## 2. Mail Proxy Deployment (Generic)

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Incoming Threat Protection</td>
<td>18</td>
</tr>
<tr>
<td>Installation</td>
<td>18</td>
</tr>
<tr>
<td>Configure Routing &amp; Connect to E-mail gateway</td>
<td>19</td>
</tr>
<tr>
<td>Verify Settings</td>
<td>21</td>
</tr>
<tr>
<td>Configuring Outgoing Threat Protection</td>
<td>23</td>
</tr>
<tr>
<td>Installation</td>
<td>23</td>
</tr>
<tr>
<td>Configure Routing &amp; Connect to E-mail gateway</td>
<td>24</td>
</tr>
<tr>
<td>Verify Settings</td>
<td>26</td>
</tr>
<tr>
<td>Configuring Recipient Verification</td>
<td>27</td>
</tr>
<tr>
<td>Reject emails not bound for local domain(s)</td>
<td>27</td>
</tr>
<tr>
<td>Verify Settings</td>
<td>28</td>
</tr>
<tr>
<td>TLS support (Incoming/Outgoing emails)</td>
<td>29</td>
</tr>
<tr>
<td>Prerequisite</td>
<td>29</td>
</tr>
<tr>
<td>Incoming TLS support</td>
<td>29</td>
</tr>
<tr>
<td>Outgoing TLS support</td>
<td>32</td>
</tr>
<tr>
<td>Export a certificate</td>
<td>33</td>
</tr>
</tbody>
</table>

## 3. Cloud Deployment

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>38</td>
</tr>
<tr>
<td>Steps</td>
<td>38</td>
</tr>
<tr>
<td>Limitation</td>
<td>38</td>
</tr>
<tr>
<td>Google Apps integration</td>
<td>38</td>
</tr>
<tr>
<td>Overview</td>
<td>38</td>
</tr>
<tr>
<td>Detailed Steps</td>
<td>38</td>
</tr>
<tr>
<td>Microsoft Office 365 Integration</td>
<td>45</td>
</tr>
<tr>
<td>Overview</td>
<td>45</td>
</tr>
<tr>
<td>Detailed Steps</td>
<td>45</td>
</tr>
</tbody>
</table>

## 4. Onsite Microsoft Exchange Deployment

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>How To Verify</td>
<td>52</td>
</tr>
<tr>
<td>How To Verify</td>
<td>53</td>
</tr>
</tbody>
</table>
5. Notification and Report

Available Notification / Report 54
Email Server For Notification 54
Customizing Disclaimers 55
Error Email Notification 55
  Description 55
  Location 55
  Run 55
  Troubleshooting 57
  Mail Agent Alerts 58
Infection Email Notification 59
Mail Agent Error Codes 60
  Log level 60
  Error Codes 60
Quarantine Reports 71
Sanitized Email Notifications 72

6. Additional Configuration

Advanced Configuration 73
  Configuration From Config File 73
  Custom Email Headers 89
  Enable Sender Policy Framework (SPF) Lookup 91
  Log collection (collectLogs.exe) 92
  Log options 93
  Multiple Metadefender Core Instances Configuration 95
Email Processing Workflow (Metadefender Core) 96
  Email Processing 96
  Metadefender Mail Workflow 96
  Modify Metadefender Core URL 97
Quarantine Email 98
  Quarantine Email On Another Mail Server 98
Skip Email Analysis 101
  Configuration 101
7. Release Notes

Other changes

Archive Release Notes

Version 3.12.5
Version 3.13.0
Version 3.14.0
Version 3.14.1
Version 3.14.2
Version 3.14.3
Version 3.14.4
Version 3.14.5
Version 3.14.6
Version 3.14.7

General and Known Issues

Limitation

Limitation for Onsite Microsoft Exchange Deployment

8. Legal

Copyright

DISCLAIMER OF WARRANTY
COPYRIGHT NOTICE

Export Classification EAR99
Second Layer of Defense for Your Email Security Gateway

Email security gateways, although offering tremendous protection, are not perfect. Metadefender Email 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 data sanitization to combat increasingly popular document-based or image-based attacks.
Key Features

- Prevent with email sanitization using 90 data sanitization engines
- 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
- RealTime Monitoring threats
- RealTime Alert / Monitoring
- Schedule Report
- High performance
- Quarantine detected/sanitized Email
Deployment Options

Mail Proxy Deployment (Generic)

Email Proxy between Mail Gateway (anti-spam) and Mail Server

Cloud Deployment

For hosted solution such as Office 365 and G Suite (formerly Google Apps for Work) Gmail
Onsite Microsoft Exchange Deployment

Metadefender Scans External and Internal Email Traffic

Use with your existing onsite MS Exchange Server

Metadefender Email Security

MS Exchange Server
If you are using Metadefender Email as mail proxy

Metadefender does not incorporate/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. Before Installation

Use of Metadefender Email Security with Metadefender Core beyond the fifteen (15) day evaluation period requires purchase of two licenses, one license for Metadefender Core and a separate license for Metadefender Email Security.

Metadefender Email provides multiple deployment options as described in this documentation. If you need additional information in selecting the optimal deployment option, OPSWAT Technical Support is available to assist. Metadefender Email's performance and capacity vary depending on the specifications of the system hosting Metadefender Email. Increasing the resources available to the Metadefender Email system will likely increase the performance of the Metadefender Email system, however this is not guaranteed.

Increase Capacity and Resiliency

Single Server Capacity

<table>
<thead>
<tr>
<th>System Profile</th>
<th>Email Consists of</th>
<th>Throughput</th>
<th>CPU usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 4 Core Processor</td>
<td>• 30% of emails with no attachment</td>
<td>300 emails / minute</td>
<td>50-100%</td>
</tr>
<tr>
<td>• 16 GB RAM</td>
<td>• 40% of emails with single attachment (sanitization is not enabled)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• 64 bit OS</td>
<td>• 12.5% of emails has PDF* attachment (sanitization is enabled)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Metadefender Core 20</td>
<td>• 12.5% of emails has DOCX* attachment (sanitization is enabled)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5% of emails has JPG* attachment (sanitization is enabled)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Files that we used for testing have the following sizes. The result may vary depending on data set you select. We strongly recommend to conduct testing based on your organization email statistics. If you need assistance on the tools for testing, contact OPSWAT support.

• DOCX: 220 KB
• PDF: 8 KB
Load Balancing Metadefender Email

For Mail Proxy and Hosted deployment, this is desired configuration to increase the resilience and performance.

In order to achieve 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).

Load Balancing (remote) Metadefender Core

This is mainly for onsite exchange deployment scenario. See Multiple Metadefender Core Instances Configuration for further instructions.

Sizing Examples

The following displays two examples in the real production environment. This will provide reference to your sizing and choice of Metadefender package. Neither of the two organizations in the examples experienced latency (more than 100 emails pending for process) in production.

<table>
<thead>
<tr>
<th></th>
<th>Number of mail box</th>
<th>Number of emails / day</th>
<th>Metadefender Package</th>
<th>Instances</th>
<th>Hardware Specification</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>organization A</td>
<td>5,000</td>
<td>35,000 emails</td>
<td>Metadefender v3 core 20</td>
<td>2</td>
<td>4 CPU cores, 24GB, 140GB disk space</td>
<td>Windows Server 2012 R2 Standard 64</td>
</tr>
<tr>
<td>organization B</td>
<td>200</td>
<td>10,000 emails</td>
<td>Metadefender v3 core 20</td>
<td>2</td>
<td>4 CPU cores, 16GB, 100GB disk space</td>
<td>Windows Server 2012 R2 Standard 64</td>
</tr>
</tbody>
</table>
System Requirements

⚠️ The following does not include the system requirement for Metadefender Core if installed on the same system.

**Hardware requirements**
- System RAM: 2 GB
- Free Hard Drive Space: 16GB
- CPU: 4 core

**Software requirements**
- Bitness: 64-bit only
- (Optional) 32-bit OpenSSL if using TLS encryption

**Additional installation of 3rd party framework/components**

<table>
<thead>
<tr>
<th>Name</th>
<th>Details</th>
<th>Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NET framework</td>
<td>4 Client Profile Extended</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>Metadefender Generic Mail Agent</td>
<td>mdfExgEmailAgent</td>
<td>by default</td>
</tr>
</tbody>
</table>
Ports that must be available

<table>
<thead>
<tr>
<th>in/out</th>
<th>component /service</th>
<th>port</th>
<th>note</th>
</tr>
</thead>
<tbody>
<tr>
<td>inbound</td>
<td>Mail Agent Service</td>
<td>10025</td>
<td>this is customizable so adjust accordingly if modified</td>
</tr>
<tr>
<td>outbound</td>
<td>Metadefender Core</td>
<td>8008</td>
<td>only if Metadefender Core is installed on a remote system.</td>
</tr>
<tr>
<td>outbound</td>
<td>Metadefender Quarantine</td>
<td>8000</td>
<td>only if Quarantine (contained in Metadefender Core) is installed on a remote system.</td>
</tr>
</tbody>
</table>

Exchange Mail Agent Supportability Matrix

Overview

This page describes the supported operating systems and Microsoft Exchange version for installing Metadefender Mail Agent for 4. 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 Mail Agent 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>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange 2007 Service Pack 3</td>
<td>✗</td>
<td>✅</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Exchange 2010 Service Pack 3</td>
<td>✗</td>
<td>✅</td>
<td>✅</td>
<td>✗</td>
</tr>
</tbody>
</table>
Testing Tool For Sending Email

Bulwarx Email client tester

The tool provides intuitive 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 and port (10025 is default port).
4. Fill out sender and recipient email address along with subject.
5. Choose either html or plan text for message format.
   a. If you choose html: MailTemplate.html will be loaded to email.
   b. If you choose text, MailTemplate.txt will be loaded to email.
   c. If you choose combine, 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 if attachment is clean.
- If email is blocked and quarantined on Metadefender if attachment is blocked by Metadefender.
- If email is sanitized and original copy of email is quarantined on Metadefender if email is sanitized.
- Administrator is getting alert for blocked email.
User is getting alert for blocked email.

**Who is 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. Mail Proxy Deployment (Generic)

Email Proxy between Mail Gateway (anti-spam) and Mail Server

Configuring Incoming Threat Protection

In order to install and configure Metadefender Email incoming threat protection, you must first install Metadefender Email and then configure the routing of the incoming threat protection, verify the routing settings, and then connect to your e-mail gateway.

Installation

Generate Metadefender Email installer package from Metadefender Core Management console. "Source">"Metadefender Email" > "Setup" page, choose "Generic / Cloud Agent". Download the Metadefender Email installer, copy it to where you want to install it, and follow the installation wizard to finish installation.
If you get Metadefender Email installer from OPSWAT portal or another source other than the Metadefender Core server you want it to process with, run the installation by opening a command prompt and type the following command:

```bash
MetadefenderEmailAgent.exe METASCANAPIKEY=<Mail Agent installer ID> METASCANURL=http://<Metadefender Core IP address>:8008/metascan_rest [ENTER]
```

Notes:

- Replace `<Mail Agent installer ID>` with the ID shown on Metadefender Core management console source page under Email setup section.
- Note: Replace `<Mail Agent installer ID>` with the ID shown on Metadefender Core management console source page under Email setup section.
- Replace `<Metadefender Core IP address>` with the IP address or hostname of the machine where you have installed Metadefender Core.
- Metadefender Email will automatically detect if Exchange Server is installed or not and install the appropriate edition (Proxy/Exchange)

**Configure Routing & Connect to E-mail gateway**

In this section, you will connect Metadefender Email to your mail server & e-mail gateway.

1. Open the Metadefender Core Management Console.
2. Select **Sources > Metadefender Email > Setup**.
3. Click **Setup** on the newly installed Metadefender Email instance.
4. In the Email Relay Out Server field, specify the IP address (or name) of your mail server and the SMTP protocol port that the mail server is listening on (usually port 25).

5. In the Email Direction field, select **Incoming**.

**Generic on Server**

**Step 1 - Connect Metadefender Email to Mail Server**

- **Email Relay Out Server**: mailserver : 25
- **Email Direction**: Incoming, Outgoing

**Step 2 - Connect Email Gateway to Metadefender Email**

On the email gateway machine, forward emails to: **SERVER:10025**
6. Configure your **3rd party e-mail gateway** to forward all e-mails to the server:port specified in the dialog.

   **Note:** By default, Metadefender Email listens on SMTP port 10025. Make sure that your firewall allows traffic on the port used by the Mail Agent. You might need to open port 10025 in Windows Firewall.

   **Generic on Server**

   **Step 1 - Connect Metadefender Email to Mail Server**
   - Email Relay Out Server: mailserver
   - Port: 25
   - Email Direction: 
     - Incoming
     - Outgoing

   **Step 2 - Connect E-mail Gateway to Metadefender Email**
   On the email gateway machine, forward emails to: **SERVER:10025**

   ![Apply and Cancel buttons]

7. Click **Apply** to save your changes.

   **Verify Settings**

   In this section, you will verify your configuration settings and confirm that Metadefender Email works as expected.

   1. Open the Metadefender Core Management Console.
   2. Select **Sources > Metadefender Email > Setup**.
   3. Click **Verify** on the newly configured Metadefender Email instance.
4. Select **Incoming** as verification type and specify an **external e-mail address as sender** and a **local mailbox as recipient**.

**Generic on Server**

**Verification Type**
- [ ] Incoming
- [ ] Recipient Verification

**Verification Input**
- **Sender e-mail address**: external@gmail.com
- **Recipient e-mail address**: local@company.com

5. **Click Verify** to perform the test. If the test is successful, Metadefender Email is configured correctly.

6. Optionally, manually send an e-mail from an external source to a local mailbox to verify that email routing from the gateway to Metadefender Email is configured correctly.

7. Go to the Metadefender Core Management Console Dashboard and verify that the e-mail has been scanned.
Configuring Outgoing Threat Protection

In order to install and configure Metadefender Email outgoing threat protection, you must first install Metadefender Email and then configure the routing of the outgoing threat protection, verify the routing settings, and then connect your mail server to Metadefender Email.

Installation

Generate Metadefender Email installer package from Metadefender Core Management console. "Source">"Metadefender Email" > "Setup" page, choose "Generic / Cloud Agent". Download the Metadefender Email installer, copy it to where you want to install it, and follow the installation wizard to finish installation.

If you get Metadefender Email installer from OPSWAT portal or another source other than the Metadefender Core server you want it to process with, run the installation by opening a command prompt and type the following command:

```
MetadefenderEmailAgent.exe METASCANAPIKEY=<Mail Agent installer ID> METASCANURL=http://<Metadefender Core IP address>:8008/metascan_rest [ENTER]
```

Notes:
- Replace `<Mail Agent installer ID>` with the ID shown on Metadefender Core management console source page under Email setup section.
• Replace `<Metadefender Core IP address>` with the IP address or hostname of the machine where you have installed Metadefender Core.

• Metadefender Email will automatically detect if Exchange Server is installed or not and install the appropriate edition (Proxy/Exchange)

**Configure Routing & Connect to E-mail gateway**

In this section, you will connect Metadefender Email to your mail server.

1. Open the Metadefender Core Management Console.
2. Select **Sources > Metadefender Email > Setup**.
3. Click **Setup** on the newly installed Metadefender Email instance.

4. In the Email Relay Out Server field, specify the **IP address (or name)** of your outbound 3rd party gateway and the SMTP protocol port that the gateway is listening on (usually port 25).
5. In the Email Direction field, select **Outgoing**.

**Generic on Server**

**Step 1 - Connect Metadefender Email to Mail Server**

- Email Relay Out Server: mailserver: 25
- Email Direction: Incoming, Outgoing

**Step 2 - Connect Email Gateway to Metadefender Email**

On the email gateway machine, forward emails to **SERVER:10025**

- **APPLY**
- **CANCEL**

6. **Configure your mail server** to forward all e-mails to the server:port specified in the dialog. **Note:** By default, Metadefender Email listens on SMTP port 10025. Make sure that your firewall allows traffic on the port used by the Mail Agent. You might need to open port 10025 in Windows Firewall.

**Generic on Server**

**Step 1 - Connect Metadefender Email to Mail Server**

- Email Relay Out Server: mailserver: 25
- Email Direction: Incoming, Outgoing

**Step 2 - Connect Email Gateway to Metadefender Email**

On the email gateway machine, forward emails to **SERVER:10025**

- **APPLY**
- **CANCEL**

7. **Click Apply** to save your changes.
Verify Settings

In this section, you will verify your configuration settings and confirm that Metadefender Email works as expected.

1. Open the Metadefender Core Management Console.
2. Select Sources > Metadefender Email > Setup.
3. Click Verify on the newly configured Metadefender Email instance.
4. Select Outgoing as verification type and specify an local mailbox as sender and an external e-mail address as recipient.

Generic on Server

Verification Type
- Outgoing
- Recipient Verification

Verification Input
- Sender e-mail address: local@company.com
- Recipient e-mail address: external@gmail.com

[VERIFY] [CLOSE]
5. Click **Verify** to perform the test. If the test is successful, Metadefender Email is configured correctly.

6. Optionally, manually send an e-mail from a local mailbox to an external source to verify that email routing from the Mail Server to Metadefender Email is configured correctly.

7. Go to the Metadefender Core Management Console Dashboard and verify that the e-mail has been scanned.

### Configuring Recipient Verification

The Generic Mail Agent is capable of performing basic recipient verification on the incoming emails in order to ensure that emails not bound for a specific domain or containing illegal characters do not enter the system. By default, recipient verification is enabled but no domains are configured so every domain will be considered an accepted domain. If recipient verification fails the email will not enter the system.

**Reject emails not bound for local domain(s)**

In order to discard emails that are not addressed to recipients in your domain(s) you need to configure Mail Agent by specifying a list of local domains that are accepted.

1. Go to the installation folder (by default C:\Program Files (x86)\OPSWAT\Metadefender Core <engine count>\Metadefender Mail Agent)

2. Open as administrator the file Metadefender.Email.Engine.Generic.Agent.dll.config for editing

3. Add a comma (,) separated list of local domains as value for the setting called **EmailRelayInLocalDomains**

```xml
<setting name="EmailRelayInLocalDomains" serializeAs="String">
  <value>opswat.com,metadefender.com</value>
</setting>
```

Note: by default the value is (*) which means all domains are accepted.

Note: Multiple domains are separated with a comma (,) character. It is possible to prefix the domain name with an * to accept sub domains. For example: *opswat.com will accept both opswat.com & subdomain.opswat.com.

4. Save the file.
Verify Settings

In this section, you will verify your recipient verification settings work as expected.

1. Open the Metadefender Core Management Console.

2. Select **Sources > Metadefender Email > Setup**.

3. Click **Verify** on the newly configured Metadefender Email instance.

4. Select **Recipient Verification** as verification type and specify an **an external e-mail address as sender**, a **local mailbox as valid recipient e-mail address** and an **invalid (unwanted) e-mail address as Invalid recipient address**.
5. Click **Apply** to perform the test. If the test is successful, recipient verification is configured correctly.

6. Optionally, manually send an e-mail from an external source to a local mailbox to verify that recipient verification is working as expected.

**TLS support (Incoming/Outgoing emails)**

Metadefender Email can both receive and send emails using TLS encryption for increased security. Refer to the sections below to enable TLS for incoming and/or outgoing emails.

**Prerequisite**

- OpenSSL 32-bit

**Incoming TLS support**

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

**I have a pcks#12 certificate:**

For these steps you will need a pcks#12 certificate (.pfx).
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 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 Mail Agent folder (default: C:\Program Files (x86)\OPSWAT\Metadefender Mail Agent)

3. Type the following command:

   ```
   enableTls.exe -i -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 TLS settings automatically updated:

   ```
   C:\Program Files (x86)\OPSWAT\Metadefender Mail Agent>enableTls.exe -i -b "<path to .pfx>" -j "<certificate password>"
   Reading Mail Agent settings...
   Updating settings...
   Mail Agent   settings updated successfully
   ```

Metadefender Email will now accept TLS encryption when receiving emails.

I have a pcks#8 certificate:

For these steps you will need a certificate file and a private key file (pcks#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 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 Mail Agent folder (default: C:\Program Files (x86)\OPSWAT\Metadefender Mail Agent)

3. Type the following command:

```
enableTls.exe -i -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 and private key and imported and TLS settings automatically updated:

```
C:\Program Files (x86)\OPSWAT\Metadefender Mail
Agent>enableTls.exe -i -y "<path to certificate file>" -z
"<path to private key file>"
Reading Mail Agent settings...
Updating settings...
Mail Agent settings updated successfully
```

Metadefender Email will now accept TLS encryption when receiving emails.

**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](https://slproweb.com/products/Win32OpenSSL.html) (unofficial distribution)

   Note: Metadefender Email 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 Mail Agent folder (default: C:\Program Files (x86)\OPSWAT\Metadefender Mail Agent)

3. Type the following command:

```
enableTls.exe -i -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)
A new certificate is generated and TLS settings automatically updated:

```bash
C:\Program Files (x86)\OPSWAT\Metadefender Mail Agent>enableTls.exe -i -e -d 365
-c US -s "California" -l "San Francisco" -o "Company"
Reading Mail Agent settings...
Generating a 4096 bit RSA private key

writing new private key to 'tls_key.pem'

-----

Updating settings...
Mail Agent settings updated successfully
```

Metadefender Email will now accept TLS encryption when receiving emails.

**Outgoing TLS support**

To enable outgoing TLS encryption, do the following:

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 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 Mail Agent folder (default: C:\Program Files (x86)\OPSWAT\Metadefender Mail Agent)

3. Type the following command:

   ```bash
   enableTls.exe -g -r "<mail_server>" -m 587 -q "<username>" -w "<password>"
   ```

   Replace any of the following parameters with desired values:

   - `-r = Email relay out SMTP server name`
   - `-m = Email relay out SMTP server port`
-q = Email relay out SMTP authentication user name. (Omit if no authentication is used)
-w = Email relay out SMTP authentication password. (Omit if no authentication is used)

4. TLS settings are automatically updated:

```
C:\Program Files (x86)\OPSWAT\Metadefender Mail
Agent>enableTls.exe -g
Reading Mail Agent settings...
Updating settings...
Mail Agent settings updated successfully
```

Metadefender Email will now use TLS when forwarding emails to your mailserver /gateway.

To enable both incoming and outgoing TLS, the parameters should be combined, for example:

```
enableTls.exe -i -b "<path to .pfx>" -j "<certificate password>" -g -r "<mail_server> -m 587 -q "<username>" -w "<password>"
```

For a complete list of available command line parameters, type: enableTls.exe -h

**Export a certificate**

If you have an existing certificate in your certificate store that you want to use with Metadefender Email 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.
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.
h. Select 'Yes, export the private key' and click 'Next >'.

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

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

j. Specify a certificate password and click 'Next >'.
k. Specify a file name for the exported certificate and click 'Next >'.

l. Click 'Finish' to complete the export.
m. A dialog will display that export was successful.

Once the export is complete, refer to TLS support (Incoming/Outgoing emails) for instructions how to install the certificate in Metadefender Email.
3. Cloud Deployment

Overview

For hosted solution such as Office 365 and G Suite (formerly Google Apps for Work) Gmail

Steps

1. Configure the hosted email server to accept email from Metadefender Email server.
2. Configure Metadefender Email to relay out to hosted email server and use port 25.
3. Update MX record to point to Metadefender Email server.

Limitation

- SPF enforcement will be skipped on the hosted email server

Google Apps integration

Overview

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

**Step 1.1**
Go to [https://admin.google.com](https://admin.google.com) and login to your Google Apps subscription.

**Step 1.2**
Click 'MORE CONTROLS'.

**Step 1.3**
Click 'Apps'.
Step 1.4
Click 'Google Apps'.

Step 1.5
Click 'Gmail'.
Step 1.6

Click 'Advanced settings'.
Step 1.7  
Scroll down to the 'Inbound gateway' section and click 'CONFIGURE'.

Step 1.8  
Specify a gateway name (Metadefender Email Relay) and the IP address of the Metadefender Email server. Check 'Automatically detect external IP (recommended)', 'Reject all mail not from gateway IPs' and 'Require TLS connection from the email gateways listed above'. 
Step 1.9
Click 'SAVE' at the bottom right of the screen to save the changes.

Step 2.1
Connect to the Mail agent server and run the following REST POST request (using, for example, POSTMAN) to http://localhost:8000/MailAgent/Settings

```json
{
    "EmailRelayInDirection": 0,
    "EmailRelayInLocalDomains": [],
    "EmailRelayInPort": 25,
    "EmailRelayOutPassword": null,
    "EmailRelayOutPort": 25,
    "EmailRelayOutServer": "alt1.aspmx.l.google.com",
    "EmailRelayOutUseTls": true,
    "EmailRelayOutUsername": null
}
```
Step 2.2
 Verify routing settings by sending an email to a Google Apps recipient directly to the Metadefender Email server and verify that it arrives correctly in the recipient inbox.

Step 3.1
 Refer to your Internet domain registrar for details how to change MX record to point to Metadefender Email IP address. Verify email routing by sending an email to a Google Apps recipient.

⚠️ Make sure that your MX record changes have propagated before verifying email routing.

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
Microsoft Office 365 Integration

Overview

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

Detailed Steps

Configure the hosted email server to accept email from Metadefender Email server

2. Go to Office 365 Portal > Admin > Admin Centers > Exchange. Once the Exchange Admin has opened, go to mail flow > connectors and click + to add a new connector.
3. Select From: Partner organization and To: Office 365, then click Next
4. Specify a name for the connector (in this case Metadefender Email) and ensure that the option ‘Turn it on’ is checked. Then click Next.

5. Select 'Use the sender’s domain' and click Next.
6. Click on the +.

7. Enter * as domain and click OK. Then click Next.
8. 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 +
9. Specify your public IP address (in this case (213.149.186.214) and click OK. Then click Next.

10. Verify connector properties and click Save to save the connector.
Configure Metadefender Email to relay out to hosted email server.

1. Obtain your MX record address by going to https://portal.office.com > Admin > Settings > Domain and click on your domain. Copy the MX Record value to the clipboard.

2. Connect to the Mail agent server and run the following REST POST request (using, for example, POSTMAN) to http://localhost:8000/MailAgent/Settings. Specify the MX record address obtained in the previous step and enter it in the EmailRelayOutServer value:

   ```json
   {
     "EmailRelayInDirection": 0,
     "EmailRelayInLocalDomains": [],
     "EmailRelayInPort": 25,
     "EmailRelayOutPassword": null,
     "EmailRelayOutPort": 25,
     "EmailRelayOutServer": "<MX record address>",
     "EmailRelayOutUseTls": true,
     "EmailRelayOutUsername": null
   }
   ```

3. Verify routing settings by sending an email to a Office365 recipient directly to the Metadefender Email server and verify that it arrives correctly in the recipient inbox.
Update MX record to point to Metadefender Email server.

Refer to your Internet domain registrar for the details how to change MX record to point to Metadefender Email IP address. Verify email routing by sending an email to a Office365 recipient.

⚠️ Make sure that your MX record changes have propagated before verifying email routing.
4. Onsite Microsoft Exchange Deployment

- Metadefender Email can only be installed on Hub or Edge role Exchange Servers (2007, 2010, 2013 or 2016).
- Metadefender Core must be installed on separate machine than the Exchange Server.

Installation

Generate Metadefender Email installer package from Metadefender Core Management console. Go to "Source"->"Metadefender Email" > "Setup" page, choose "Exchange Agent". Download the Metadefender Email installer, copy it to the Exchange server, and follow the installation wizard to finish installation.

If you get Metadefender Email installer from OPSWAT portal or another source other than the Metadefender Core server you want it to process with, run the installation by opening a command prompt and type the following command:
MetadefenderEmailAgent.exe METASCANAPIKEY=<Mail Agent installer ID> METASCANURL=http://<Metadefender Core IP address>:8008/metascan_rest [ENTER]

Notes:

- Replace `<Mail Agent installer ID>` with the ID shown on Metadefender Core management console source page under Email setup section.
- Replace `<Metadefender Core IP address>` with the IP address or hostname of the machine where you have installed Metadefender Core.
- Metadefender Email will automatically detect if Exchange Server is installed or not and install the appropriate edition (Proxy/Exchange)

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 'OPSWAT Metadefender' is listed and its enabled state is 'True'

```
[PS] C:\Windows\system32>Get-TransportAgent

Identity                        Enabled   Priority
--------                        -------   --------
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
OPSWAT Metadefender             True     8
```
5. Notification and Report

Available Notification / Report

- Infection Email Notification
- Sanitized Email Notifications
- Quarantine Reports

Email Server For Notification

1. In the Metadefender Core Management Console, go to Sources > Metadefender Email > Settings

2. If you have already configured the SMTP settings and the Status is connected, skip to step 3.
   a. Click Update.
   b. In the Host field, specify the IP address or name of your mail server. **Note:** You may also use an alternative mail server to deliver reports and notifications. To do this, replace the Host value with your alternative mail server address and specify Port, SSL, Username and Password settings as required for the alternative mail server.
   c. Click Save.
   d. SMTP connection will be validated and the status is updated to **Connected** if connection is established successfully.
### Customizing Disclaimers

Currently customizing disclaimers are only supported using script or tools. Please contact OPSWAT support to obtain the instructions and tools.

### Error Email Notification

**Description**

Metadefender Email can send a notification to the Administrator if unexpected events occur, such as loss of connection to Metadefender Core, Mail Sever/Gateway or queue build ups.

For a complete list of notifications please see [Mail Agent Alerts](#).

**Location**

The tool is called `configNotification.exe` and is shipped with the installer.

The default location will be `C:\Program Files (x86)\OPSWAT\Metadefender Core <x>\Metascan Quarantine`

**Run**

If you run `configNotification.exe -h` you will be able to see the help info:

```bash
configNotification.exe -h
Usage: configNotification.exe [OPTIONS]
Example: configNotification.exe -t All -s administrator@opswat.local -r administrator@opswat.local --orgRecipients --debug
```
Options:

- \texttt{-t, --type=NOTIFICATION TYPE} \\
  \texttt{[REQUIRED]} the NOTIFICATION TYPE you wish to change \\
  Possible values:
  All \rightarrow \text{Enables all notifications (errors, blocked, sanitized, quarantined)}
  QuarantinedEmail \rightarrow \text{Enables the notification which is triggered when an email is sent to Quarantine}
  QuarantinedFile \rightarrow \text{Enables the notification which is triggered when a file is sent to Quarantine}
  Blocked \rightarrow \text{Enables the notification which is triggered when an email is blocked by Mail Agent}
  Sanitized \rightarrow \text{Enables the notification which is triggered when an email is sanitized by Mail Agent}
  OnlyErrors \rightarrow \text{Enables the error notifications}
  NonErrors \rightarrow \text{Enables the non-error notifications (blocked, sanitized, quarantined)}

- \texttt{-s, --sender=SENDER EMAIL} \\
  \texttt{[REQUIRED]} the SENDER EMAIL from where the notification(s) will be sent

- \texttt{-r, --recipients=RECIPIENT EMAIL(S)} \\
  \texttt{[REQUIRED]} if notification type is All/OnlyErrors otherwise \texttt{[OPTIONAL]} \\
  The RECIPIENT EMAIL(S) where to send the notification(s) \\
  For non-errors email notifications, when this parameter is not set, the notification will be sent to both original sender and recipient(s) \\
  Note: multiple email addresses can be separated by comma

- \texttt{--orgSender} \\
  \texttt{[OPTIONAL]} applicable only to non-errors notifications \\
  If this option is set the notification will be sent to the original sender of the email that triggered the notification

- \texttt{--orgRecipients} \\
  \texttt{[OPTIONAL]} applicable only to non-errors notifications \\
  If this option is set the notification will be sent to the original recipient(s) of the email that triggered the notification

- \texttt{-u, --url=ENDPOINT} \\
  \texttt{[OPTIONAL]} the url ENDPOINT where Quarantine is located \\
  if it is not on the same machine

- \texttt{--https}
If you run the tool on the machine where Mail Agent is installed and HTTPS is not enabled

```
configNotification.exe -t OnlyErrors -s administrator@opswat.local -r administrator@opswat.local
```

If you run the tool on the machine where Mail Agent is installed and HTTPS is enabled

```
configNotification.exe -t OnlyErrors -s administrator@opswat.local -r administrator@opswat.local -https
```

If you don't run the tool on the machine where Mail Agent is installed

```
configNotification.exe --t OnlyErrors -s administrator@opswat.local -r administrator@opswat.local -u http://<mail_agent_ip>:8000/Quarantine/EmailAlerts
```

Troubleshooting
If you encounter any problems running the tool, please run with "-d" option so you can get debugging information:

```
configNotification.exe -t OnlyErrors -s administrator@opswat.local -r administrator@opswat.local -d
```

Example, if the problem is an invalid email address:

```
configNotification.exe -s this.isnot.valid -d
```
There was a problem updating email alerts: Invalid email address. You need to specify a valid email. System.Exception: Invalid email address. You need to specify a valid email.

This information will help us further investigate the problem.

**Mail Agent Alerts**

Mail Agent has a built-in monitoring system that is used to alert the administrator in certain circumstances. Below is a list of alerts.

**Metadefender Core down/not responding alert**

When Metadefender Core cannot be contacted (either on Mail Agent service startup or each time a scan is performed) the 'ErrorMetascanDownTemplate' will be sent.

> This alert can potentially be sent more than once an hour. During a continuous failure, the notification will be sent maximum once an hour, but if MD Core starts to respond again, this span is reset and a notification will be sent as soon as a connection failure occurs again.

**Generic Agent: Email relay server down alert**

A connectivity check is done by connecting to the remote (relay) server. When the SMTP service cannot be contacted the 'ErrorEmailRelayServerDownTemplate' will be sent.

> This alert can potentially be sent more than once an hour. During a continuous failure, the notification will be sent maximum once an hour, but if the email relay server starts to respond again, this span is reset and a notification will be sent as soon as a connection failure occurs again.

**Generic Agent: Inbound queue alert**

The Generic Mail Agent In folder (C:\Program Files (x86)\OPSWAT\Metadefender Core <engine count>\Metadefender Mail Agent\GenericAgent\In) is monitored. When the number of envelope files exceed the threshold set in Metadefender.Email.Engine.Generic.Agent.dll.config > EmailRelayInQueueThreshold (default 100) the 'ErrorInboundQueueThresholdTemplate' will be sent.
**Generic Agent: Outbound queue alert**

The Generic Mail Agent Out folder (C:\Program Files (x86)\OPSWAT\Metadefender Core <engine count>\Metadefender Mail Agent\GenericAgent\Out) is monitored. When the number of .envelope files exceed the threshold set in Metadefender.Email.Engine.Generic.Agent.dll.config > EmailRelayOutQueueThreshold (default 100) the ‘ErrorOutboundQueueThresholdTemplate’ will be sent.

**Generic Agent: Emails rejected by email relay server alert**

The Generic Mail Agent Out folder (C:\Program Files (x86)\OPSWAT\Metadefender Core <engine count>\Metadefender Mail Agent\GenericAgent\Out) is monitored for .bad files. These are files that have been rejected one or more times by the relay server, but not yet moved to permanent failed. When the number of .bad files exceed the threshold set in Metadefender.Email.Engine.Generic.Agent.dll.config > EmailRelayOutQueueBadThreshold (default 10) the ‘ErrorOutboundQueueBadThresholdTemplate’ will be sent.

**Generic Agent: Emails in permanent failure alert**

The Generic Mail Agent Permanent Failure folder (C:\Program Files (x86)\OPSWAT\Metadefender Core <engine count>\Metadefender Mail Agent\GenericAgent\Permanent Failure) is monitored for .envelope files. These are files that have been rejected by the email relay server repeatedly and cannot be delivered. When the number of .envelope files exceed the threshold set in Metadefender.Email.Engine.Generic.Agent.dll.config > EmailRelayOutPermanentFailureThreshold (default 1) the ‘ErrorOutboundQueuePermanentFailureThresholdTemplate’ will be sent.

**Infection Email Notification**

To send email notifications when an infected email is detected, move the On/Off slider to on, and specify a Sender email address, and modify subject and body as desired.

Notification email will be sent to the sender or recipient of the email with contents you configure on the following setting.
Mail Agent Error Codes

Below is a legend for all error codes in the Mail Agent. Refer to this lookup table when analyzing log files etc.

**Log level**

The numeric error code and optional message is written to the log file.

**Example log entry**


**Error Codes**

0x00001100

*Component code (01 - FFFFF)*

*Error type (1 = Error, 2 = Warning)*

*Error code (0-FF)*
<table>
<thead>
<tr>
<th>Component name</th>
<th>Component code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadefender.Scanner.dll</td>
<td>1</td>
</tr>
<tr>
<td>Metadefender.Email.Engine.Processor.dll</td>
<td>2</td>
</tr>
<tr>
<td>Metadefender.Email.Engine.Service.exe</td>
<td>4</td>
</tr>
<tr>
<td>Metadefender.Engine.Common.dll</td>
<td>5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Error code</th>
<th>Numeric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_MAILAGENT_MDCORE_READ_EMAIL_SCAN_SETTINGS</td>
<td>0x00001100</td>
<td>Failed to read Email Scanner settings from database</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_UPDATE_EMAIL_SCAN_SETTINGS</td>
<td>0x00001101</td>
<td>Failed to update Email Scanner settings in database</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_READ_EMAIL_DISCLAIMER_SETTINGS</td>
<td>0x00001102</td>
<td>Failed to read Email Disclaimer settings from database</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_UPDATE_EMAIL_DISCLAIMER_SETTINGS</td>
<td>0x00001103</td>
<td>Failed to update Email Disclaimer settings in database</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_ADD_EMAIL_DISCLAIMER</td>
<td>0x00001104</td>
<td>Failed to add disclaimer to email message</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SCAN</td>
<td>0x00001105</td>
<td>Failed to scan email</td>
</tr>
</tbody>
</table>

0x00001106
<table>
<thead>
<tr>
<th>Error code</th>
<th>Numeric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR_MAILAGENT_MDCORE_SCAN_ATTACHMENT</td>
<td></td>
<td>Failed to scan email attachment</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SCAN_REQUEST</td>
<td>0x00001107</td>
<td>Failed to receive a response from a scan request/MD Core not responding</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SCAN_UNEXPECTED_JSON</td>
<td>0x00001108</td>
<td>Unexpected JSON in MD Core response</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SCAN_TIMEOUT</td>
<td>0x00001109</td>
<td>Timeout while waiting for MD Core response</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_LOOKUP_HASH</td>
<td>0x0000110A</td>
<td>Failed to lookup hash in MD Core/MD Core not responding</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SANITIZE_ATTACHMENT</td>
<td>0x0000110B</td>
<td>Failed to sanitize an attachment</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SANITIZE_ATTACHMENT_SERVER_RESPONSE</td>
<td>0x0000110C</td>
<td>Failed to sanitize an attachment (unexpected server response)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_REPLACE_SANITIZED_ATTACHMENT</td>
<td>0x0000110D</td>
<td>Failed to replace an attachment in email (during sanitization)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_REMOVE_BLOCKED_ATTACHMENT</td>
<td>0x0000110E</td>
<td>Failed to remove an attachment in the email (during sanitization/filtering)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SANITIZE_BODY</td>
<td>0x0000110F</td>
<td>Failed to sanitize message body</td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_UNKNOWN_BODY</td>
<td></td>
<td>Email has an unknown body type</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SANITIZE_BODY_SERVER</td>
<td>0x00001111</td>
<td>Metadefender Core server has failed to sanitize the body.</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_SCAN_BODY</td>
<td>0x00001112</td>
<td>Failed to scan a email body</td>
</tr>
<tr>
<td>ERR_MAILAGENT_MDCORE_ADD_EMAIL_SUBJECT_TAG</td>
<td>0x00001113</td>
<td>Failed to add a tag to the email subject</td>
</tr>
<tr>
<td>WARN_MAILAGENT_MDCORE_CREATE_PERFORMANCE_COUNTERS</td>
<td>0x00001200</td>
<td>Could not create performance counters at startup</td>
</tr>
<tr>
<td>WARN_MAILAGENT_MDCORE_READ_EMAIL_SCAN_SETTINGS</td>
<td>0x00001201</td>
<td>Failed to read Emai Scanner settings from database (attempting to use default settings)</td>
</tr>
<tr>
<td>WARN_MAILAGENT_MDCORE_READ_EMAIL_DISCLAIMER_SETTINGS</td>
<td>0x00001202</td>
<td>Failed to read Emai Disclaimer settings from database (attempting to use default settings)</td>
</tr>
<tr>
<td>WARN_MAILAGENT_MDCORE_SCAN_TIMEOUT</td>
<td>0x00001203</td>
<td>A scan timeout has occurred. Attempting next MD Core scanner (if available)</td>
</tr>
<tr>
<td>WARN_MAILAGENT_MDCORE_SANITIZE_ATTACHMENT</td>
<td>0x00001204</td>
<td></td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>----------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Failed to replace an attachment in email (during sanitization), will attempt to remove the attachment instead</td>
<td></td>
<td></td>
</tr>
<tr>
<td>WARN_MAILAGENT_MDCORE_NO_BODY</td>
<td>0x00001205</td>
<td>Email message has no body to be scanned</td>
</tr>
<tr>
<td>An error occurred while processing an email request (REST)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An error occurred while processing an email request</td>
<td>0x00002101</td>
<td></td>
</tr>
<tr>
<td>An error occurred while processing an agent request</td>
<td>0x00002102</td>
<td></td>
</tr>
<tr>
<td>An error occurred while processing an agent exists request (REST)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An error occurred while processing an agent enabled query request (REST)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>An error occurred while processing an agent enabled request (REST)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>An error occurred while processing an agent enable request (REST)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_REST_DISABLE</td>
<td>0x00002107</td>
<td>An error occurred while processing an agent disable request (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_REST_REGISTERED</td>
<td>0x00002108</td>
<td>An error occurred while processing an agent registration query request (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_REST_ADD</td>
<td>0x00002109</td>
<td>An error occurred while processing an agent add request (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_REST_REMOVE</td>
<td>0x0000210A</td>
<td>An error occurred while processing an agent remove request (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_REGISTER</td>
<td>0x0000210B</td>
<td>An error occurred while attempting to register an agent</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_UNREGISTER</td>
<td>0x0000210C</td>
<td>An error occurred while attempting to unregister an agent</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_SERVICE_STATUS</td>
<td>0x0000210D</td>
<td>An error occurred while attempting to change the agent service status</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_AGENT_STATUS</td>
<td>0x0000210E</td>
<td>An error occurred while attempting to change the agent status</td>
</tr>
<tr>
<td>0x0000210F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_CONFIG_REST_EXPORT</td>
<td></td>
<td>An error occurred while processing an configuration export request</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_CONFIG_REST_IMPORT</td>
<td>0x00002110</td>
<td>An error occurred while processing an configuration import request</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_PERFORM_ACTION</td>
<td>0x00002111</td>
<td>An error occurred while performing an action</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_HANDLE_REQUEST</td>
<td>0x00002112</td>
<td>An error occurred while processing a request (email)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_SPF_LOOKUP</td>
<td>0x00002113</td>
<td>An error occurred while performing an SPF lookup</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_QUARANTINE</td>
<td>0x00002114</td>
<td>An error occurred while moving an email to quarantine</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_QUARANTINE_COPY</td>
<td>0x00002115</td>
<td>An error occurred while moving a original copy of an email to quarantine</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_QUARANTINE_DUPLICATE_LIST</td>
<td>0x00002116</td>
<td>An error occurred while attempting to add the quarantine id to the processing duplicate list.</td>
</tr>
<tr>
<td>ERR_MAILAGENT_PROCESSOR_NOTIFICATIONS_VERIFY</td>
<td>0x00002117</td>
<td>An error occurred while attempting to check the status of a notification/alert.</td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>WARN_MAILAGENT_PROCESSOR_AGENT_READ_REGISTRATIONS</td>
<td>0x00002200</td>
<td>Failed to read agent registrations from MD Core. Using configuration files.</td>
</tr>
<tr>
<td>WARN_MAILAGENT_PROCESSOR_INVALID_XHEADER_NAME</td>
<td>0x00002201</td>
<td>The custom x-header contains one or more invalid characters and cannot be added.</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_PROCESS_REST_REQUEST</td>
<td>0x00003100</td>
<td>An error occurred while sending a process request (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_AGENT_REST_REQUEST</td>
<td>0x00003101</td>
<td>An error occurred while sending an agent request (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_AGENT_REST_STATUS</td>
<td>0x00003102</td>
<td>An error occurred while sending an agent status request (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_AGENT_PROCESS</td>
<td>0x00003103</td>
<td>An error occurred while sending an agent request</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_AGENT_PROCESS_RESULT</td>
<td>0x00003104</td>
<td>An error occurred while processing an agent request response</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_AGENT_RESULT</td>
<td>0x00003105</td>
<td>An error occurred while processing a process request response</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_DELETE_ENVELOPE_FILE</td>
<td>0x00003106</td>
<td>An error occurred while attempting to delete a processed .envelope file</td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_PARSE_RETRY_DATE</td>
<td>0x00003107</td>
<td>An error occurred while attempting to parse the retry date in an .envelope file</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_FAST_PROCESSING</td>
<td>0x00003108</td>
<td>An error occurred while attempting to fast process an email</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_MONITOR_INIT</td>
<td>0x00003109</td>
<td>An error occurred while initializing the generic agent file monitor</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_MONITOR_STOP</td>
<td>0x0000310A</td>
<td>An error occurred while stopping the generic agent file monitor</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_MONITOR_ERROR</td>
<td>0x0000310B</td>
<td>An error in the generic agent file monitor thread</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_MONITOR_DELETE_OBSOLETE_FILE</td>
<td>0x0000310C</td>
<td>An error occurred while attempting to delete an obsolete file</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_MONITOR_RETRY_PROCESS_BAD_FILE</td>
<td>0x0000310D</td>
<td>An error occurred while attempting to read a .bad file</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_MONITOR_RETRY_ERROR</td>
<td>0x0000310E</td>
<td>An error in the generic agent file monitor retry thread</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_MONITOR_REST_SETTINGS</td>
<td>0x0000310F</td>
<td>An error occurred while reading/writing generic mail agent settings (REST)</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_EMAILRELAY_START</td>
<td>0x00003110</td>
<td></td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-----------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_EMAILRELAY_DELETE_ORPHAN_FILE</td>
<td>0x00003111</td>
<td>An error occurred when attempting to start an emailrelay process</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_PROCESS_PREPARE</td>
<td>0x00003112</td>
<td>An error occurred while preparing a email processing request</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_TASK_ERROR</td>
<td>0x00003113</td>
<td>An error occurred in a task</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_WORKER_THREAD_ERROR</td>
<td>0x00003114</td>
<td>An error occurred in a agent worker thread</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_WORKER_THREAD_DELETE_FILE</td>
<td>0x00003115</td>
<td>An error occurred while attempting to delete a file</td>
</tr>
<tr>
<td>ERR_MAILAGENT_AGENT_WORKER_THREAD_CREATE_FILE</td>
<td>0x00003116</td>
<td>An error occurred while attempting to create a file</td>
</tr>
<tr>
<td>WARN_MAILAGENT_AGENT_MONITOR_JOIN_THREAD</td>
<td>0x00003200</td>
<td>Timeout while joining threads when shutting down</td>
</tr>
<tr>
<td>WARN_MAILAGENT_AGENT_CREATE_PERFORMANCE_COUNTERS</td>
<td>0x00003201</td>
<td>Failed to create performance counters</td>
</tr>
<tr>
<td>WARN_MAILAGENT_AGENT_EMAILRELAY_KILL</td>
<td>0x00003202</td>
<td>Failed to kill an emailrelay process</td>
</tr>
<tr>
<td>Error code</td>
<td>Numeric</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------------</td>
<td>----------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>ERR_MAILAGENT_SERVICE_START</td>
<td>0x00004100</td>
<td>Failed to start service</td>
</tr>
<tr>
<td>ERR_MAILAGENT_ENGINESERVICE_START</td>
<td>0x00005100</td>
<td>The mail agent service failed to start</td>
</tr>
<tr>
<td>ERR_MAILAGENT_ENGINESERVICE_STOP</td>
<td>0x00005101</td>
<td>The mail agent service failed to stop</td>
</tr>
<tr>
<td>ERR_MAILAGENT_ENGINESERVICE_MDCORE_UNRESPONSIVE</td>
<td>0x00005102</td>
<td>Metadefender Core is not responding and mail agent cannot start</td>
</tr>
<tr>
<td>ERR_MAILAGENT_ENGINESERVICE_COMPONENT_LOAD</td>
<td>0x00005103</td>
<td>An error occurred while loading a Mail Agent component</td>
</tr>
<tr>
<td>ERR_MAILAGENT_ENGINESERVICE_COMPONENT_CREATE</td>
<td>0x00005104</td>
<td>An error occurred while creating a Mail Agent component</td>
</tr>
<tr>
<td>WARN_MAILAGENT_ENGINESERVICE_MDCORE_UNRESPONSIVE_REST</td>
<td>0x00005200</td>
<td>Metadefender Core REST is not responding (continuing to wait)</td>
</tr>
<tr>
<td>WARN_MAILAGENT_ENGINESERVICE_MDCORE_UNRESPONSIVE_UPDATE</td>
<td>0x00005201</td>
<td>Metadefender Core is updating (continuing to wait)</td>
</tr>
<tr>
<td>WARN_MAILAGENT_ENGINESERVICE_STATUS_CHECK</td>
<td>0x00005202</td>
<td>An unhandled error occure while performing status checks</td>
</tr>
</tbody>
</table>
Quarantine Reports

You can configure Metadefender Core so that it notifies administrator(s) of any e-mails that have been quarantined or sanitized during scanning.

1. In the Metadefender Core Management Console, go to Quarantine and click **Configure Quarantine Reports**.

2. Configure the SMTP settings and set the status to Connected. If you have already done this step, go to step 3.

   ![SMTP Configuration Settings](image)

   a. In the SMTP Configuration Settings section, click **Update**.

   a. In the Host field, specify the IP address or name of your mail server.

   **Note:** You may also use an alternative mail server to deliver reports and notifications. To do this, replace the Host value with your alternative mail server address and specify Port, SSL, Username and Password settings as required for the alternative mail server.

   b. Click **Save**.

   c. Metadefender Core will verify that the SMTP connection can be established with your mail server and if so, the Status field is updated to Connected.

3. Enable Quarantine Reports by moving the On/Off slider to **On**.
4. Specify the scheduling interval for report generation, along with the sender, recipient and optional subject and message body.

5. Click **Save** to save the quarantine report settings.

**Sanitized Email Notifications**

To send email notifications when an email is sanitized, move the On/Off slider to on. Specify a sender email address, and modify subject and body as desired. Notification email will be sent to the sender or recipient of the email with contents you configure on the following setting.
6. Additional Configuration

Advanced Configuration

Configuration From Config File

The Metadefender Mail Agent includes a set of configuration files that can be used to customize the application behavior and not most of the configurations are not available on management console.

Metadefender.Common.dll.config

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>InstallationFolder</td>
<td>Installation folder</td>
<td>Run-time location of Metascan.Common.dll file</td>
</tr>
<tr>
<td>LogsFolder</td>
<td>Logs folder</td>
<td>[Installation folder]\Logs</td>
</tr>
<tr>
<td>LogMaxSize</td>
<td>Possible values are, for example 100MB, or 4DAYS.</td>
<td>7DAYS</td>
</tr>
<tr>
<td>LogFormat</td>
<td>Possible values are Text or Xml</td>
<td>Text</td>
</tr>
<tr>
<td>LogLevel</td>
<td>Possible values are Debug, Info, Warn, Error, Fatal</td>
<td>Debug</td>
</tr>
<tr>
<td>RestClientTimeoutMs</td>
<td>Default timeout in milliseconds until a REST call times out</td>
<td>60000</td>
</tr>
</tbody>
</table>


Any change on this config file requires restarting Microsoft Exchange Transport service.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PickupPath</td>
<td>Exchange Server Replay Path</td>
<td>Added at install time</td>
</tr>
<tr>
<td>AgentGuid</td>
<td>Agent Guid. Should be unique.</td>
<td>Added at install time</td>
</tr>
<tr>
<td>AgentStatusCheckInterval</td>
<td>Durations between agent status checks</td>
<td>00:00:20</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol to use when sending process requests. Possible values are: REST</td>
<td>REST</td>
</tr>
<tr>
<td>RestBaseUrl</td>
<td>REST base url (Should point to Mail Agent, not MD Core)</td>
<td><a href="http://localhost:8000/">http://localhost:8000/</a></td>
</tr>
<tr>
<td>UseQueueFile</td>
<td>Use a temp queue file when submitting email instead of streaming content via protocol</td>
<td>True</td>
</tr>
</tbody>
</table>

**Metadefender.Email.Engine.Generic.Agent.dll.config**

- Change will be applied within 30 seconds without restarting mail agent service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WorkExtension</td>
<td>File extension to use when processing an email.</td>
<td>.work</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>BadExtension</td>
<td>File extension to use for a file that cannot be parsed or processed</td>
<td>.bad</td>
</tr>
<tr>
<td>AgentGuid</td>
<td>Agent Guid. Should be unique.</td>
<td>Added at install time</td>
</tr>
<tr>
<td>AgentStatusCheckInterval</td>
<td>Durations between agent status checks</td>
<td>00:00:20</td>
</tr>
<tr>
<td>Protocol</td>
<td>Protocol to use when sending process requests. Possible values are REST</td>
<td>REST</td>
</tr>
<tr>
<td>StartRestServer</td>
<td>Start the REST server</td>
<td>True</td>
</tr>
<tr>
<td>RestoreWorkItemsOnStartup</td>
<td>Rename any items with a work extension (.work) to .eml on service startup</td>
<td>True</td>
</tr>
<tr>
<td>EmailProcessedHeaderName</td>
<td>MIME Header name for emails processed by Mail Agent in order to avoid duplicates</td>
<td>X-Metadefender-EmailSecurity-Id</td>
</tr>
<tr>
<td>EmailRelayInProcessName</td>
<td>Process name for emailrelay.exe application</td>
<td>emailrelay</td>
</tr>
<tr>
<td>EmailRelayOutProcessName</td>
<td>Process name for emailrelayout.exe application</td>
<td>emailrelayout</td>
</tr>
<tr>
<td>EmailRelayInStart</td>
<td>Start Email relay process on service startup. (To monitor for incoming SMTP traffic)</td>
<td>True</td>
</tr>
<tr>
<td>EmailRelayInPort</td>
<td>Port to monitor by email relay</td>
<td>10025</td>
</tr>
<tr>
<td>EmailRelayInParameters</td>
<td>Parameters that are passed to email relay application</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>EmailRelayOutStart</td>
<td>Start Email relay process on service startup. (To monitor outgoing email and forward via SMTP)</td>
<td>True</td>
</tr>
</tbody>
</table>
| EmailRelayOutHosts          | List of Name (or IP adress) and port of server(s) to forward all email to. Multiple servers are separated with a comma (,)  
*For example: server1:25,server2:25*  
Note: Ensure that when the setting is updated the config file doesn't contain settings called 'EmailRelayOutServer' or 'EmailRelayOutPort' (delete them if they exist). | localhost:25                                                                  |
| EmailRelayOutParameters     | Parameters that are passed to email relay application                       | --no-daemon --hidden --no-smtp --poll 1 --forward-to localhost:25 --spool-dir "<dir>" |
| EmailRelayInDirection       | Determine the direction of emails. Possible values:  
0 = Incoming  
1 = Outgoing  
2 = Determine email direction using the local domain list in parameter `EmailRelayInLocalDomains` | 0                                                                             |
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailRelayInLocalDomains</td>
<td>List of local domains. Separate multiple domains with a semi colon (;). For example opswat.com;mycompany.com. Used to perform recipient verification (any recipient with a domain different than the specified domain(s) will be rejected at the SMTP protocol level). Also used when EmailRelayInDirection is set to 2 in order to determine direction.</td>
<td>* (by default all domains are accepted)</td>
</tr>
<tr>
<td>EmailRelayInQueueThreshold</td>
<td>Maximum inbound email queue size (exceeding this value will generate an email alert)</td>
<td>100</td>
</tr>
<tr>
<td>EmailRelayOutQueueThreshold</td>
<td>Maximum outbound email queue size (exceeding this value will generate an email alert)</td>
<td>100</td>
</tr>
<tr>
<td>EmailRelayOutRetryStart</td>
<td>Start the retry monitor thread (for emails that failed submission)</td>
<td>True</td>
</tr>
<tr>
<td>EmailRelayOutRetryInterval</td>
<td>Duration between submit retries (increasing with retry count).</td>
<td>00:00:30</td>
</tr>
<tr>
<td>EmailRelayOutRetryMaxInterval</td>
<td>Maximum duration between retries.</td>
<td>00:10:00</td>
</tr>
<tr>
<td>EmailRelayOutRetryCount</td>
<td>Maximum number of submit retries before email is moved to permanent failure</td>
<td>60</td>
</tr>
</tbody>
</table>

v3.14.7
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EmailRelayOutQueue</strong></td>
<td>Maximum number of .bad files in email queue (exceeding this value cause email alert to be generated)</td>
<td></td>
</tr>
<tr>
<td><strong>BadThreshold</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EmailRelayOutPermanent</strong></td>
<td>Maximum number of items in permanent failure (exceeding this value cause email alert to be generated)</td>
<td>1</td>
</tr>
<tr>
<td><strong>FailureThreshold</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>EmailRelayOutMaxConnections</strong></td>
<td>Maximum number of simultaneous SMTP connections when forwarding emails to remote server.</td>
<td>OS dependant</td>
</tr>
<tr>
<td><strong>EmailRelayInRetryStart</strong></td>
<td>Start the retry monitor thread (for emails that failed processing)</td>
<td>True</td>
</tr>
<tr>
<td><strong>EmailRelayInRetryInterval</strong></td>
<td>Minimum duration between process retries</td>
<td>00:01:00 (1 minute)</td>
</tr>
<tr>
<td><strong>EmailRelayInRetryCount</strong></td>
<td>Maximum number of process retries before email is moved to process failure</td>
<td>10</td>
</tr>
<tr>
<td><strong>MaxMonitorProcessThreads</strong></td>
<td>Maximum number of emails processed simultaneously</td>
<td>Dynamically calculated</td>
</tr>
<tr>
<td><strong>FastNoAttachment</strong></td>
<td>Avoid sending emails without attachments for processing (improved performance)</td>
<td>True</td>
</tr>
<tr>
<td><strong>ProcessingEnabled</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>LowPriorityMinSize</strong></td>
<td>Minimum size (in MB) for emails that will be processed on the low priority threads</td>
<td>1.5</td>
</tr>
<tr>
<td><strong>HighPriorityMaxSize</strong></td>
<td>Maximum size (in MB) for emails that will be processed on the high priority threads</td>
<td>0.1</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>-----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td><strong>UseAdjustingThreads</strong></td>
<td>Specifies if monitoring threads for incoming emails should adjust thread count dynamically or have fixed count</td>
<td>yes</td>
</tr>
<tr>
<td><strong>AddressValidation</strong></td>
<td>Specifies if Mail Agent should perform address validation on the incoming emails to detect invalid address (e.g. root@smth, ..@stop, inv'/alid)</td>
<td>true</td>
</tr>
<tr>
<td><strong>EmailRelayInUseTls</strong></td>
<td>Enable TLS for incoming SMTP connections</td>
<td>false</td>
</tr>
<tr>
<td><strong>EmailRelayInForceTls</strong></td>
<td>Force all incoming SMTP connections to use TLS (only used when EmailRelayInUseTls is true)</td>
<td>false</td>
</tr>
<tr>
<td><strong>EmailRelayOutUseTls</strong></td>
<td>Enable TLS for outgoing SMTP connections</td>
<td>false</td>
</tr>
<tr>
<td><strong>EmailRelayInTlsCertificate</strong></td>
<td>TLS certificate for incoming SMTP connections (only used when EmailRelayInUseTls is true) Example: -----BEGIN CERTIFICATE----- MIIFYDCCA0igAwIBAgIJALmTg... -----END CERTIFICATE-----</td>
<td>null</td>
</tr>
<tr>
<td><strong>EmailRelayInTlsKey</strong></td>
<td>TLS certificate private key for incoming SMTP connections (only used when EmailRelayInUseTls is true) Example: -----BEGIN PRIVATE KEY----- MIIJQgIBADANBgkqhkiG9w0BA.... -----END PRIVATE KEY-----</td>
<td>null</td>
</tr>
<tr>
<td><strong>EmailRelayOutClientCertificate</strong></td>
<td></td>
<td>null</td>
</tr>
</tbody>
</table>
### Metadefender.Quarantine.Mail.dll.config

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>StartRestServer</strong></td>
<td>Start the REST server (SmtpConfiguration)</td>
<td>True</td>
</tr>
<tr>
<td><strong>SubmitCommandTimeout</strong></td>
<td>Timeout for SMTP commands</td>
<td>00:01:00 (1 minute)</td>
</tr>
<tr>
<td><strong>EmailSubmission</strong></td>
<td>TTL (Time To Live) for an SMTP submit request. If email has not been submitted within this timespan the request is lost</td>
<td>01:00:00 (1 hour)</td>
</tr>
</tbody>
</table>

### Metadefender.Engine.History.dll.config

- **HistoryEntryExpireSpan**: Duration to keep history entries in the database. Default value is 91:00:00 (91 days).
- **StartRestServer**: Start the REST server (History). Default value is True.

---

Any change on this config file requires restarting Mail agent service.
### Metadefender.Email.Engine.Processor.dll.config

> Any change on this config file requires restarting Mail agent service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>StartRestServer</strong></td>
<td>Start the REST server (Processor)</td>
<td>True</td>
</tr>
<tr>
<td><strong>ConvertTnefMessagesToSmtp</strong></td>
<td>Convert TNEF encoded emails to MIME format</td>
<td>False</td>
</tr>
<tr>
<td><strong>MonitorMode</strong></td>
<td>Enables a monitoring mode of the Mail Agent. When set, no emails will be sanitized or quarantined (even when infected etc.)</td>
<td>False</td>
</tr>
<tr>
<td><strong>AddXHeadersToOutgoingEmail</strong></td>
<td>Force Mail Agent to add x-headers (Custom Email Headers) to outgoing emails</td>
<td>False</td>
</tr>
<tr>
<td><strong>EmailProcessedHeaderName</strong></td>
<td>MIME Header name for emails processed by Mail Agent in order to avoid duplicates</td>
<td>X-Metadefender-EmailSecurity-Id</td>
</tr>
<tr>
<td><strong>EmailAddCustomXHeaders</strong></td>
<td>Add custom x-headers to each email processed by Mail Agent. See Custom Email Headers for more information.</td>
<td></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>
<td>REST</td>
</tr>
<tr>
<td><strong>EmailSanitizedQuarantineMode</strong></td>
<td></td>
<td>REST</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></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>
<td></td>
</tr>
<tr>
<td>EmailQuarantineHeaderName</td>
<td>The name of the X-Header that will be added to emails when EmailBlockedQuarantineMode or EmailSanitizedQuarantineMode is set to SMTP. Header value will always be 'True'</td>
<td>X-Metadefender-To-Quarantine</td>
</tr>
<tr>
<td>DoSpfCheck</td>
<td>Enables SPF (Sender Policy Framework) lookups in Mail Agent. Result is placed in a header.</td>
<td>False</td>
</tr>
<tr>
<td>SpfCheckHeaderName</td>
<td>The name of the X-Header where to store the SPF lookup result</td>
<td>X-Metadefender-Spf-Result</td>
</tr>
<tr>
<td>SpfCheckReasonName</td>
<td>The name of the X-Header where to store a reason for a failed/skipped SPF lookup</td>
<td>X-Metadefender-Spf-Reason</td>
</tr>
</tbody>
</table>

**Metadefender.Scanner.dll.config**

- Change will be applied within 30 seconds without restarting mail agent service.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MetascanMode</td>
<td>Possible values are COM, RESTv1 and RESTv2</td>
<td>RESTv2</td>
</tr>
<tr>
<td>MetascanScanTimeout</td>
<td>Scanning timeout</td>
<td>00:05:00</td>
</tr>
<tr>
<td>MetascanScanQueueTimeout</td>
<td>Metadefender Core In Queue timeout</td>
<td>00:05:00</td>
</tr>
<tr>
<td>MetascanScanProgressPauseMS</td>
<td>Used in RESTv2 mode. Pause (in ms) between progress request calls</td>
<td>100</td>
</tr>
<tr>
<td>MaxMetadefenderCoreInQueueThreshold</td>
<td>If this limit is exceeded an alert will be sent saying that Metadefender Core is unresponsive and email delivery might be slower</td>
<td>250</td>
</tr>
<tr>
<td>MetadefenderUnavailableRetrySpan</td>
<td>Minimum pause for retry after a Metadefender Core goes down (only applicable if multiple scanners are configured)</td>
<td>00:01:00</td>
</tr>
<tr>
<td>MetadefenderAverageScanTimeSpan</td>
<td>Span for for scan times when calculating average scan time (when using multiple MD Cores)</td>
<td>00:01:00</td>
</tr>
<tr>
<td>UrlPrioritzationMethod</td>
<td>Metadefender Core Url prioritization method. Possible values: RoundRobin, Circular, ScanTime</td>
<td>RoundRobin</td>
</tr>
<tr>
<td>LogAllRequests</td>
<td>Increased logging. When set to true it will log all GET requests for getting scan settings and email disclaimers</td>
<td>false</td>
</tr>
</tbody>
</table>

**Metadefender.Quarantine.dll.config**

⚠️ Any change on this config file requires restarting Mail agent service.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaintenanceInterval</td>
<td>Interval between checking folder actions &amp; auto-deliver</td>
<td>00:00:30</td>
</tr>
<tr>
<td>RunAutoActionThread</td>
<td>Start the thread checking folder actions &amp; auto-deliver</td>
<td>True</td>
</tr>
<tr>
<td>CompressionMode</td>
<td>Quarantine item compression mode. Possible values are None, Zip</td>
<td>Zip</td>
</tr>
<tr>
<td>MonitoringFolderId</td>
<td>Predefined Quarantined folder id</td>
<td></td>
</tr>
<tr>
<td>QuarantineReportId</td>
<td>Predefined Quarantine Report id</td>
<td></td>
</tr>
<tr>
<td>StartRestServer</td>
<td>Start the REST server (Quarantine)</td>
<td>True</td>
</tr>
<tr>
<td>ReportUidExpireSpan</td>
<td>Expiry time for entries used to record which quarantine items were included in Quarantine Reports</td>
<td>1095:00:00</td>
</tr>
<tr>
<td>MaxQuarantineItemSize</td>
<td>Maximum buffer size when accepting quarantine items via REST</td>
<td>long max value</td>
</tr>
<tr>
<td>EmailAlertExpireSpan</td>
<td>The minimum interval between unique email alerts (errors). This is used to prevent too many alerts being sent during continuous errors</td>
<td>01:00:00</td>
</tr>
</tbody>
</table>

**Metadefender.Email.Engine.Service.exe.config**

⚠️ Any change on this config file requires restarting Mail agent service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LogName</td>
<td>Log name</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LogFilename</td>
<td>Log file name</td>
<td>Metascan.Email.Engine.Service.log</td>
</tr>
<tr>
<td>ComponentList</td>
<td>List of component loaded by service at startup</td>
<td></td>
</tr>
<tr>
<td>RestBaseUrl</td>
<td>REST server base URL</td>
<td>http://&lt;computer_name&gt;:8000</td>
</tr>
<tr>
<td>QuarantineBaseUrl</td>
<td>Metadefender Core Quarantine server base URL</td>
<td>http://&lt;computer_name&gt;:8000</td>
</tr>
<tr>
<td>MetascanUrl</td>
<td>Metadefender Core REST URL</td>
<td>http://&lt;core_url&gt;:8008/metascan_rest</td>
</tr>
<tr>
<td>MetascanApiKey</td>
<td>Metascan API key (encrypted)</td>
<td></td>
</tr>
<tr>
<td>StatusCheckInterval</td>
<td>Interval between component status checks (for error alerts)</td>
<td>00:00:30</td>
</tr>
<tr>
<td>UsePerformanceCounters</td>
<td>Creates a performance counter category (Metadefender Generic Mail Agent) for monitoring and recording processing data</td>
<td>False</td>
</tr>
<tr>
<td>ScanEmailBody</td>
<td>Specifies if Mail Agent should scan the body of the email</td>
<td>True</td>
</tr>
<tr>
<td>MaxRetries</td>
<td>Maximum number of retries before quit trying to connect to Metadefender Core</td>
<td>10000</td>
</tr>
<tr>
<td>TimeBetweenRetries</td>
<td></td>
<td>6000</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>----------------------------------------</td>
</tr>
<tr>
<td>UpdateUrlsOnStartup</td>
<td>Specifies if the service should attempt to update config URLs at startup.</td>
<td>True</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>
<td></td>
</tr>
</tbody>
</table>
| MetadefenderCoreIsLocal      | Specifies if Metadefender Core is installed locally                        | True when installed with Metadefender Core  
False when installed remotely |
| ConnectionCheckOnStartup     | 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. | False                                  |

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

⚠️ Any change on this config file requires restarting Mail agent service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MongoDbUrl</td>
<td>Mongo DB URL</td>
<td>mongodb://localhost:27018</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td><strong>MongoDbUrlEncryptionMode</strong></td>
<td>MongoDb Url value encryption mode. Possible values are None, Encrypted</td>
<td>None</td>
</tr>
<tr>
<td><strong>MongoDbName</strong></td>
<td>MongoDB database name</td>
<td>MetadefenderQuarantine</td>
</tr>
<tr>
<td><strong>MongoDBStartupTimeout</strong></td>
<td>Timeout to wait for MongoDB to respond</td>
<td>00:00:30</td>
</tr>
<tr>
<td><strong>LogName</strong></td>
<td>Log name</td>
<td>Metascan.Email.Engine.Quarantine.Service</td>
</tr>
<tr>
<td><strong>LogFilename</strong></td>
<td>Log file name</td>
<td>Default is Metascan.Email.Engine.Quarantine.Service.log</td>
</tr>
<tr>
<td><strong>ComponentList</strong></td>
<td>List of component loaded by service at startup</td>
<td></td>
</tr>
<tr>
<td><strong>RestBaseUrl</strong></td>
<td>REST server base URL</td>
<td>http://&lt;computer_name&gt;:8000</td>
</tr>
<tr>
<td><strong>QuarantineBaseUrl</strong></td>
<td>Metadefender Core Quarantine server base URL</td>
<td>http://&lt;computer_name&gt;:8000</td>
</tr>
<tr>
<td><strong>MetascanUrl</strong></td>
<td>Metadefender Core REST URL</td>
<td>http://&lt;core_url&gt;:8008/metascan_rest</td>
</tr>
<tr>
<td><strong>MetascanApiKey</strong></td>
<td>Metadefender API key (encrypted)</td>
<td></td>
</tr>
<tr>
<td><strong>WebBaseUrl</strong></td>
<td>Metadefender Web Site base URL</td>
<td>http://&lt;core_url&gt;:8008//management/#</td>
</tr>
<tr>
<td><strong>MongoDBStartupTimeout</strong></td>
<td>Time to wait for MongoDB database to start</td>
<td>00:00:30</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>UpdateUrlsOnStartup</td>
<td>Specifies if the service should attempt to update config URLs at startup</td>
<td>True</td>
</tr>
<tr>
<td>MetadefenderCoreIsLocal</td>
<td>Specifies if Metadefender Core is installed locally</td>
<td>True when installed with Metadefender Core</td>
</tr>
<tr>
<td></td>
<td></td>
<td>False when installed remotely</td>
</tr>
</tbody>
</table>

**Metadefender.Engine.Statistics.dll.config**

⚠️ Any change on this config file requires restarting Mail agent service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartRestServer</td>
<td>Start the REST server (Statistics)</td>
<td>True</td>
</tr>
<tr>
<td>StatisticsEntryExpireSpan</td>
<td>Duration to keep statistics entries in the database</td>
<td>31:00:00</td>
</tr>
<tr>
<td>StatisticsEntryInterval</td>
<td>Interval used when storing statistics. Possible values are Minute, TenMinute, Hour, Day</td>
<td>Minute</td>
</tr>
</tbody>
</table>

**Metadefender.Engine.Events.dll.config**

⚠️ Any change on this config file requires restarting Mail agent service.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Default Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EventEntryExpireSpan</td>
<td>Duration to keep system event entries in the database</td>
<td>91:00:00 (91 days)</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Default Value</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------------------</td>
<td>---------------</td>
</tr>
<tr>
<td>StartRestServer</td>
<td>Start the REST server (Events)</td>
<td>True</td>
</tr>
</tbody>
</table>

**XML schema for config file**

Below is a sample configuration file.

```xml
<?xml version="1.0"?>
<configuration>
  <applicationSettings>
    <[namespace]>
      <setting name="[name]" serializeAs="String">
        <value>[value]</value>
      </setting>
    </[namespace]>
  </applicationSettings>
</configuration>
```

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>namespace</td>
<td>For display reasons only. For example: Metadefender.Common</td>
</tr>
<tr>
<td>name</td>
<td>Setting name. Example: InstallationFolder</td>
</tr>
<tr>
<td>value</td>
<td>Setting value. Example: c:\MyInstallFolder</td>
</tr>
</tbody>
</table>

**Custom Email Headers**

The following custom email headers are added once processed by Metadefender Email. These can be used for custom rules on mail servers such as spam rules using **X-Metadefender-Core-Result**.

**X-Metadefender-Core-Uris**

The Metadefender Core REST API URL used in scanning operations for this email. If multiple MD Core scanners are configured and have been used for scans (this can happen when an email has multiple attachments) the list is comma separated.
Note: the field is empty if the email doesn't contain attachments.

Note: the URL will contain the hostname of the machine. If hostname is not available it will contain the machine name. If machine name is not available it will contain "localhost".

X-Metadefender-Core-Result
When workflow is enabled (default), this header value will contain the Metadefender Core process result. For Blocked results, the reason is also displayed (separated by a / character). Example values:

- Allowed (or Delivered - if email doesn't contain attachments)
- Blocked/Dirty
- Blocked/Filtered

If workflow is disabled this value will be the Metadefender Core scan result for the email. Refer to Description of Scan Results for details.

X-Metadefender-To-Quarantine
See Quarantine Email On Another Mail Server for more details.

X-Metadefender-EmailSecurity-Sanitized
This header is added to all emails that have been sanitized by the Mail Agent (header value 'True')

X-Metadefender-EmailSecurity-OriginalCopy
This header is added to all original copies of sanitized emails (header value 'True')

Your Own Custom X-headers
In addition to the above headers, Mail Agent can also add custom x-headers to every email processed. These X-Headers are configured in Metadefender.Email.Engine.Processor.dll. config as follows:

```xml
<setting name="EmailAddCustomXHeaders" serializeAs="String">
  <value>X-MyHeader:MyHeaderValue,X-MyHeaderNoValue:</value>
</setting>
```

v3.14.7
The above will add the following 2 X-headers to the email:

X-myheader: myheadervalue
X-myheadernovalue:

- If header name is not prefixed by X- it will automatically be added to the header name. (myheadername → X-myheadername)
- Header names should only contain 7-bit characters (ASCII 33-126 included) excluding colon (:). See https://tools.ietf.org/html/rfc2822 for more details. Any header name that does not comply with these restrictions will be ignored (and not added)
- If no text is added after : the header value will be empty
- If emails are not processed (Skip Email Analysis), the customers headers will not be appended.
- X-Headers are only added to emails when direction is configured as Incoming (Web MC > Sources > Metadefender Email > Setup). To force Mail Agent to also add X-Headers to outgoing emails, set AddXHeadersToOutgoingEmail in Metadefender.Email.Engine.Processor.dll.config (See Configuration From Config File)

Enable Sender Policy Framework (SPF) 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 Mail Agent to perform SPF checks on the "FROM" address(es) and add a header to the email with the SPF result.

How to Enable SPF checks

1. Go to the installation directory (by default C:\Program Files (x86) \OPSWAT\Metadefender Core <engine count>\Metadefender Mail Agent) and open the file Metadefender.Email.Engine.Processor.dll.config for editing.
2. Find the setting called DoSpfCheck and modify the value to true.
3. (Optionally) Find the setting called SpfCheckHeaderName and modify the value to the desired value to be used for the header name that will be added to the email. This header value will contain the SPF result.
Possible SPF results

After the SPF check is performed a header will be added to the email (by default `X-Metadefender-Spf-Result`) and the value will be one of the following:

- Pass
- NoRecord
- SoftFail
- HardFail
- Error
- Neutral
- Unknown
- UnknownMechanism

Please note that you will be required to add a rule on the target (destination) server to check for this header and take action based on the value (e.g delete the message, send to quarantine, etc).

Informational headers `X-Metadefender-Spf-Sender` & `X-Metadefender-Spf-Ip` are added to inform which email address & ip address was used in the SPF record lookup. An optional header (`X-Metadefender-Spf-Reason`) is added if the SPF check has failed or is skipped.

Log collection (collectLogs.exe)

Metadefender Email provides a tool to collect logs into a single archive to aid troubleshooting issues.

Usage

1. To create a debug log archive, open a command prompt and navigate to the Metadefender Email folder and run the collectLogs.exe application:

   ```
   C:\>cd "Program Files (x86)\OPSWAT\Metadefender Core X\Metadefender Mail Agent"
   C:\Program Files (x86)\OPSWAT\Metadefender Core X\Metadefender Mail Agent>collectLogs.exe
   Collecting data:
   ....
   Logs collected and saved to file:
   C:\Program Files (x86)\OPSWAT\Metadefender Core X\Metadefender Mail Agent\md-email-logs-2016-11-17_02-59-00-PM.zip
   ```
2. The collected log file will be compressed as an archive file (e.g., md-email-logs-2016-11-17_02-59-00-PM.zip)

> When Metadefender Email is installed on the same computer as Metadefender Core, additional information from Metadefender Quarantine will also be collected.

### Advanced options

The collectLogs.exe application also options to, for example, password protect the archive or prevent certain information from being collected.

- **-o (–output)**
  Override the default output archive name.

- **-p (–password)**
  Protect the output archive with a password.

### Log options

By default Metadefender Email writes log information to a Logs sub-folder, but it is also possible to customize the logging destination, for example log to a SysLog server. Below are a few examples how to log to different targets.

**SysLog**

In this example we will configure Metadefender Email to send logging to a Kiwi SysLog server (http://www.kiwisyslog.com/products/kiwi-syslog-server/product-overview.aspx):

1. Open Notepad and paste the following text to the new document:

   (Replace [log server] with the name/IP address of your SysLog server)

   ```xml
   <log4net>
   <appender name="RemoteSyslogAppender" type="log4net.Appender.RemoteSyslogAppender">
   <layout type="log4net.Layout.PatternLayout" value="%date{dd/MM/yyyy hh:mm:ss,fff} %thread %level %logger %username %P{log4net:HostName} dev %message %exception |
   
   <remoteAddress value="[log server]" />
   <filter type="log4net.Filter.LevelRangeFilter">
   ```
2. Save the document as Metadefender.Email.Engine.Service.Log.xml in the Metadefender Email folder (default C:\Program Files (x86)\OPSWAT\Metadefender Mail Agent)

3. Restart the Metadefender Generic Mail Agent service.

More examples

Below are more examples of SysLog configurations:

**UTF-8 encoded data on UDP port 11000**

```xml
<log4net>
  <appender name="UdpAppender" type="log4net.Appender.UdpAppender">
    <remoteAddress value="[log server]" />
    <remotePort value="11000" />
    <layout type="log4net.Layout.PatternLayout, log4net">
      <conversionPattern value="%date{dd/MM/yyyy hh:mm:ss,fff} | %thread | %level | %logger | %username | %P{log4net:HostName} | dev | %message | %exception | " />
    </layout>
    <encoding value="utf-8" />
  </appender>
  <root>
    <level value="DEBUG" />
    <appender-ref ref="UdpAppender" />
  </root>
</log4net>
```

Additional information

More details on log configuration options can be found at https://logging.apache.org/log4net/release/manual/configuration.html
Multiple Metadefender Core Instances Configuration

Overview

Single Mail Agent instance connecting to more than one Metadefender Core. Once it is configured, email will be processed depending on the number of ongoing jobs on each Metadefender Core instance.

How

2. Modify MetascanUrl setting
   a. Append the secondary MD instance IP, using semicolon (i.e.;) - as a separator.
3. Save and Close the file
4. Restart the Metadefender Mail Agent service to make change effective

MetascanUrl Configuration

```xml
<applicationSettings>
    <setting name="MetascanUrl" serializeAs="String">
      <value>http://server1:8008/metascan_rest;
    </setting>
</applicationSettings>
```

Unavailable Metadefender Core

If a Metadefender Core server becomes unavailable, process requests will be skipped until it becomes available again. Once it becomes unavailable, the Mail Agent will try to attempt again periodically.
Email Processing Workflow (Metadefender Core)

Email Processing

An email message consists of the email body and any attachments. Email attachments are application specific file formats while the email body format can be RTF, plain text, or HTML depending on how senders compose the message or which email client they use. When email is processed (e.g., multi-scan and data sanitization) by Metadefender, these components are scanned separately instead of being processed as a whole. By doing this Metadefender increases the detection of malware, file type mismatch and more. Also, Metadefender’s data sanitization technology can be applied to the specific contents where it is applicable.

For example, an email body could be in HTML format and have two attachments, one PDF file and one mp3 audio file. If Metadefender administrators configure to scan all file types and sanitize PDF and HTML file types, the email body and PDF file attachment will be scanned and sanitized while the mp3 will only be scanned. The email will be recreated with these sanitized components and sent to the recipient.

Metadefender Mail Workflow

Metadefender Mail Workflow relies on Metadefender Core’s "Mail Agent" workflow. You can modify the workflow through the following pages.

- Sources > Metadefender Email > Workflows

<table>
<thead>
<tr>
<th>Sources</th>
<th>Workflows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadefender Client</td>
<td>Click on the link below to edit the Mail Agent workflow</td>
</tr>
<tr>
<td>Metadefender Proxy</td>
<td>Name</td>
</tr>
<tr>
<td>Metadefender Email</td>
<td>Description</td>
</tr>
<tr>
<td>Setup</td>
<td>Mail Agent</td>
</tr>
<tr>
<td>Settings</td>
<td></td>
</tr>
</tbody>
</table>

- Metadefender Core > configuration > Workflows
Modify Metadefender Core URL

1. Navigate to the Metadefender Mail agent folder (by default, this is C:\Program Files (x86) \OPSWAT\Metadefender Core X\Metadefender Mail Agent).

2. Open Metadefender.Email.Engine.Service.exe.config in a text editor and change the following section, replacing *DNS_or_IP* with your server's real DNS hostname or IP address.

<table>
<thead>
<tr>
<th>Original</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;setting name=&quot;RestBaseUrl&quot; serializeAs=&quot;String&quot;&gt;</code></td>
<td><code>&lt;setting name=&quot;RestBaseUrl&quot; serializeAs=&quot;String&quot;&gt;</code></td>
</tr>
<tr>
<td><code>&lt;value&gt;http://*DNS_or_IP*:8000&lt;/value&gt;</code></td>
<td><code>&lt;value&gt;https://*DNS_or_IP*:8000&lt;/value&gt;</code></td>
</tr>
<tr>
<td><code>&lt;setting name=&quot;QuarantineBaseUrl&quot; serializeAs=&quot;String&quot;&gt;</code></td>
<td><code>&lt;setting name=&quot;QuarantineBaseUrl&quot; serializeAs=&quot;String&quot;&gt;</code></td>
</tr>
<tr>
<td><code>&lt;value&gt;http://*DNS_or_IP*:8000&lt;/value&gt;</code></td>
<td><code>&lt;value&gt;https://*DNS_or_IP*:8000&lt;/value&gt;</code></td>
</tr>
<tr>
<td><code>&lt;setting name=&quot;QuarantineProtocol&quot; serializeAs=&quot;String&quot;&gt;</code></td>
<td><code>&lt;setting name=&quot;QuarantineProtocol&quot; serializeAs=&quot;String&quot;&gt;</code></td>
</tr>
<tr>
<td><code>&lt;value&gt;REST&lt;/value&gt;</code></td>
<td><code>&lt;value&gt;REST&lt;/value&gt;</code></td>
</tr>
<tr>
<td><code>&lt;setting name=&quot;MetascanUrl&quot; serializeAs=&quot;String&quot;&gt;</code></td>
<td><code>&lt;setting name=&quot;MetascanUrl&quot; serialize=&quot;String&quot;&gt;</code></td>
</tr>
<tr>
<td><code>&lt;value&gt;http://*DNS_or_IP*:8008/metascan_rest&lt;/value&gt;</code></td>
<td><code>&lt;value&gt;https://*DNS_or_IP*:8008/metascan_rest&lt;/value&gt;</code></td>
</tr>
</tbody>
</table>
3. Restart the Metadefender Mail Agent service

Quarantine Email

Metadefender Email provides quarantine capability either when email (including attachments) are marked as threat (blocked) or are sanitized. When sanitized, original copy of the email will be quarantined while sanitized email will be delivered. Once quarantine is enabled, any emails that are blocked will be moved to quarantine. To enable quarantine, go to Metadefender Core Management Console > Sources > Metadefender Email > Settings.

Quarantine Settings

- Quarantine any e-mails flagged as a threat

If you want to quarantine email on 3rd party solution (e.g., hosted email solution), refer to Quarantine Email On Another Mail Server.

When emails are quarantined the following disclaimer is added to the email body (by default): This email was quarantined by Metadefender. For more information on Metadefender's Email Security technology please visit www.opswat.com.

Quarantine Email On Another Mail Server

Metadefender Email 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 onsite mail server) has quarantine management capability for each user, it is recommended to quarantine email on your email server. By default, Metadefender Email will quarantine emails on Metadefender Quarantine but you can change this behavior.

Change Quarantine Mode For Blocked Email

Changing this setting will allow you to quarantine emails that are detected as blocked by Metadefender on a different email server by changing EmailBlockedQuarantineMode to SMTP. By doing this a header will be appended to the email for which you can configure a rule on your email server to quarantine emails that contain this header.
1. (Prerequisite): Quarantine should be enabled. Refer to Quarantine Email for the instructions.

2. Edit configuration file "C:\Program Files (x86)\OPSWAT\Metadefender Core 4\Metadefender Mail Agent\Metadefender.Email.Engine.Processor.dll.config"

3. Change the EmailBlockedQuarantineMode setting value to SMTP. If you want to restore the behavior, use REST instead.

   Excerpt from the config file

   ```
   <setting name="EmailBlockedQuarantineMode" serializeAs="String">
      <value>SMTP</value>
   </setting>
   ```

4. [Optionally] You can change the name of the header by modifying X-Metadefender-To-Quarantine to something else.

   Excerpt from the config file

   ```
   <setting name="EmailQuarantineHeaderName" serializeAs="String">
      <value>X-Metadefender-To-Quarantine</value>
   </setting>
   ```

5. Restart the Generic Mail Agent service

   ```
   net stop mdfExgEmailAgent
   net start mdfExgEmailAgent
   ```

Change Quarantine Mode For Sanitized Email

Changing this setting will allow you to quarantine original copies of emails that have been sanitized by Metadefender on a different email server by changing EmailSanitizedQuarantineMode to SMTP. By doing this a header will be appended to the email for which you can configure a rule on your email server to quarantine emails that contain this header.

1. (Prerequisite): Quarantine should be enabled. Refer to Quarantine Email for the instructions.
2. Edit configuration file "C:\Program Files (x86)\OPSWAT\Metadefender Core 4\Metadefender Mail Agent\Metadefender.Email.Engine.Processor.dll.config"

3. Change the EmailSanitizedQuarantineMode setting value to SMTP. If you want to restore the behavior, use REST instead.

Excerpt from the config file

```
<setting name="EmailSanitizedQuarantineMode" serializeAs="String">
  <value>SMTP</value>
</setting>
```

4. [Optionally] You can change the name of the header by modifying X-Metadefender-To-Quarantine to something else.

Excerpt from the config file

```
<setting name="EmailQuarantineHeaderName" serializeAs="String">
  <value>X-Metadefender-To-Quarantine</value>
</setting>
```

5. Restart the Generic Mail Agent service

```
net stop mdfExgEmailAgent
net start mdfExgEmailAgent
```

How To Verify

If you open the message headers for an email that should be quarantined you will see something similar to this:

```
Received: from ALING-PC ([192.168.16.16]) by alig-win8-dev.local with ESMTP; Fri, 2 Sep 2016 16:45:18 +0300
MIME-Version: 1.0
From: administrator@mailagent-testing.email
To: administrator@mailagent-testing.email
Date: 2 Sep 2016 16:45:18 +0300
Subject: Checking new Quarantien mode
Content-Type: multipart/mixed;
    boundary=--boundary_2_95887891-94da-4b66-8dc9-f2bcebf4394d9
```
Notice the header **X-Metadefender-To-Quarantine** is set to *True* and this won't exist if email is NOT quarantined.

**Skip Email Analysis**

Emails without attachments can be skipped from being analyzed in order to increase throughput. If email body analysis is enabled this setting will not apply.

**Configuration**

To enable this functionality, make the following configuration file modification.

```
<setting name="FastNoAttachmentProcessingEnabled" serializeAs="String">
    <value>true</value>
</setting>
```
7. Release Notes

Other changes

- Updated the EULA in the installer

Archive Release Notes

Version 3.12.5

New Features

- Support Microsoft Exchange servers
- Support multiple relay-out mail servers for mail proxy deployment

Other Changes

- Many bug fixes

Version 3.13.0

New Features

- Separate Installation from Metadefender Core
- Improve error notifications
- Automatic setting verification (no more telnet based smoke-test)
- Support syslog as additional target logging
- Tool to collect and package mail agent logs for troubleshooting
- Add TLS support (Incoming/Outgoing emails)

Other Changes

- Many bug fixes
Version 3.14.0

New Features
- Improved log collection for troubleshooting

Bug Fixes
- Multiple bug fixes including TSL support, email header and email relay server connection issues

Version 3.14.1

New Features
- Updated the message in default disclaimer
- Added RTF as a supported file type for sanitization

Other Changes
- Multiple bug fixes

Version 3.14.2

New Features
- Fixed Invalid Email Inbox problem
- Separate mail agent upgrade
- Syslog encoding for Hebrew

Other Changes
- Email History shows new status "Delivery Failed" for invalid inboxes.
- Invalid recipient fixes with new error codes added
- Subject tag fixed for Exchange
Version 3.14.3

New Features

- Improve error codes in case of relay looping

Other Changes

- Email sanitization disabled by default
- Password protected documents quarantined
- REST API minor update

Version 3.14.4

New features

None.

Other changes

- Embedded objects within sanitized Rich Text (RTF) retain position in email body
- Email content not corrupted even in case of non-RFC compliant email clients

Version 3.14.5

New features

None.

Other changes

- Image locations in HTML are retained even when images are sanitized.

Version 3.14.6

New features

- Re-interpreted, fresh OPSWAT identity

v3.14.7
Other changes

- Positions lost for Exchange internal TNEF encoded emails
- Attachment sanitization failed, sanitized files were not sent
- After upgrading Mail Agent, old setup files don't disappear

Version 3.14.7

Other changes

- Updated the EULA in the installer

General and Known Issues

Limitation

- If target server requires authentication, multiple target servers (relay out) is supported when same credential is configured.
- A separate SMTP server is required for notification.
- Exchange (malware agent configuration) may block release from quarantine.
- Email sanitization to HTML may be blocked and attachment may be replaced with text "This attachment was removed because it contains data that could pose a security risk."
- An attachment that has been sanitized may be larger than the original attachment. As a result, it may be necessary to increase the maximum attachment size setting on your mail server
- Rich Text (RTF) body sanitization & disclaimers only available when Mail Agent is installed on Exchange server. Unable to render JIRA issues macro, execution error.
- Email preview does not work for RTF formatted emails in quarantine. Unable to render JIRA issues macro, execution error.

Limitation for Onsite Microsoft Exchange Deployment

- Mail agent will be installed on Metadefender Core server by default even if separate installation is required on exchange server.
- Installing Metadefender Core on the exchange server is not supported.
8. Legal

- Copyright
- Export Classification EAR99

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.

Export Classification EAR99

EAR99 (Export Administration Regulation 99) is an export classification category regulated by the U.S. Department of Commerce that covers most commercial items exported out of the U.S. OPSWAT’s software is designated as EAR99, and there are no export restrictions other than embargoed countries and persons.