&gt;</td>
<td>.zip</td>
</tr>
<tr>
<td>Email file</td>
<td>&lt;subject&gt;_&lt;unique ID&gt;</td>
<td>.eml</td>
</tr>
</tbody>
</table>

### 4.5 Refused emails

- Refused emails
- Conditions of refusal

Refused emails is the list of emails which were refused to be processed on the inbound SMTP interface.

**Refused emails**

The refused emails list can be accessed under **Audit > Refused Emails** in the Web Management Console.

---

⚠️ **Refused emails moved**

Starting with MetaDefender Email Gateway Security version 4.7.0, the former **Dashboard > Refused emails** entry has been moved to **Audit > Refused Emails** menu entry.
### Response sent to client

The RESPONSE SENT TO CLIENT column displays the exact SMTP status code and message that was responded to the client that was attempting to submit the email message.

### Conditions of refusal

An email gets refused if any of the following conditions occur:

<table>
<thead>
<tr>
<th>Condition</th>
<th>RESULT shown in Refused emails</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 There is no rule matching this email</td>
<td>NO RULE</td>
<td>4.2 Security rules</td>
</tr>
<tr>
<td>2 Sender email address is invalid</td>
<td>INVALID SENDER</td>
<td></td>
</tr>
<tr>
<td>3 Recipient email address is invalid</td>
<td>INVALID RECIPIENT</td>
<td></td>
</tr>
</tbody>
</table>
4.6 Specific email headers

- Identification header
  - X-MD-Email-Security-Id

- Scan information headers
  - X-Metadefender-Core-Url
    - Example
  - X-Metadefender-Core-Result
    - Examples
  - X-Metadefender-EmailSecurity-Sanitized
  - X-Metadefender-EmailSecurity-OriginalCopy
  - X-Metadefender-Core-Rule
    - Examples

- External quarantine header
  - X-Metadefender-To-Quarantine

- Sender policy framework lookup header
  - X-Metadefender-Spf-Result

- Custom headers

The following email headers are added once the email is processed by MetaDefender Email Gateway Security. These headers can be used for example for custom rules on mail servers such as spam rules using X-Metadefender-Core-Result.

⚠ In header keys only a specific set of characters are allowed. 153230588 are validated for allowed characters.

In header values only a specific set of characters are allowed. If a forbidden character is provided (for example : (colon, which is the separator between the header key and value)), then the whole value gets encoded.

For details see the Syntax of encoded-words section in RFC 2047.
Identification header

**X-MD-Email-Security-Id**

This header contains the unique identifier of this email within MetaDefender Email Gateway Security.

Scan information headers

**X-Metadefender-Core-Url**

This header contains the MetaDefender Core REST API URL used in scanning operations for this email.

⚠️ This header will contain exactly the same value that is configured for the appropriate server in the applied server profile. For details about server profiles see: [3.7 Server profiles](#).

Example

<table>
<thead>
<tr>
<th>Server profile setting</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CORE URI ADDRESS</strong></td>
</tr>
<tr>
<td><a href="http://172.16.201.28:8008">http://172.16.201.28:8008</a></td>
</tr>
<tr>
<td>File scan</td>
</tr>
</tbody>
</table>

**X-Metadefender-Core-Result**

This header value will contain the MetaDefender Core process result. For Blocked results, the reason is also displayed (separated by a / character).
Examples

<table>
<thead>
<tr>
<th>Header</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>X-Metadefender-Core-Result: Allowed</td>
<td>None of the scan engines found a threat in the email and thus it was treated as clean.</td>
</tr>
<tr>
<td>X-Metadefender-Core-Result: Blocked/Dirty</td>
<td>Some (or all) of the scan engines found threat(s) in the email.</td>
</tr>
</tbody>
</table>

**X-Metadefender-EmailSecurity-Sanitized**

This header is added to all emails indicating whether the email have been sanitized by the Email Gateway Security or not (header value: True or False).

**X-Metadefender-EmailSecurity-OriginalCopy**

This header is added to all original copies of blocked or sanitized emails (header value: True).

**X-Metadefender-Core-Rule**

This header value will contain the name (or the value Automatic) of the MetaDefender Core rule that was configured to be used to scan this email. For details see [3.7 Server profiles](#).

Examples

<table>
<thead>
<tr>
<th>Server profile setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>CORE URI ADDRESS</td>
</tr>
<tr>
<td><a href="http://172.16.201.28:8008">http://172.16.201.28:8008</a></td>
</tr>
</tbody>
</table>
External quarantine header

X-Metadefender-To-Quarantine
If external quarantining is configured then this header is added to every email that is to be quarantined. For details see 3.6.1 Quarantine emails on another mail server.

Sender policy framework lookup header

X-Metadefender-Spf-Result
If performing SPF lookups is enabled then this header is added to every email containing the validation results. For details see the Sender Policy Framework lookup section in 3.4 General settings.

Custom headers
In addition to the above headers, Email Gateway Security can also add custom headers to every email processed. These headers are configured in the security policy.
For details see the Actions and Advanced scan settings sections in 4.2 Security rules.

4.7 Support for password protected attachments

- Problem
- Solution
  - Marking emails with password protected attachments
  - Rescan and provide password
    - For administrators
    - For recipients
  - Specialities
    - Multiple recipients
- Software requirements
- Limitations
  - Supported file types
  - Depth
    - Examples
Problem
Communicating parties apply encryption to maintain confidentiality of their communiquès. Given by the nature of encryption, real - potentially malicious - contents of an encrypted file are hidden from MetaDefender Email Gateway Security, thus encrypted files are blocked by default.

Solution

Marking emails with password protected attachments
Emails with password protected attachments are blocked by default. If Email Gateway Security is set accordingly, then these emails will then put into the quarantine.

Blocked emails, where the blocking reason was that attachments were password protected, are marked with a padlock icon in the RESULT column in the quarantine.

Rescan and provide password
When rescanning an email that has password protected attachments, password for the encrypted items is requested by Email Gateway Security. For details about rescan see the Rescan section in 4.3 Quarantine.

Rescan may be initiated by two parties:
1. Email Gateway Security administrators
2. Recipients of the email

For administrators

Administrators who are authorized to rescan on the Web Management Console, can initiate to rescan any blocked email under Dashboard > Quarantine. In this case administrators need to enter the password for the encrypted attachments.

To initiate a rescan move your mouse over the email which needs to be rescanned and click on the *Rescan* icon ( ).

Clicking on the *Rescan* will display a pop-up window where you can enter passwords for each supported password protected attachments. You have to provide the correct password for each attachment and click the *Rescan Email* button when finished.
If every password were correct and the attachments were not blocked by MetaDefender Core then you will see the *Email rescanned successfully* message and your email will be sent to the original recipients and in the meantime it will be removed from the quarantine.
If one of the passwords was wrong or MetaDefender Core blocked one or more of the attachments you will see a *Failed to rescan email* error message and the email will be kept in quarantine.
For recipients

Recipients of the blocked email may receive a notification (for details see 4.2 Security rules) about the fact that the email was blocked, and a link where rescanning can be initiated.

The link, where rescanning can be initiated, has a limited availability that can be configured under Settings > Global settings. For details see the Notification and report settings section in 3.4 General settings.

⚠️ Rescan link visibility

Please note that if the Public Server Address is not set under Settings > Global settings then the rescan link won't be included in the notification email.

A notification email for the recipients with the public rescan link should look like this:
By clicking on the link the recipient should see a page where she can provide the password for the attachments
If every password were correct and the attachments were not blocked by MetaDefender Core then you will see the *The email has successfully been rescanned* message and your email will be sent to the original recipients and in the meantime it will be removed from the quarantine.
If one of the passwords was wrong or MetaDefender Core blocked one or more of the attachments you will see a *Failed to rescan email* error message and the email will be kept in quarantine.
When opening a rescan link with expired link availability you should see the following error:
When opening the rescan link for an email which have been already rescanned you should see the following error:

<table>
<thead>
<tr>
<th>OPSEWAT.</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender</td>
</tr>
<tr>
<td>Email Security</td>
</tr>
</tbody>
</table>

Specialities

### Multiple recipients

<table>
<thead>
<tr>
<th>Case</th>
<th>Who is to provide the passwords?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recipients are matched by the same rule under Policy &gt; Security rules</td>
<td>Only one of the recipients need to provide the passwords. If the rescan succeeds, then all original recipients will receive the email after the rescan. (This behavior can be overwritten by turning on &quot;SEND UNIQUE RESCAN LINK FOR EVERY RECIPIENT&quot; option in the Security rules.)</td>
</tr>
<tr>
<td>Recipients are matched by different rules under Policy &gt; Security rules</td>
<td>All recipients need to provide the passwords. Only that recipient receives the email after the successful rescan, that provided the correct passwords.</td>
</tr>
</tbody>
</table>
Software requirements

<table>
<thead>
<tr>
<th>File type category to process</th>
<th>MetaDefender Core side engine required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive files</td>
<td>Archive engine</td>
</tr>
</tbody>
</table>

Limitations

Supported file types

MetaDefender Email Gateway Security supports the following file types as password protected attachments

<table>
<thead>
<tr>
<th>Email Gateway Security version</th>
<th>MetaDefender Core version</th>
<th>Supported file type category</th>
<th>Examples</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td></td>
<td>Archive files</td>
<td>.zip, .rar, .7z</td>
<td></td>
</tr>
<tr>
<td>4.6.1</td>
<td>4.14.3 (or newer)</td>
<td>Portable Document Format</td>
<td>.pdf</td>
<td>☢️ Core 4.14.3 required</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Microsoft Office</td>
<td>.docx</td>
<td></td>
</tr>
</tbody>
</table>

Depth

MetaDefender Email Gateway Security supports root elements only as password protected attachments.
Examples

<table>
<thead>
<tr>
<th>Archive structure</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Root level <strong>password protected archive</strong></td>
<td>Supported</td>
</tr>
<tr>
<td>• Embedded text file</td>
<td></td>
</tr>
<tr>
<td>• Embedded archive</td>
<td></td>
</tr>
<tr>
<td>• Root level archive</td>
<td>Not supported</td>
</tr>
<tr>
<td>• Embedded text file</td>
<td></td>
</tr>
<tr>
<td>• Embedded <strong>password protected archive</strong></td>
<td></td>
</tr>
</tbody>
</table>

4.8 Support for signed emails

• **Modification rules for signed emails**
  • Email content was blocked
  • Email content was sanitized
  • Email content was allowed
  • Email was bypassed

• **Adding extra headers to the email**

MetaDefender Email Gateway Security gives you an option to skip the modification of emails which are digitally signed so the signature can remain valid after MetaDefender Email Gateway Security processed the email. This behavior is enabled by default. To disable it per rule please check the Advanced scan settings section in 4.2 Security rules.

If an email was signed/encrypted you will see a key icon (🔍) in the Email History next to the recipients.

**Modification rules for signed emails**

**Email content was blocked**

Due to security reasons if there is a blocked content in a signed email MetaDefender Email Gateway Security will either block the whole email or modify its content depending on what action is selected for the blocked emails in 4.2 Security rules. If the selected action is to delete
blocked contents then the blocked contents will be removed and (if configured) disclaimer will be added to the email. If the selected action is to deliver blocked contents then the contents will be delivered but disclaimer won't be added to the email. When the selected action is to block emails then modifying the email is irrelevant.

**Email content was sanitized**

When a signed email has a content which gets sanitized by MetaDefender Core then MetaDefender Email Gateway Security won't replace the original content with its sanitized counterpart and won't add disclaimer to the email. If a sanitization failure occurs during processing a signed email the email won't get blocked as it normally would.

Any attachment which were blocked and sanitized will be removed regardless of other settings.

**Email content was allowed**

MetaDefender Email Gateway Security won't add disclaimer to the email and the content won't be modified.

**Email was bypassed**

MetaDefender Email Gateway Security won't add disclaimer to the email and the content won't be modified.

**Adding extra headers to the email**

Since adding extra headers to the email won't break the signature you can safely configure security rules to add specific headers to the emails if you would like to do that.

4.9 Integration with MetaDefender Vault

- **About MetaDefender Vault**
- **Example use cases**
  - Accessing false positive attachments
  - Accessing original version of sanitized files
  - Sending larger attachments and saving email storage
- **Prerequisites and limitations**
- **Configuring Security Rules**
  - Upload attachments to
  - Uploaded attachment types
• Upload blocked attachments
• Upload sanitized attachments
• Upload partially sanitized attachments
• Upload original of sanitized attachments
• Upload attachments that failed sanitization
• Upload bypassed attachments
• Upload allowed attachments

• Options
  • Remove uploaded attachments from email
  • Include scan result
  • Upload to user's own vault account

• Example
• Attachment notification

• Browsing email attachments in MetaDefender Vault
• Upload information in Processing history

• Troubleshooting
  • Problems during upload
  • Unexpected host in MetaDefender Vault URLs

**About MetaDefender Vault**

From MetaDefender Vault's documentation: "MetaDefender Vault (previously Metadefender Secure File Transfer) offers a safe process for transferring files to and from secure networks as well as a way to safely store and limit access to files. With the native integration between MetaDefender Vault and Metadefender Core, you can be sure that only files that were not detected as a threat will be accessible by your organization.

By integrating MetaDefender Vault with MetaDefender Email Gateway Security you will be able to investigate blocked files easier, store the original version of sanitized files on a separate storage, save email storage by replacing attachments with URLs and more.

**Inline images**

To maintain a good end user experience MetaDefender Email Gateway Security won't upload/delete inline images when integrated with MetaDefender Vault.
Example use cases

Accessing false positive attachments

Having an attachment removed because of a false positive scan result can harden both the end users and the administrator's everyday life. By enabling MetaDefender Email Gateway Security to upload blocked files to MetaDefender Vault an end-user can try to download the file from Vault later. MetaDefender Vault can rescan files periodically so if a file becomes clean later the user will be able to download it.

You can also give a protection about false negatives. For more information please check MetaDefender Vault's Outbreak Prevention.

Accessing original version of sanitized files

If you have sanitization enabled for emails you may would like to access the original files or have them on a separate storage. You can configure MetaDefender Email Gateway Security to upload original versions of sanitized files and add URLs for accessing them into the modified email.

---
MetaDefender Email Security has removed one or more attachments in this email because it contained potentially malicious embedded objects. For more information on MetaDefender Email Security, please visit https://www.opswat.com/products/metadefender/email-security.

The following attachment(s) are available for download from OPSWAT Vault: FalsePositive: http://187.0.1.8060/file/93fd6de0844f4f7e9885320e5f803f

---
MetaDefender Email Security sanitized this email in order to remove any potentially malicious embedded objects. For more information on MetaDefender Email Security, please visit https://www.opswat.com/products/metadefender/email-security.

The following attachment(s) are available for download from OPSWAT Vault: original.png: http://187.0.1.8060/file/1dc0d9d628f4d0f2666cc5558f0ede0786

original_sanitized_by_OPSWAT_MetaDefender_7069425a19d473891586730cb40e651.png

---
Sending larger attachments and saving email storage

MetaDefender Email Gateway Security can upload your attachments to MetaDefender Vault while removing them from the original email and adding URLs for accessing them. This feature makes possible for end users to send/receive attachments which exceeds the email server's file limit and it can also save precious storage space on your email server.

![Email attachment example]

Prerequisites and limitations

You will need a running and accessible MetaDefender Vault and an API token which can be used for uploading files. Please check this page for more information about API tokens. Authentication requirement for downloading files should be turned off on MetaDefender Vault.

No MetaDefender Vault related action will take place for emails with blocked content if the selected action in the security rule is to block the whole email.

Configuring Security Rules

You can setup MetaDefender Vault for every security rule separately under the "Vault" tab. If you want to upload attachments in a given security rule you should enable "UPLOAD ATTACHMENTS TO VAULT" and configure the following settings.
Upload attachments to

The MetaDefender Vault type server profile must be specified here to which the attachments will be uploaded according to the configuration below.

Uploaded attachment types

You can select which attachments to upload based on their scan verdicts.

Upload blocked attachments

By selecting this option every attachment which was blocked will be uploaded to MetaDefender Vault.

Upload sanitized attachments

By selecting this option every attachment which was sanitized will be uploaded to MetaDefender Vault.
**Upload partially sanitized attachments**

By selecting this option every attachment which was partially sanitized will be uploaded to MetaDefender Vault.

- This requires the 'Distinguish partial archive sanitization result' option checked in the MetaDefender Core rule used to scan content with. See MetaDefender Core > 3.6.2. Workflow template configuration for more information.

**Upload original of sanitized attachments**

By selecting this option every attachment which was an origin for a sanitized one will be uploaded to MetaDefender Vault.

**Upload attachments that failed sanitization**

By selecting this option every attachment where the sanitization failed will be uploaded to MetaDefender Vault.

- If both
  1. UPLOAD ORIGINAL OF SANITIZED ATTACHMENTS and
  2. UPLOAD ATTACHMENTS THAT FAILED SANITIZATION

and the sanitization fails—then the original file will be uploaded only once.

**Upload bypassed attachments**

By selecting this option every attachment that was bypassed by Email Gateway Security will be uploaded to MetaDefender Vault.

**Upload allowed attachments**

By selecting this option every attachment which was allowed will be uploaded to MetaDefender Vault.

- **Allowed vs original of sanitized**
Please note that if an attachment is allowed but gets sanitized then it won't be uploaded if only the "Upload allowed attachments" is selected. If you want to upload these kind of attachments you should have "Upload original of sanitized attachments" enabled.

Options

Remove uploaded attachments from email
By enabling this option every attachment which was successfully uploaded to MetaDefender Vault will be removed from the email. If uploading an attachment fails the removal will be skipped. Blocked files will be removed regardless this setting if the action for blocked contents is to "Delete blocked contents".

Include scan result
By enabling this option, Email Gateway Security will upload the scan results to Vault besides the attachment as metadata. As a result Vault will know the verdict of the scan and can make the file available immediately.

Upload to user's own vault account
Depending whether the email was matched by an inbound or an outbound rule, based on the email addresses, the files will be uploaded to the recipients' (inbound) or senders' (outbound) own Vault accounts (when the account exists on the Vault at all). This feature requires appropriate permissions (impersonation) on Vault.

If no account exist with the recipient email address on the Vault, then the file will be uploaded to the account that is assigned to the API key specified in the MetaDefender Vault type server profile set for the matching rule.

Example
Error rendering macro 'drawio' : null

Attachment notification
You can setup custom notification text for plain text and HTML emails and you can also select the position of the notification (before or after the original content).
Removal of URL list placeholder

You should not remove `%[vault_list]` from the notification texts as it would lead to missing URLs.

Browsing email attachments in MetaDefender Vault

MetaDefender Email Gateway Security will upload attachments to MetaDefender Vault using this folder structure for easier browsing: "MetaDefender Email Gateway Security/<date>/<subject>_<<sender address>>_<<<message id>>/".

For example:

- MetaDefender Email Gateway Security
  - 2018-09-28
    - Test subject_<test1@local>_<12345>
      - Attachment 1
      - Attachment 2
    - Test subject 2_<test1@local>_<No Message Id (456)>
      - Attachment 1
  - 2018-09-27
    - Test_<test1@local>_<555>
      - Attachment 1

No message ID

If an email doesn't have a message id "No Message Id (<random ID>)" will be used instead for unique identification.

Lookin up emails on Vault

Knowing an email's message ID or sender address (you can easily check it in email details) makes it simple to look the email up using the Vault's search functionality.
Upload information in Processing history

You can find information about attachment upload to Vault in the *processing history* of an email. You will see if an attachment was successfully uploaded or if there was some error while uploading it.

**Successful upload:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-09-28</td>
<td>13:31:18</td>
<td>StatusChange</td>
<td>Status changed from Processing to Sending</td>
</tr>
<tr>
<td>2018-09-28</td>
<td>13:31:18</td>
<td>VaultUpload</td>
<td>Attachment 'LargeAttachment' was uploaded to Vault</td>
</tr>
</tbody>
</table>

**Failed upload:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-09-28</td>
<td>13:40:03</td>
<td>StatusChange</td>
<td>Status changed from Processing to Sending</td>
</tr>
<tr>
<td>2018-09-28</td>
<td>13:40:03</td>
<td>VaultUpload</td>
<td>Attachment 'LargeAttachment' could not be uploaded to Vault (Error: The underlying connection was closed: An unexpected error occurred on a send.)</td>
</tr>
</tbody>
</table>

Troubleshooting

**Problems during upload**

If you are getting errors for upload please check the followings:

- Vault URL is correct:
  - You are using the correct format: `http(s)://<host>:<port>/vault_rest`
  - You are using http scheme for Vault without HTTPS and using http scheme for Vault with HTTPS
  - You are using the port for REST API and not the port for UI
- Vault API key is correct
- Vault is accessible from the machine where MetaDefender Email Gateway Security is installed
- If Vault is used with HTTPS enabled then the certificate can be trusted on the machine where MetaDefender Email Gateway Security is installed

**Unexpected host in MetaDefender Vault URLs**

URLs inserted into emails are generated by MetaDefender Vault. If you experience URLs with unexpected host in them then you should configure MetaDefender Vault's host which is used for accessing the UI and link generation. More information can be found [here](#).
4.10 Search

- Filtering columns
  - Tokenization
  - Example
    - List
    - Search results
- Value only search
  - Example
    - List
    - Search results
  - Lists with value only search
- Full text search (FTS)
  - Example
    - List
    - Search results
  - Lists with FTS

Filtering columns

By clicking on the filtering columns icon (▽) a new row will appear below the table header with filters for the given columns.

Using these filters you can search for emails which have to meet multiple criteria e.g. emails where the sender is test1@test.com and the recipient is test4@test.com at the same time. This indicates that there is AND relation between the filters.
Tokenization

When using text filters, like Sender you would expect that writing "te" in the filter would return every rows where the sender starts with or contains "te" however this is not the case. The search is based on tokens so only emails like te@test.com will be returned. If you would like to receive emails like test1@test.com you would have to write "te*" as the filter string.

Example

List

<table>
<thead>
<tr>
<th>ID</th>
<th>SENDER</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><a href="mailto:test1@test.com">test1@test.com</a></td>
</tr>
<tr>
<td>2</td>
<td><a href="mailto:te@test.com">te@test.com</a></td>
</tr>
<tr>
<td>3</td>
<td><a href="mailto:test4@test.com">test4@test.com</a></td>
</tr>
<tr>
<td>4</td>
<td><a href="mailto:another@example.com">another@example.com</a></td>
</tr>
</tbody>
</table>

Search results

<table>
<thead>
<tr>
<th>Search term</th>
<th>Matching rows</th>
</tr>
</thead>
<tbody>
<tr>
<td>te</td>
<td>2</td>
</tr>
<tr>
<td>te*</td>
<td>1,2,3</td>
</tr>
<tr>
<td>test</td>
<td>1,2,3</td>
</tr>
<tr>
<td>example</td>
<td>4</td>
</tr>
</tbody>
</table>

Value only search

By default it is possible to search for a certain value among the values of all columns.
Example

List

<table>
<thead>
<tr>
<th>ID</th>
<th>RESULT</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ALLOWED</td>
<td>BLOCKED</td>
</tr>
<tr>
<td>2</td>
<td>BLOCKED</td>
<td>COMPLETED</td>
</tr>
</tbody>
</table>

Search results

<table>
<thead>
<tr>
<th>Search term</th>
<th>Matching rows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCKED</td>
<td>1, 2</td>
</tr>
</tbody>
</table>

Lists with value only search

The following lists in MetaDefender Email Gateway Security implement value only search:

1. Audit > Config history

Full text search (FTS)

MetaDefender Email Gateway Security implements the SQLite MATCH feature of SQLite FTS3 and FTS4 Extensions (see section 3. Full-text Index Queries). In addition to the capabilities the value only search provides, using the MATCH feature makes it possible to search for certain values in certain fields.

Example

List

<table>
<thead>
<tr>
<th>ID</th>
<th>RESULT</th>
<th>STATUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>ALLOWED</td>
<td>BLOCKED</td>
</tr>
<tr>
<td>2</td>
<td>BLOCKED</td>
<td>COMPLETED</td>
</tr>
<tr>
<td>ID</td>
<td>RESULT</td>
<td>STATUS</td>
</tr>
<tr>
<td>----</td>
<td>-----------------</td>
<td>------------</td>
</tr>
<tr>
<td>3</td>
<td>NOT BLOCKED</td>
<td>COMPLETED</td>
</tr>
<tr>
<td>4</td>
<td>BLOWN</td>
<td>BLOCKED</td>
</tr>
</tbody>
</table>

Search results

<table>
<thead>
<tr>
<th>Search term</th>
<th>Matching rows</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLOCKED</td>
<td>1, 2</td>
</tr>
<tr>
<td>RESULT:BLOCKED</td>
<td>1, 3</td>
</tr>
<tr>
<td>RESULT:^BLOCKED</td>
<td>1</td>
</tr>
<tr>
<td>RESULT:BLO*</td>
<td>1, 3, 4</td>
</tr>
<tr>
<td>RESULT:^BLO*</td>
<td>1, 4</td>
</tr>
</tbody>
</table>

For a more complete reference of possible search terms see https://www.sqlite.org/fts3.html.

Lists with FTS

The following lists in MetaDefender Email Gateway Security implement full text search:

1. Audit > Email History
2. Audit > Refused Emails
3. Quarantine

4.11 Config history

Config history

Audit > Config History shows information about configuration changes made via the Web Management Console.
See actual changes

Configuration differences are shown for each entry inline, if the changes fit the screen. For other cases click the <Click here to see the details> text to display the full view of configuration changes.

No direct config file changes

Changes made directly in the configuration file are not reflected here.

On the Config history page you can search for USER, TYPE, CHANGE TYPE, PARAMETER, OLD VALUE or NEW VALUE. Also you can filter the list by DATE.

No auto refresh

Due to usability reasons the Config history list is not updated automatically. Click the Refresh icon to update.
<table>
<thead>
<tr>
<th>DATE (GMT+2)</th>
<th>USER</th>
<th>TYPE</th>
<th>CHANNEL</th>
<th>PARAMETER</th>
<th>OLD VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2019-05-27</td>
<td>LOCAL/admin</td>
<td>rule</td>
<td>edit</td>
<td>Default rule rule_config</td>
<td></td>
</tr>
<tr>
<td>2019-05-27</td>
<td>LOCAL/admin</td>
<td>settings</td>
<td>update</td>
<td>admin/config/example_server_address</td>
<td><a href="http://localhost:8088">http://localhost:8088</a></td>
</tr>
<tr>
<td>2019-05-27</td>
<td>LOCAL/admin</td>
<td>server profile</td>
<td>modify</td>
<td>uri_list</td>
<td></td>
</tr>
<tr>
<td>2019-05-24</td>
<td>LOCAL/admin</td>
<td>server profile</td>
<td>modify</td>
<td>uri_list</td>
<td></td>
</tr>
<tr>
<td>2019-05-24</td>
<td>LOCAL/admin</td>
<td>rule</td>
<td>edit</td>
<td>Default rule rule_config</td>
<td></td>
</tr>
<tr>
<td>2019-05-24</td>
<td>LOCAL/admin</td>
<td>server profile</td>
<td>create</td>
<td>data</td>
<td></td>
</tr>
<tr>
<td>2019-05-24</td>
<td>LOCAL/admin</td>
<td>server profile</td>
<td>modify</td>
<td>server_preference name</td>
<td>Vault</td>
</tr>
<tr>
<td>2019-05-24</td>
<td>LOCAL/admin</td>
<td>server profile</td>
<td>modify</td>
<td>server_preference type</td>
<td>Vault</td>
</tr>
</tbody>
</table>
5 Troubleshooting MetaDefender Email Gateway Security

- 5.1 How to create support package
- 5.2 How to read the MetaDefender Email Gateway Security log
- 5.3 Inaccessible Web Management Console
- 5.4 Understanding email processing statuses
- 5.5 Whitelisting recipients of encrypted files
- 5.6 Proof-of-concept scenarios
- 5.7 Can't view scan details
- 5.8 Understanding information in block notification emails

5.1 How to create support package

A support package contains essential information regarding the operating system and OPSWAT software found on the machine.

Security and privacy concerns

The contents of the generated package may contain sensitive information that may require special handling.

To create a package you must start the script found under the installation directory of the product, by default this is `C:\Program Files\OPSWAT\Metadefender Email Security\mdemailsecurity-collect-support-data.bat`.

The batch file must be executed with Administrator privileges. Start a command prompt as Administrator, change to the installation directory and run the batch file:

```
> cd C:\Program Files\OPSWAT\Metadefender Email Security
> mdemailsecurity-collect-support-data.bat
```
Running the batch file directly from File Explorer –even with Administrator privileges (Run as Administrator)– may give unexpected results.

As the script processes the necessary information, the script generates the support package output.

The package files is a zip archive with the following name:

```
mdemailsecurity-<VERSION>-support-<TIMESTAMP>.zip
```

Where the timestamp is the date when the package was generated.

Example:

```
mdemailsecurity-4.1.2-support-1439983514.zip
```

The generated package will be placed in the same location as the script that was called.

**Content of the created package**

The support package contains the following elements:

<table>
<thead>
<tr>
<th>Relative path</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>directory</td>
<td>The configuration files of OPSWAT software found on the machine</td>
</tr>
<tr>
<td>config/config.config copy</td>
<td>file (binary)</td>
<td>Config database without user data</td>
</tr>
<tr>
<td>log</td>
<td>directory</td>
<td>The log files of OPSWAT software found on the machine</td>
</tr>
<tr>
<td>os.info</td>
<td>file (text)</td>
<td>Operating system information</td>
</tr>
<tr>
<td>hw.info</td>
<td>file (text)</td>
<td>Hardware information</td>
</tr>
<tr>
<td>network.info</td>
<td>file (text)</td>
<td>Network information</td>
</tr>
<tr>
<td>files.info</td>
<td>file (text)</td>
<td>OPSWAT software directory information</td>
</tr>
</tbody>
</table>
You are recommended to check the contents of the generated package to make sure it does not contain any confidential information.

5.2 How to read the MetaDefender Email Gateway Security log

On Windows systems logging is done via Event Log.

MetaDefender Email Gateway Security logs can be found under Windows Logs / Application and are labelled with MetaDefender Email or with MetaDefender Email Security source.

5.3 Inaccessible Web Management Console

Connection refused or browser is waiting

The Web Management Console can not be accessed from browser. You get an error message (connection refused) or your browser is waiting for reply.

Solution

1. Please make sure your computer can access the MetaDefender Email Gateway Security IP address.
2. Please make sure you entered the correct URL into your browser.
3. Please make sure you opened the firewall port on the MetaDefender Email Gateway Security server for the Web Management Console. Consult your Linux Distribution manual on how to configure a firewall in your distribution.

5.4 Understanding email processing statuses

- Workflow statuses
  - Pending
  - Processing
  - Sending
  - Completed
  - Sent
• Blocked
• Temporary failure statuses
  • Reprocessing
    • Possible causes
  • Resending
    • Possible causes
• Permanent failure statuses
  • Failed
    • Possible actions
  • Forbidden
    • Possible actions
• Other statuses
  • Quarantined
    • Possible actions
  • Deleted

Below is a legend explaining the various email processing statuses.

Workflow statuses
Emails with statuses listed below are progressing through the MetaDefender Email Gateway Security workflow.

Pending
Email is queued waiting to be processed.

Processing
Email is currently being processed.

Sending
Email has been processed and is being delivered to the SMTP relay server.

Completed

This status is deprecated since 4.4.0. It was replaced by Sent and Blocked
Email has been successfully processed and sent forward or blocked.

**Sent**
Email has been successfully processed and forwarded.

**Blocked**
Email has been blocked.

**Temporary failure statuses**
Emails with statuses listed below are in automatic retry sequence.

**Reprocessing**
MetaDefender Email Gateway Security has failed to process the email and it is currently pending a retry.

**Possible causes**
- MetaDefender Core server down/not responding
- Archive engine is not active on MetaDefender Core
Enable archive handling is not enabled for the rules on MetaDefender Core (that are defined in the Core server policies that are in use by the rules on MetaDefender Email Gateway Security)
Resending

MetaDefender Email Gateway Security has failed to forward the email to the SMTP relay server and is currently pending retry.

Possible causes

- SMTP relay server down/not responding
• SMTP relay server rejects the email

Permanent failure statuses
Emails with statuses listed below require user interaction, since retry sequence is exhausted.

Failed
Email has exceeded the retry count and cannot be processed/delivered.

Possible causes
• Exhausted 149343374 lead to this permanent failure status.

Possible actions
• Manually retry/delete email from the MetaDefender Email Gateway Security web interface.

Forbidden
No policy rule is found matching the email and requires manual delivery.

Possible actions
• Manually retry/delete email from the MetaDefender Email Gateway Security web interface.

Other statuses

Quarantined
Email is located in quarantine.

Possible actions
• Manually deliver/delete/forward email from the MetaDefender Email Gateway Security web interface.

Deleted
Emails with this status has been manually deleted by a user.
5.5 Whitelisting recipients of encrypted files

⚠️ Page is obsolete

MetaDefender Email Gateway Security has out-of-the-box support for password protected attachments. For details see 4.7 Support for password protected attachments.

As a consequence, this page is obsolete and may be removed in the future.

With default settings MetaDefender Email Gateway Security (and the underlying MetaDefender Core) may block emails with encrypted contents.

ℹ️ The reason for this is that given by the nature of encryption it is not possible to tell whether an encrypted file is infected or not, whether it needs sanitization or not.

To allow encrypted files through MetaDefender Email Gateway Security for authorized recipients, follow these steps:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Sub-step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Create a new rule in MetaDefender Core under Policy > Security rules | A | 1. Limit to specified user agents: mdemaiisecurity  
2. Visibility of scan result  
   a. Role: Everybody  
   b. Visibility: FULL DETAILS  
3. Restrict access to following roles: Everybody |
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Sub-step</th>
<th>Description</th>
<th>Screenshots</th>
</tr>
</thead>
</table>

**Screenshots**

- **OPSWAT MetaDefender Core**
  - Dashboard
  - Process
  - **Policy**
    - Security zones
    - Analysis workflows
    - Security rules
  - Inventory
  - Settings

---

4.9.1
License Expiration
12/31/2028
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Sub-step</th>
<th>Description</th>
<th>Screenshots</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>B</td>
<td><img src="image.png" alt="Screen Shot" /></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1. ADVANCED tab</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. OVERRIDE SCAN RESULTS CLASSIFIED AS ALLOWED: enable</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>a. Encrypted archive: enable</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Sub-step</td>
<td>Description</td>
<td>Screenshots</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
<tr>
<td>2</td>
<td>Create a new Core server profile in MetaDefender Email Gateway Security under Inventory &gt; Server profiles</td>
<td>A</td>
<td>1. RULE: select the rule you created in the previous step</td>
<td>![Screenshot of MetaDefender Core interface]</td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Sub-step</td>
<td>Description</td>
<td>Screenshots</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>----------</td>
<td>-------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| 3    | Create a new rule in MetaDefender Email Gateway Security under Policy > Security rules | A | 1. DIRECTION: INBOUND  
2. RECIPIENT DOMAIN OR ADDRESS: list recipient addresses here who are granted to receive encrypted contents | ![Screenshots](image-url) |
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Sub-step</th>
<th>Description</th>
<th>Screenshots</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>1. SCAN tab</td>
<td></td>
<td></td>
<td><img src="image.png" alt="Screen Shot" /></td>
</tr>
<tr>
<td></td>
<td>a. ALLOW SCAN: enable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>b. METADEFENDER CORE: select the profile you created in the previous step</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Sub-step</td>
<td>Description</td>
<td>Screenshots</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>----------</td>
<td>-------------</td>
<td>------------</td>
</tr>
<tr>
<td>C</td>
<td>1. ACTIONS tab</td>
<td></td>
<td>a. HANDLING OF THE EMAIL: DELIVER BLOCKED CONTENTS</td>
<td><img src="image" alt="Screenshots" /></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Sub-step</td>
<td>Description</td>
<td>Screenshots</td>
</tr>
<tr>
<td>------</td>
<td>--------------------------------------------------</td>
<td>----------</td>
<td>--------------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>4</td>
<td>Put the new rule in MetaDefender Email Gateway</td>
<td></td>
<td>Security into the appropriate order</td>
<td>![Screenshots]</td>
</tr>
</tbody>
</table>

4.7.4
5.6 Proof-of-concept scenarios

- 5.6.1 Stand-alone PoC environment
- 5.6.2 High availability

5.6.1 Stand-alone PoC environment

- Design
  - Components
• Traffic flow
• Domains
• Direction
  • Inbound
  • Outbound
• Prerequisites
  • Host
  • Web client
  • Email client
  • Mail server
  • MetaDefender Core and MetaDefender Email Gateway Security
• Setup
  • MetaDefender Core
  • hMailServer
    • Installation
    • Configuration
  • MetaDefender Email Gateway Security
    • Installation and configuration
    • Security rules
      • Inbound
      • Outbound
      • Email traffic redirection
  • Email client
• Sending emails programatically
  • Bulk emails
  • Infected email

Design

Components

Error rendering macro 'drawio' : null
Traffic flow
Error rendering macro 'drawio' : null

Domains
We will have two domains in the examples below:

1. the domain local as the organization internal domain, for inbound email traffic and
2. the domain other as the external domain, for outbound email traffic.

Direction

Inbound
Error rendering macro 'drawio' : null

Outbound
Error rendering macro 'drawio' : null

Prerequisites

Host
Any of the components above may be deployed to different, or to the same host.
In the examples of this page all components will be deployed to the same host, thus localhost or 127.0.0.1 will be used as host address.

Web client
Any web client that is supported by MetaDefender Core and MetaDefender Email Gateway Security can be used.
We assume that the web client is pre-installed on the host.

Email client
In the examples of this page Microsoft Mail will be used
We assume that the email client is pre-installed on the host.
Mail server
In the examples of this page hMailServer will be used (https://www.hmailserver.com/).

MetaDefender Core and MetaDefender Email Gateway Security
The latest available version will be used.

Setup

MetaDefender Core
Install MetaDefender Core following the instructions in 1. Quick Start with MetaDefender Core.

hMailServer

Installation

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1. Download hMailServer from <a href="https://www.hmailserver.com/download">https://www.hmailserver.com/download</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. Verify the integrity of the downloaded package</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Launch the installer</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>3</td>
<td>Accept the License Agreement</td>
<td><img src="image" alt="License Agreement" /></td>
</tr>
</tbody>
</table>

**Welcome to the hMailServer Setup Wizard**

This will install hMailServer 5.6.6-82383 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

**License Agreement**

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

**hMailServer License Terms**

**Preamble**

This is a legal agreement between you and the author of this software, Martin Knafve. By installing this software, hMailServer, you agree to be bound by the terms of this agreement to the maximum extent permitted by law.

- [ ] I accept the agreement
- [ ] I do not accept the agreement
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Select destination directory</td>
<td><img src="image1.png" alt="Screenshot" /></td>
</tr>
<tr>
<td>5</td>
<td>Select components. Do select both Server and Administrative tools</td>
<td><img src="image2.png" alt="Screenshot" /></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>6</td>
<td>Select database type (default)</td>
<td><img src="image1.png" alt="Screenshot" /></td>
</tr>
<tr>
<td>7</td>
<td>Specify Start Menu folder</td>
<td><img src="image2.png" alt="Screenshot" /></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>8</td>
<td>Create <em>Administrator</em> account</td>
<td><img src="image1" alt="Screenshot" /></td>
</tr>
<tr>
<td>9</td>
<td>Finalize installation</td>
<td><img src="image2" alt="Screenshot" /></td>
</tr>
</tbody>
</table>
## Configuration

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
</table>
| 1    | Start *hMailServer Administrator*  
Select the *Administrator* account and click *Connect* | ![Screenshot of Connect](image1)
<p>| 2    | Click <em>Add domain</em> and start adding our two domains <em>local</em> and <em>other</em> according to the 149495854 | <img src="image2" alt="Screenshot of Add domain" /> |</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>In each of <em>local</em> and <em>other</em> domains create one-one account for email sending and receiving <em>one</em> and <em>two</em> respectively:</td>
<td><img src="image" alt="Screenshot" /></td>
</tr>
<tr>
<td></td>
<td>1. Select <em>Domains / local / Accounts</em> in the left tree view and click <em>Add</em>...</td>
<td></td>
</tr>
<tr>
<td></td>
<td>a. Create account for <em>one</em> according to the screenshot.</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Remember to specify a password.</td>
<td></td>
</tr>
</tbody>
</table>
| 2.   | Select **Domains / other / Accounts** in the left tree view and click **Add...**  
  a. Create account for two according to the screenshot. Remember to specify a password. |
MetaDefender Email Gateway Security

Installation and configuration

Install and configure MetaDefender Email Gateway Security following the instructions in Quick start with MetaDefender Email Gateway Security.

Security rules

Modify the rules created in the previous section according to the following.

Inbound

<table>
<thead>
<tr>
<th>Field</th>
<th>Direction</th>
<th>Sender IP</th>
<th>Recipient domain or address</th>
<th>Server IP/Domain</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>INBOUND</td>
<td>blank</td>
<td>.+@local</td>
<td>127.0.0.1</td>
<td>25</td>
</tr>
</tbody>
</table>

Outbound

<table>
<thead>
<tr>
<th>Field</th>
<th>Direction</th>
<th>Sender IP</th>
<th>Recipient domain or address</th>
<th>Server IP/Domain</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>OUTBOUND</td>
<td>blank</td>
<td>.+@.+ (or optionally .+@other)</td>
<td>127.0.0.1</td>
<td>25</td>
</tr>
</tbody>
</table>

Email traffic redirection

Skip 1.6 Email traffic redirection as the appropriate settings will be configured with the email client.

Email client

The same email client will be the source and the final destination of emails. As a consequence it will receive emails from hMailServer and send emails towards MetaDefender Email Gateway Security.

Configure the two accounts one and two in Microsoft mail:
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Click Accounts / Add account</td>
<td><img src="image1.png" alt="Screenshot" /></td>
</tr>
<tr>
<td>2</td>
<td>Select Advanced setup</td>
<td><img src="image2.png" alt="Screenshot" /></td>
</tr>
</tbody>
</table>

**Manage Accounts**

- Select an account to edit:
- Link inboxes
- Add account
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Choose an account</strong></td>
<td><img src="logo_exchange.png" alt="Exchange" /> Exchange, Office 365 <img src="logo_google.png" alt="Google" /> Google <img src="logo_yahoo.png" alt="Yahoo" /> Yahoo <img src="logo_icloud.png" alt="iCloud" /> iCloud <img src="logo_other_account.png" alt="Other account" /> POP, IMAP <img src="logo_advanced_setup.png" alt="Advanced setup" /> Advanced setup</td>
</tr>
</tbody>
</table>

3. Select *Internet email*
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Advanced setup</strong>&lt;br&gt;Choose the kind of account you want to setup. If you’re not sure, check with your service provider.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Exchange ActiveSync</strong>&lt;br&gt;Includes Exchange and other accounts that use Exchange ActiveSync.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Internet email</strong>&lt;br&gt;POP or IMAP accounts that let you view your email in a web browser.</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Configure the account <em>one</em></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>5</td>
<td>Repeat the previous step for the account two</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>6</td>
<td>Send a test email</td>
<td><img src="image" alt="Screenshot" /></td>
</tr>
</tbody>
</table>

**Internet email account**

**Email address**

two@other

**User name**

two@other

Examples: kevinc, kevinc@contoso.com, domain/kevinc

**Password**

***

**Account name**

two@other

**Send your messages using this name**

two@other

**Incoming email server**

127.0.0.1:1143

**Account type**

IMAP4

**Outgoing (SMTP) email server**

127.0.0.1:10025

- [ ] Outgoing server requires authentication
- [x] Use the same user name and password for sending email
- [ ] Require SSL for incoming email
- [ ] Require SSL for outgoing email

[Cancel] [Sign in]
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Check if the email pops up in MetaDefender Email Gateway Security</td>
<td>![Email Screenshot]</td>
</tr>
</tbody>
</table>

From: two@other
To: one@local

test
test|

Sent from Mail for Windows 10
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Check if the email arrives to the recipient</td>
<td><img src="image" alt="Email History Screenshot" /></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td></td>
<td><img src="image" alt="Screenshot" /></td>
</tr>
</tbody>
</table>

- New mail
- Accounts
  - one@local
  - one@local
- two@other
  - two@other
- Folders
- Inbox
- Drafts
- Sent Items
- More
- Search

Inbox
- test
- test: Sent from Mail for Windows 10 scanned
Sending emails programatically

Bulk emails

The following Perl example sends 100 outbound emails using the example settings above.

```perl
use strict;
use warnings;

use Email::Sender::Simple qw(sendmail);
use Email::Sender::Transport::SMTP;
use Email::Simple;
use Email::Simple::Creator;

my $smtpserver = '127.0.0.1';
my $smtpport = 10025;

my $transport = Email::Sender::Transport::SMTP->new(
    {  
        Host => $smtpserver,
        Port => $smtpport,
    }  
);
```
host => $smtpserver,
    port => $smtpport,
);)

my $email = Email::Simple->create(
    header => [
        To      => 'one@local',
        From    => 'two@other',
        Subject => 'bulk email',
    ],
    body => 'This is the message',
);

for ( my $i = 0 ; $i < 100 ; $i++ ) {
    sendmail( $email, { transport => $transport } );
    sleep(int(rand(60)));
}

Infected email
The previous Perl example can be modified to be potentially identified by some of the scan engines as Eicar infected.

The Eicar test string is not copied into this document as text to avoid being identified as threat. Here only images are used instead.

Most probably the resulted Perl program can be saved in the filesystem with no problem.

The email sent by the program will, however, be blocked by some of the engines in MetaDefender Core.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Screenshot</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Go to <a href="https://2016.eicar.org/86-0-Intended-use.html">https://2016.eicar.org/86-0-Intended-use.html</a></td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Screenshot</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
<td>-----------</td>
</tr>
<tr>
<td>2</td>
<td>Copy the Eicar test string</td>
<td><img src="image" alt="Eicar Test String" /></td>
</tr>
<tr>
<td>3</td>
<td>Append the Eicar test string to the end of the body text in the previous example</td>
<td><code>body =&gt; 'This is the message: X50!P%@AP[4\PZX54(P^)7CC7]\$ICAR-STANDARD-ANTIVIRUS-TI</code></td>
</tr>
</tbody>
</table>

5.6.2 High availability

**LB/HA Core servers**

LB/HA of Core servers is supported out of the box. For details see 3.7 Server profiles.

**LB/HA MetaDefender Email Gateway Security servers**

In this scenario a load balancer (Load balancer A in the figure above) will be set up to balance the email traffic between two MetaDefender Email Gateway Security instances.

**Load balancer**

The following software will be used on Load balancer A:

1. Operating system: CentOS 7 (minimal)
2. Load balancer: NginX

**Prerequisites**

Install NginX
# yum install epel-release
# yum install nginx

**Disable SELinux**

For the sake of POC and simplicity SELinux will be disabled here.

⚠️ In a production environment SELinux must not be disabled.

```bash
# vi /etc/sysconfig/selinux
...  
SELINUX=disabled  
...  
```

The system must be restarted this configuration to make effect.

**NginX configuration**

NginX will be configured making changes in its configuration file.

```bash
# vi /etc/nginx/nginx.conf
```

**Failover setup**

With the configuration below two MetaDefender Email Gateway Security instances are configured in a failover fashion. The second server receives traffic only when the first server is unreachable (consecutively for three seconds for three times).

```bash
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

# Load dynamic modules. See /usr/share/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;

events {
   worker_connections 1024;
}
```
Load balancing setup

With the configuration below two MetaDefender Email Gateway Security instances are configured in a load balancing fashion. The first server receives five times much traffic than the second server.

```
stream{
    upstream cluster_mdemailsecurity_smtp {
        server mdemailsecurity1.example.com:10025
        max_fails=3 fail_timeout=3s;
        server mdemailsecurity2.example.com:10025 backup;
    }
    server {
        listen 10025;
        proxy_pass cluster_mdemailsecurity_smtp;
    }
}
```

Load balancing

user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

# Load dynamic modules. See /usr/share/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

stream{
    upstream cluster_mdemailsecurity_smtp {
        server mdemailsecurity1.example.com:10025
        weight=1;
        server mdemailsecurity2.example.com:10025
        weight=4;
    }
    server {
        listen 10025;
        proxy_pass cluster_mdemailsecurity_smtp;
    }
}

4.7.4
The backend name (cluster_mdemailsecurity_smtp) can be replaced with a name of any choice.

All backend servers are defined by their internal DNS hostnames in the examples above, but IP addresses may be used instead.

**Backup servers**

Directive `backup`.

The backup server will only handle traffic when the other node goes down, and will remain idle when the other node is healthy.

**Passive health check**

Directives:

- `max_fails`
- `fail_timeout`

Define the conditions when the switchover must happen.

https://www.nginx.com/resources/admin-guide/http-health-check/

**Weight values**

Directive `weight`.

The lower the value, the more traffic the server will receive relative to the other servers. `mdemailsecurity2` will be assigned a higher weight of 4 to minimize its load. It will receive every 5th (1+4) connection.

---

**Marking a Server as down (offline)**

When there is a need to bring one of the servers down for emergency maintenance without impacting the users, the `down` directive will allow doing this:

```plaintext
upstream cluster_mdemailsecurity_smtp {
    server mdemailsecurity1.example.com:10025 max_fails=3 fail_timeout=3s down;
    server mdemailsecurity2.example.com:10025 backup;
    check interval=5000 rise=2 fall=5 timeout=2000 type=smtp;
}
```
5.7 Can't view scan details

The View scan details link on Audit > Email history / Email details or Quarantine > Email details points to the scan details on the MetaDefender Core instance where the actual scanning took place.

For further details see 4.4 Email history or 4.3 Quarantine.

Symptoms

Core Dashboard instead of scan details

The View scan details link leads to the Dashboard on the referenced Core instead of the scan details.

Reason

The View scan details link works with MetaDefender Core version 4.7.0 (or later) only.

Connection refused or browser is waiting

The Web Management Console can not be accessed from the browser. You get an error message (connection refused) or your browser is waiting for reply.

Reason

View scan details links stop working after the referenced Core is uninstalled or migrated to a new address.

Page not found

The browser displays a page not found error, however everything seems to be configured properly.
**Reason**

*View scan details* links use the IP addresses configured at the Core inventory. If these IP addresses are not accessible from the machine where the actual browsing happens, then the details page can not be displayed.

**Core login page instead of scan details**

The *View scan details* link leads to the login page on the referenced Core instead of the scan details.

**Reason**

MetaDefender Email Gateway Security starting with version 4.2.0 uses batch scanning. Viewing the details of a batch scan needs authentication on the Core side. After logging into the Core and opening the *View scan details* link again the details should be visible.

**5.8 Understanding information in block notification emails**

**Block notification email**

When your *Security rules* are set to block emails and notify the recipients when an issue occurs a notification email like this one below will be sent:
Below you can find an explanation of the information found in the notification.

**Date**

This is the value of the "Date" header in the original email. This date represents when the email was originally sent in UTC timezone.

The date in the notification email is not the same as the date in the email history. The date in the email history is the date Email Gateway Security received or modified the email.
**Message id**

Message id is a unique id for every email generated by email clients or mail servers. Some email clients can omit generating a message id so if the original email does not have it then "N/A" will be displayed. This id can be used to easily track down the email in different parts of it's flow. You can also use this id in the search fields in the Web Management Console to locate emails.

> If an email without a valid message-id is quarantined Email Gateway Security will automatically generate a unique message-id for the email.

**Sender**

The value of the sender email address specified in the MAIL FROM command sent by the remote MTA. It is used to identify who submitted the message. This is usually the same as the From header (which is who the message is from) but it can differ in some cases where a mail agent is sending messages on behalf of someone else.

**From**

The value of the original email's "From" header. This identifies who the message is from.

**To**

The value of the original email's "To" header.

**CC**

The value of the original email's "CC" header.

**Subject**

The subject of the original email (value of the "Subject" header).

**Result**

Result will show the main reason about why the email was blocked. This is often the scan result from the MetaDefender Core but it can be anything else, like a failed sanitization.
**Scan result**

Scan result contains a link for viewing the public scan details on the given MetaDefender Core where the scan took place.
## 6 Release Notes

<table>
<thead>
<tr>
<th>4.7.4 MetaDefender Email Gateway Security release</th>
<th>MetaDefender Email Gateway Security 4.7.4 is a maintenance release focusing on minor improvements and fixes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 22, 2019</td>
<td></td>
</tr>
</tbody>
</table>

## New & Improved

<table>
<thead>
<tr>
<th>Notification on encrypted attachments only</th>
<th>Email Gateway Security now has the option to send a notification email only in case when an email was blocked due to encrypted attachment (and not for every blocked email). To configure Email Gateway Security to send notifications for blocked emails with password protected attachments only, go to your rule under Security Rules and set the value of SEND NOTIFICATION FOR to ONLY EMAILS WITH PASSWORD PROTECTED ATTACHMENTS.</th>
</tr>
</thead>
</table>
For further details see 4.2 Security rules.

Due to some lack of optimization in the database, the user interface was irresponsive or slow in certain cases and under heavy load.
### Data retention did not clean up properly

The configuration under **Settings > Data Retention** was not correctly applied.

### HTTPS could not be specified for Vault

HTTPS scheme couldn't have been specified for MetaDefender Vault type `se URI ADDRESS`.

### Previous releases

<table>
<thead>
<tr>
<th>Feature</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7.0</td>
<td>4.7.1</td>
</tr>
<tr>
<td>4.6.0</td>
<td>4.6.1</td>
</tr>
<tr>
<td>4.5.0</td>
<td>4.5.1</td>
</tr>
<tr>
<td>4.4.0</td>
<td>4.4.1</td>
</tr>
</tbody>
</table>

### 6.1 Changelog

- Version 4.7.4
- Version 4.7.3
- Version 4.7.1
- Version 4.7.0
- Version 4.6.2
- Version 4.6.1
- Version 4.6.0
- Version 4.5.3
- Version 4.5.2
- Version 4.5.1
Version 4.7.4

New & Improved:

- Notification on encrypted attachments only

Fixed issues:

- Response was slow on the user interface
- Data retention did not clean up properly
- HTTPS could not be specified for Vault

Version 4.7.3

New & Improved:

- Expiration date / time in rescan notifications
- Added sender address to file name on Vault
- All files are created in the installation directory

Fixed issues:

- Empty email bodies caused Deep CDR errors
- Could not change Settings > Global Settings
Version 4.7.1

New & Improved:

- SMTP server component of Email Security now listens on IPv6 when it is available
- Email Security now has an option to send alert emails when emails get bypassed
- Emails get bypassed when there is no license to ensure email business continuity
- The default disclaimer for messages with encrypted contents have been updated

Fixed issues:

- Product schema is invalid error when adding ICAP Server to Central Management
- Rescan pages of password protected attachments sometimes took very long to load
- Certain emails got refused by the SMTP component without an apparent reason

Version 4.7.0

New & Improved:

- New, simplified navigation structure
- Improved dashboard look and feel
- Display statistics on the dashboard
- Support partial archive sanitization

Fixed issues:

- "Illegal characters in path" errors

Version 4.6.2

New & Improved:

- Upload attachments to recipients' Vault folders
- Upload failed-to-sanitize attachments to Vault
- Send alert emails when Vault is unresponsive
- Option to enable scanning email headers
- Support for new AMP HTML body MIME type
- Enhanced log correlation with logs from Core
- Vault configuration moved to server profiles

Fixed issues:

- Wrong time format in email headers
Sanitized twice when integrated with Vault

**Version 4.6.1**

New & Improved:

- Support for *Data Loss Prevention* results
- Support for password protected documents
- Provide details about sanitization failures
- Notify sender on blocked outbound emails
- Cleanup functionality for *Failed Emails*
- *Scan start* entry in processing histories

Fixed issues:

- Syslog syntax error in case of CEF logs
- Wrong code reported for refused emails
- *Contact sharing invitations were corrupted*
- Allowed items appeared in quarantine reports

**Version 4.6.0**

New & Improved:

- Multiple deployment modes for evaluation scenarios
- Email alerts for improved monitoring capabilities
- Improved Dashboard
- Disclaimer styles to increase end-user awareness

Fixed issues:

- Fixed syslog issue (TCP protocol)
- Improved HTML sanitization support for international character sets
- Improved password protected archive support

**Version 4.5.3**

Fixed issues:

- SMTP server protocol now fully supports TLS 1.2
- MetaDefender Core communication protocol now fully supports TLS 1.2
- SMTP server 4.x & 5.x messages now describes reason for rejection
Version 4.5.2
Fixed issues:
  • URL encoding of long subjects which included 3 or 4 bytes UTF-8 characters could fail
  • Fixed a memory leak

Version 4.5.1
Fixed issues:
  • MetaDefender Email Security did not add 'Received' header for emails
  • Improved interprocess communication to prevent random reading failures
  • Inbound SMTP port is now monitored

Version 4.5.0
New & improved features:
  • Integration possibility with MetaDefender Vault
  • Option to not list sanitized emails in quarantine reports
  • Option to use local timezone in remote syslog
  • Improved readability of the Action tab in Security Rules
Fixed issues:
  • A batch was opened and closed without file to scan
  • Domain based filtering was not working without regex
  • Typo and renaming

Version 4.4.1
Fixed issues:
  • Rescan link was missing from encrypted archive disclaimers when there was an infected
    attachment next to the encrypted archive
  • Zero byte emails resulted in warnings and failed emails, they are now refused

Version 4.4.0
Important features:
  • Support for S/MIME and PGP signed emails
  • Security rules can be filtered based on sender domain or address
Recipients of notification emails can be customized in security rules.

Added a new disclaimer for encrypted archives which contains the rescan link.

Added additional pages to wizard for easier setup of the product.

Added a more advanced filtering to the history pages next to the basic search.

Enhancement and new features:

- Sanitization information is now available in email details.
- Position of disclaimers can be selected in security rules.
- Introduced disclaimer variables.
- Server's local timezone can be used instead of UTC in notification emails and disclaimers.
- Improved quarantine report look when there were no new entries in the quarantine since the last report.
- Replaced Completed status with Sent and Blocked.
- Improved the amount of information logged.
- Welcome wizard now allows creating user with the name "admin".

Fixed issues:

- Header only emails could not be parsed without closing CRLF.
- Charset is parsed from HTML content if headers don't contain information about the used charset.
- There could be orphan emailrelay instances after an unexpected product crash.
- Failed emails were displayed in the Email history too. They are now displayed only in the Failed Emails page.
- Could not start the product when exchange_exclude_probe_emails registry key was present.
- Attachments were always regarded as inline when Content-ID was present.
- Security rules could disappear after service restart if a server profile was deleted which was used in an already deleted security rule.

Version 4.3.3

Fixed issues:

- User guide was missing.
- Emails with "Deleted" status were not removed during automatic cleanup.
- Crash could occur during login.
Version 4.3.2

Fixed issues:

- Emails could have a large delay due to slow queries within a larger database
- Fixed a typo in Security Rules → Advanced (Override Default Behavior had an extra "Test" string at the end)
- Fixed crash possibility which could occur if C# terminated unexpectedly while processing an email

Version 4.3.1

Enhancement and new features:

- Block notification emails now show results per attachment

Fixed issues:

- Emails with unexpected message id format could fail
- Certificate based client authentication was always checked when an SMTP profile had an address with smtps scheme
- Block notification emails could missing sanitization failure information
- Fixed crash possibility

Version 4.3.0

Important features:

- Introduced welcome wizard
- Added an option to Security rules → Actions for sending a unique re-scan link for every recipient when receiving password protected archives
- Added an option to Security rules → Advanced for sanitization behavior override: it is now possible to send the original file if the sanitization failed, or to send the sanitized file if the original file was blocked
- Message ids are now searchable and displayed in email details and in the block notifications

Enhancement and new features:

- Added support for Layer 7 load balanced Core
- Inbound TLS support now uses Window’s Secure Channel: SSL/TLS versions, ciphers etc. can be configured via system configuration
- Replaced our SMTP receiver component
• Introduced a **throttling** mechanism

• Updated the **block notification email**: it now contains the message id, and the original Sender which may differ from the value of the "From" header. Also clarified links for MetaDefender Cloud.

**Fixed issues:**

• Fixed a **search** issue which caused the display of irrelevant emails and displaying "Invalid email job status" error upon viewing their details

• Inline images without a Content-Disposition header could be displayed as an attachment after sanitization

• The information "error during sanitization" was always false in the logs

**Version 4.2.1**

**Important features:**

• Added a **download option** for failed emails

**Enhancement and new features:**

• Added a link pointing to the Web Management Console in Quarantine Reports when a Public Server Address is available

• Enhanced logging of actions in **Failed emails**. This includes logging of deletion, downloading, forwarding, releasing and retrying of emails

• Enhanced SMTP error logging to now contain the **SMTP response code and error message**.

• Added logging of scan verdicts for every attachment in the Email details

• Added size of the email to email details

• Made several clarifications in the UI

**Fixed issues:**

• Fixed a query which displayed emails in Dashboard → Failed emails incorrectly

• Emails with a subject longer than 65519 characters were failing

• Parsing emails were failing if "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing" security setting was enabled on the system

• Removed "OVERRIDE SMTP RESULTS" from Security rules → Advanced when running in Exchange mode

• User agent specific to Email Security was sent in a wrong header which caused scans to fail when the used Core rule was limited to a specific user agent
• Re-scanning emails from Quarantine did not work when the used Core rule had a restricted access
• Fixed memory leaks
• Fixed an issue with HTML sanitization. HTML files are now sent to Core using charset defined in HTML source

**Version 4.2.0**

Important features:

• Support for encrypted archive handling in attachment
  • Public server can be configured for reprocessing the file and generate notification and reports
  • Rescan functionality is provided via the public server if configured
• New Refused email history page under Dashboard
• Dashboard → Quarantine, added pinning options to retain records without be cleaned up via data retention
• Dashboard → Email History, added details for processing history per Email

Enhancement and new features:

• Sanitized file names are now formatted via Rules defined inside MetaDefender Core which connected with Email Security
• SMTP errors now can be overridden via settings inside Policy → Security Rules
• Revamped notification email look and feel with more detailed results information
• Inventory → Server profile name can now be entered as long as 256 characters
• General UI improvements
• Dashboard → Email history, now added Force retry option for immediate action
• Dashboard → Quarantine, now added bulk operations for batch processing records
• Inventory → Server profiles, reorder functionality is added to switch orders of the servers
• Dashboard → Failed Emails, now added bulk operations for retry
• Dashboard → Quarantine, quarantined emails can now be downloaded
• Policy → Security Rules, added configuration for scan timeout
• Inventory → Server Profiles, API keys can be set for URI addresses
• Added more information level to syslog

Fixed issues:
• MetaDefender Central Management connectivity issue
• Missing X-headers
• Parsing scan result now works with every scan visibility level
• Closing emailrelay_ssl.exe on service stop
• Inventory entry details couldn't be read with read-only permission
• Updated database cleanup mechanism
• Keeping inline image positions after sanitization
• Incorrect quarantine statistics could be displayed on the Dashboard
• Raw email view was missing from quarantine details
• Emailrelay.exe is now not started when using MetaDefender Email Security in Exchange mode

Version 4.1.3

New features:
• Re-interpreted, fresh look and feel
• New message ID for forked emails
• Central Management connectivity

Fixed issues:
• Sanitization skipped for nested emails
• Sanitized attachment isn't in quarantine

Version 4.1.2

Fixed issues:
• Adding RTF disclaimer can fail randomly
• Same hash can cause sanitization failure
• Email can be quarantined when scan fails
• Limited (short) length of attachment names
• Dashboard always shows 24 hours data
• Hardcoded suffix for sanitized attachments
• Case-sensitive email address counting
**Version 4.1.1**

Fixed issues:

- Option to skip scanning the email body

**Version 4.1.0**

New features:

- Improved email processing performance
- Microsoft Exchange Server plugin mode
- Sender Policy Framework (SPF) lookups
- Core load balancing and high availability
- Handling emails that failed permanently
- Bypass scanning if Cores are unreachable
- Option to entirely block malicious emails
- Support quarantining on external server
- View headers and contents in quarantine
- Specific email filenames in Core history
- Customization of HELO/EHLO headers
- TLS version negotiation on inbound SMTP

Fixed issues:

- Emails without a subject line are processed with a delay

**Version 4.0.0**

Features:

- Standalone product offering
- Web based user interface for management, configuration and monitoring
- Role based user management with multiple admin users and Active Directory integration
- Multiple email security policies with filters and advanced scan configuration
- Different policy filter settings based on sender node or recipient address
### 6.2 Archived release notes

#### 6.2.1 Version 4.4.1

<table>
<thead>
<tr>
<th>4.4.1 MetaDefender Email Security release</th>
<th>MetaDefender Email Security 4.4.1 is a maintenance release focused on fixing missing rescan links when infected attachments are present.</th>
</tr>
</thead>
<tbody>
<tr>
<td>19 September, 2018</td>
<td></td>
</tr>
</tbody>
</table>

**Fixed**

<table>
<thead>
<tr>
<th>Rescan link was missing from encrypted archive disclaimers</th>
<th>When disclaimers for encrypted archives was enabled with the action &quot;Delete Blocked Contents&quot;, the rescan link was missing from the disclaimer even if the public server address was filled out and if there was an infected attachment next to the encrypted archive.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Zero byte emails resulted in warnings and failed emails</th>
<th>When MetaDefender Email Security received an email which had absolutely no content (0 bytes: no headers, no body, no attachments), the processing of this email resulted in warnings and the email went into a failed state. These emails are now rejected as they only contain sender and recipient info, but nothing else.</th>
</tr>
</thead>
</table>
### 6.2.2 Version 4.5.0

<table>
<thead>
<tr>
<th><strong>4.5.0 MetaDefender Email Security release</strong></th>
<th>MetaDefender Email Security 4.5.0 is a feature release focused on introducing MetaDefender Vault integration and adding an option for skipping sanitized emails from quarantine report</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New &amp; improved</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Integration with MetaDefender Vault</strong></td>
<td>Added the ability to integrate with MetaDefender Vault. You can now upload email attachments directly to MetaDefender Vault while they are processing, and replace the attachments with a URL to the uploaded file. For more details and example uses cases click here.</td>
</tr>
<tr>
<td><strong>Option to not list sanitized emails in quarantine reports</strong></td>
<td>Added an option to Settings → Quarantine reports to list only blocked emails. By enabling this option, emails which are in quarantine due to sanitization won't show up in the quarantine report.</td>
</tr>
<tr>
<td><strong>Improved readability of the Actions tab in Security Rules</strong></td>
<td>&quot;Notify recipients if email is blocked&quot; displayed only when the selected action is &quot;Block email&quot;. Disabled disclaimers are hidden. Added more noticeable section separators.</td>
</tr>
<tr>
<td><strong>Option to use local timezones in remote syslog</strong></td>
<td>It's now possible to configure a remote syslog to use the server's local timezone in the log messages instead of UTC.</td>
</tr>
<tr>
<td>Fixed</td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td></td>
</tr>
<tr>
<td><strong>A batch would open and close without a file to scan</strong></td>
<td>When you turned off the scanning for email bodies and received an email without an attachment, a batch was still opened and closed without files to scan. These unnecessary steps have been removed.</td>
</tr>
<tr>
<td><strong>Domain based filtering was not working without regex</strong></td>
<td>When filtering for emails from/to a given domain one should write &quot;<a href="mailto:.+@exampledomain.com">.+@exampledomain.com</a>&quot;. Now a simpler format &quot;exampledomain.com&quot; can also be used.</td>
</tr>
</tbody>
</table>
| **Typo and renaming** | - "Sanitization failed" status in email details was fixed to "Sanitization failed"  
- "OVERRIDE DEFAULT BEHAVIOR" was renamed to "OVERRIDE ERROR HANDLING BEHAVIOR" in Security Rules → Advanced tab |

**6.2.3 Version 4.5.1**

<table>
<thead>
<tr>
<th>4.5.1 MetaDefender Email Security release</th>
<th>MetaDefender Email Security 4.5.1 is a maintenance release focused on stability improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release Date: November 19, 2018</td>
<td></td>
</tr>
<tr>
<td><strong>MetaDefender Email Security did not add the 'Received' header for emails</strong></td>
<td>When MetaDefender Email Security received emails to be processed, the delivery did not include the necessary 'Received' header</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td><strong>Improved TCP read functionality in processor communication to prevent random read failures</strong></td>
<td>TCP read functionality was improved to decrease read timeout problems between internal processes</td>
</tr>
<tr>
<td><strong>Inbound SMTP port is now monitored</strong></td>
<td>Added a monitoring mechanism which regularly checks the inbound SMTP port and restarts the service if it seems to be down</td>
</tr>
</tbody>
</table>

### 6.2.4 Version 4.5.2

<table>
<thead>
<tr>
<th><strong>4.5.2 MetaDefender Email Security release</strong></th>
<th>MetaDefender Email Security 4.5.2 is a maintenance release focused on stability improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release Date:</strong> December 19, 2018</td>
<td></td>
</tr>
</tbody>
</table>

**Fixed**

<p>| <strong>URL encoding of long</strong> | When MetaDefender Email Security received emails with 3 or 4 byte UTF-8 character subject content then parsing of the email could fail and subsequently prevent the email from being processed and delivered. |</p>
<table>
<thead>
<tr>
<th>subjects which included 3 or 4 bytes UTF-8 characters could fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Memory leak A minor memory leak detected in MetaDefender Email Security was fixed.</td>
</tr>
</tbody>
</table>

### 6.2.5 Version 4.5.3

**4.5.3 MetaDefender Email Security release**

**Release Date:**
January 16, 2019

**Fixed**

- **TLS 1.2 support**
  - SMTP server protocol now fully supports TLS 1.2.
  - MetaDefender Core communication protocol now fully supports TLS 1.2.

- **Improved SMTP response messages**
  - SMTP server 4.x & 5.x messages now describes reason for rejection.

### 6.2.6 Version 4.6.0

MetaDefender Email Security 4.6.0 is a feature release focused on improving evaluation scenarios and better monitoring.
### New & improved

**Deployment modes**  
Support for  
- Protection mode for MetaDefender Email Security to protect your email from known and unknown threats.  
- Inline monitoring mode to evaluate MetaDefender Email Security in your regular mail flow.  
- Out-of-band monitoring mode to evaluate MetaDefender Email Security outside of your regular mail flow.

**Email alerts**  
Monitor your MetaDefender Email Security and get instantly notified if unexpected events occur.

**Improved Dashboard**  
A reworked dashboard to provide better details to help you monitor your mail flow.

**Disclaimer styles**  
Assign predefined styles to disclaimers to increase end-user awareness.

### Fixed

**Syslog issue (TCP protocol)**  
When sending log data to your Syslog server via TCP all data is retained.

Better support for international character sets when sanitizing HTML content.
<table>
<thead>
<tr>
<th>Improved HTML sanitization support</th>
<th>Better support for re-scanning password protected archive content.</th>
</tr>
</thead>
</table>

### 6.2.7 Version 4.6.1

**4.6.1 MetaDefender Email Security release**

Release Date: April 15, 2019

**New & improved**

#### Support for Data Loss Prevention results

Email Security now utilizes MetaDefender Core’s Data Loss Prevention results.

#### Support for password protected documents

Email Security now supports rescanning password protected Portable Document Format (.pdf, .docx, etc.) document attachments, when Email Security is paired with MetaDefender Core version 4.14.3 or newer.

⚠️ **Core 4.14.3 required**

Rescanning Portable Document Format and Microsoft Office document content is only supported when MetaDefender Core version 4.14.3 (or newer) is in use.
For further details please read 4.7 Support for password protected attachmer

Provide details about sanitization failures

Processing history and email alerts provide now more details about the reasons of sanitization failures.

Before

After

Notify sender on blocked outbound emails

The sender is notified when the outbound email is blocked.

This will allow the sender to provide the password (for a password protected document or archive) scanned before it is sent out the organization.

Dashboard > Failed Emails now has a CLEANUP function. This function makes possible to delete certain failed emails that are older then the timeframe selected.
4.7.4 Cleanup functionality for Failed Emails

Scan start entry in processing histories

Email details / PROCESSING HISTORY for Dashboard > Email History, Dashboard > Quarantine and Dashboard > Failed Emails now contains an entry logging when the email was sent for scanning to MetaDefender Core. This entry can help administrators to learn how much time of its processing was spent in scanning, outside of Email Security.

Fixed

Syslog syntax error in case of CEF logs

When logging was set to Common Event Format (CEF), log messages were...
Wrong code reported for refused emails

When an email was refused -due to unlicensed product, for example- with SMTP code 450, erroneously Email Security reported 550 in **Refused Emails > Email details**.

<table>
<thead>
<tr>
<th>Before</th>
<th>After</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Before Image]</td>
<td>![After Image]</td>
</tr>
</tbody>
</table>

Contact sharing invitations were corrupted

Microsoft Exchange Server **contact sharing invitations** got corrupted in the final emails when **Disarm & Reconstruction (CDR; Data Sanitization / DS)** was enabled in the Email Security.

Allowed items appeared in quarantine reports

Allowed (but otherwise quarantined; e.g. emails with sanitized attachments) items were included in quarantine reports even when quarantine reports were **configured** to contain blocked emails only.

### 6.2.8 Version 4.6.2

**4.6.2 MetaDefender Email**

MetaDefender Email Security 4.6.2 is a maintenance release focused on fixir
### Security release

**Release Date:** May 07, 2019

### New & improved

#### Upload attachments to recipients’ Vault folders

Enabling the **Policy > Security rules / add/modify / VAULT/ UPLOAD TO USER'S OWN VAULT ACCOUNT** option, Email Security will upload the attachments (depending on the other, Vault related settings) to the recipients Vault account.

The Vault account is identified by the recipient email address.

⚠️ If no account exist with the recipient email address on the Vault, then it will be uploaded to the account that is assigned to the API key specified in the **MetaDefender Vault type server profile** set for the matching rule.
### Upload failed-to-sanitize attachments to Vault

Enabling the **Policy > Security rules / add/modify / VAULT / UPLOAD ATTACHMENTS** configured to upload the original copy of attachments that failed **sanitization** (sanitization).

If both

1. **UPLOAD ORIGINAL OF SANITIZED ATTACHMENTS** and
2. **UPLOAD ATTACHMENTS THAT FAILED SANITIZATION**
are enabled—and the sanitization fails—then the original file will be uploaded.

Send alert emails when Vault is unresponsive

Enabling the **Settings > Email Alerts** / Alert types / **METADEFENDER VAULT** email alerts when a Vault server configured in the MetaDefender Vault type...
4.7.4

Option to enable scanning email headers

Enabling the **Policy > Security rules** / add/modify / SCAN / SCAN EMAIL HEADER placed into email headers (e.g. sender, subject, etc.). This function can help –for example– to prevent leaking sensitive information through email subjects. For further details see the Scan settings section in 4.2 Security rules.
Email Security now supports emails with **AMP HTML** body.

Email Security now writes `data_id` values (that it receives from Core) into it.
4.7.4 Enhanced log correlation with logs from Core

The data_id values are highlighted in the Email Security log entry below that was written for a simple text email that consists of a header and a body section:

```
changed vault configuration moved to server profiles
```

MetaDefender Vault instances can now only be configured as server profiles.

Remember, that:

- Vault REST is configured by default on port 8000,
- Vault REST is available under the URI path `/vault_rest`. 
Prior to Email Security 4.6.2, the Vault server must have been specified directly under `/add/modify/VAULT/UPLOAD ATTACHMENTS TO`. From version 4.6.2 this setting will point to the appropriate MetaDefender Vault type server profile.
Email Security inserted date and time headers with a wrong value and format and the text representation of the day of week and month values were displayed as question marks.
A file may have been sanitized twice when Email Security was integrated with Vault.

Previous releases

<table>
<thead>
<tr>
<th>Feature</th>
<th>Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.6.0</td>
<td>4.6.1</td>
</tr>
<tr>
<td>4.5.0</td>
<td>4.5.1</td>
</tr>
<tr>
<td>4.4.0</td>
<td>4.4.1</td>
</tr>
</tbody>
</table>

6.2.9 Version 4.7.0

MetaDefender Email Security 4.7.0 is a feature release focusing on the new dashboard look & feel and the new navigation structure.

New & improved

<table>
<thead>
<tr>
<th>New, simplified navigation structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Security page navigation has been restructured. Some pages have been raised or moved. See Dashboard, 4.3 Quarantine and 4.4 Email history.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Old entry</th>
<th>Change</th>
<th>New entry</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dashboard &gt; Overview</td>
<td>raised to top level</td>
<td>Dashboard</td>
</tr>
<tr>
<td>Dashboard &gt; Email History</td>
<td>moved</td>
<td>Audit &gt; Email History</td>
</tr>
<tr>
<td>Old entry</td>
<td>Change</td>
<td>New entry</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Dashboard &gt; Failed Emails</td>
<td>moved &amp; merged into</td>
<td>Audit &gt; Email</td>
</tr>
<tr>
<td>Dashboard &gt; Refused emails</td>
<td>moved</td>
<td>Audit &gt; Refused</td>
</tr>
<tr>
<td>Dashboard &gt; Config History</td>
<td>moved</td>
<td>Audit &gt; Config</td>
</tr>
<tr>
<td>Dashboard &gt; Quarantine</td>
<td>raised to top level</td>
<td>Quarantine</td>
</tr>
<tr>
<td>Improved dashboard look and feel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>----------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email Security Dashboard has been completely redesigned so that it can provide the users with really useful information and provide shortcuts to important pages. For details see 4.1 Dashboard.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Email Security now has some new statistics about the threats prevented and emails handled. For details see [link].

**4.1 Dashboard**

To see the statistics details, click on the `Show details` link at each widget.

**Malicious attacks prevention**

This view shows the top file formats that have been sanitized.
Advanced threat detection

This view shows the top malware that was detected and prevented by the system.

Data loss prevention

This view shows the top data loss threats that were detected and prevented.
Inbound and outbound emails

These views show the top email senders and recipients.

There is the new SKIP PARTIAL SANITIZATIONS option under **Policy > Security > BEHAVIOR**, that will instruct Email Security to **not replace partially sanitized** data for these files.
For emails, where partial sanitization was skipped, Audit > Email History /
Email Security reported *illegal characters in path* errors for certain emails. The failure: the emails were available on the filesystem.
## 6.2.10 Version 4.7.1

<table>
<thead>
<tr>
<th>4.7.1 MetaDefender Email Security release July 1, 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender Email Security 4.7.1 is a maintenance release focusing on fixing improvements.</td>
</tr>
</tbody>
</table>

### New & Improved

<table>
<thead>
<tr>
<th>SMTP server component of Email Security now listens on IPv6 when it is available</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender Email Security's SMTP server component now listens on both IPv4 and IPv6 (if IPv6 is configured).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email Security now has an option to send alert emails when emails get bypassed</th>
</tr>
</thead>
<tbody>
<tr>
<td>A new option is available under <code>Settings &gt; Email Alerts</code> / EMAIL BYPASSED. Email Security bypassed scanning an email. This alert will be sent for every</td>
</tr>
</tbody>
</table>
If MetaDefender Email Security's license is invalid, then it will bypass all emails. A bypass workflow is applied in these cases, meaning that the bypass disclaimer is applied to the email (if enabled at the matching rule) and a bypass alert email is sent (if enabled under /EMAIL Settings > Email Alerts). For details about actions to bypass emails and bypass disclaimers see the **BYPASSED**. For details about email alerts see the *Email alerts* section in **3.5.1 Configuration**.
The default disclaimer for messages with encrypted contents have been updated

<table>
<thead>
<tr>
<th>Old disclaimer</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender Email Security has removed one or more attachments in because it contained potentially malicious embedded objects or it was pass protected. To initiate the rescan and provide the password(s), click the follow (within %[rescan_link_expiry]% hours): &lt;a href=&quot;%[rescan_link_url]&quot;&gt;%rescan_link_url[Your administrator did not set a public server address for rescan]&quot;&gt;% For more information on MetaDefender Email Security, please visit &lt;a href=&quot;https://www.opswat.com/products/metadefender/email-security&quot;&gt;<a href="https://www.opswat.com/products/metadefender/email-security">https://www.opswat.com/products/metadefender/email-security</a>. &gt;</td>
</tr>
</tbody>
</table>

For details about support for emails with password protected attachments see 4.7 Support for password protected attachments

For details about actions to handle emails with password protected attachment see 4.2 Security rules

For details about disclaimer variables see 4.2.1 Disclaimer variables.

<table>
<thead>
<tr>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product schema is invalid error when adding Email Security to Central Management</td>
</tr>
<tr>
<td>When trying to add MetaDefender Email Security 4.7.0 to the recent versions error message is shown.</td>
</tr>
<tr>
<td>This error is the result of some modifications introduced in Email Security 4.7</td>
</tr>
</tbody>
</table>

| Rescan pages of password protected attachments sometimes |
| MetaDefender Email Security can be configured to let users to provide the password contents to re-scan. Re-scanning can be initiated on a public page of Email. |
| This page took in certain cases even minutes to load. |
| For details about support for emails with password protected attachments see 4.7 Support for password protected attachments |

4.7.4
<table>
<thead>
<tr>
<th>took very long to load</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain emails got refused by the SMTP component without an apparent reason</td>
</tr>
</tbody>
</table>

Email Security refused some emails on its SMTP interface without an apparent reason. These emails had contents with non-standard formatting. Email Security parser is now enhanced to be able to process even this kind of non-standard email formats.
## 6.2.11 Version 4.7.2

### 4.7.2 MetaDefender Email Gateway Security release

MetaDefender Email Gateway Security 4.7.2 is a maintenance release focusing on fixing a recent Central Management integration issue and on adding some minor improvements.

### New & Improved

#### Uploading partially sanitized archives to MetaDefender Vault

The new option to upload partially sanitize archives to MetaDefender Vault is available in **Policy > Security Rules >[Rule name] > Vault**.

![Security Rules](image)

**Note**

This requires the 'Distinguish partial archive sanitization result' option check in the MetaDefender Core rule used to scan content with. See [MetaDefender Core > 3.6.2. Workflow template configuration](#) for more information.

#### Improved Proactive DLP support

The Proactive DLP support is now improved to support watermarks, metadata removal etc. even when Deep CDR is disabled.
<table>
<thead>
<tr>
<th>DKIM signature verification</th>
<th>It is now possible to perform DKIM signature verification for emails. Result will be added to each email's header information (X-Metadefender-Dkim-Result [Valid/Invalid/None]).</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPSWAT Central Management v7 support</td>
<td>You can now configure your MetaDefender Email Gateway Security instance from OPSWAT Central Management v7.</td>
</tr>
<tr>
<td>Fixed</td>
<td></td>
</tr>
<tr>
<td>SMTP server stability improvements</td>
<td>The SMTP server monitoring and stability has been improved.</td>
</tr>
<tr>
<td>Performance improvements</td>
<td>The overall email processing performance has been improved.</td>
</tr>
<tr>
<td>SPF IPv6 support</td>
<td>Sender Policy Framework (SPF) now supports lookup for IPv6 addresses.</td>
</tr>
<tr>
<td>MetaDefender Vault archive password support</td>
<td>MetaDefender Email Gateway Security will now provide MetaDefender Vault with any archive passwords provided by a user in MetaDefender Email Gateway Security.</td>
</tr>
<tr>
<td>Note</td>
<td></td>
</tr>
<tr>
<td>------</td>
<td></td>
</tr>
<tr>
<td>MetaDefender Email Gateway Security or MetaDefender Vault does not store any of the provided passwords.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Not scanned emails displayed in dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any emails not scanned by MetaDefender Email Gateway Security ([Policy &gt; Security Rules &gt; [Rule name] &gt; Scan &gt; Allow scan set to false]) will be recorded as an allowed email.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Email Alert improvements</th>
</tr>
</thead>
<tbody>
<tr>
<td>The email alerts SMTP RELAY NOT RESPONDING, METADEFENDER CORE NOT RESPONDING, METADEFENDER VAULT NOT RESPONDING are only sent once per unique URL/hour.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Headers content file type mismatch fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>The header content provided to MetaDefender Core is now correctly identified as ASCII text.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Emails delivery uninterrupted in case of unlicensed product</th>
</tr>
</thead>
<tbody>
<tr>
<td>If the MetaDefender Email Gateway Security license expires, emails will still be accepted and forwarded (unscanned &amp; unmodified) according to security rule configuration.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Email Alert sender &amp; recipient information is provided an alert will also be sent informing the administrator of the licensing issue.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4.7.2.1898 MetaDefender Email Gateway Security Hotfix Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 22, 2019</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7.4</td>
</tr>
<tr>
<td>Selected rule not highlighted</td>
</tr>
</tbody>
</table>
## 6.2.12 Version 4.7.3

### 4.7.3 MetaDefender Email Gateway Security release

MetaDefender Email Gateway Security 4.7.3 is a maintenance release focusing on minor fixes.

### September 30, 2019

## New & Improved

### Expiration date / time in rescan notifications

In its notifications MetaDefender Email Gateway Security can now tell exactly when the re-scan link expires for emails containing password protected attachments.

For further details see [4.7 Support for password protected attachments](#)
<table>
<thead>
<tr>
<th>Added sender address to file name on Vault</th>
<th>To be easier to look up uploaded emails, Email Gateway Security now adds the sender address to the file name on Vault. For details see 4.9 Integration with MetaDefender Vault.</th>
</tr>
</thead>
<tbody>
<tr>
<td>All (temporary) files created are now located under the Email Gateway Security installation directory. Previously some temporary files were written into the Windows Temp folder</td>
<td></td>
</tr>
<tr>
<td>All files are created in the installation directory</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Fixed</td>
<td></td>
</tr>
</tbody>
</table>
| Empty email bodies caused Deep CDR errors | **Sanitization** of the body of emails that had an *empty body* failed in certain circumstances (e.g. when the sending user agent was on iOS 13.1, or later).

Email Gateway Security now skips scanning / sanitization for empty content without a content. |
| Could not change Settings > Global Settings | After upgrading from version 4.7.1 to 4.7.2, it was not possible to modify certain setting under **Settings > Global settings**.

Saving the modified configuration resulted in the error: *Error while modifying configuration* |
7. Legal

- Copyright
- MetaDefender Export Classification

Copyright

DISCLAIMER OF WARRANTY
OPSWAT Inc. makes no representation or warranties, either express or implied by or with respect to anything in this document, and shall not be liable for any implied warranties of merchantability or fitness for a particular purpose or for any indirect special or consequential damages.

COPYRIGHT NOTICE
OPSWAT, OESIS, Metascan, Metadefender, AppRemover and the OPSWAT logo are trademarks and registered trademarks of OPSWAT, Inc. All other trademarks, trade names and images mentioned and/or used herein belong to their respective owners.

No part of this publication may be reproduced, stored in a retrieval system or transmitted, in any form or by any means (photocopying, recording or otherwise) without prior written consent of OPSWAT Inc. No patent liability is assumed with respect to the use of the information contained herein. While every precaution has been taken in the preparation of this publication, OPSWAT Inc. assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

MetaDefender Export Classification

MetaDefender United States Export Classification Number (ECCN) is 5D002, subparagraph c.1 Exports and re-exports of MetaDefender are subject to U.S. export controls and sanctions administered by the Commerce Department’s Bureau of Industry and Security (BIS) under the U.S. Export Administration Regulations (EAR).

This page provides export control information on MetaDefender. MetaDefender provides encryption features that are subject to the EAR and other U.S. laws. These features have been approved for export from the United States, subject to certain requirements and limitations. You may find the information on this page useful for determining exportability to particular countries or parties, and for completing export or shipping documentation, recordkeeping, or post-shipment reporting.
Although we provide the information on this page, you remain responsible for exporting or re-exporting MetaDefender in accordance with U.S. law. We encourage you to seek appropriate legal advice and/or consult the EAR and the BIS Information Technology Controls Division before exporting, re-exporting, or distributing MetaDefender. The information provided here is subject to change without notice.
8. Knowledge Base Articles

- **Page:** Emails released or forwarded from Quarantine and retried from Failed emails, fail permanently on Exchange Server
- **Page:** How do I perform a clean re-install of MetaDefender Email Security v4?
- **Page:** How long is the support life cycle for a specific version/release of MetaDefender Email Security v4?
- **Page:** Manually registering MetaDefender Email Security in Exchange server
- **Page:** What is the difference between MetaDefender Email Security 3.X vs 4.X?

**Emails released or forwarded from Quarantine and retried from Failed emails, fail permanently on Exchange Server**

The "MessageExpirationTimeout" parameter of Microsoft Exchange Server specifies the maximum time that a particular message can remain in the queue. If a message remains in the queue for longer than the value defined in "MessageExpirationTimeout", the message will be returned to the sender as a permanent failure.

This parameter is likely to affect the delivery of emails released or forwarded from Quarantine (see 4.3 Quarantine) or emails retried from Audit > Email History (see 4.4 Email history).

The default value of "MessageExpirationTimeout" is 2 days. This means that if an email spends more than 2 days in Quarantine or in Audit > Email History then releasing or forwarding and retrying (accordingly) after 2 days will fail.

The maximum value that "MessageExpirationTimeout" can be extended to is 90 days.

For further details see 3.10 Onsite Microsoft Exchange deployment.

*This article pertains to MetaDefender Email Security v4.0.0 or above*

*This article was last updated on 2019-10-09*

VM

**How do I perform a clean re-install of MetaDefender Email Security v4?**

- **Overview**
- **Details**
  - Uninstall the previous version
- Delete installation directory
- Clean-up Windows registry
- Install the current version

**Overview**

In certain cases (e.g. upgrading to a newer release candidate, or downgrading to a previous version) a clean install of the product is required.

⚠️ In case of a clean reinstall, data from the previous installation will be lost.

For a clean re-installation:

1. Uninstall the previous version.
2. Delete installation directory.
3. Clean-up Windows registry.
4. Install the current version.

**Details**

**Uninstall the previous version**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><img src="image" alt="Control Panel" /> &gt; Control Panel &gt; Programs &gt; Uninstall a program</td>
<td><img src="image" alt="Uninstall a program" /></td>
</tr>
</tbody>
</table>

4.7.4
Step | Description | Details
--- | --- | ---
| 4.7.4 | In Programs and Features, find **MetaDefender Email Security**. Right click and select **Uninstall**. | ![Image](image.png)
| 3 | Follow the steps of the installer | ![Image](image.png)

**Delete installation directory**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Delete the directory and its contents where MetaDefender Email Security is installed.</td>
<td>The default is <code>C:\Program Files\OPSWAT\MetaDefender Email Security</code>.</td>
</tr>
</tbody>
</table>

⚠️ Deleting the installation directory may be blocked by running applications that hold or use files that are included in the installation directory.

A common example of this issue is `emailrelay.exe`, which is not stopped by the uninstallation process.

Please lookup `emailrelay.exe` in the task manager and stop it manually. After this, try deleting the folder again.
## Clean-up Windows registry

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start Registry Editor:</td>
<td><img src="image" alt="Registry Editor" /></td>
</tr>
<tr>
<td></td>
<td><code>&gt; regedit</code></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Navigate to the following key:</td>
<td><img src="image" alt="Registry Editor" /></td>
</tr>
<tr>
<td></td>
<td>HKEY_LOCAL_MACHINE\SOFTWARE\OPSWAT\MetaDefender Email Security</td>
<td></td>
</tr>
<tr>
<td>Step</td>
<td>Description</td>
<td>Details</td>
</tr>
<tr>
<td>------</td>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>3</td>
<td>Delete the MetaDefender Email Security key and all of its subkeys</td>
<td><img src="image-url" alt="Registry Editor Screenshot" /></td>
</tr>
</tbody>
</table>
## Step 4: Confirm deletion

*Confirm deletion*

### Details

**Install the current version**

Follow the instructions in [1.1 Installation](#) to install the new version of the product.

*This article pertains to MetaDefender Email Security v4.0.0 or above*

*This article was last updated on 2019-10-09*

*VM*
How long is the support life cycle for a specific version/release of MetaDefender Email Security v4?

OPSWAT provides support on each release of MetaDefender Email Security v4 for **18 months** after the publication of the next release of the product (i.e. once a new release is published, you have 18 more months of support on the previous release). However, bug fixes and enhancements are applied only to the next release of a product, not to the current release or historical releases, even when those releases are still under support. In some cases, hot-fixes can be provided for the current release of the product and then incorporated as a regular fix in the next release.

OPSWAT strongly encourages customers to upgrade to the latest release on a regular basis and not to wait until the end of a release supported life-cycle.

<table>
<thead>
<tr>
<th>Release number</th>
<th>Release date</th>
<th>End-of-life date</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.7.3</td>
<td>30 Sep 2019</td>
<td></td>
</tr>
<tr>
<td>4.7.2</td>
<td>22 Aug 2019</td>
<td>30 Mar 2021</td>
</tr>
<tr>
<td>4.7.1</td>
<td>01 Jul 2019</td>
<td>22 Feb 2021</td>
</tr>
<tr>
<td>4.7.0</td>
<td>31 May 2019</td>
<td>01 Jan 2021</td>
</tr>
<tr>
<td>4.6.2</td>
<td>07 May 2019</td>
<td>30 Nov 2020</td>
</tr>
<tr>
<td>4.6.1</td>
<td>15 Apr 2019</td>
<td>07 Nov 2020</td>
</tr>
<tr>
<td>4.6.0</td>
<td>12 Mar 2019</td>
<td>15 Oct 2020</td>
</tr>
<tr>
<td>4.5.3</td>
<td>16 Jan 2019</td>
<td>12 Sep 2020</td>
</tr>
<tr>
<td>4.5.2</td>
<td>19 Dec 2018</td>
<td>16 Jul 2020</td>
</tr>
<tr>
<td>4.5.1</td>
<td>27 Nov 2018</td>
<td>19 Jun 2020</td>
</tr>
<tr>
<td>4.5.0</td>
<td>11 Oct 2018</td>
<td>27 May 2020</td>
</tr>
<tr>
<td>4.4.1</td>
<td>19 Sep 2018</td>
<td>11 Apr 2020</td>
</tr>
</tbody>
</table>
Manually registering MetaDefender Email Security in Exchange server

In case MetaDefender Email Security Transport Agents registrations are missing or failed to register at installation time this step can also be performed manually as described below.

1. Open an Exchange Management Shell.
2. Check which transport agents are registered by typing:

   `Get-TransportAgent`
3. If the following transport agent registrations are present, MetaDefender Email Security is already registered. Otherwise, proceed to next step to start registration.

<table>
<thead>
<tr>
<th>Identity</th>
<th>Enabled</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadefender Email Security Smtp Agent</td>
<td>True</td>
<td>[n]</td>
</tr>
<tr>
<td>Metadefender Email Security Routing Agent</td>
<td>True</td>
<td>[n]</td>
</tr>
</tbody>
</table>

4. Register the MetaDefender Email Security Smtp Agent by typing:

```
Install-TransportAgent
```

a. Provide the path to the Metadefender.Email.Exchange.dll file (adjust the path as required):

```
AssemblyPath: C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost\Metadefender.Email.Exchange.dll
```

b. Provide the transport agent name:

```
Name: Metadefender Email Security Smtp Agent
```

c. Specify the transport agent factory as below:

```
```

5. If the transport agent registration is successful, the following information is displayed:

<table>
<thead>
<tr>
<th>Identity</th>
<th>Enabled</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadefender Email Security Smtp Agent</td>
<td>True</td>
<td>[n]</td>
</tr>
</tbody>
</table>
Metadefender Email Security Smtpl Agent
False   [n]
WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect: MSExchangeTransport

6. Enable the newly created transport agent by typing:

```
Enable-TransportAgent
```

a. Specify the transport agent identity as below:

```
Identity: Metadefender Email Security Smtpl Agent
```

7. Continue to register the MetaDefender Email Security Routing Agent by typing:

```
Install-TransportAgent
```

a. Provide the path to the Metadefender.Email.Exchange.dll file (adjust the path as required):

```
AssemblyPath: C:\Program Files\OPSWAT\Metadefender Email Security\mailagenthost\Metadefender.Email.Exchange.dll
```

b. Provide the transport agent name:

```
Name: Metadefender Email Security Routing Agent
```

c. Specify the transport agent factory as below:

```
```

8. If the transport agent registration is successful, the following information is displayed:
<table>
<thead>
<tr>
<th>Identity</th>
<th>Enabled</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadefender Email Security Routing Agent</td>
<td>False</td>
<td>n</td>
</tr>
</tbody>
</table>

WARNING: Please exit Windows PowerShell to complete the installation.
WARNING: The following service restart is required for the change(s) to take effect: MSExchangeTransport

9. Enable the transport agent by typing:

`Enable-TransportAgent`

a. Specify the transport agent identity as below:

Identity: Metadefender Email Security Routing Agent

10. Complete the transport agent installation by restarting the Microsoft Exchange Transport service.

a. Stop the service by typing:

`net stop MSExchangeTransport`

b. Re-start the service by typing:

`net start MSExchangeTransport`

Transport agent registration is now complete.

This article pertains to MetaDefender Email Security v4.0.0 or above

This article was last updated on 2019-10-09

VM
What is the difference between MetaDefender Email Security 3.X vs 4.X?

If you are running a previous version of MetaDefender Email Security, OPSWAT recommends upgrading to the latest released version whenever it is practically possible. For users who may be using MetaDefender Email Security 3.X, there are significant architectural differences when upgrading to the latest version. To help with the upgrade, the table below compares the functionality between the two generations of the product and provides links to any relevant documentation.

<table>
<thead>
<tr>
<th>Feature</th>
<th>MetaDefender Email 3.X</th>
<th>MetaDefender Email Security 4.X</th>
<th>3.X Documentation</th>
<th>4.X Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetaDefender Core compatibility</td>
<td>CORE V3</td>
<td>CORE V4.7.0+</td>
<td></td>
<td>2.1.2 System re</td>
</tr>
<tr>
<td>Licensing</td>
<td>BUNDLED INTO CORE</td>
<td>STANDALONE</td>
<td></td>
<td>2.4 MetaDefend Security licensing</td>
</tr>
<tr>
<td>Based on count of recipient email addresses</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td>2.4.3 Maximum email addresses</td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountability</td>
<td>SINGLE ACCOUNT</td>
<td>PER USER ACCOUNT</td>
<td></td>
<td>3.3 User manag</td>
</tr>
<tr>
<td>Human Authentication</td>
<td>GROUP PASSWORD</td>
<td>PER USER PASSWORD</td>
<td></td>
<td>3.3 User manag</td>
</tr>
</tbody>
</table>

<p>|                  | API KEY                | API KEY                         |                   | 3.3 User manag    |</p>
<table>
<thead>
<tr>
<th>Feature</th>
<th>MetaDefender Email 3.X</th>
<th>MetaDefender Email Security 4.X</th>
<th>3.X Documentation</th>
<th>4.X Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Machine Authentication</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound SMTP TLS version negotiation</td>
<td><strong>TLS 1.0 ONLY</strong></td>
<td><strong>NEGOTIABLE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS version customization</td>
<td><strong>NO</strong></td>
<td><strong>YES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS cipher customization</td>
<td><strong>NO</strong></td>
<td><strong>YES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inbound SMTP over TLS</td>
<td><strong>NO</strong></td>
<td><strong>YES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access control</td>
<td><strong>EXPLICIT</strong></td>
<td><strong>RBAC</strong></td>
<td></td>
<td><strong>3.3 User management</strong></td>
</tr>
<tr>
<td>Role based access control</td>
<td><strong>NO</strong></td>
<td><strong>YES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User management</td>
<td><strong>NO</strong></td>
<td><strong>YES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Active Directory integration</td>
<td><strong>NO</strong></td>
<td><strong>YES</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User interface</td>
<td>BUNDLED INTO CORE</td>
<td>STANDALONE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------</td>
<td>------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dashboard</td>
<td>BUNDLED INTO CORE</td>
<td>OWN</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dashboard auto-refresh</td>
<td>NO</td>
<td>CONFIGURABLE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email history</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan details in email history</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email history cleanup</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration history</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configuration diffs</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>History auto cleanup</td>
<td>YES</td>
<td>YES</td>
<td>Configuration From Config File (MetaDefender.Engine. History.dll.config &gt; HistoryEntryExpireSpan)</td>
<td></td>
</tr>
</tbody>
</table>

**Dashboard**

- BUNDLED INTO CORE
- OWN

**Dashboard**

- Refresh • 30 secs

**Email History**

- YES

**Configuration History**

- NO

**Configuration Diffs**

- NO

**Audit > Email History**

- CLEANUP

**Audit > Email History**

- CLEANUP

3.4 General settings

Configuration From Config File (MetaDefender.Engine. History.dll.config > HistoryEntryExpireSpan)
<table>
<thead>
<tr>
<th>Feature</th>
<th>MetaDefender Email 3.X</th>
<th>MetaDefender Email Security 4.X</th>
<th>3.X Documentation</th>
<th>4.X Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>History</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>custom date filtering</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Search keys</td>
<td>NAME</td>
<td>MULTIPLE</td>
<td>Not documented</td>
<td>4.10 Search.html</td>
</tr>
<tr>
<td>Full-text search</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td>4.10 Search.html</td>
</tr>
<tr>
<td>Policy</td>
<td>PARTIAL</td>
<td>YES</td>
<td>Single workflow</td>
<td>4.2 Security rule</td>
</tr>
<tr>
<td>Inventory</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td>3.7 Server profil</td>
</tr>
<tr>
<td>Web-based configuration</td>
<td>PARTIAL</td>
<td>YES</td>
<td>Some global settings configurable via UI or REST API, others via config files</td>
<td>3.4 General sett</td>
</tr>
<tr>
<td>settings</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Batch operations</td>
<td>PARTIAL</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Resource management</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>MetaDefender Email 3.X</td>
<td>MetaDefender Email Security 4.X</td>
<td>3.X Documentation</td>
<td>4.X Documentation</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Core load balancing</td>
<td>YES</td>
<td>YES</td>
<td>Configuration From Config File (MetaDefender.Scanner.dll.config)</td>
<td>3.7 Server profil</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.7.1 MetaDefender specific inventory</td>
<td></td>
</tr>
<tr>
<td>Core high availability</td>
<td>YES</td>
<td>YES</td>
<td>Configuration From Config File (MetaDefender.Scanner.dll.config)</td>
<td>3.7 Server profil</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.7.1 MetaDefender specific inventory</td>
<td></td>
</tr>
<tr>
<td>SMTP relay load balancing</td>
<td>NO</td>
<td>YES</td>
<td>3.7 Server profil</td>
<td></td>
</tr>
<tr>
<td>SMTP relay high availability</td>
<td>YES</td>
<td>YES</td>
<td>Configuration From Config File (MetaDefender.Email.Engine.Generic.Agent.dll.config &gt; EmailRelayOutHosts)</td>
<td>3.7 Server profil</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Workflow</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security rules</td>
<td>IMPLICIT</td>
<td>YES</td>
<td>4.2 Security rule</td>
<td></td>
</tr>
<tr>
<td>Workflow</td>
<td>SINGLE</td>
<td>PER RULE</td>
<td>Email Processing Workflow (MetaDefender Core)</td>
<td>4.2 Security rule</td>
</tr>
<tr>
<td>Email filtering</td>
<td>NO</td>
<td>PER RULE</td>
<td>4.2 Security rule</td>
<td></td>
</tr>
<tr>
<td>Email routing</td>
<td>SINGLE</td>
<td>PER RULE</td>
<td>4.2 Security rule</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>MetaDefender Email 3.X</td>
<td>MetaDefender Email Security 4.X</td>
<td>3.X Documentation</td>
<td>4.X Documentation</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------------------</td>
<td>----------------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Override Core results</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bypass Core</td>
<td>NO</td>
<td>PER RULE</td>
<td></td>
<td>4.2 Security rule scan settings)</td>
</tr>
<tr>
<td>Core rule selection</td>
<td>SINGLE</td>
<td>PER RULE</td>
<td></td>
<td>4.2 Security rule</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Email processing</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan emails and attachments</td>
<td>YES</td>
<td>YES</td>
<td>Email Processing Workflow (MetaDefender Core)</td>
<td>4.2 Security rule</td>
</tr>
<tr>
<td>Sanitize emails and attachments</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Block emails and attachments</td>
<td>ATTACHMENTS ONLY</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclaimers</td>
<td>SINGLE</td>
<td>PER RULE</td>
<td>Customizing Disclaimers</td>
<td>4.2 Security rule</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Infection Email Notification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Sanitized Email Notifications</td>
<td></td>
</tr>
<tr>
<td>Merge fields</td>
<td>PARTIAL</td>
<td>YES (LIMITED)</td>
<td>Infection Email Notification</td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>MetaDefender Email 3.X</td>
<td>MetaDefender Email Security 4.X</td>
<td>3.X Documentation</td>
<td>4.X Documentation</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>------------------------</td>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Subject rewriting</td>
<td>PARTIAL</td>
<td>PLANNED</td>
<td>Sanitized Email Notifications</td>
<td></td>
</tr>
<tr>
<td>Custom email headers</td>
<td>SINGLE</td>
<td>PER RULE</td>
<td>Custom Email Headers</td>
<td>4.2 Security rule</td>
</tr>
<tr>
<td>Scan information headers</td>
<td>YES</td>
<td>YES</td>
<td>Custom Email Headers</td>
<td></td>
</tr>
<tr>
<td>Retry mechanism</td>
<td>YES</td>
<td>YES</td>
<td>Requires manual monitoring of notifications and folders</td>
<td>3.4 General sett</td>
</tr>
<tr>
<td>Handling permanent failures</td>
<td>MANUAL</td>
<td>YES</td>
<td>Manual reprocessing of failed items</td>
<td>4.4 Email histor</td>
</tr>
<tr>
<td>Handling refused emails</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Support for password-protected</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>attachments</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quarantine</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>MetaDefender Email 3.X</td>
<td>MetaDefender Email Security 4.X</td>
<td>3.X Documentation</td>
<td>4.X Documentation</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------</td>
<td>---------------------------------</td>
<td>------------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Quarantine location</td>
<td>BUNDLED INTO CORE</td>
<td>OWN</td>
<td></td>
<td>4.3 Quarantine</td>
</tr>
<tr>
<td>Quarantine original copy</td>
<td>GLOBAL</td>
<td>PER RULE</td>
<td>Quarantine Email</td>
<td>4.2 Security rule</td>
</tr>
<tr>
<td>Email details</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operations (Download, Release, Forward, Delete)</td>
<td>PARTIAL</td>
<td>YES</td>
<td>Not documented</td>
<td>4.3 Quarantine</td>
</tr>
<tr>
<td>Batch operations</td>
<td>GENERAL</td>
<td>YES</td>
<td>2.6. Quarantine Management</td>
<td></td>
</tr>
<tr>
<td>External quarantine</td>
<td>YES</td>
<td>YES</td>
<td>Quarantine Email On Another Mail Server</td>
<td>3.6.1 Quarantine another mail server</td>
</tr>
<tr>
<td>Quarantine reports</td>
<td>YES</td>
<td>YES</td>
<td>Quarantine Reports</td>
<td>3.6 Quarantine</td>
</tr>
<tr>
<td>Quarantine report contents</td>
<td>GENERAL</td>
<td>SPECIFIC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom quarantine report schedule</td>
<td>NO</td>
<td>NO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Feature</td>
<td>MetaDefender Email 3.X</td>
<td>MetaDefender Email Security 4.X</td>
<td>3.X Documentation</td>
<td>4.X Documentation</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>------------------------</td>
<td>--------------------------------</td>
<td>-------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td><strong>Notification emails</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email threat alerts</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td>4.2 Security rules</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service status alerts</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td>3.5.1 Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SMTP relay</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email flow direction (per deployment)</td>
<td>ONE-WAY</td>
<td>BIDIRECTIONAL</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>TLS configuration</td>
<td>EXTERNAL TOOL</td>
<td>BUILT-IN</td>
<td></td>
<td>3.2 Configuring</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SPF lookups</td>
<td>YES</td>
<td>YES</td>
<td></td>
<td>3.4 General settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>HELO/EHLO domain customization</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td>3.1.2 Windows I configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Integration</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>YES</td>
<td>YES</td>
<td></td>
<td>4. Onsite Microsoft Exchange Deployment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3.10 Onsite Microsoft Exchange deployment</td>
</tr>
</tbody>
</table>

**Feature**

**MetaDefender Email 3.X**

**MetaDefender Email Security 4.X**

**3.X Documentation**

**4.X Documentation**
<table>
<thead>
<tr>
<th>Feature</th>
<th>MetaDefender Email 3.X</th>
<th>MetaDefender Email Security 4.X</th>
<th>3.X Documentation</th>
<th>4.X Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Exchange plugin</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud (AppRiver, Google Apps, Office 365)</td>
<td>YES</td>
<td>YES</td>
<td>3. Cloud Deployment</td>
<td>3.9 Cloud deplo configuration</td>
</tr>
</tbody>
</table>

**Operation**

<table>
<thead>
<tr>
<th>Monitoring</th>
<th>LIMITED</th>
<th>ADVANCED</th>
<th>Dashboard / Mail Agent</th>
<th>4.1 Dashboard</th>
</tr>
</thead>
<tbody>
<tr>
<td>General audit logs</td>
<td>YES</td>
<td>YES</td>
<td>Email Event Log</td>
<td></td>
</tr>
<tr>
<td>Configuration audit logs</td>
<td>NO</td>
<td>INTEGRATED</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Syslog integration</td>
<td>LIMITED</td>
<td>YES</td>
<td>Logging Configuration</td>
<td>3.5.1 Configurat</td>
</tr>
<tr>
<td>Multiple log destinations</td>
<td>YES</td>
<td>YES</td>
<td>Apache log4net</td>
<td>3.5.1 Configurat</td>
</tr>
<tr>
<td>Unique message ID</td>
<td>NO</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*This article pertains to MetaDefender Email Security v4.0.0 or above*

*This article was last updated on 2019-10-09*