Trend Micro InterScan Messaging Security Virtual Appliance 8.5

Best Practice Guide
# Table of Contents

Table of Contents ................................................................................................... 3

Chapter 1: Preface ..................................................................................................... 5

Chapter 2: Product Description .............................................................................. 6

Chapter 3: Hardware ................................................................................................. 7
  3.1 Sizing Guidelines ................................................................................................. 7
  3.2 Recommended Hardware ....................................................................................... 9
     3.2.1 IMSVA Server ................................................................................................. 9

Chapter 4: Software .................................................................................................. 10
  4.1 Recommendations ............................................................................................... 10
     4.1.1 LDAP ............................................................................................................... 10
     4.1.2 TMCM ............................................................................................................. 10
     4.1.3 Logging ........................................................................................................... 10
     4.1.4 DDA server version requirement ..................................................................... 11

Chapter 5: Deployment .............................................................................................. 12
  5.1 Network Topology ............................................................................................... 12
     5.1.1 INTERNET → IMSVA → Mailbox servers ..................................................... 12
     5.1.2 INTERNET → MTA → IMSS → Mailbox servers ............................................ 12
  5.2 Component Layout ............................................................................................. 13
  5.3 Fault Tolerance and Load Balancing ................................................................... 16

Chapter 6: Product Configuration .......................................................................... 18
  6.1 GUI Configuration ............................................................................................... 18
     6.1.1 Scanning Exceptions ....................................................................................... 18
     6.1.2 Notifications .................................................................................................. 20
     6.1.3 SMTP Routing .............................................................................................. 21
     6.1.4 Cloud Pre-Filter .......................................................................................... 22
     6.1.5 Steps to enable DDA integration ................................................................... 23
  6.2 Policy Settings .................................................................................................... 23
     6.2.1 Policy Routing .............................................................................................. 23
     6.2.2 Global Antivirus Rule .................................................................................... 24
     6.2.3 Regular Expressions ...................................................................................... 24
     6.2.4 Filter Ordering .............................................................................................. 29
     6.2.5 Creating “Global White List” for Inbound Mails .......................................... 30
     6.2.6 Separating Phishing/WRS Checking from Anti-Spam Rule ....................... 31
     6.2.7 Scan Method ................................................................................................. 32
     6.2.8 C&C Contact Alert Services ....................................................................... 32
     6.2.9 Scan Engine ................................................................................................. 33
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3 &gt; Configuration Files</td>
<td>33</td>
</tr>
<tr>
<td>6.3.1 imss.ini File</td>
<td>33</td>
</tr>
<tr>
<td>6.3.2 foxdns.ini File</td>
<td>33</td>
</tr>
<tr>
<td>6.4 &gt; Database</td>
<td>34</td>
</tr>
<tr>
<td>6.4.1 Updating the configuration settings in the database</td>
<td>35</td>
</tr>
<tr>
<td>6.4.2 Database Maintenance Schedule</td>
<td>38</td>
</tr>
<tr>
<td>6.5 &gt; Others</td>
<td>39</td>
</tr>
<tr>
<td>6.5.1 Spam Settings</td>
<td>39</td>
</tr>
<tr>
<td>6.5.2 EUQ SMTP Authentication</td>
<td>41</td>
</tr>
<tr>
<td>6.5.3 Rule Samples</td>
<td>42</td>
</tr>
<tr>
<td>Chapter 7: Backup and Disaster Recovery</td>
<td>48</td>
</tr>
<tr>
<td>7.1 &gt; Backup and Restore from the GUI</td>
<td>48</td>
</tr>
<tr>
<td>7.2 &gt; Manual Database Backup and Recovery</td>
<td>48</td>
</tr>
<tr>
<td>7.3 &gt; Backing up and Restoring Cloud Pre-filter account settings</td>
<td>51</td>
</tr>
<tr>
<td>Chapter 8: References</td>
<td>53</td>
</tr>
<tr>
<td>8.1 &gt; Communication Ports</td>
<td>53</td>
</tr>
<tr>
<td>8.2 &gt; ERS Console</td>
<td>55</td>
</tr>
<tr>
<td>8.3 &gt; TLS (Transport Layer Security) Settings</td>
<td>56</td>
</tr>
<tr>
<td>8.4 &gt; Product Updates</td>
<td>56</td>
</tr>
<tr>
<td>8.5 &gt; Upgrade/Migration</td>
<td>57</td>
</tr>
</tbody>
</table>
Chapter 1: Preface

Welcome to Trend Micro InterScan Messaging Security Virtual Appliance v8.5 Best Practices Guide. This document is designed to help resellers and customers develop a set of best practices when deploying and managing the InterScan Messaging Security Virtual Appliance (IMSVA).

This document is also designed to be used in conjunction with the following guides, both of which provide more details about IMSVA than are given here:

- Trend Micro InterScan Messaging Security Virtual Appliance v8.5 Installation Guide
- Trend Micro InterScan Messaging Security Virtual Appliance v8.5 Administrator’s Guide
- Trend Micro IMSVA 8.5 Reviewers Guide.
Chapter 2: Product Description

InterScan Messaging Security Virtual Appliance (IMSVA) is a comprehensive antivirus and content management solution for the Internet mail gateway. There are 5 major components in an IMSVA environment that need to be identified when architecting the deployment. Each component is briefly described below.

1. Central Controller – The main IMSS server that allows administrators to manage multiple IMSS Scanners using one IMSS Web Console

2. Scanner Service – Accepts and scans SMTP and POP3 connections.

3. EUQ Service – End User Quarantine service allows end users to checked their quarantined “spam” mails to check if they are spam or not. The first server where you will install EUQ on will become the Primary EUQ server where end-users will connect. Secondary EUQ servers provide load-balancing and better performance.

4. Cloud Pre-Filter – Managed email security service powered by the Trend Micro Email Security Platform. This allows the inbound messages to be scanned for spam, phishing, malware, and other messaging threats before reaching the network.

5. IP-Filter – Consists of Email Reputation Service and IP-Profiler modules. The two modules provide anti-spam capability that can filter SMTP connection based on the IP-address of the connecting SMTP server.

6. Email Reputation Services – First part of the IP-Filtering module, which prevents spam mails. It identifies and blocks spam using RBL to block SMTP connection based on the IP-address of the connecting MTA server.

7. IP Profiler – Second part of the IP-filtering module. It allows administrators to block SMTP connections based on security violations and threshold settings.
Chapter 3: Hardware

On top of the normal MTA tasks of receiving and delivering emails, IMSS has to disassemble, evaluate, scan and reassemble the emails. This makes IMSVA a CPU and disk I/O intensive application. Careful planning needs to be done to make sure the IMSVA hardware can handle the email load of the environment.

3.1 Sizing Guidelines

Important: This information can be used as a starting reference only. Actual performance will vary depending on features enabled, topology, performance tweaks, and scan-exclusions as outlined throughout this best practice document. This Sizing Guidelines are based off IMSVA 7.0.

When doing sizing planning for IMSVA 8, the main goal is to determine how many IMSVA Scan Servers are needed using the two given customer environment data. These are the Average Message Size and the Total Throughput.

1. Average Message Size (KBytes)
   This is the average message size as seen in your environment. 100 KBytes is a common size for an environment if the other details are unknown.

2. Total Throughput (Messages/hour)
   This is the number of messages passing through the SMTP gateway per hour. If growth is expected, size for the planned growth. This is the number of messages passing through the proposed IMSS gateway. If IMSS is to be used to filter both incoming and outgoing mail, the total number of mail messages must be used. Internal messages that do not pass through IMSS at the gateway should not be included the “Total Throughput” variable. Messages that will be filtered by the IP-Filtering (ERS or IP-Profiler) module should not be included.

STEP 1: Using Ave. Message Size, determine the Maximum Steady Throughput. Maximum Steady Throughput is the max number of messages/hr IMSVA can process without queuing.
   Use the following tables to determine the Maximum Steady Throughput. Please take note that these data assumes that the user is using the 2 default IMSVA filters (Antivirus and AntiSpam Filters). The values may vary if additional Filters are used but these numbers make a very good baseline as seen in other customers.
### Table

<table>
<thead>
<tr>
<th>Volume Category</th>
<th>Estimated Seats per Server</th>
<th>Throughput</th>
<th>Server Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Item 0</td>
<td>Item information</td>
<td>~240,100 Messages per hour (67 Messages per second)</td>
<td>VMware ESX 3.5 Virtual Machine</td>
</tr>
<tr>
<td>High Volume</td>
<td>~38,000</td>
<td></td>
<td>-4 Virtual CPUs</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-4 GB RAM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-VM Network adapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-LSI Logic SCSI controller</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-80 GB Virtual Disk</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Host Server Hardware</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-3.16 GHz Intel Xeon CPU</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-8 GB available on Host</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-Perc 6/I SAS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-3 x 73 GB 15,000 RPM</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SAS hard drive</td>
</tr>
</tbody>
</table>

### NOTE

- Dedicated host (only one IMSVA 7.0 virtual machine running on this host)
- Default Configuration of IMSVA 7.0:
  - Antivirus + Anti-spam active
  - ERS, IP Profiling, Web EUQ inactive
- The above sizing estimates imply no message queuing on the IMSVA server.
- An “average user” is defined:
  - 50 messages sent/received across the gateway per 8 hour day (total)
  - Average message size 108 KB
- This is mildly aggressive sizing to ensure accurate capacity planning
- If only antivirus or anti-spam is enabled, increase throughput by 10 percent in Table 1
- Content filtering can be more expensive in resource consumption than both Antivirus and Anti-spam depending on the number and type of filters used. If the customer requires many content filters.

### STEP 2:

Determine the number of IMSS servers required.

**Number of servers** = Total Throughput / Max Steady Throughput.
Le. Ave Msg size is 100KB. IMSVA 7 with the High Volume specs and the Total Throughput is 300,000 Mgs/hour

Number of servers = 300,000/240,100

= 1.25

In this example, the number of IMSVA servers recommended is 2 (1.25 rounded up)

NOTE: The data present is based of IMSVA 7.0. Using Content Filter with complex rules and other options can greatly reduce the throughput.

### 3.2 Recommended Hardware

IMSVA performs heavy disk I/O operations similar to most SMTP applications. Leveraging the fastest disk RPM and RAID configuration is known to significantly improve performance. IMSVA will also automatically spawn more processes to keep up with incoming traffic. Therefore, adding more RAM is another key element to increasing performance.

#### 3.2.1 IMSVA Server

Below are the recommended hardware specifications for an IMSVA Server. Please note that these are not the minimum system requirements for this product.

**CPU:**
- Four Intel Xeon processors 3.16GHz.

**RAM:**
- 8 GB

**Disk Drive:**
- 15,000RPM hard disk drive or faster.
Chapter 4: Software

This section will go over software best practices for IMSVA. Since IMSVA is a virtual appliance, you do not need to worry about hardening or tuning the software. This section will give you guidelines on the third party software that are used by IMSVA.

4.1 Recommendations

4.1.1 LDAP

IMSVA supports the following three types of LDAP servers:

- Microsoft Active Directory 2003, 2008 or Global Catalog
- IBM Lotus Domino 6.5 and 8.5
- Sun One LDAP 5.2 or above
- OpenLDAP 2.3.43-3

4.1.2 TMCM

- Version 5.5 Service Pack 1 Patch 3
- Version 6.0 Patch 3

4.1.3 Logging

To maintain optimum performance for the modules that read and write information from the database, Trend recommends maintaining the database to the smallest possible size. To do this, you can decrease the configured number of days for storing event logs (under Logs | Settings) and quarantined/archived events.
(under Quarantine & Archive | Settings) and lessen the number of reports to save (under Reports | Settings).

### 4.1.4 DDA server version requirement

DDA 2.92 and DDA3.0
Chapter 5: Deployment

This section will go over deployment best practices for IMSVA. Here we will give recommendations as to the placement of IMSVA in relation to the mailboxes and your MTA(s). You will get information on which components you can enable/disable on each IMSVA and different load balancing / fault tolerance techniques that are commonly used.

5.1 > Network Topology

IMSVA 8.5 comes with Postfix, which is a complete MTA. This allows you to put IMSVA anywhere in your email topology just like any other MTA. However, if you intend to use the IP Profiler and ERS features, you must place your IMSVA on the edge of the network. Cloud Pre-Filter has no impact on how IMSVA should be deployed. With Cloud Pre-Filter, Trend Micro recommends adding the IMSVA’s address to the domain’s MX records, and the placing IMSVA at a lower priority than the Cloud Pre-Filter. This allows IMSVA to provide email service continuity as a backup to Cloud Pre-Filter.

Below are some common topologies with IMSVA.

5.1.1  INTERNET → IMSVA → Mailbox servers

This is the ideal setup especially if ERS and IP-Profiler will be used. The Postfix MTA that comes with IMSVA will act as the front MTA server. Postfix is fully compatible with all the ERS and IP-Profiler features.

5.1.2  INTERNET → MTA → IMSS → Mailbox servers

This setup is recommended if you don’t want to replace your current front MTA server with IMSVA. Although you will not be able to use IP Profiler, you can still use ERS depending on which MTA server you are running. Almost all popular MTAs support RBL feature which is the technology behind ERS.

Please follow the links below for more information about how to enable ERS on other MTA servers.

ERS Standard:

ERS Advanced:


For more deployment options, refer to the InterScan Messaging Security Virtual Appliance Installation Guide.

5.2 Component Layout

Please see the InterScan Messaging Security Virtual Appliance Instation Guide and InterScan Messaging Security Virtual Appliance 8.0 Administrator’s Guide for an explanation on the parent-child relationship between the IMSVA and groups.

IMSVA 8.5 has major components that can run separately on different virtual machines. This allows IMSVA to support a distributed type of deployment. Although it can also support the single-server type of deployment, distributed deployment provides better performance and fault-tolerance. Below are different types of deployments and their advantages.

Figure 1 Single Server Deployment

- All IMSVA Components are on the same server.

This is the simplest type of deployment, which is best for small network environments. Use this option if the server’s hardware specifications can handle the amount of emails that will go through IMSVA.

Considerations:

- If you intend to use ERS and IP Profiler, the server should be the “edge” of the network. An edge MTA is the one that accepts emails directly from the Internet.
- Since there is only one IMSVA server in the environment, there is a single point of failure, which may interrupt email flow if the server goes down.
Figure 2 Distributed Deployment (medium-size environment)

- Server 1 has parent virtual appliance with Scanner, Policy, and EUQ services all started.
- Server 2 has a child virtual appliance with Scanner, Policy, and EUQ services all started.
- Server N has a child virtual appliance with Scanner, Policy, and EUQ services all started.

Use this type of deployment for better scalability. In this type of deployment, you can easily add more virtual appliances in the future if necessary. Since there are multiple Scanner servers that can accept emails, this setup provides fault-tolerance, which avoids the interruption of email flow if one IMSVA goes down. The EUQ client access load is distributed to multiple secondary EUQ Servers by the parent EUQ Servers.

**NOTE**: see Section 3.1 Sizing Guidelines to determine how many IMSS Scanner servers are necessary to support your environment.

Considerations:

- If you intend to use ERS and IP Profiler, the IMSVA Scanner servers should be at the edge of the network. The IMSVA Scanner servers should be ones accepting emails directly from the Internet.
- EUQ Users should have access to Server 1, which is hosting the Primary EUQ Server.
- The parent server may become the bottleneck depending on the amount of logs, quarantined events, etc. that needs to be stored.
- Even with the Scanner service running on the parent, you can set this to be the least priority in the mail routing so it has more resources to run its other tasks.
- In environments with more than two child devices, the Scanning, Policy, and EUQ services should be disabled on the parent virtual appliance, if possible, to avoid its overload.
Figure 3 Distributed Deployment (large-size environment)

- Server 1 has the parent virtual appliance with the Scanner, Policy, and EUQ services all disabled.
- Dedicated child virtual appliances with only Scanners and Policy services enabled.
- Dedicated child virtual appliances with only EUQ service enabled

Use this type of deployment to achieve the highest level of performance, scalability and fault-tolerance. In this setup, users can add more IMSVA Scanner servers in the future if necessary. Disabling all the services on the parent device provides better performance especially if there are several child devices to manage. Specializing appliances to run either the Scanner/Policy Services or EUQ service will provide the best performance output.

**NOTE** see Section 3.1 Sizing Guidelines to determine how many IMSS Scanner servers are necessary to support your environment.

Considerations:

- If you intend to use ERS and IP Profiler, the IMSVA running the Scanner and Policy services should be at the edge of the network.
- EUQ Users should have access to Server 1, which is hosting the main EUQ Server.

**Multiple-location Considerations**

IMSVA works well in a multiple-location environment. Below are things to be aware of when implementing IMSVA on a multiple-location environment.

- Deploy at least one parent virtual appliance in each location.
- Use TMCM to manage multiple parent appliances.
5.3 Fault Tolerance and Load Balancing

Why Load Balance

Load balancing provides the following network benefits:

- Increased / and or sustained traffic throughput without increased latency (when compared to a non-load balanced solution).
- Rudimentary high availability capabilities.

Load Balancing Methods

There are several methods for accomplishing load balancing for both SMTP and HTTP. These are:

- Hardware load balancing
- DNS round robin

Hardware Load Balancing

Many organizations consider hardware load balancing the preferred solution. This is because it provides a balanced delivery of services to end users. A hardware solution typically balances traffic for OSI Layers 4 through 7 and is otherwise known as an application switch. By using a hardware load balancer, all the work to determine which node should process which request is handled by the hardware, away from the nodes. Adding, removing, or updating equipment to the group also is easier. Hardware load balancing also provides several ways to balance the network, whether that solution includes a high-end switch or an additional network appliance.

General Configuration for a Hardware Load Balancer for Inbound SMTP Traffic

Configuring a hardware load balancer involves:

- Selecting the pool of IP addresses that the load-balanced devices are going to use.
- Configuring the load balancer to use a virtual server IP address for the load-balanced pool of devices.
- Choosing destination protocol triggers that send only the specified protocol from the virtual server to the load-balanced pool.
No additional changes need to be made to external DNS MX records, unless the new virtual server IP address is different from the published MX record.

**DNS Round Robin**

Round robin works by having separate DNS name records (Name Record A) bound to the same canonical name record (Name Record C) for each server that provides a specific service. These A and C name records use the zone’s minimum time-to-live value (TTL) to specify the time period the DNS record is kept before it is requested again. In this way, when DNS clients request the C name record for a service, the DNS server resolves the list of servers, but only returns one entry. The client requesting the C name record uses that server for the duration of the TTL. When the end of the TTL period is reached, the query is performed again. Using this technique, a DNS record that is sent to Client A could be different from that sent to Client B – thus, Client A’s traffic might go to Server A and Client B’s traffic might go to Server B. The effect of using DNS Round Robin is that each of the Record A servers is used in the most efficient way possible to provide the service to the end client.

**Example (DNS Zone Configuration):**

<table>
<thead>
<tr>
<th>Server Name</th>
<th>Type</th>
<th>Host Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>server1.mydomain.tld</td>
<td>IN A</td>
<td>192.168.1.20</td>
</tr>
<tr>
<td>server2.mydomain.tld</td>
<td>IN A</td>
<td>192.168.1.21</td>
</tr>
<tr>
<td>server3.mydomain.tld</td>
<td>IN A</td>
<td>192.168.1.22</td>
</tr>
<tr>
<td>server4.mydomain.tld</td>
<td>IN A</td>
<td>192.168.1.23</td>
</tr>
<tr>
<td>proxy.mydomain.tld</td>
<td>IN CNAME</td>
<td>server1.mydomain.tld</td>
</tr>
<tr>
<td>proxy.mydomain.tld</td>
<td>IN CNAME</td>
<td>server2.mydomain.tld</td>
</tr>
<tr>
<td>proxy.mydomain.tld</td>
<td>IN CNAME</td>
<td>server3.mydomain.tld</td>
</tr>
<tr>
<td>proxy.mydomain.tld</td>
<td>IN CNAME</td>
<td>server4.mydomain.tld</td>
</tr>
</tbody>
</table>

In the above example, all MTA’s would be configured to use proxy.mydomain.tld and could use one of four possible servers for each TTL period.
Chapter 6: Product Configuration

This section will go over the different configuration best practice for IMSVA. You can change the IMSVA configuration in three ways.

- Via the GUI
- Via local configuration files (ini files)
- Via the database

Changes made in the GUI are stored in either the local configuration files and/or the database. The priority in which IMSS will use the configuration settings if there is a conflict between the local files and the database is it will prioritize the setting specified in the local ini files. If the particular setting is not found in the local ini files, IMSS will use the setting in the database.

The next sections will focus on the different configuration methods.

6.1 > GUI Configuration

6.1.1 Scanning Exceptions

Policy -> Scanning Exceptions -> Security Settings Violations

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # recipients exceeds</td>
<td>The maximum number of recipients allowed within a single message. Messages with a lot of recipients can cause increased latency in message rule matching.</td>
</tr>
<tr>
<td>Total # embedded layers in compressed</td>
<td>A layer is defined by a compressed file within a compressed file. Has been used in previous attacks to hide malware deeper than scan</td>
</tr>
</tbody>
</table>
**Category** | **Description**
--- | ---
file exceeds engines previously scanned. Recommended value is 5. The default value is set at 20 layers.
Total decompressed size of any single file exceeds This setting is to prevent zip file attacks. The size set here should be relative to your total message size limit. Example: If you set your maximum message size to 5MB, the total size should not exceed 50MB. The default value is set at 50 MB.
Total # files in compressed file exceeds This setting is to prevent zip file attacks. Having a zip file with 50,000 files inside of it, although small in size, could cause significant scan time. Set this at a reasonable rate for the message size you are accepting. The default value is at 1000 files.

---

**Category** | **Description**
--- | ---
Database log update interval Logs are uploaded for reports and message tracking at this interval. For quicker updates to Message tracking, you can lower this to one minute. However, you will have more regular connections to the database instead of fewer connections but sending more data during each. The default value is set at 1 minute.
Number of days to keep logs for query. This is the amount of days to keep the logs in the database which can be used to control the size of the database. Remember if you set it under 30 days, you will lose monthly report functionality. The default value is set at 30 days.
Number of days to keep in log files Log files should be kept as long as necessary. Care should be taken to keep past log files for an extended period of time to prevent hard drive space consumption. Input 0 to remove any size restriction. Clear the input box to prevent IMSS from deleting any log files. The default value is set at 90 days.
Maximum log file size for each service Acceptable values are between 100 and 2048. As above, please keep hard drive storage in mind. Input 0 to remove any size restriction. The default value is set at 2000 MB.
Administration -> Updates -> Components

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>USAGE / NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Scheduled Update</td>
<td>It is recommended to enable scheduled update to be performed at least hourly. If hourly is specified, change the minute interval so all Trend Micro products do not update at a single time which could cause a drop in the amount of bandwidth available.</td>
</tr>
</tbody>
</table>

### 6.1.2 Notifications

Administration -> Notifications -> Events

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>USAGE / NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery queue contains more messages than</td>
<td>This number should be scaled based on the amount of messages received by the IMSS installation. (Example: If you receive 100,000 emails a day, it should be set much lower than if you receive 1,000,000 emails a day). The default value is set at 20000 messages</td>
</tr>
<tr>
<td>Retry queue folder contains more messages than</td>
<td>Much like the delivery queue, this number should be scaled based on the amount of messages received by the IMSS installation. The default value is at 10000 messages</td>
</tr>
</tbody>
</table>

**NOTE** It is best to get the baseline of Mails in Delivery Queue and Mails in Deffered Queue during peak operation to set the values. Also, note that if the there is a large influx of emails, the notification can be trigger, so the setting can be increased to reflect this normal behavior.

Administration -> Notifications -> Delivery Settings

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>USAGE / NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>To Addresses</td>
<td>This should list all of the administrative email addresses which require notifications in the “Events” tab. All policy based notifications are configurable for different addresses.</td>
</tr>
<tr>
<td>Server name or IP Address SMTP Server Port</td>
<td>The server IP address of the IMSVA machine should be listed here with a port number of 10026. This is a bypass port where no scanning will occur. If you’d like to filter your own notifications, a port of 10025 or 25 can be used. Care should be taken as this adds additional load to the server and notifications could get filtered by your policies.</td>
</tr>
</tbody>
</table>
6.1.3 SMTP Routing

Administration -> SMTP Routing -> Connections

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simultaneous Connections</td>
<td>This is the Postfix simultaneous SMTP client connection setting (maxproc column for smtpt in master.cf). The default value is 200. That is good number to start with then can be increased gradually depending on the available CPU and RAM of the server, if needed.</td>
</tr>
<tr>
<td>Incoming Transport Layer Security Settings</td>
<td>See Section 8.3 for more information about TLS and certificates</td>
</tr>
</tbody>
</table>

Administration -> SMTP Routing -> Message Rule

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Message Size</td>
<td>This is the Postfix message size limit setting (message_size parameter in main.cf). The value depends on the company policy. In most customers, the limit is 5mb to 10mb. The default value is at 20 MB. If the size is larger than this, it will be rejected during the mail transaction. This is more efficient than taking action on the size of the message in Security Settings or a Size policy.</td>
</tr>
<tr>
<td>Maximum number of recipients (1 to unlimited)</td>
<td>This is the Postfix single message recipient limit setting (smtpd_recipient_limit parameter in main.cf). This is the maximum number of recipients allowed for a single message. A large number of recipients can cause delays during policy matching. If more recipients are specified in the mail envelope, they will receive a 452 Too many recipients error and it’s up to the sending mail server to split and retry the message. Most of the time, legitimate mails will only have less than 100 recipients. The default value is at 1000 recipients.</td>
</tr>
<tr>
<td>Incoming Message Settings</td>
<td>This is a Postfix anti-relay setting (relay_domains parameter in main.cf). To ensure that IMSVA receives incoming messages, Trend Micro recommends adding all internal domains in your network.</td>
</tr>
<tr>
<td>Permitted Senders of Relayed Mail</td>
<td>This is another Postfix anti-relay setting (mynetworks parameter in main.cf). Add the ip addresses or network addresses of the hosts that you want to be able to send mails through postfix regardless of the destination domain.</td>
</tr>
</tbody>
</table>
Administration -> SMTP Routing -> Domain-based Delivery

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>USAGE / NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Delivery Settings</td>
<td>All domains should be listed that to be used as SmartHosts. IMSVA will use DNS to delivery other domains.</td>
</tr>
</tbody>
</table>

### 6.1.4 Cloud Pre-Filter

In order to use Cloud Pre-Filter, administrator should has control on their MX records, or at least has a way to request MX records change.

**Mail flow impact for inbound mail**

Enabling Cloud Pre-filter will change the inbound mail flow demonstrated as below:

- **Without Cloud Pre-Filter**

- **With Cloud Pre-Filter**
6.1.5 Steps to enable DDA integration

1. Open IMSVA web console, navigate to Policy ➔ Scan Engine, and select “Enable Advanced Threat Scan Engine” to enable ATSE.

2. Navigate to Administration ➔ IMSVA Configuration ➔ Deep Discovery Advisor Configuration, enable DDA and configure DDA server info. An example as following chart:

<table>
<thead>
<tr>
<th>Server:</th>
<th>192.168.0.58</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server port:</td>
<td>443</td>
</tr>
<tr>
<td>API key:</td>
<td>65B56780-A817-4270-AD8A-3948E3625CA3</td>
</tr>
</tbody>
</table>

// Administrator can get API key from DDA console ➔ Administrator ➔ About info.

1. Administrator can query DDA analysis status from IMSVA web console:

6.2 > Policy Settings

6.2.1 Policy Routing

Enter the “Internal Addresses” which can be either domains or LDAP groups. When selecting “Both Incoming and Outgoing”, you will have to specify all the internal domains for which IMSS is accepting mail.
The easiest way is to gather all your internal domains in a text file. The file can be imported under the “Internal Addresses” area so IMSS will correctly know Incoming vs. Outgoing in the reports. If you are using incoming messages or outgoing messages, in the Recipients and Senders section of the policy creation, you can create a new Address Group and import all your domains.

6.2.2 Global Antivirus Rule

Scanning Conditions

For the scanning conditions of the Global Antivirus Rule in the GUI (Policy -> Policy List -> Global antivirus rule -> And scanning conditions match), it is recommended to have IntelliTrap turned on for better protection. Please also enable as many Spyware/Grayware Scan options as your company policy will allow.

Action on Special Viruses

For the actions on special viruses found in the Policy -> Policy List -> Global antivirus rule -> The action is --> Special Viruses, it is recommended to keep the setting for mass-mailing viruses enabled and the action to be delete. This way all email messages that are detected to be mass-mailers will be deleted and will not enter your network.

6.2.3 Regular Expressions

InterScan Messaging Security Virtual Appliance (IMSVA) 8.5 treats all keyword expressions as regular expressions and supports the following regular expressions.

Characters

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>. (dot)</td>
<td>Any character (byte) except newline</td>
</tr>
<tr>
<td>x</td>
<td>The character 'x'</td>
</tr>
<tr>
<td>\</td>
<td>The character ''</td>
</tr>
<tr>
<td>\a</td>
<td>The alert (bell) character (ASCII 0x07)</td>
</tr>
<tr>
<td>\b</td>
<td>1. If this meta-symbol is within square brackets [] or “”, it will be treated as the backspace character (ASCII 0x08). For example, \b or &quot;\b&quot;</td>
</tr>
</tbody>
</table>
Regular Expression | Description
--- | ---
| 2. If this meta-symbol is at the beginning (or end) of a regular expression, it means any matched string of the regular expression must check whether the left (or right) side of the matched string is a boundary. For example, 
a) \bluck \rightarrow left side must be boundary. 
b) luck\b \rightarrow right side must be boundary. 
c) \bluck\b \rightarrow both sides must be boundary. 
3. If this meta-symbol appears in the middle of a regular expression, it would cause a syntax error.
\f | The form-feed character (ASCII 0x0C)
\n | The newline (line feed) character (ASCII 0x0A)
\r | The carriage-return character (ASCII 0x0D)
\t | The normal (horizontal) tab character (ASCII 0x09)
\v | The vertical tab character (ASCII 0x0B)
\n | The character with octal value 0n (0 <= n <= 7)
\nnn | The character with octal value 0nn (0 <= n <= 7)
\mnnn | The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh | The character with a hexadecimal value 0xhh, for example, \x20 means the space character

Bracket Expression and Character Classes

Bracket expressions are a list of characters and/or character classes enclosed in brackets ‘[]’. Use bracket expressions to match single characters in a list, or a range of characters in a list. If the first character of the list is the carat “^” then it matches characters that are not in the list.

For example:

<table>
<thead>
<tr>
<th>Expression</th>
<th>Matches</th>
</tr>
</thead>
<tbody>
<tr>
<td>[abc]</td>
<td>a, b, or c</td>
</tr>
<tr>
<td>[a-z]</td>
<td>a through z</td>
</tr>
<tr>
<td>[^abc]</td>
<td>Any character except a, b, or c</td>
</tr>
<tr>
<td>[[:alpha:]]</td>
<td>Any alphabetic character (see below)</td>
</tr>
</tbody>
</table>

Each character class designates a set of characters equivalent to the corresponding standard C isXXX function. For example, [alpha] designates those characters for which isalpha() returns true, i.e. any alphabetic character. Character classes must be within bracket expression.
### Character class

<table>
<thead>
<tr>
<th>Character class</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:alpha:]</td>
<td>Alphabetic characters</td>
</tr>
<tr>
<td>[:digit:]</td>
<td>Digits</td>
</tr>
<tr>
<td>[:alnum:]</td>
<td>Alphabetic characters and numeric characters</td>
</tr>
<tr>
<td>[:cntrl:]</td>
<td>Control character</td>
</tr>
<tr>
<td>[:blank:]</td>
<td>Space and tab</td>
</tr>
<tr>
<td>[:space:]</td>
<td>All white space characters</td>
</tr>
<tr>
<td>[:graph:]</td>
<td>Non-blank (not spaces, control characters, or the like)</td>
</tr>
<tr>
<td>[:print:]</td>
<td>Like [:graph:], but includes the space character</td>
</tr>
<tr>
<td>[:punct:]</td>
<td>Punctuation characters</td>
</tr>
<tr>
<td>[:lower:]</td>
<td>Lowercase alphabetic</td>
</tr>
<tr>
<td>[:upper:]</td>
<td>Uppercase alphabetic</td>
</tr>
<tr>
<td>[:xdigit:]</td>
<td>Digits allowed in a hexadecimal number (0–9a–fA–F)</td>
</tr>
</tbody>
</table>

For a case-insensitive expression, [:lower:] and [:upper:] are equivalent to [:alpha:].

### Boundary Matches

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Beginning of line</td>
</tr>
<tr>
<td>$</td>
<td>End of line</td>
</tr>
</tbody>
</table>

### Greedy Quantifiers

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>R?</td>
<td>Matches R, once or not at all</td>
</tr>
<tr>
<td>R*</td>
<td>Matches R, zero or more times</td>
</tr>
<tr>
<td>R+</td>
<td>Matches R, one or more times</td>
</tr>
<tr>
<td>R(n)</td>
<td>Matches R, exactly n times</td>
</tr>
<tr>
<td>R(n, )</td>
<td>Matches R, at least n times</td>
</tr>
</tbody>
</table>
R\{n,m\}  \quad \text{Matches R, at least n but no more than m times}

- R is a regular expression.
- Trend Micro does not recommend using ".*" in a regular expression. ".*" matches any length of letters and the large number of matches may increase memory usage and affect performance.
  - For example: If the content is 123456abc, the regular expression ".*abc" match results are:
    - 12345abc
    - 23455abc
    - 3456abc
    - 456abc
    - 56abc
    - 6abc
  - abc
  
  In this example, replace ".*abc" with "abc" to prevent excessive use of resources.

### Logical Operators

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RS</td>
<td>R followed by S (concatenation)</td>
</tr>
<tr>
<td>R\mid S</td>
<td>Either R or S</td>
</tr>
<tr>
<td>R\slash S</td>
<td>An R but only if it is followed by S</td>
</tr>
<tr>
<td>(R)</td>
<td>Grouping R</td>
</tr>
</tbody>
</table>

- R and S are regular expressions.

### Shorthand and meta-symbol

eManager provides the following shorthand for writing complicated regular expressions. eManager will pre-process expressions and translate the shorthand into regular expressions. For example, \{D\}+ would be translated to [0-9]+. If a shorthand is enclosed in bracket expression (i.e., \{\}) or double-quotes, then eManager will not translate that shorthand to regular expression.

<table>
<thead>
<tr>
<th>Shorthand</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(D)</td>
<td>[0-9]</td>
</tr>
<tr>
<td>(L)</td>
<td>[A-Za-z]</td>
</tr>
</tbody>
</table>
Shorthand | Description
--- | ---
(SP) | \[(),\|\@\|\]}
(NUMBER) | [0-9]+
(WORD) | [A-Za-z]+
(CR) | \r
(LF) | \n
(LWSP) | [ \t]
(CRLF) | (\r\n)
(WSP) | [ \t\f]+
(ALLC) | .

eManager also provides the following meta-symbols. The difference between shorthand and meta-symbols is that meta-symbols can be within a bracket expression.

<table>
<thead>
<tr>
<th>Meta-symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>\s</td>
<td>[[[:space:]]]</td>
</tr>
<tr>
<td>\S</td>
<td>[^[[:space:]]]</td>
</tr>
<tr>
<td>\d</td>
<td>[[[:digit:]]]</td>
</tr>
<tr>
<td>\D</td>
<td>[^[[:digit:]]]</td>
</tr>
<tr>
<td>\w</td>
<td>[_[[:alnum:]]]</td>
</tr>
<tr>
<td>\W</td>
<td>[^[[:alnum:]]]</td>
</tr>
</tbody>
</table>

Any keyword used by default will be used as a partial match. “keyword” matches akeyword and mykeywords. To specify the exact match, surround your keyword with “\s” without the quotations.

\skeyword\s will match “keyword” only.

Literal string and escape character of regular expressions:
To match a character that has a special meaning in regular expressions (e.g. ‘+’), you need to use the backslash ‘\’ escape character. For example, to match string “C/C++”, use the expression C\/C\+/+.

Sometimes, you have to add many escape characters to your expression (e.g. C\/C\+/+). In this situation, enclose the string “C/C++” in double-quotes (e.g. .REG “C/C++”) then the new expression is equivalent to the old one. Characters (except ‘\’ which is an escape character) within double-quotes are literal. Following are some examples,

<table>
<thead>
<tr>
<th>Expression</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>“C/C++”</td>
<td>Match string “C/C++” (does not include double-quotes)</td>
</tr>
<tr>
<td>“Regular\x20Expression”</td>
<td>Match string “Regular Expression” (does not include double-quotes), where \x20 means the space character.</td>
</tr>
<tr>
<td>&quot;[xyz]&quot;foo&quot;</td>
<td>Match the literal string: [xyz]&quot;foo</td>
</tr>
</tbody>
</table>

**NOTE** It is not recommend to use the wild card expression. i.e. “.*” This is CPU intensive and can cause performance issues. It is best be as specific in the expression to minimize the false positives.

### 6.2.4 Filter Ordering

The best practice for ordering filters is putting everything that will block the most email towards the top of the list, especially if the action is Delete. It is our practice for our hosted services to apply spam filtering first before any other rule. Using the figure below which is taken from actual client data; we can determine that the majority of mail is removed at the IP and SMTP level. (~75% when ERS with the QIL database and Recipient Checking via LDAP are enabled) Normally, virus activity accounts for .01% of all valid emails and usually much less.
6.2.5 Creating “Global White List” for Inbound Mails

In order to avoid false positive, administrator sometimes might have a request that IMSVA not to do any scanning for some end users’ mails.

Administrator can address this request with referring to the following steps:

1) Open IMSVA web console.

2) Navigate to Policy ➔ Address Groups, and create a new address agroup, named “Global White List” with some end users mail address in this group.

3) Go to Policy ➔ Policy List, and add a new incoming rule:
   a) **Recipients and Senders**: From “Anyone” to “Global White List” address agroup.
   b) **Scanning Conditions**: None, this means every mail that sends to “Global White List” address agroup will trigger this rule.
   c) **Actions**: Hand off to mail server.
   d) **Rule Name**: Global White List

**NOTE**: If the Default spam rule is not deleted, the Global antivirus rule could be used first for security reason.
e) **Order Number:** Can be set to under antivirus rule, and above spam rule, such as 2.

4) Save the rule and do some testing to make sure IMSVA works fine.

   ![Policy List > Rule Summary](image)

   With this setting, any incoming mail that sends to “Global White List” address agroup will trigger this rule, and IMSVA will then hand off the triggered mails to mail server directly without checking the remained rules.

### 6.2.6 Separating Phishing/WRS Checking from Anti-Spam Rule

IMSVA 8.5 can synchronize all quarantined messages that do not violate virus, phishing, or Web reputation rules, to the EUQ database. Some IMSVA users did not notice this. If administrator wants to enable Phishing/WRS checking, in order to avoid misunderstanding & convenient to manage WRS/Phishing mails, we suggest separating Phishing/WRS checking from Anti-Spam rule.

1) Make sure to uncheck Phishing/WRS in anti-spam rule (Default spam rule).

2) Create a new rule with enable Phishing/WRS checking. (To use WRS, spam detection settings will be enabled.)
   a) **Recipients and Senders:** Similar as anti-spam rule.
   b) **Scanning Conditions:** Enable Phishing or WRS as needs.
   c) **Actions:** Quarantine or any other action, such as tag subject.
   d) **Rule Name:** Could be such as “Phishing & WRS”.

   ![If recipients and senders are](image)
   ![And scanning conditions match](image)
   ![Then action is](image)
6.2.7 Scan Method

IMSVA 8.5 contains two types of scan method:

<table>
<thead>
<tr>
<th>Scan Method</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Scan</td>
<td>High detection rate and can only use global smart scan server.</td>
</tr>
<tr>
<td>Conventional Scan</td>
<td>Better performance. This is default setting.</td>
</tr>
</tbody>
</table>

6.2.8 C&C Contact Alert Services

With C&C Contact Alert Services, IMSVA has the ability to inspect the sender, recipients and reply-to addresses in a message's header, as well as URLs in the message body, to see if any of them matches known C&C objects.

If enabled “Synchronize all messages that do not violate virus, phishing, or Web reputation rules, to the EUQ database”, IMSVA will synchronize C&C filter quarantined mails to EUQ database.
We suggest having a separate C&C rule for those who wants to use C&C Contact Alert service. Administrators can configure IMSVA to quarantine such messages and send a notification when a message is flagged.

### 6.2.9 Scan Engine

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus Scan Engine (VSAPI)</td>
<td>- The Virus Scan Engine employs basic pattern matching and heuristic scanning technology to identify threats.</td>
</tr>
<tr>
<td></td>
<td>- Lower false positive.</td>
</tr>
<tr>
<td>ATSE (Advanced Threat Scan Engine)</td>
<td>- ATSE performs aggressive scanning to check for less conventional threats such as document exploits.</td>
</tr>
<tr>
<td></td>
<td>- Better detection rate.</td>
</tr>
<tr>
<td></td>
<td>- Malware name starts with either HURE_ or EXPL_.</td>
</tr>
<tr>
<td></td>
<td>- With DDA, IMSVA can send ATSE detects possible advanced threats to DDA for further analysis.</td>
</tr>
</tbody>
</table>

### 6.3 Configuration Files

IMSx 8.5 utilizes a database to store all system-wide configurations. This includes policy, system settings, and program configurations. Each configuration file in use by IMSVA utilizes the same database naming convention and takes effect over any settings stored in the database. The majority of entries will be commented out by adding “#” at the start of the line. When a line is commented out, IMSS uses the setting from the database. Configuration files are marked with “.ini” while you can easily see what settings IMSS is getting from the database by viewing the “.ini.db” files. The “.ini.db” files are only to view the configuration settings currently set in the database. Changing the “.db” files will have no effect.

#### 6.3.1 imss.ini File

The imss.ini contains all configurations related to the scan processes for both SMTP and POP3. There are also some program configurations such as log file locations. The scan process is able to scale automatically to increase load conditions. The default settings are recommended.

The configuration in this file has the higher priority than the configuration in database.

#### 6.3.2 foxdns.ini File

This is IP Profiler configuration file.
By default, the IP Profiler function does not automatically remove a temporarily blocked IP address. Mail clients from these blocked IP addresses will always get a 421 error.

These IP addresses have to be manually removed by the IMSS administrator. There is a hidden key “keep_tempblocked_mins” that should be added to the foxdns.ini file. This will remove the blocked IP address automatically and according to the interval set by the key.

Refer to the following KB for details:


### 6.4 Database

A text file of the settings in the database **table tb_global_setting** can be found on IMSVA server in the `/opt/trend/imss/config/imss.ini.db` file. These db files are just copies of the settings in the database. If the settings in the database are changed, the db files get overwritten with the new settings.

IMSVA uses the setting in the database table **tb_global_setting** if this setting is not seen in the imss.ini file. If you would like to change the setting of IMSS, you can do the following.

- If you are going to update the configuration in the database, check the corresponding configuration file and use the parameter, its description and the value as a basis for your update.

- If the configuration parameter is not listed in the configuration file, check the configuration file database (db-file). The `imss.ini.db` file keeps the definitions of the configuration settings that can be used in the `imss.ini` file.

**NOTE** Changes made to the database will affect all of the IMSS in a group. Changes made to local files will only affect the local appliance.
6.4.1 Updating the configuration settings in the database

Although it’s a lot easier to manipulate database entries using a GUI-based Postgres client, you can also use the `psql` interpreter supplied with the PostgreSQL server to manage the global configuration settings in the database. A short summary of `psql` commands is seen below.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>IMPLEMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Establish new connection / Change the database / Change the username</td>
<td><code>psql &lt;DbName&gt; &lt;User&gt;</code> \c &lt;DbName&gt; \c - &lt;UserName&gt;</td>
</tr>
<tr>
<td>Exit</td>
<td><code>\q</code></td>
</tr>
<tr>
<td>Execute SQL-query</td>
<td><code>&lt;Query&gt; ;</code></td>
</tr>
<tr>
<td>Execute SQL-script</td>
<td><code>\i &lt;ScriptFile&gt;</code></td>
</tr>
<tr>
<td>Describe a structure of a stored object</td>
<td><code>\d &lt;ObjectName&gt;</code></td>
</tr>
<tr>
<td>Duplicate standard output into a file</td>
<td><code>\o &lt;File&gt;</code></td>
</tr>
</tbody>
</table>

The example below shows how to view the num_sockets parameter in section socket of the imss.ini configuration file using the SELECT SQL-command:

```
[root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/psql imss sa
Welcome to psql 8.1.3, the PostgreSQL interactive terminal.
Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit
imss=# select value from tb_global_setting where section='socket' and
name='num_sockets' and inifile='imss.ini';
value
```
The example below shows how to set the downstream_smtp_server_port parameter in the smtp section of the imss.ini file to 10026 using the UPDATE SQL command.

```
[root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/psql imss sa
Welcome to psql 8.1.3, the PostgreSQL interactive terminal.
Type:   \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit
imss=# update tb_global_setting set value='10026' where name='downstream_smtp_server_port' and section='smtp' and inifile='imss.ini';
```

```
UPDATE 1
imss=# \q
[root@imsva85 ~]#
```

If the configuration parameter does not exist in the tb_global_setting table (for example, when the default values is used), use the INSERT SQL command to define this configuration setting. The following example shows how to define the generic_greeting_msg setting in the [pop3] section of the imss.ini and set it to ‘Have a great day!’:

```
```
[root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/psql imss sa

Welcome to psql 8.1.3, the PostgreSQL interactive terminal.

Type: \copyright for distribution terms

\h for help with SQL commands
\? for help with psql commands
\g or terminate with semicolon to execute query
\q to quit

imss=# insert into tb_global_setting values ('pop3', 'generic_greeting_msg', 'Have a great day!', 'imss.ini', ' ');

\g

Recommended database configuration changes

- Whole Mail Scan

Some viruses and malwares might hide themselves in different parts of the email. This makes scanning of only a few parts of the email ineffective in detecting such viruses and malwares. To prevent hiding virus or malware codes in different parts of the email, IMSS has the Whole Mail Scan feature that scans not only the parts of the email extracted by the Message Module but also the whole email as it is. To configure this behavior, an administrator should set the VSIWholeMailScan parameter to “1” in the tb_global_setting table in the Administration Database. This can be accomplished using the psql tool as shown below:

imss=# update tb_global_setting set value='1' where name='VSIWholeMailScan' and section='virus' and inifile='imss.ini';

For the configuration change in the database to take effect, the imssd daemon must be restarted either via the Administration Console or by running the S99IMSS script.

- ProxyAddresses with Microsoft Exchange
When Exchange is installed, it extends the existing Active Directory schema by adding a number of attributes for every user. One of these attributes, “proxyAddresses”, is used to store multiple email addresses for a particular user. By default, IMSS does not analyze the email addresses stored there. To enable this check, change the mail attribute to “proxyAddresses” by updating the database:
imss=# update tb_global_setting set value='proxyAddresses' where name='mail_attr';
UPDATE 1

6.4.2 Database Maintenance Schedule

The pre-configured maintenance jobs, IMSVA will do by default, vary a little depending on the version you have installed. In GM build (1165), it will only be a bare minimum which should be fine for the average use of IMSVA, but might not be sufficient if you were stingy with the disc space you granted IMSVA or if you are processing a lot of messages.

Problem 1 – Running out of transaction IDs
You will most likely never see this unless you process more than a million messages a day and have your IMSVA running for a very long time.
In short; Due to a field size limitation, PostgreSQL only has a limited number of XIDs (transaction IDs) which will at some point wrap around and cause the DB to stop working as a preventive measurement.
You can find all the technical details here at THIS link.
http://www.postgresql.org/docs/8.1/static/maintenance.html#VACUUM-FOR-WRAPAROUND

To avoid this issue happening on your IMSVA parent, please make sure IMSVA build newer than 1266 (Suggest to install Patch 1 once it is available). It will run the maintenance job of (vacumdb -Usa -az) every Saturday at 3 AM by default.

More details can be found in the Patch readme.

Problem 2 - The database keeps growing
Neither two existing maintenance jobs reclaim unused disc space back from the DB because this task might consume a lot of time and resources. Therefore the admin “you” will need to arrange these jobs in accordance to your system load, maintenance schedule and whatever is necessary. The FULL VACUUM will block tables while cleaning up which might delay or even cause minor failures for message processing. So keep this in mind when scheduling this job.

You could run the FULL VACUUM in an interactive session using “screen” or “nohup” to avoid a session timeout from killing your vacuum job.
Preferably you should create a crontab that will do this task on a routinely bases.
For a manual execution type: `/opt/trend/imss/PostgreSQL/bin/vacuumdb -af -U sa`
Please see the crontab manual on how to configure the task according to your needs.

6.5 > Others

6.5.1 Spam Settings

The typical SPS scanning result is presented using the following three X-headers:

The descriptions of the important sections of the X-headers are listed below.

**Trend Score:** This score is determined using all the Rule Files of the anti-spam engine. Every match of the rule or the database entry has a numeric value (score). The Trend Score is a sum of the scores for all matches.

**Trend Type:** This has a value of 1 (spam) by default. The value 2 (phish) appears if there is a match in the phish database. The other two values (3 and 4) are not currently used and are there for future enhancements.

**Trend Category:** The anti-spam engine identifies the most probable category for the content using its rule file. IMSA currently ignores the Trend Category and does not use it for the spam / not spam decision. Categorization may be included in future releases.

**Detection Threshold:** Each Threshold corresponds to the Administration Console settings configured for the Spam Rule.
The calculated Trend Score is compared with the Detection Threshold. If the Trend Score is higher or equal, the email is classified as spam:

\[
\text{Trend\_Score} \geq \text{Detection\_Threshold}
\]

Depending on the email characteristics coming into your environment, you will have to adjust the spam thresholds on the Administration Console settings. If you get a header result similar to the one above and you feel that the email message is not spam, you can change the spam threshold to Low or specify a threshold of 6 in order for the message to get through.

### White Listing

If you would like to receive email messages that are being tagged as spam by IMSVA, you can add the sender of these messages to the Approved Senders list in the Spam Rule. This will prevent future messages from this sender from being tagged as spam.
Submitting Samples to Trend Micro

If you feel you have instances when the anti-spam engine is giving a low score to spam messages (not detecting spam) or giving a high score to non-spam messages (false positives), please submit these samples to Trend Micro. This will help enhance our anti-spam engine rules. Please see the following solution bank articles on how to submit samples.


6.5.2 EUQ SMTP Authentication

The classic End User Quarantine with LDAP authentication comes with some limitations. The one most noticeable is that it does only support the use of a single LDAP group which consists of up to 2 LDAP servers for a single architecture. Once a secondary group is added, for an alternative architecture or domain for example, the EUQ will be disabled.

SMTP authentication will provide an alternative for environments that need to support a larger mixed set of end users that might be in different LDAP domains, architectures or possibly not within an LDAP group at all.

To enable this new method, you simply select SMTP-AUTH in the AdminUI and configure each domain and its corresponding SMTP server that can do the authentication. Subdomains and wildcards are also supported as seen in the screenshot below.
End-User Quarantine

![EUQ Management](image)

**Enable EUQ Feature**

- Use LDAP for EUQ authentication
- Use SMTP Server for EUQ authentication

Specify recipient domains and SMTP server addresses.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Server/Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain1.com</td>
<td>1.2.3.4:25</td>
</tr>
<tr>
<td>domain2.com</td>
<td>1.2.3.5:25</td>
</tr>
<tr>
<td>*subdomain1.com</td>
<td>1.2.3.6:25</td>
</tr>
</tbody>
</table>

6.5.3 Rule Samples

- Creating “Global White List” for Inbound Mails

Refer to section 6.2.5 for details.
Enhanced Anti-Spoofing Feature

IMSVA contains Anti-Spoofing filter, it can detects and takes action on a message that has the sender domain that is the same as the recipient(s) domain, and the message does not come from an internal IP address.

This will only check envelope address.

In order to check both envelope address and mail header address as following chart, administrator can create a rule to check both anti-spoofing filter and mail header address.

Assume domain is corelab.cn, the related rule could be set as below:

1. Click Policy → Keywords & Expression, and create a new keyword expression “From” as below:

2. Create a new incoming rule (Other type), from Anyone to *@corelab.cn;
3. For Scanning Conditions, use default “any condition matched (OR)”, and select “Header keyword expressions” & “Spoofed internal messages” filter.
4. For “Header keyword expressions” filter, check **From** header, and use the keyword expression “**From**” that created in Step 1.

1. For “Spoofed internal messages” filter, set the **Trusted Internal IP**, we usually need to add mail server IP as Trusted Internal IP. IMSVA will not checking the mails from listed IP addresses.

2. Set the action as want, such as quarantine the mail.
3. Set the rule name & rule order number, such as set rule name “Anti Spoofing Rule”. Rule summary info as below chart:

<table>
<thead>
<tr>
<th>Policy List &gt; Rule Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enable</strong></td>
</tr>
<tr>
<td><strong>Rule Name:</strong> Anti Spoofing Rule</td>
</tr>
<tr>
<td><strong>Order Number:</strong> 10</td>
</tr>
</tbody>
</table>

If recipients and senders are
- incoming
- to *@corelab.cn*
- AND
- from Anyone

And scanning conditions match
- Specified Header matches ...
- OR
- Spoofed internal messages

Then action is
- Quarantine message

1. Doing some testing to make sure this rule works fine.
   - Insert disclaimer for outgoing email messages

Email disclaimer usually been practiced as a standard in corporate email messaging systems.

Administrators can generate disclaimer referring to following steps.

1.1. On IMSVA web console, click Policy ➔ Stamps, add a “Disclaimer” stamp.
1.2. Click Policy ➔ Policy List, add a new outgoing rule (other type), from internal domain to anyone.
1.3. Leave blank for “Scanning Conditions” setting.
1.4. For “Action” part, select “Do not intercept messages” and “Insert stamp in body”, and use “Disclaimer” as stamp.
2. Save the rule with name “Disclaimer”. Rule summary info as below chart:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td></td>
</tr>
<tr>
<td>Rule Name:</td>
<td>Disclaimer</td>
</tr>
<tr>
<td>Order Number:</td>
<td>11</td>
</tr>
</tbody>
</table>

If recipients and senders are outgoing to Anyone AND from *@corelab.cn

And scanning conditions match

Then action is Insert stamp in body

3. Doing some testing to make sure the rule works fine.
Chapter 7: Backup and Disaster Recovery

This section will provide best practices for backing up the IMSA configuration files and for disaster recovery. Backing up and restoring the configuration files and the database are two major parts of this section.

7.1 > Backup and Restore from the GUI

Backup

Backing up IMSVA configuration files is simple. Just go to the GUI -> Administration -> Import/Export -> Export configuration files. Download the package and store.

Restore

To restore the IMSVA configuration previously backed up, go to the GUI -> Administration -> Import/Export -> Import configuration files. Browse to your backup and click Import.

7.2 > Manual Database Backup and Recovery

The Backup and Restore procedure above will back up the IMSA configurations. It is also a good idea to back up the database itself. You can backup the imss and imsseuq database for recovery at a later time. Below is the procedure. Just change all instances of imss to imsseuq if the euq database is the one being worked on.

Backup
You can use the `pg_dump` command to backup or create a dump of the existing database. This command creates an SQL-script containing the statements required to create, initialize and insert data in the database.

The example below shows how to create a dump of the `imss` database in the `/tmp/imss_dump.sql` file:

```
[root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/pg_dump -U sa -f /tmp/imss_dump.sql imss
[root@imsva85 ~]#
```

The example below shows how to create a dump of the `imss` database in the `/tmp/imss_dump.gz` compressed file:

```
[root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/pg_dump imss -U sa | gzip >
```

The example below shows how to backup the `imsseuq` database to the `/tmp/imsseuq_dump.sql` file:

```
[root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/pg_dump -U sa -f /tmp/imsseuq_dump.sql imsseuq
[root@imsva85 ~]#
```

Recovery

If you have a backup you can recreate the database and import the data from backup using the following procedure. If you are recovering the `imsseuq` database, just replace all instances of `imss` with `imsseuq`.

- Use the `rcImss` script to stop the IMSS software:
  
  ```
  [root@imsva85 ~]#/etc/init.d/rcImss stop
  Shutting down imssmgrmon 9951 ...
  Shutting down imssmgr 10177 ...
  ...
  Central Controller stopped.
  waiting for postmaster to shut down.... done
  postmaster stopped
  ```

  1. Use the `dbctl.sh` script to start the PostgreSQL database server:

  ```
  [root@imsva85 ~]#/opt/trend/imss/script/dbctl.sh start
  ```
waiting for postmaster to start.... done
postmaster started

- Use the dropdb command to drop the existing database:

  [root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/dropdb -h 127.0.0.1 -U sa imss

  DROP DATABASE

Use the createdb command to create the new imss database:

  [root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/createdb -h 127.0.0.1 -U sa -E unicode imss

  CREATE DATABASE

- Use the createlang command to add procedure language to the database:

  [root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/createlang -h 127.0.0.1 -U sa -d imss plpgsql

  [root@imsva85 ~]#

- Restore the database from the backup:

  [root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/psql imss sa < /tmp/imss_dump.sql > /dev/null

  ERROR: language "plpgsql" already exists

  [root@imsva85 ~]#

- Restore the database from the backup compressed file:

  [root@imsva85 ~]# /usr/bin/gunzip –c /tmp/imss_dump.gz | psql imss –u sa

  [root@imsva85 ~]#
Recovering a lost GUI password

The password of the “admin” user is stored in the database, in hashed form. To recover from the lost password, run the following command from shell:

```bash
[root@imsva85 ~]# /opt/trend/imss/PostgreSQL/bin/psql imss sa -c "update tb_administrator set md5_digest='bdd725fd5707063fd845b763b5237600' where admin_name='admin';"
```

The next time you log into the GUI, your password will be reset to the default password, 'imsva'.

7.3 > Backing up and Restoring Cloud Pre-filter account settings.

- **Whole IMSVA configuration file**
  IMSVA configuration file contains Pre-Filter account info. This is also the most convenient way to backup & restore whole IMSVA settings that include Pre-Filter account setting.
  From IMSVA web console, navigate to Administration → Import/Export, administrator can export & import configuration file.

- **Backup Cloud Pre-Filter Account**
  1. On IMSVA web console, navigate to Cloud Pre-Filter page, and click “Cloud Pre-Filter Account Information”.
  2. On the new opened Pre-Filter account page, you can find account name info. Click “Export Key File” button to export the key.
  3. Save the key file with the filename contains account name, such as Pre-Filter_AccountName.key.

- **Restore Cloud Pre-Filter Account**
  Administrator can register a new Pre-Filter account or restore an exist Pre-Filter account on IMSVA server without Pre-Filter info included.
  1. On IMSVA web console, navigate to Cloud Pre-Filter page.
  2. Select “Yes” for “Do you have a Cloud Pre-Filter account” item.
  3. Provide Pre-Filter account name and key file, and click “Authentication” button.
Please be noted that all of the Pre-Filter related settings are stored in the cloud, restore previous backup info will not restore Pre-Filter settings.
Chapter 8: References

8.1 Communication Ports

If there are firewalls or similar devices between IMSS components, it is important to open specific IMSS communication ports.

The tables below are the list of communication ports used by different IMSS components when communicating with each other. The first column is the IMSS Components while the third column is the remote components it is connecting.

<table>
<thead>
<tr>
<th>IMSS Component</th>
<th>Port</th>
<th>Remote IMSS Component to connect to</th>
<th>When to open</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scanner Server</td>
<td>TCP/UDP 53 (DNS port)</td>
<td>Central Controller Server</td>
<td>open this port when using IP-Profiler</td>
</tr>
<tr>
<td></td>
<td>TCP 15505</td>
<td>Central Controller Server &amp; EUQ Server</td>
<td>open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 5432 (Postgres)</td>
<td>IMSS Admin Database</td>
<td>open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 25 (SMTP)</td>
<td>Upstream and Downstream MTA servers</td>
<td>open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 110 (POP3)</td>
<td>Upstream POP3 servers and POP3 clients</td>
<td>open this port when POP3 scanning is enabled.</td>
</tr>
<tr>
<td></td>
<td>TCP 5060</td>
<td>Policy Server</td>
<td>open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 163 (SNMP)</td>
<td>SNMP server</td>
<td>open this port when using SNMP Notification</td>
</tr>
<tr>
<td></td>
<td>TCP 389 or 3268 (LDAP)</td>
<td>Directory Server</td>
<td>open this port when LDAP is enabled</td>
</tr>
<tr>
<td></td>
<td>TCP/UDP 53 (DNS port)</td>
<td>Network DNS server</td>
<td>open this port when using NRS</td>
</tr>
<tr>
<td></td>
<td>TCP 443/80</td>
<td>TMCM Server and WRS</td>
<td>open this port when CM-Agent is enabled</td>
</tr>
<tr>
<td></td>
<td>UDP 10323 (HTTPS/HTTP)</td>
<td>TMCM Server</td>
<td>open this port when CM-Agent is enabled</td>
</tr>
<tr>
<td>IMSS Component</td>
<td>Port</td>
<td>-Remote IMSS Component to connect to</td>
<td>-When to open?</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------</td>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Central Controller</td>
<td>TCP 15505</td>
<td>-Scanner Server</td>
<td>-open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 5432</td>
<td>-IMSS Admin Database</td>
<td>-open all the time</td>
</tr>
<tr>
<td></td>
<td>(Postgres)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 389 or 3268</td>
<td>-Directory Server</td>
<td>-open this port when LDAP is enabled</td>
</tr>
<tr>
<td></td>
<td>(LDAP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 8445</td>
<td>-hosts that need to access IMSS Web Admin Console</td>
<td>-open all the time</td>
</tr>
<tr>
<td></td>
<td>UDP 10323</td>
<td>-TMCM Server</td>
<td>-open this port when CM-Agent is enabled</td>
</tr>
<tr>
<td></td>
<td>(HTTPS/HTTP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 443/80</td>
<td>- TMCM Server</td>
<td>-open this port when CM-Agent is enabled</td>
</tr>
<tr>
<td></td>
<td>(HTTPS/HTTP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 9000</td>
<td>- Cloud Pre-Filter</td>
<td>-open this port when using Cloud Pre-Filter is enabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMSS Component</th>
<th>Port</th>
<th>-Remote IMSS Component to connect to</th>
<th>-When to open?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary EUQ Server</td>
<td>TCP 8446</td>
<td>-Secondary EUQ servers</td>
<td>-open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 389 or 3268</td>
<td>-Directory Server</td>
<td>-open all the time</td>
</tr>
<tr>
<td></td>
<td>(LDAP)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP 445</td>
<td>-Directory Server</td>
<td>-open this port to use Single Sign On</td>
</tr>
<tr>
<td></td>
<td>TCP 8447</td>
<td>-hosts that need to access IMSS Web EUQ Console</td>
<td>-be open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 15505</td>
<td>-Scanner Server</td>
<td>-open all the time</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IMSS Component</th>
<th>Port</th>
<th>-Remote IMSS Component to connect to</th>
<th>-When to open?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary EUQ Server</td>
<td>TCP 8446</td>
<td>-Primary EUQ Server</td>
<td>-open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 15505</td>
<td>-Scanner Server</td>
<td>-open all the time</td>
</tr>
<tr>
<td></td>
<td>TCP 389 or 3268</td>
<td>-Directory Server</td>
<td></td>
</tr>
</tbody>
</table>
### 8.2 ERS Console

The ERS part of the IP-Filter module has an online configuration console where you can do administrative tasks necessary to implement ERS effectively.

https://tmspn.securecloud.com/ers

Since ERS is an online database shared by other users, there will be situations where you have to tweak ERS settings to fit your environment. Below are some of the common settings you may want to change.

1. Dynamic (QIL) Sensitivity Setting (Policy | Reputation Settings)

   If you use the Dynamic (database), there will be isolated situations where in some emails, that you want to reach your network, will be temporarily blocked if the sender’s IP is in our Dynamic database. It is because an automated system, which is comprised of “catch servers” and spam analyzers, is use to update the Dynamic database. The system will list the IP on the Dynamic database for a specific amount of time depending on the amount of spams it received.

   The Dynamic Settings allows you to select the level of aggressiveness fit for your environment. Select Level 3 to start with then adjust if necessary.

2. Policy Settings (Policy | Settings)

   An IP-address will end up in our database only if we received SPAM mails from it or our investigation showed that it is a known spammer. If you need to receive emails from an IP-address regardless if it is sending SPAMS or not, Trend recommends using the Approved and Blocked lists instead of submitting an IP-Removal request.

   Trend cannot just remove IP-Addresses from its online database because it also needs to protect other users from SPAMs from these IP-addresses.

   You can do the following under the Policy Settings sections.
• Add an IP-address to the Approved List or Blocked List.
• Add an entire IP block to the Approved List or Blocked List. ERS console accepts CIDR format
• Add an entire ISP to the Approved List or Blocked List.
• Add an entire country to the Approved List or Blocked List.

**IP-Removal Requests**

Trend accepts IP-Removal requests to remove IP-addresses from any of its databases. However, it is also very important to maintain the integrity of the database to be effective in stopping spams. This is why it is important for the requester to follow the below guidelines before Trend can facilitate the removal of IP-addresses.

• Trend will only coordinate the removal process with the owner of the IP-address.
• Trend will only provide spam samples to the owner of the IP-Address
• The request should be sent to the correct email address depending on the block list the IP was found. Use the URL below to know which block list the IP is included.

http://mail-abuse.com/lookup.html

Please go to www.mail-abuse.com website for more detailed information.

**8.3 > TLS (Transport Layer Security) Settings**

IMSVA 8.5 has default TLS certificate files included, and administrator can enable TLS directly with default key files.

Please refer to IMSVA 8.5 administration’s guide “Chapter 12: Configuring Transport Layer Security Settings” for more detailed information.

**8.4 > Product Updates**

Please keep your product up-to-date at all times. You can check the link below for the latest Service Pack or Patch for IMSVA 8.5
8.5 > Upgrade/Migration

- IMSVA 8.5 supports to:
  - Upgrade from IMSVA 8.2 SP2 with critical patch 17000 applied.
  - Migrate from:
    - IMSS 7.1 Windows
    - IMSS 7.1 Linux
    - IMSVA 8.0 Patch2
    - IMSVA 8.2 SP2

Please see Chapter 5, “Upgrading From Previous Versions”, of the Trend Micro InterScan Messaging Security Virtual Appliance v8.5 Installation Guide.