



Trend Micro InterScan Messaging Security Virtual Appliance 9.1

Best Practice Guide



Anti-Spyware



Anti-Spam



Antivirus



Anti-Phishing



Content & URL
Filtering



Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Copyright © 2017 Trend Micro Incorporated. All rights reserved.

No part of this publication may be reproduced, photocopied, stored in a retrieval system, or transmitted without the express prior written consent of Trend Micro Incorporated.

All other brand and product names are trademarks or registered trademarks of their respective companies or organizations.

Authors: Bryan Xu

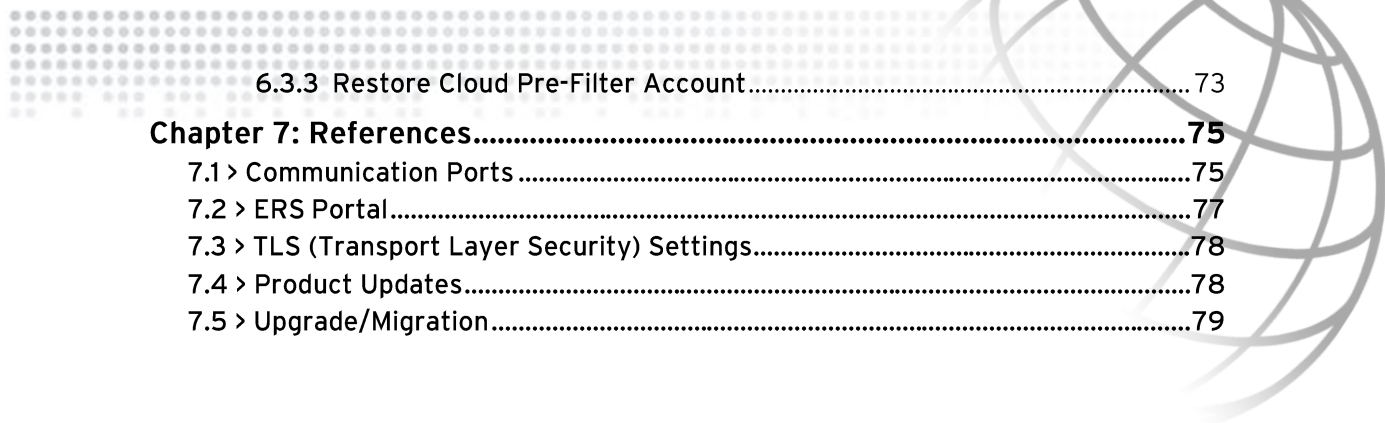
Released: Oct 2017



Table of Contents

Table of Contents	3
Preface	6
Chapter 1: Product Description	7
Chapter 2: Hardware	8
2.1 > IMSVA 9.1 Performance	8
2.1.1 Testing environment	8
2.1.2 Testing Messages	8
2.1.3 Testing Scenarios	10
2.1.4 Testing Results	10
2.2 > Sizing Guidelines	12
2.3 > Recommended Hardware	14
2.3.1 IMSVA Server	14
Chapter 3: Software	15
3.1 > Recommendations	15
3.1.1 LDAP	15
3.1.2 TCM	15
3.1.3 Database	15
3.1.4 Logging	16
3.1.5 Syslog	16
3.1.6 Virtual Analyzer (DDAN) server version requirement	16
Chapter 4: Deployment	17
4.1 > Network Topology	17
4.1.1 INTERNET → IMSVA → Mailbox servers	17
4.1.2 INTERNET → MTA → IMSVA → Mail box servers	17
4.2 > Component Layout	18
4.3 > Fault Tolerance and Load Balancing	22
Chapter 5: Product Configuration	24
5.1 > GUI Configuration	24
5.1.1 Scanning Exceptions	24
5.1.2 Notifications	26
5.1.3 SMTP Routing	27
5.1.4 Message Delivery Settings	28
5.1.5 Cloud Pre-Filter	29
5.1.6 Syslog Log	29
5.1.7 Steps to enable Virtual Analyzer (DDA / DDAN) integration	30
5.2 > Policy Settings	31

5.2.1 Policy Routing	31
5.2.2 Global Antivirus Rule.....	32
5.2.3 Regular Expressions.....	32
5.2.4 Filter Ordering.....	37
5.2.5 Creating “Global White List” for Inbound Mails	38
5.2.6 Compliance (DLP).....	39
5.2.7 Separating Phishing/WRS Checking from Anti-Spam Rule	40
5.2.8 Scan Method.....	41
5.2.9 Email Encryption	41
5.2.10 C&C Contact Alert Services	42
5.2.11 Scan Engine	42
5.2.12 Submission of messages to the Virtual Analyzer	42
5.2.13 DKIM.....	45
5.2.14 Time-of-Click Protection	54
5.3 > Integrating IMSVA with Virtual Analyzer.....	55
5.4 > Configuration Files.....	55
5.4.1 imss.ini File.....	55
5.4.2 foxdns.ini File	55
5.4.3 foxproxy.ini File	56
5.5 > Database.....	56
5.5.1 Updating the configuration settings in the database.....	58
5.5.2 Database Maintenance Schedule.....	61
5.5.3 Problem 1 - Running out of transaction IDs	61
5.5.4 Problem 2 - The database keeps growing	62
5.6 > Ransomware Protection	62
5.6.1 Improve Ransomware Detections Visibility	62
5.6.2 Handling Macro Files.....	64
5.6.3 Handling Executable Files.....	64
5.7 > Others	65
5.7.1 Spam Settings	65
5.7.2 White Listing.....	66
5.7.3 Submitting Samples to Trend Micro	66
5.7.4 EUQ SMTP Authentication	67
5.7.5 Rule Samples	68
Chapter 6: Backup and Disaster Recovery	70
6.1 > Backup and Restore from the GUI	70
6.1.1 Backup	70
6.1.2 Restore	70
6.2 > Manual Database Backup and Recovery	70
6.2.1 Backup.....	70
6.2.2 Recovery.....	71
6.2.3 Recovering a lost GUI password.....	73
6.3 > Backing up and Restoring Cloud Pre-filter account settings.....	73
6.3.1 Whole IMSVA configuration file	73
6.3.2 Backup Cloud Pre-Filter Account.....	73



6.3.3 Restore Cloud Pre-Filter Account.....	73
Chapter 7: References.....	75
7.1 > Communication Ports.....	75
7.2 > ERS Portal.....	77
7.3 > TLS (Transport Layer Security) Settings.....	78
7.4 > Product Updates.....	78
7.5 > Upgrade/Migration.....	79



Preface

Welcome to *Trend Micro InterScan Messaging Security Virtual Appliance v9.1 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 v9.1 Installation Guide
- Trend Micro InterScan Messaging Security Virtual Appliance v9.1 Administrator's Guide
- Trend Micro IMSVA 9.1 Reviewers Guide.

Chapter 1: 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 IMSVa server that allows administrators to manage multiple IMSVa Scanners using one IMSVa Web Console.
2. **Scanner Service** – Accepts and scans SMTP and POP3 connections.
3. **EUQ Service** – End User Quarantine service which allows end users to check their quarantined “spam” mails to verify if they are spam or not. The first server where EUQ will be installed on, will become the Primary EUQ server the end-users will connect to. The 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 2: Hardware

On top of the normal MTA tasks of receiving and delivering emails, IMSVA 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.

2.1 > IMSVA 9.1 Performance

2.1.1 Testing environment

ESX Platform:

12 CPUs , E5-2620v2 @ 2.10GHz

32GB memory,

1.8 TB SCSI 15k rpm disk

Gbps NIC

Software: VMware ESX 5.5

Virtual Machine: 8 CPU / 16G Memory / 250GB

IMSVA configuration: GM build with schedule update disabled

2.1.2 Testing Messages

Average of testing messages size: 177(KBytes). Test profile/sample definition:

Component	Detail	Ratio (%)	Rule Match	Avg size (KB)
Spam		16	spam	3.5
Virus	joke test virus - Spyware/grayware dragimgcntrl -	0.2	Global antivirus rule: Virus spyware/grayware	43

	virus(one of them trigger Smartscan method)			
Probable advanced threat	Atse level 2 sample	0.1	ATSE probable advanced threat, send to DDA	52
password protected	password protected	0.5	Default rule for the attachment protected by password	11
DKIM	DKIM enforcement not trigger	1		2
Suspicious SO	CTD	0.2		646
Suspicious URL	CTD	1		2
WRS	WRS	1		4
url rewrite	URL time of click(11 url with 4 unrated)	1		2
Attachment normal	zip	4		357
	eml file	4		18
	excel	4		516
	jpg	4		323
	pdf	4		1330
	ppt	4		819
	word	4		501
plain text, normal		26		60
Other clean sample		25		19
Total		100		177

2.1.3 Testing Scenarios

With the same policy and same samples, four scenarios were tested on SMTP performance:

- Comparison of SMTP Scan performance with default rule of IMSVA9.1 and IMSVA 9.0
- DDAN load balance performance in IMSVA 9.1
- SMTP Traffic Throttling performance in IMSVA9.1
- Connected Threat Defense (CTD) performance in IMSVA9.1
- All new features enabled performance in IMSVA 9.1

2.1.4 Testing Results

- **Basic SMTP scan performance**

This is the SMTP performance test result for IMSVA9.1 and IMSVA9.0 with default setting and rules:

Scenario	Throughput(msg/s)	CPU	IO_wait	Memory usage
IMSVA 9.0	46.4	64.65	1.76	39.63
IMSVA 9.1	45.83(-1.2%)	70.45(+9%)	2.68	41.22

Compared with IMSVA 9.0, IMSVA 9.1 CPU usage increased. The main reason is that IMSVA 9.1 enables some new features by default.

- **DDAN load balance Performance**

Scenario	Throughput(msg/s)	CPU	IO_wait	Memory usage
IMSVA 9.1 basic	45.83	70.45	2.68	41.22
IMSVA 9.1 with 1 DDAN enabled	45.30	71.53	3.01	41.95
IMSVA 9.1 with 1 DDAN enabled	45.30	71.14	2.97	41.35

During testing, with DDAN enabled, IMSVA 9.1 sent 0.1% of all samples to DDAN server. The performance on IMSVA 9.1 is almost not affected. When integrated with DDAN, the bottleneck is DDAN's performance.

- **SMTP Traffic Throttling Performance**

Scenario	Throughput(msg/s)	CPU	IO_wait	Memory usage
IMSVA 9.1 basic	45.83	70.45	2.68	41.22
Enables SMTP Traffic Throttling	44.20 (-3.6%)	71.61 (+1.6%)	2.62	40.00

SMTP Traffic Throttling is one of IMSVA 9.1's new features. When enabled, throughput is downgraded (3.6%) compared to its basic SMTP scan performance.

- **Connected Threat Defense (CTD) performance**

Scenario	Throughput(msg/s)	CPU	IO_wait	Memory usage
IMSVA 9.1 basic	45.83	70.45	2.68	41.22
Enables CTD	44.77 (-2.3%)	75.00 (+6.5%)	3.08	42.15

With CTD enabled, CPU usage will increase and throughput will drop a little.

- **All new features enabled performance**

IMSVA configuration:

- Enable WRS
- Enable ATSE
- Configure 2 DDAN servers
- Configure 2 local SPS servers
- Enable LDAP encrypted communication
- Enable Syslog Server setting
- Enable SMTP Traffic Throttling
- Enable Time-of-Click unrated URL rule

- Enable TCMC
- Enable CTD
- Use External database

Scenario	Throughput(msg/s)	CPU	IO_wait	Memory usage
IMSVa 9.1 basic	45.83	70.45	2.68	41.22
All new features on with internal DB	40.67 (-11.3%)	79.65 (+13.1%)	2.9	40.16
All new features on with external DB	44.63 (-2.6%)	72.56 (+3%)	2.0	42.45

Using external DB improves IMSVA 9.1's scanning performance.

2.2 > 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 on IMSVA 9.1 performance testing results.

When sizing planning for IMSVA 9.1, 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** in testing environment.

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 IMSVA gateway. If IMSVA 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 IMSVA at the gateway should not be included in 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/hour IMSVA can process without queuing.

Use the following tables to determine the Maximum Steady Throughput. Take note that these data assumes that the user is using the default IMSVA settings and rules. The values may vary if additional rules are used but these numbers make a very good baseline as seen in other customers.

Volume Category	Estimated Seats per Server	Throughput	Server Hardware
High Specification	~30,000	270,000 Messages per hour (75 Messages per second)	12 CPUs Intel Xeon E5-2620v2 64GB RAM 1.8TB SCSI 15k rpm Disk
Virtualized Deployment	~20,000	162,000 Messages per hour (45 Messages per Second)	Intel Xeon E5-2620v2 CPU 8 virtual CPUs 16GB RAM 250G Disk

NOTE 📖 Notes on Test Results

- Dedicated host (only one IMSVA 9.1 virtual machine running on this host)
- Default Configuration of IMSVA 9.1
- LDAP / EUQ inactive
- The above sizing estimates imply no message queuing on the IMSVA server.
- Average message size 177 KB
- Any customized rules will downgrade the performance.
- 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.
- With one Compliance (DLP) template enabled, performance would downgrade about 51%.
- With all Compliance (DLP) template enabled, performance would downgrade about 79%.

STEP 2: Determine the number of IMSVA servers required.

Number of servers = Total Throughput / Max Steady Throughput

Assume that the max steady throughput could be the 50% of max throughput.

I.e. Ave Msg size is 177KB. IMSVA 9.1 with the High Volume specs and the Total Throughput is 300,000 Mgs/hour

$$\begin{aligned}\text{Number of servers} &= 300,000 / (270,000 * 0.5) \\ &= 2.22\end{aligned}$$

In this example, the number of IMSVA servers recommended is 3 (1.25 rounded up).

NOTE 📖 The data present is based on IMSVA 9.1. Using Content Filter with complex rules and other options can greatly reduce the throughput. Please refer to IMSVA 9.1 performance testing results for more detailed information.

2.3 > 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.

IMSVA 9.1 uses CentOS 6.4 x86_64, for bare mental installation, the server which supports CentOS 6.4 x86_64 would support IMSVA 9.1.

2.3.1 IMSVA Server

Below are the recommended hardware specifications for an IMSVA Server:

NOTE 📖 These are not the minimum system requirements for this product.

CPU: Intel(TM) Xeon(TM) E5-2620v2 or above

RAM: 16 GB or above

Disk Drive: 15,000RPM hard disk drive or faster

Chapter 3: Software

This section will go over software best practices for IMSVA. Since IMSVA is a virtual appliance, there is no need to worry about hardening or tuning the software. This section will give guidelines on the third party software that are used by IMSVA.

3.1 > Recommendations

3.1.1 LDAP

IMSVA supports the following three types of LDAP servers:

- Microsoft Active Directory 2008 R2, 2012 or 2012 R2
- IBM Lotus Domino 8.0, 8.5, 9.0
- Sun One LDAP 5.2 or above
- OpenLDAP 2.4.23

3.1.2 TMCM

- Version 5.5 Service Pack 1 Patch 4
- Version 6.0 Service Pack 3 Patch1 Hotfix 3262

3.1.3 Database

IMSVA 9.1 supports external PostgreSQL database. The admin database and EUQ database can be installed either on the internal or external database server.

If required to use external DB, please do the following:

1. Make sure the account used to install the IMSVA admin database has the super user role.

2. Manually change the maximum number of database connections to 600:
 - a) Edit postgresql.conf file.
 - b) Set `max_connection = 600` (default 100).
 - c) Restart DB service (service postgresql-9.2 restart OR systemctl restart postgresql).
3. Make sure that IMSVA and the external database server use the same timezone and time settings. Otherwise, some unexpected issues may happen.

3.1.4 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, the configured number of days for storing event logs (under **Logs | Settings**) and quarantined/archived events (under **Quarantine & Archive | Settings**) can be decreased and lessen the number of reports to save (under **Reports | Settings**).

3.1.5 Syslog

IMSV 9.1 supports sending logs through the syslog protocol to multiple external syslog servers in a structured format. You can send different event log types to multiple syslog servers.

3.1.6 Virtual Analyzer (DDAN) server version requirement

- DDAN 5.0
- DDAN 5.5
- DDAN 5.8

Chapter 4: Deployment

This section will go over deployment best practices for IMSVA. Here, recommendations are given to the placement of IMSVA in relation to the mailboxes and the MTA(s). Information can be taken on which components that can be enabled/disabled on each IMSVA and different load balancing / fault tolerance techniques that are commonly used.

4.1 > Network Topology

IMSVA 9.1 comes with Postfix, which is a complete MTA. This allows to IMSVA anywhere in the email topology just like any other MTA. However, if there is an intention to use the IP Filtering and Graymail features, we suggest placing IMSVA on the edge of the network. If IMSVA could not be placed on the edge while still preferring to use IP Filtering and Graymail features, the administrator should enable known hosts feature (UI → Administration → IMSVA Configuration → Known Hosts), so that IMSVA will use upstream MTA's IP address instead of known hosts' IP address for scanning.

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 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.

4.1.1 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.

4.1.2 INTERNET → MTA → IMSVA → Mail box servers

In this scenario, if IP Filtering is to be used, the administrator needs to enable Known Host feature add MTA's IP as known host.

4.2 > Component Layout

See the InterScan Messaging Security Virtual Appliance Installation Guide and InterScan Messaging Security Virtual Appliance 9.1 Administrator's Guide for an explanation on the parent-child relationship between the IMSVA and groups.

IMSVA 9.1 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.

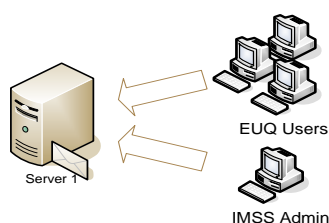


Figure 1. Single Server Deployment

- 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 ERS and IP Profiler are intended to be used and the IMSVA server is not on the “edge” of the network, Known Host feature should be used so that IMSVA will use upstream MTA's IP address instead of known hosts' IP address for scanning.
- If more than one LDAP server is enabled, EUQ using LDAP authentication and EUQ single sign-on cannot be enabled.
- 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.

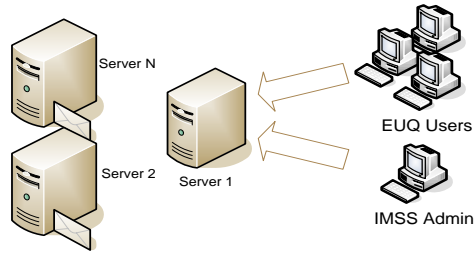


Figure 2. Distributed Deployment (medium-size environment)

- 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.

More virtual appliances can be added 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 2.2 Sizing Guidelines to determine how many IMSVA Scanner servers are necessary to support the environment.

Considerations:

- If ERS and IP Profiler are intended to be used and the IMSVA server is not on the “edge” of the network, Known Host feature should be used so that IMSVA will use upstream MTA’s IP address instead of known hosts’ IP address for scanning.
- EUQ users should have access to Server 1, which is hosting the Primary EUQ Server.
- If more than one LDAP server is enabled, EUQ using LDAP authentication and EUQ single sign-on cannot be enabled.
- 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, this can be set 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 could be disabled on the parent virtual appliance, if possible, to avoid its overload.

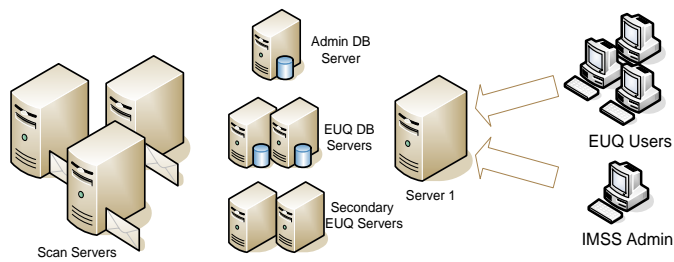


Figure 3. Distributed Deployment (large-size environment)

- 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 2.2 Sizing Guidelines to determine how many IMSVA Scanner servers are necessary to support the environment.

Considerations:

- If ERS and IP Profiler are intended to be used and the IMSVA server is not on the “edge” of the network, Known Host feature should be used so that IMSVA will use upstream MTA’s IP address instead of known hosts’ IP address for scanning.
- EUQ users should have access to Server 1, which is hosting the main EUQ Server.
- If more than one LDAP server is enabled, EUQ using LDAP authentication and EUQ single sign-on cannot be enabled.

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.

4.3 > 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 that determines which node should process which request is handled by the hardware, away from the nodes. Adding, removing, or updating equipment to the group is also 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 As) 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):

server1.mydomain.tld	IN	A	192.168.1.20;
server2.mydomain.tld	IN	A	192.168.1.21;
server3.mydomain.tld	IN	A	192.168.1.22;
server4.mydomain.tld	IN	A	192.168.1.23;
proxy.mydomain.tld	IN	CNAME	server1.mydomain.tld;
proxy.mydomain.tld	IN	CNAME	server2.mydomain.tld;
proxy.mydomain.tld	IN	CNAME	server3.mydomain.tld;
proxy.mydomain.tld	IN	CNAME	server4.mydomain.tld;

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 5: Product Configuration

This section will go over the different configuration best practice for IMSVA. The IMSVA configuration can be changed 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 IMSVA will use the configuration settings if there is a conflict between the local files and the database, is based on the setting specified in the local ini files. If the particular setting is not found in the local ini files, IMSVA will use the setting in the database.

The next sections will focus on the different configuration methods.

5.1 > GUI Configuration

5.1.1 Scanning Exceptions

Policy -> Scanning Exceptions -> Security Settings Violations

Category	Description
Total message size exceeds	This is the maximum size a message including attachment can be. Set this according to the company policy. The default value is set to 30 MB.
Total # recipients exceeds	The maximum number of recipients allowed within a single message. Messages with a lot of recipients can cause increased latency in message rule matching.
Total # embedded layers in compressed file exceeds	A <i>layer</i> is defined by a compressed file within a compressed file, and has been used in previous attacks to hide malware deeper than scan 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 used to prevent zip file attacks. The size set here should be relative to the total message size limit. As an example, if the maximum message size is set 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, although small in size, could cause significant scan time. Set this at a reasonable rate for the message size being accepted. The default value is at 1000 files.

Logs -> Settings

Category	Description
Database log update interval	Logs are uploaded for reports and message tracking at this interval. For quicker updates to Message tracking, it may be lowered to one minute. However, there will be 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. If set under 30 days, the monthly report functionality may be lost. The default value is set at 30 days.
Application log detail level:	The level of log detail. Default is "Normal". Diagnostic or debug logs might consume excessive IMSVA resources and could reduce system performance. Debug level is normally used for troubleshooting purposes.
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 IMSVA 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 stated above, keep hard drive storage in mind. Input 0 to remove any size restriction. The default value is set at 2000 MB.

Administration -> Updates -> Components

PARAMETER	USAGE / NOTES
Enable Scheduled Update	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.

5.1.2 Notifications

Administration -> Notifications -> Events

PARAMETER	USAGE / NOTES
Delivery queue contains more messages than	This number should be escalated based on the amount of messages received by the IMSVA installation. (Example: If 100,000 emails a day is received, it should be set much lower than if receiving 1,000,000 emails a day). The default value is set at 20000 messages.
Retry queue folder contains more messages than	Much like the delivery queue, this number should be scaled based on the amount of messages received by the IMSVA installation. The default value is at 10000 messages

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

Administration -> Notifications -> Delivery Settings

PARAMETER	USAGE / NOTES
To Addresses	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.
Server name or IP Address SMTP Server Port	The default setting is to use 127.0.0.1:10026 as notification server, and it is suggested to keep it on default.

5.1.3 SMTP Routing

Administration -> SMTP Routing -> Connections

Category	Description
Simultaneous Connections	This is the Postfix simultaneous SMTP client connection setting (<code>maxproc</code> column for <code>smtpd</code> in <code>master.cf</code>). The default value is 200, which is a good number to start with, then can be increased gradually depending on the available CPU and RAM of the server, if needed.

Note: Suggest to keep the default setting for this page.

Administration -> SMTP Routing -> Message Rule

Category	Description
Maximum Message Size	This is the Postfix message size limit setting (<code>message_size</code> parameter in <code>main.cf</code>). The value depends on the company policy. In most customers, the limit is 5mb to 10mb. The default value is at 10 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.
Maximum number of recipients (1 to 99999)	This is the Postfix single message recipient limit setting (<code>smtpd_recipient_limit</code> parameter in <code>main.cf</code>). 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 is 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.
Relay Control	<ul style="list-style-type: none"> Reject unknown sender domains. //This will reject client request if DNS lookup cannot find a matching sender's domain. Reject unknown recipients. (by checking LDAP) //With LDAP configured, this feature can block those non-existent recipients. For Microsoft AD & Exchange environment, please enable alias supporting. Administration → End-User Quarantine → User Quarantine Access, and select "Allow end users to retrieve quarantined email messages with alias email addresses". Reject unknown IP address. //RDNS checking.

Category	Description
Incoming Message Settings	This is a Postfix anti-relay setting (<code>relay_domains</code> parameter in <code>main.cf</code>). To ensure that IMSVA receives incoming messages, Trend Micro recommends adding all internal domains in the network.
Permitted Senders of Relayed Mail	This is another Postfix anti-relay setting (<code>mynetworks</code> parameter in <code>main.cf</code>). Add the IP addresses or network addresses of the hosts where the mails will be sent through postfix regardless of the destination domain. The IP addresses in the list are allowed to use IMSVA to relay the mails out.

Administration -> SMTP Routing -> Message Delivery

PARAMETER	USAGE / NOTES
Message Delivery Settings	All destination domains should be listed that to be used as SmartHosts. IMSVa will use DNS to deliver other domains.

5.1.4 Message Delivery Settings

From IMSVA 9.0 contains a new feature that allows you to group multiple downstream MTA for better load balance and failover capabilities.

In order to address this, IMSVA uses the Delivery Policy Server **imssdps** daemon to listen on port 10030 and determine the next SMTP hop.

IMSVa 8.5 and previous version, the delivery setting in Postfix `main.cf` file is stated as:

```
transport_maps = hash:/opt/trend/imss/postfix/etc/postfix/transportList
```

From IMSVA 9.0, the delivery setting in Postfix `main.cf` file is stated as:

```
transport_maps = tcp:127.0.0.1:10030
```

In order to make sure to only delivery the mails to available destination MTA, IMSVA can check the connection to the next MTA periodically, so that IMSVA would only deliver the mails to the available MTA.

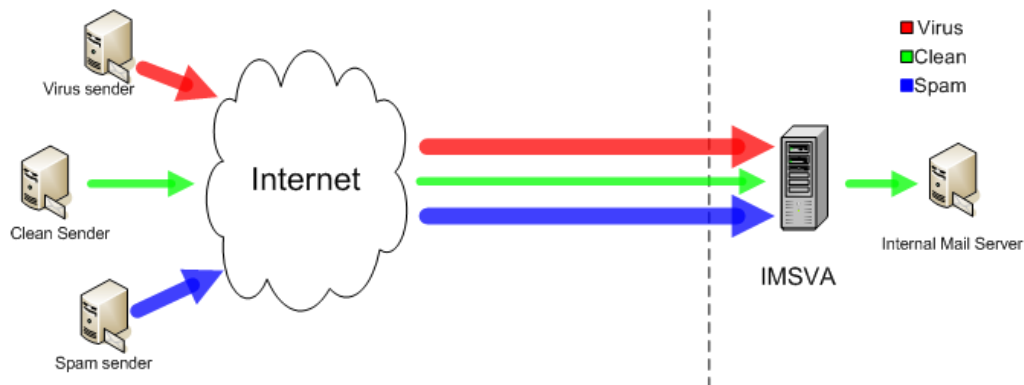
5.1.5 Cloud Pre-Filter

In order to use Cloud Pre-Filter, the administrator has control over the MX records, or at least have a way to request MX records change.

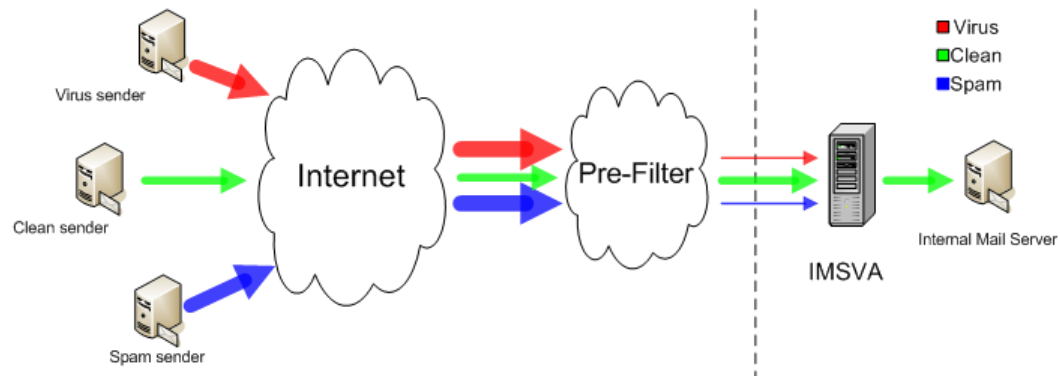
Mail flow impact for inbound mail

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

- Without Cloud Pre-Filter



- With Cloud Pre-Filter



5.1.6 Syslog Log

IMSVA 9.1 supports sending logs through the syslog protocol to multiple external syslog servers in a structured format. You can send different event log types to multiple syslog servers.

- Open the IMSVA web console, Navigate to **Logs > Syslog Settings**.
- The administrator can add a syslog server, and select which type of logs will send to syslog server.

Below are the logs mapping between log types on UI and local log files:

- **Message tracking:** msgtra.imss.*

- **Policy events:** polevt.imss.*
- **System events:** sysevt.imss.*
- **MTA events:** /var/log/maillog*, imssdps.*, tlsagent.*
- **Sender filtering:** foxdns.log.*, foxmsg.*, foxreport.*, ers.imss.*, foxnullmsg.*, connblocked.imss.*, smtpconnagent.*
- **Content scanning:** log.imss.*, imssps.*, wrsagent.*, dtasagent.*
- **Administration:** imssui.*, imssmgr.*, imsstasks.*, euqerror.imss.*, euqretry.imss.*, euqsynch.imss.*, msgsync.imss.*, msgretry.imss.*, Agent.log*, EntityMain.log*

5.1.7 Steps to enable Virtual Analyzer (DDA / DDAN) integration

1. Open the IMSVA web console. Navigate to **Policy > Scan Engine**, and select **Enable Advanced Threat Scan Engine** to enable ATSE. (For SNAP, “True file type” messages & “Name or extension” messages, it is not necessary to enable ATSE scanning.)
2. Navigate to **Policy > Virtual Analyzer**. The **Virtual Analyzer Settings** tab appears by default.
3. For Security Level Settings, choose Low (default) for a more conservative security level. Selecting High will provide a more aggressive security level.
4. For Timing Settings, it is suggested to keep it to default, 1800.

This setting defines the maximum waiting time for the analysis result. If IMSVA cannot get the analysis result from Virtual Analyzer (DDAN) in the maximum waiting time, it will trigger Virtual Analyzer scanning exceptions.

Virtual Analyzer Settings		Server Management
<input checked="" type="checkbox"/> Submit email messages to Virtual Analyzer		
Security Level Settings		
After Virtual Analyzer evaluates the risk level of a message, IMSVA performs the specified action on the message based on the security level configured below.		
<input type="radio"/> High	Apply action on all messages exhibiting any suspicious behavior	
<input type="radio"/> Medium	Apply action on messages with a moderate to high probability of being malicious	
<input checked="" type="radio"/> Low	Apply action only on messages with a high probability of being malicious (recommended)	
Timing Settings		
Maximum time allowed for analysis:	1800	seconds (Value range: 300-1800)

5. Go to **Server Management** tab, and set the DDAN server info.

Server Management > Add Server

Virtual Analyzer Server

☒ Enable

Server:

Example: server.us.trendnet.org or 10.1.1.1

Port:

API key:


Preference:

- Administrators can get the API key from the DDAN web console under **Help > About** info.
 - IMSVA 9.1 supports multiple DDAN servers, and **Preference** represents each server's priority.
6. An Administrator can set the multiple DDAN servers here. The lower the **Preference**, the higher the priority.


Virtual Analyzer Settings

Server Management



Server List



Add



Delete

<input type="checkbox"/>	Server	Port	API Key	Preference	Enable
<input type="checkbox"/>	192.168.0.155	443	91E140D4-2C57-4239-AE55-B26213A63CED	10	
<input type="checkbox"/>	192.168.0.151	443	82C33C43-1182-4827-9BD6-DE10AC9E7185	10	

5.2 > Policy Settings

5.2.1 Policy Routing

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

5.2.2 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), also enable as many Spyware/Grayware Scan options as the 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 the network.

5.2.3 Regular Expressions

IMSV 9.1 treats all keyword expressions as regular expressions and supports the following regular expressions.

Characters

Regular Expression	Description
. (dot)	Any character (byte) except newline
x	The character 'x'
\\	The character '\'
\a	The alert (bell) character (ASCII 0x07)
\b	1. If this meta-symbol is within square brackets [] or "", it will be treated as the backspace character (ASCII 0x08). For example, [\b] or "\b" 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 -> left side must be boundary. b) luck\b -> right side must be boundary.

	c) \bluck\b -> 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 On (0 <= n <= 7)
\nn	The character with octal value Onn (0 <= n <= 7)
\mnn	The character with octal value Omnn (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 is 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:

Expression	Matches
[abc]	a, b, or c
[a-z]	a through z
[^abc]	Any character except a, b, or c
[:alpha:]	Any alphabetic character (see below)

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

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

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

Boundary Matches

Expression	Description
^	Beginning of line
\$	End of line

Greedy Quantifiers

Expression	Description
R?	Matches R, once or not at all
R*	Matches R, zero or more times
R+	Matches R, one or more times
R{n}	Matches R, exactly n times
R{n,}	Matches R, at least n times

Expression	Description
R{n,m}	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

Expression	Description
RS	R followed by S (concatenation)
R S	Either R or S
R/S	An R but only if it is followed by S
(R)	Grouping R

- 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.

Shorthand	Description
{D}	[0-9]
{L}	[A-Za-z]

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.

Meta-symbol	Description
\s	[[:space:]]
\S	[^[:space:]]
\d	[[:digit:]]
\D	[^[:digit:]]
\w	[_[:alnum:]]
\W	[^_[:alnum:]]

Any keyword used by default will be used as a partial match. “Keyword” matches a keyword and mykeywords. To specify the exact match, surround the 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. ‘+’), there is a need to use the backslash ‘\’ escape character. For example, to match string “C/C++”, use the expression C\C\+\+.

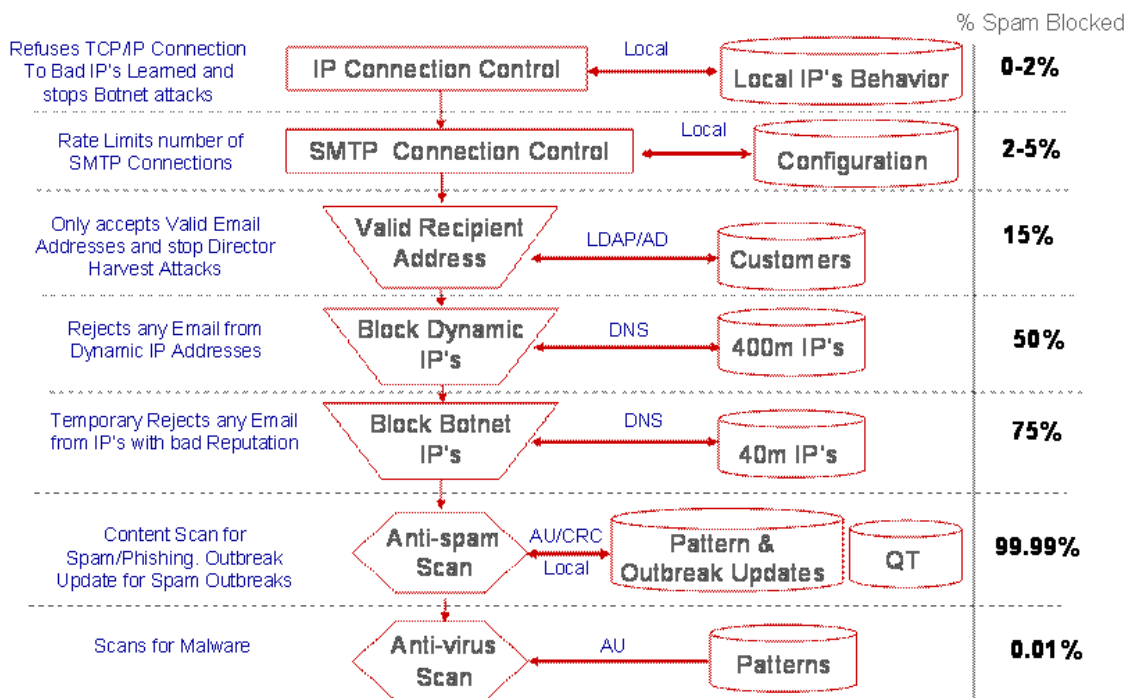
Sometimes, there may be a need to add string “C/C++” in double-quotes (e.g. .REG “C/C++”) then the new expression is equivalent to the old one. Characters (except ‘\’ which is an escape character) within double-quotes are literal. Following are some examples,

Expression	Description
“C/C++”	Match string “C/C++” (does not include double-quotes)
“Regular\x20Expression”	Match string “Regular Expression” (does not include double-quotes), where \x20 means the space character.
“[xyz]\”foo”	Match the literal string: [xyz]”foo

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.

5.2.4 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 the practice for the hosted services to apply spam filtering first before any other rule. Using the figure below which is taken from actual client data; it can be determined 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.



NOTE If the Default spam rule is not deleted, the Global antivirus rule could be used first for security reason.

5.2.5 Creating "Global White List" for Inbound Mails

In order to avoid false positive, an administrator may sometimes request that IMSVA not do any scanning for some end users' mails.

Administrators can address this request by referring to the following steps:

1. Open IMSVA web console.
2. Navigate to Policy → Address Groups, and create a new address a group 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 group.
 - b) **Scanning Conditions:** None, this means every mail that sends to "Global White List" address group will trigger this rule.
 - c) **Actions:** Hand off to mail server.

- d) **Rule Name:** Global White List
 - 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 properly.

[Policy List](#) > Rule Summary

Rule	Notes
<input checked="" type="checkbox"/> Enable	
Rule Name: <input type="text" value="Global White List"/>	
Order Number: <input type="text" value="2"/>	
If recipients and senders are [Edit]	
incoming to Global White List AND from Anyone	
And scanning conditions match [Edit]	
Then action is [Edit]	
Handoff to 192.168.0.8:25	

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

5.2.6 Compliance (DLP)

IMSVA 9.1 DLP supports both predefined and customized DLP compliance templates based on various data identifiers.

IMSVA 9.1 comes with a set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted. Administrators can check the predefined templates from web console > Policy > DLP Compliance Templates.

The predefined templates use a set of predefined expressions, while those expressions also cannot be modified or deleted.

Administrators can go to Policy > Policy Objects > DLP Data Identifiers and view settings for predefined expressions. They can refer to those predefined expressions to customize his/her own DLP expressions.

For example, “China: Mobile Phone Number” uses `[^\d]{0,3}((13)|(15)|(18))\d{9}[^\d]` expression to check 11 digital numbers which begin with 13, 15 or 19.

Follow these major steps to create a customized template with customized expression:

1. Go to **Policy > Policy Objects > DLP Data Identifiers**.
2. Click **Add** to add a new expression.
3. Create the new DLP expression as required.
4. Go to **Policy > Policy Objects > DLP Compliance Templates**.
5. Click **Add** to add a new template.
6. Create the new DLP template using the newly created DLP expression above. Below is a screenshot.

[DLP Compliance Templates](#) > Add Compliance Template

Name and Description

Name*: Bryan_Template

Description:

Digital Asset Definition

Select an asset, adjust the threshold setting if needed, click Add, and then declare the condition.

+ Expression Bryan_Expression Occurrences: 1

Add Clear

Compliance Template Definition

1 Bryan_Expression (1)

Save Cancel

7. Go to **Policy > Policy List**, and add a new DLP rule.
8. For the scanning conditions setting, select “DLP compliance templates” condition, and select newly created DLP template above.
9. Save the rule and test to make sure it works as expected.

5.2.7 Separating Phishing/WRS Checking from Anti-Spam Rule

IMSV 9.1 can synchronize all quarantined messages that do not violate virus, phishing, or Web reputation rules, to the EUQ database. Some IMSV users do not notice this.

If an administrator wants to enable Phishing/WRS checking, in order to avoid misunderstanding make it convenient to manage WRS/Phishing mails, separating Phishing/WRS checking from Anti-Spam rule is suggested:

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 needed.
 - c) **Actions:** Quarantine or any other action, such as tag subject.
 - d) **Rule Name:** Could be such as “Phishing & WRS”.
 - e) **Order Number:** Can be set to under anti-spam rule.
3. IMSVA admin can check the quarantined mails that triggered this rule.

Mail Areas & Queues Management



Quarantine | Archive | Postpone | Deferred

Criteria

Search: Any quarantine | Any reason | All Products

Dates: 08/15/2013 22:00 to

Sender: |

Recipient(s): |

Rule: Phishing & WRS

Display Log

Any reason
 Virus or malicious code
 Probable advanced threats
 Spyware/grayware
 C&C email
 Spam/phish
 Web Reputation
 DKIM enforcement
 Size
 Attachment
 Content
 Compliance
 Scanning exceptions
 Spam Tagged by Cloud Pre-Filter
 Others

All 4 Entries | Deliver | Reprocess | D

1-4 of 4 | Page 1

Result as of 2013年8月22日 23:53:50

Timestamp	Sender	Recipient(s)	Subject	Reason
2013年8月15日 23:37:32	bryan_xu@qq.com	bryan_xu2@corelab.cn	ccca_url	Web Reputation
2013年8月15日 23:37:32	bryan_xu@qq.com	bryan_xu2@corelab.cn	THISISFORTESTPURPOSE	Spam/Phish
2013年8月15日 23:37:32	bryan_xu@qq.com	bryan_xu2@corelab.cn	ccca_url	Web Reputation
2013年8月15日 23:37:32	bryan_xu@qq.com	bryan_xu2@corelab.cn	THISISFORTESTPURPOSE	Spam/Phish

Display: 15 per page

5.2.8 Scan Method

IMSVA 9.1 contains two types of scan method:

Scan Method	Description
Smart Scan	Has high detection rate and can only use global smart scan server
Conventional Scan	Has better performance. This is default setting.

5.2.9 Email Encryption

In order to use this feature, the administrator needs to refer to AG to register the internal domain first, then create a rule setting the action as “Encrypt message” to excrypt the outbound mails.

Below is a similar rule information:

- If recipients and senders are: Set from internal domain to external domain. Administrator to define the detailed domain/addresses info which the mail needs to be encrypted.
- And scanning conditions match: Set the scanning conditions. If kept blank, all mails that the sender/recipient fit to this rule would trigger the rule.
- Then action is: Set the Intercept to “Do not intercept messages”, and Modify as “Encrypt message”.

When the recipient gets an encrypted mail, he can follow the steps mentioned in the encrypted mail to register / log on with the recipient address to decrypt the mail.

5.2.10 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.

Having a separate C&C rule is suggested for those who want to use C&C Contact Alert service.

Administrators can configure IMSVA to quarantine such messages and send a notification when a message is flagged.

5.2.11 Scan Engine

Technology	Description
Virus Scan Engine (VSAPI)	<ul style="list-style-type: none">- The Virus Scan Engine employs basic pattern matching and heuristic scanning technology to identify threats.- Lower false positive.
ATSE (Advanced Threat Scan Engine)	<ul style="list-style-type: none">- ATSE performs aggressive scanning to check for less conventional threats such as document exploits.- Better detection rate.- Malware name starts with either HURE_ or EXPL_.- With DDAN, IMSVA can send ATSE detects suspicious files to DDAN for further analysis.

5.2.12 Submission of messages to the Virtual Analyzer

IMSVA will submit messages to the Virtual Analyzer (DDAN) when enabled. This task is performed in any of the following scenarios:

- When ATSE detects messages containing possible virus, IMSVA will submit these messages to the Virtual Analyzer for double confirmation.
If DDAN’s analysis result shows “No risk”, IMSVA will dismiss ATSE’s detection and pass the mail to the next rule.
- If the Administrator enables the **Social Engineering Attack Protection** (SNAP) feature, and this feature detects messages, IMSVA will submit these messages to the Virtual Analyzer for double verification.

[Policy List](#) > [Rule Summary](#) > Scanning Conditions

Take rule action when: any condition matched (OR) ▼

Save

Cancel

C&C Email	
<input type="checkbox"/>	C&C email settings
Phishing/Social Engineering Attack/Spam	
<input checked="" type="checkbox"/>	Phishing email
<input type="checkbox"/>	Social Engineering Attack Protection ⓘ
<input checked="" type="checkbox"/>	Spam detection settings

Figure 4

Scanning process flow:

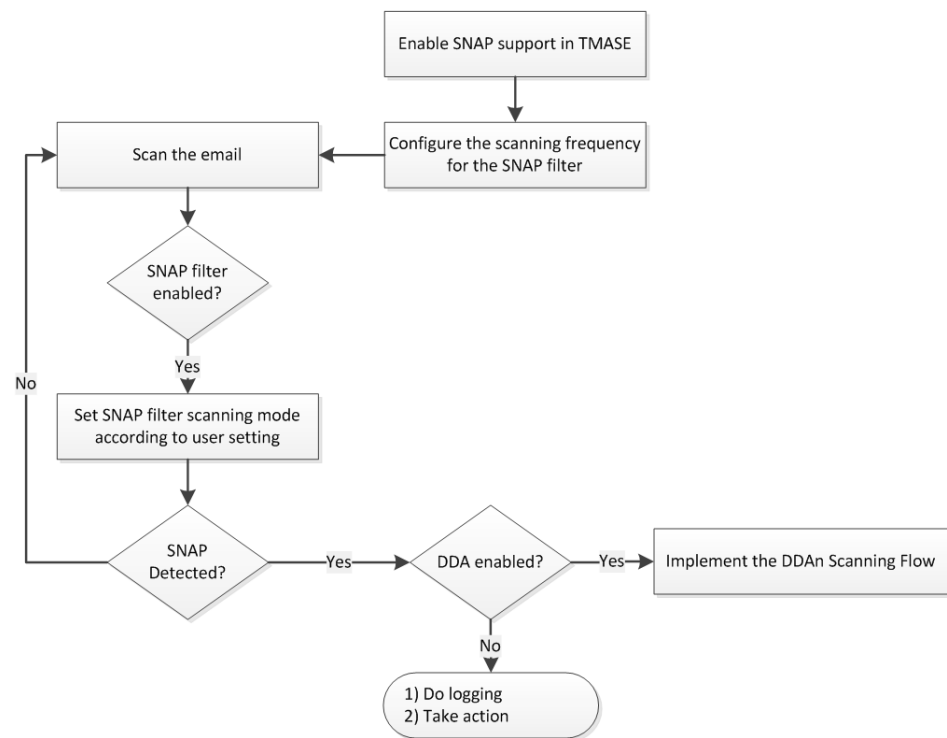


Figure 5

- If the Administrator set to submit any true file type attachments to DDAN, IMSVA will submit the related messages to the Virtual Analyzer for analyzing. Such would be creating a rule to submit executable files, documents and compressed files to Virtual Analyzer for analyzing.

True File Type Selection

Select: Selected attachment types

☒ Executable

☒ Document

☐ Image

☐ Media

☒ Compressed files

☐ Microsoft Windows shortcuts

Virtual Analyzer Scanning

☒ Submit files to Virtual Analyzer

Figure 6

- If the Administrator set to submit any name or extension attachments to DDAN, IMSVA will submit the related messages to the Virtual Analyzer for analyzing. Such would be creating a separate rule to submit *.js files to Virtual Analyzer for analyzing.

Name or Extension Settings

Select: Selected attachment names ▼

☐ File extensions to scan (recommended) ▼

☐ File extensions to consider scanning (more commonly exchanged) ▼

☒ Attachments named Import

Use the full filename (not the extension) and separate each entry

*.js

Virtual Analyzer Scanning

☒ Submit files to Virtual Analyzer ⓘ

Figure 7

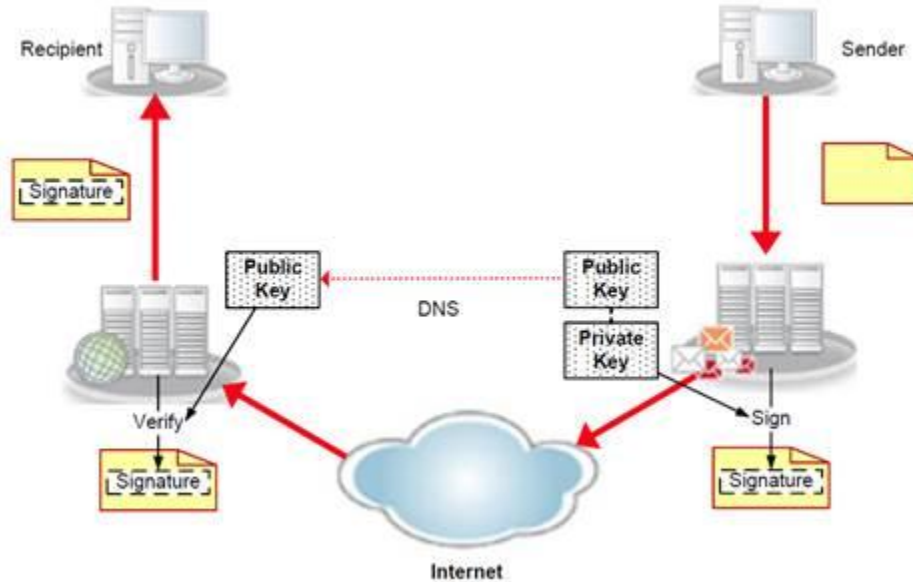
Note: If it is preferred to submit both **True File Type** messages and **Name or Extension** messages to Virtual Analyzer for analyzing, it is suggested to create separate rules to address this - one rule for True File Type messages and another rule for Name or Extension messages.

5.2.13 DKIM

What is DKIM?

DomainKeys Identified Mail (DKIM) is an email authentication method designed to detect email spoofing. It allows the receiver to check that an email claimed to have come from a specific domain was indeed authorized by the owner of that domain. It is intended to prevent forged sender addresses in emails, a technique often used in phishing and email spam.

By using public key infrastructure, DKIM helps protect the email integrity and sender's authority.



The DKIM definition and specification can be found in [RFC6376](#).

How does IMSVA implement DKIM?

On IMSVA, DKIM is implemented with two independent features - DKIM verification and DKIM signing.

DKIM verification

Users can utilize DKIM verification to filter spam, spoofing, and phishing mail.

How it works:

1. Extract the DKIM signature and claimed From: domain from the email headers.
2. Retrieve the public key from the DNS system for the claimed From: domain.
3. Use the public key to verify the signature. A match effectively proves that the email was truly sent from the claimed domain, and that the related the message headers and content have not been altered during transit.
4. If the DKIM verification failed, the configured action will be performed.

Pre-requisites:

- IMSVA is deployed at the edge, or
- IMSVA is NOT deployed at the edge, but the edge MTA and other device before IMSVA will never alter

the mails (Except for adding mail headers).

IMPORTANT NOTE:

If mails could be modified before reaching IMSVA, for example, mails could be stamped at edge MTA, do NOT enable DKIM verification on IMSVA, or IMSVA could falsely block those modified mails.

Best practice (procedure to enable)

1. Determine the sender domains supporting DKIM.
 - a. Usually the well-known mail service providers support DKIM, for example, Microsoft live mail and Google mail. You may confirm it via their official websites, or use the method in next step to confirm it.
 - b. To confirm if a sender domain supports DKIM, do the following:
 - i. Check if the mails from the domain consist DKIM-Signature header. You may refer to this [Microsoft KB](#) to learn how to view mail headers.
 - ii. In the DKIM-Signature header, find the DKIM selector “s=<selector>”. In the following example, the selector is “proddkim1024”:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=linkedin.com;
s=proddkim1024; t=1493612202;
bh=2Ty/lKfo1rHkqpBeYCBqpJ0wqjJDYxExBNMs7F4qMdE=;
h=From:Subject:MIME-Version:Content-Type:To:Date:X-LinkedIn-Class:
X-LinkedIn-Template:X-LinkedIn-fbl;
b=Cemhlmrw928GBZ1LrS5f5o5JXWTT0oSzQMpbMn1nEbMDtTPG41hblAgPkxrDhuQsX
ma1+vjn1fn1rzFBWY7x/SUTJUKH5O6eAdHyO06mwhojyvr9bLeOMjFtvKrkXqpH9a
5nnhShBeOm7wUV1VmA9SchzhyQ9HAutN0oMOVcHs=
From: Sam Su <invitations@linkedin.com>
```

In the From header, find the sender domain. In the above sample, the sender domain is “linkedin.com”. Query the DNS TXT record of <selector>._domainkey.<senderDomain> to verify if the expected public key exists. In the above sample, the query target is proddkim1024._domainkey.linkedin.com. You may use DNS commands or access <https://mxtoolbox.com> to make the query. The output of the above sample is like the following:

TXT Lookup

▼

txt:proddkim1024._domainkey.linkedin.com

Find Problems

txt

Share Results

Type	Domain Name	TTL	Record
TXT	proddkim1024._domainkey.linkedin.com	60 min	v=DKIM1; p=MIGfMA0GCsGqSIb3DQEBAQUAA4GNADCBiQKBgQDnp6ViffGakD19jp9mLNI4+Qn5Rx/mqBYOJO+oMEUxmYRJB5+dtow7EZ2VRJQdIHwRQlYJ7+DJYX6DVvRJB7yfp119kueITuq9CfwPloMEb0Ds/TCItQNNXRBTiLzCE94p0qyEbS0x1pJA1MgaEiBhNrH5mNPRgybeu+JfnoNtQIDAQAB;

2. Enable Global DKIM Enforcement rule and add the domains verified to be supporting DKIM.
 - a. Click **Policy > Policy List**. The Policy screen appears.

Policy

Filter by: All routes All types All Groups OK

1-9 of 9 Page 1

Rules	Action	Order	Modified	Status
Global DKIM Enforcement rule	Quarantine		September 13, 2017	
Global antivirus rule	Active action	1	January 30, 2017	

- b. Click the **Global DKIM Enforcement rule** link. The Policy Summary screen appears.

Rule Notes

☒ Enable

Rule Name: Global DKIM Enforcement rule

If recipients and senders are [Edit]

incoming
to Anyone
AND
from Anyone

And domains listed here do not pass DKIM verification [Edit]

3. Click **Edit** in the And domains listed here do not pass DKIM verification row. The Scanning Conditions screen appears.

Scanning Conditions [Global DKIM Enforcement rule]

[Policy List](#) > [Rule Summary](#) > Scanning Conditions

Save Cancel


Domain List

Incoming email messages from domains in the DKIM enforcement list that fail DKIM verification or are without a DKIM-Signature are marked as spam.

Domain name:

example: *.domain.com or domain.com

NOTE: DKIM verification will only be done on the domains in the above Domain list. For domains not listed, DKIM verification will be bypassed even when Global DKIM Enforcement rule is enabled.

4. Populate the Domain List in one of the following ways:
 - Manually:
 - a. Specify a domain name.
 - b. Click **Add**.
 - Import a list:
 - a. Click **Import**. The Import DKIM Enforcement List appears.
 - b. Specify the file path and file name or click **Browse** and locate the file.
 - c. Select one of the following:
 - Merge with current list
 - Overwrite current list
 - d. Click **Import**.
5. Click **Save**.
6. Click on the  under Status column to enable the rule.

IMPORTANT NOTE:

It is suggested to add domains one by one. For example, add gmail.com, save the change and monitor mail traffic from gmail.com for a moment, then add another domain and monitor. This is because IMSVA could make high false-positive detection if the sender domain's mail infrastructure is not properly configured to support DKIM. For example, the sender's edge MTA stamps mails after DKIM signing.

IMPORTANT NOTE:

Do NOT add your internal domains to the list, or your outgoing mails may falsely be blocked.

DKIM signing on IMSVA (Available on IMSVA9.1)

Signing outgoing mails can help your recipients protect them from spam/phishing mails spoofing your domain.

How it works:

1. IMSVA users generate key pairs on IMSVA Web UI.
2. The private key is stored on IMSVA and used to sign the outgoing mails.
3. IMSVA users manually copy the public key to their DNS record, so that the public key can be publicly available for DKIM verification.

Pre-requisites:

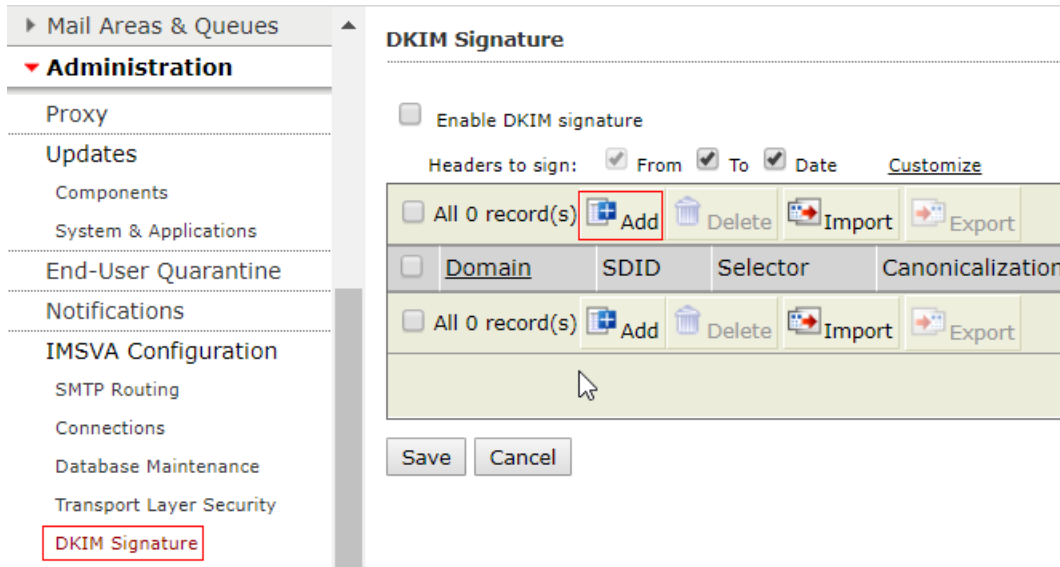
- IMSVA is deployed at the edge, or
- IMSVA is NOT deployed at the edge, but the edge MTA and other device before IMSVA will not alter the mails (except for adding mail headers), after DKIM Signing.

IMPORTANT NOTE:

If mails could be modified after leaving IMSVA (for example, mails could be stamped at edge MTA), do NOT enable DKIM signing on IMSVA, or the signed mails could falsely be blocked by recipients doing DKIM verification.

Best practice (procedure on adding a DKIM Signature)

1. Go to **Administration > IMSVA Configuration > DKIM Signature**. The DKIM Signature appears.



2. Select one or multiple headers to sign.
3. Click **Add**. The Add DKIM Signature screen appears.
4. Specify the general settings (refer to the following screenshots in case you are not familiar with the options)
 - Domain: Specify the domain where email messages are sent, for example, `example.com`.
 - SDID: Specify the signing domain identifier, for example, `example.com`.
 - Selector: Specify the selector to subdivide key namespace or retain the default value.
 - Private key: Upload a private key or request IMSVA to create a private key. If you want to generate a private key, select the key length before generation.
5. (Optional) Specify the advanced settings.
 - Header canonicalization: Select Simple or Relaxed (Relaxed is recommended).
 - Body canonicalization: Select Simple or Relaxed (Relaxed is recommended).

☒ Sign messages from this domain

General

Domain: *

SDID: *

Selector: *

Private key: *

☐ Upload

No file chosen

☒ Create bits

Some DNS hosting service providers don't support record longer than 255, choose 1024 in such situation.

Advanced

Header canonicalization:

Body canonicalization:

☐ Enable signature expiration: days(1-30)

☐ Enable body length: bytes

Leave other options as default if you are not familiar with them.

AUID:

Exempt domain:

Note: Specify subdomains of the domain you set. Use a comma to separate multiple entries.

NOTE:

Two canonicalization algorithms are defined for each of the email header and the email body: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping.

- Click **Save** to save the changes.
- Click **Save** again to save the list, or the configuration will be LOST.

DKIM Signature

☐ Enable DKIM signature

Headers to sign: ☒ From ☒ To ☒ Date [Customize](#)

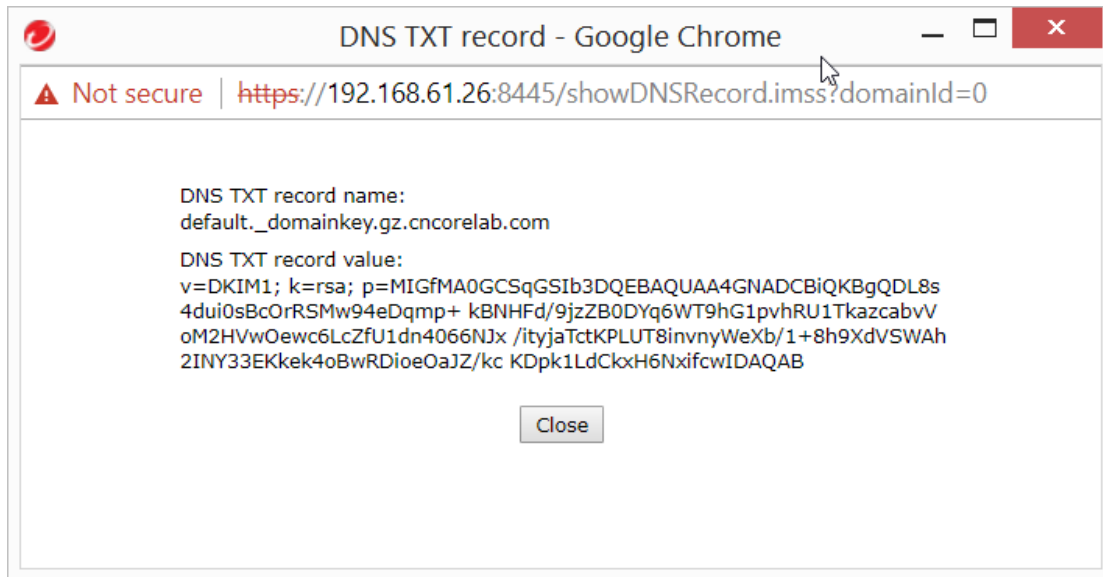
<input type="checkbox"/>	Domain	SDID	Selector	Canonicalization	DNS Record	status
<input type="checkbox"/>	gz.cncorelab.com	gz.cncorelab.com	default	Relaxed / Relaxed	DNS Record	

1-1 of 1 Page 1

Display: 15 per page

Your changes have been saved.

- Click **DNS Record** to retrieve the public key and the related DNS information. Below is an example:



Adding DNS TXT record

Log on to your DNS hosting service provider's website, and add DNS TXT record with DNS TXT record name and DNS TXT record value retrieved from the above step.

Different domain registrars use different names for the fields associated with a TXT record. For example, GoDaddy has fields named TXT Name and TXT Value, while Name.com calls the same fields Record Host and Record Answer. Regardless of which provider you use, enter the text under DNS TXT record name in the first field and the text under DNS TXT record value in the second field.

If your domain host is EasyDNS, add a period and your domain name to the end of the DNS TXT record name value. The value you enter should have the form `default._domainkey.your_domain.com`, where `your_domain.com` is the name of your domain.

If your domain provider supports the 2048-bit domain key length but limits the size of the TXT record value to 255 characters, you can't enter the DKIM key as a single entry in the DNS records. In this case, split the key into multiple quoted text strings and enter them together in the TXT record value field. For example, split the DKIM key into 2 parts as follows:

```
"v=DKIM1; k=rsa;  
p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAraC3pqvqTkAfXhUn7Kn3JU  
NMwDkZ65ftwXH58anno/bElnTDAd/idk8kWpslrQIMsvVKAe+mvmBEnpXzJL+0LgTNVTQct  
UujyilWvcONRd/z37I34y6WUIbFn4ytkzkdoVmeTt32f5LxegfYP4P/w7QGN1mOcnE2Qd5SKIZ  
v3Ia1p9d6uCaVGI8brE/7zM5c/"
```

```
"zMthVPE2WZKA28+QomQDH7ludLGhXGxpc7kZZCoB5lQiP0o07Ful33fcED73BS9Bt1SNhnr  
s5v7oq1pIab0LEtHsFHAZmGJDjybPA7OWWaV3L814r/JfU2NK1eNu9xYJwA8YW7WosL45CS  
kyp4QeQIDAQAB"
```

You may refer to [this Google article](#) to get more details.

Different DNS hosting service providers or DNS registrar implement the limitation differently. For example, some of them allow you to paste the long strings to one TXT record while splitting them at the backend; some of them only accept the long strings when you split them to multiple short strings with quotes; some of them won't allow you to input strings longer than 255 to a record, but you can create multiple TXT records with the same name.

Therefore, if you want to use 2048bit key, please **consult your DNS hosting service provider** to find the solution, and schedule extra time to verify the solution.

Enable DKIM signing on IMSVA

1. Go to **Administration > IMSVA Configuration > DKIM Signature**.
2. Select **Enable** and then save the change.

5.2.14 Time-of-Click Protection

Time-of-Click Protection protects users against malicious URLs in email messages at the time of click.

Administrator can judge whether needs to enable this feature or not based on the real situation.

Administrator can refer following steps to enable this feature.

1. Open the IMSVA web console. Navigate to **Policy > Time-of-click Protection**, and set the actions for each type of URLs.
2. Edit spam rule (or create a new rule), with enabling **Web Reputation settings** (WRS).

3. Enable **Time-of-Click Protection** on **Web Reputation settings** page, and select which type of URLs will be applied for this feature.

Time-of-Click Protection ⓘ

- ☒ Enable Time-of-Click Protection
 - ☐ Apply to URLs that have not been tested by Trend Micro
 - ☐ Apply to URLs marked by Web Reputation Services with smart flags
 - ☒ Apply to all URLs
- ☐ Apply to URLs in digitally signed messages ⓘ

5.3 > Integrating IMSVA with Virtual Analyzer

You can refer to Trend Micro [KB 1114131](#) for the separate IMSVA Virtual Analyzer Integration Best Practice Guide, which also has Connected Threat Defense (CTD) included.

5.4 > Configuration Files

IMSVA 9.1 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, IMSVA uses the setting from the database. Configuration files are marked with “.ini” while administrators can easily see what settings IMSVA 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.

5.4.1 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.

5.4.2 foxdns.ini File

This is the 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 IMSVA 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 [KB 1057132](#) for details.

5.4.3 foxproxy.ini File

This is the FoxProxy module configuration file.

From IMSVA 9.0, it enhanced the ERS feature to log sender/recipient address. In order to address this feature, it uses FoxProxy to do ERS checking.

The following configuration settings in the foxproxy.ini file control the flow through FoxProxy:

[proxy]/ proxy_port Port where FoxProxy accepts incoming connections (Default: 25)

[backend_server]/ backend_server_address and backend_server_port

IP-address and TCP-port where FoxProxy forwards the SMTP traffic (Default: 127.0.0.1 and 2500).

With set log_level=4 in this file, FoxPorxy will write very detailed logs in foxproxy-general.* log file.

5.5 > 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. To change the setting of IMSVA, the following can be performed:

- 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 the 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 IMSVA in a group. Changes made to local files will only affect the local appliance.

5.5.1 Updating the configuration settings in the database

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

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

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
```

```
-----  
3  
(1 row)  
  
imss=# \q  
[root@imsva85 ~]#
```

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 the value 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',' ');
INSERT 0 1
imss=# \q
```

Recommended database configuration changes

Whole Mail Scan

Some viruses and malwares may 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 this, IMSVA 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 **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';
UPDATE 1
```

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, IMSVA 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
```

If EUQ is enabled, administrator also can address this function from UI:

Go to **Administration > End-User Quarantine > User Quarantine Access**, and select “Allow end users to retrieve quarantined email messages with alias email addresses”.

For AD LDAP with Exchange as mail server, it is strongly suggested to use proxyAddresses instead.

5.5.2 Database Maintenance Schedule

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

5.5.3 Problem 1 - Running out of transaction IDs

Most likely, it is not visible unless more than a million received messages a day is processed and have IMSVA running for a very long time.

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 measure.

All the technical details are found at this [link](#).

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

More details can be found in the patch Readme file.

5.5.4 Problem 2 - The database keeps growing

Neither two existing maintenance jobs reclaim unused disc space back from the DB because this task may consume a lot of time and resources. Therefore, the administrator will have to arrange these jobs in accordance to the 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. Keep this reminder in mind when scheduling this job.

The FULL VACUUM can be run in an interactive session using “screen” or “nohup” to avoid a session timeout from killing the vacuum job.

Preferably, a crontab should be created 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 the needs.

5.6 > Ransomware Protection

Ransomware may spread via email, either by attaching itself directly or pasting malicious URL on the email body.

For known ransomware which are defined in VSAPI pattern file, IMSVA can detect it as normal virus.

For known ransomware URL which are listed in WRS, IMSVA can use WRS to detect it out as WRS-type of ransomware.

IMSVA can also use TMASE's TLSH feature to detect ransomware defined in TMASE pattern file.

For unknown ransomware, it may exist in executable files, or in Microsoft document files which contain macros. IMSVA can take action for those files, such as strip macro, block *.exe file, or submit the macro file / executable file to DDAn for future analysis.

5.6.1 Improve Ransomware Detections Visibility

From IMSVA 9.0 build 1579, IMSVA contains enhancements for ransomware detections visibility.

Administrators can add the **Ransomware Detections** widget to dashboard, and also can query ransomware detection logs on policy log query page:

1. Add the “Ransomware Detections” widget to dashboard ((It is suggested to add it to the “Message Traffic” tab.):
 - a. On the web console go to **Dashboard > Message Traffic** tab, and click **Add Widgets** on the right side of the screen.

Add Widgets

Most Recent Widgets (0)

All Widgets (1)

Cloud Pre-Filter (0)

IP Filtering (0)


Message Traffic (1)

System (0)

ransomware

Records: 1 - 1 / 1 10 per page

☒ Ransomware Detections



Displays the security filter that detects by each filter compared to the total nu

Category: Message Traffic

09-21-2013

< Previous 1 Next >

Add

Cancel

1 widgets selected

- b. Type keywords to search for "Ransomware Detections". Select it, and click **Add**.
- c. The “Ransomware Detections” widget will appear on the “Message Traffic” tab.

Message Traffic

IP Filtering

Cloud Pre-Filter

+

Tab Settings

Add Widgets

ransomware

Latest data refresh: 2016-05-28 21:50:13

IMSVA Scan Performance

Ransomware Detections

Latest data refresh: 2016-05-28 21:50:13

Range: 24 hours

IMSVA: ALL

Detected by	Total	%
Total	72	100%
Virus Scan	44	61.11%
Spam Detection	3	4.17%
Web Reputation	12	16.67%
Virtual Analyzer	13	18.06%

Scanning Conditions

Latest data refresh: 2016-05-28 21:50:30

- 2. On the web console go to **Logs > Query**. “Ransomware” category is added to “Policy events” type. It also contains four sub categories: Virus Scan, Spam Detection, Web Reputation and Virtual Analyzer.

Criteria

Type: Policy events Ransomware

Detected by: All

Dates: 21 01 to 05/28/2016 22 01
hh mm mm/dd/yyyy hh mm

Sender: Subject:

Recipient(s): Violating Attachment(s):

Rule: Message ID:

Use semi-colons to separate multiple search items in Recipient and Attachment fields

To specify an exact match, just type the keyword. For a partial match, use the asterisk wildcard "*". For example, "**username" searches for any character string that ends with "username".

Display Log

Policy Events Results per page: 15

Print current page Export to CSV 1-15 of 72 Page: 1

Timestamp	Action	Sender	Recipient(s)	Subject	Detected by
2016年5月28日 8:40:40	Message deleted	test1@test1.com	test2@test2.com	Sample: TROJ_CRYPTWALL.YYY	Virtual Analyzer
2016年5月28日 8:26:30	Message deleted	test1@test1.com	test2@test2.com	Sample: TROJ_CRYPTWALL.XXRT	Virtual Analyzer
2016年5月28日 8:26:30	Message deleted	test1@test1.com	test2@test2.com	Sample: TROJ_CRYPTWALL.XXKL	Virtual Analyzer
2016年5月28日 8:26:30	Message deleted	test1@test1.com	test2@test2.com	Sample: TROJ_CRYPTWALL.CC	Virtual Analyzer
2016年5月28日 8:26:29	Message deleted	test1@test1.com	test2@test2.com	Sample: TROJ_CRYPTWALL.BTM	Virtual Analyzer
2016年5月28日 8:26:29	Message deleted	test1@test1.com	test2@test2.com	Sample: TROJ_CRYPTWALL.XXTXL	Virtual Analyzer

5.6.2 Handling Macro Files

Macro virus is one of the most common types of file infections in Microsoft Office documents.

Administrators may refer to [KB 1113805](#) for macro file handling in IMSVA. For macro files, the most aggressive way is strip the macro directly from document (Option 1 in KB 1113805).

If DDAn is integrated, it is suggested to take both option 2 and option 3 for handling macro files.

5.6.3 Handling Executable Files

If DDAn is not integrated, administrators may consider blocking EXE files directly.

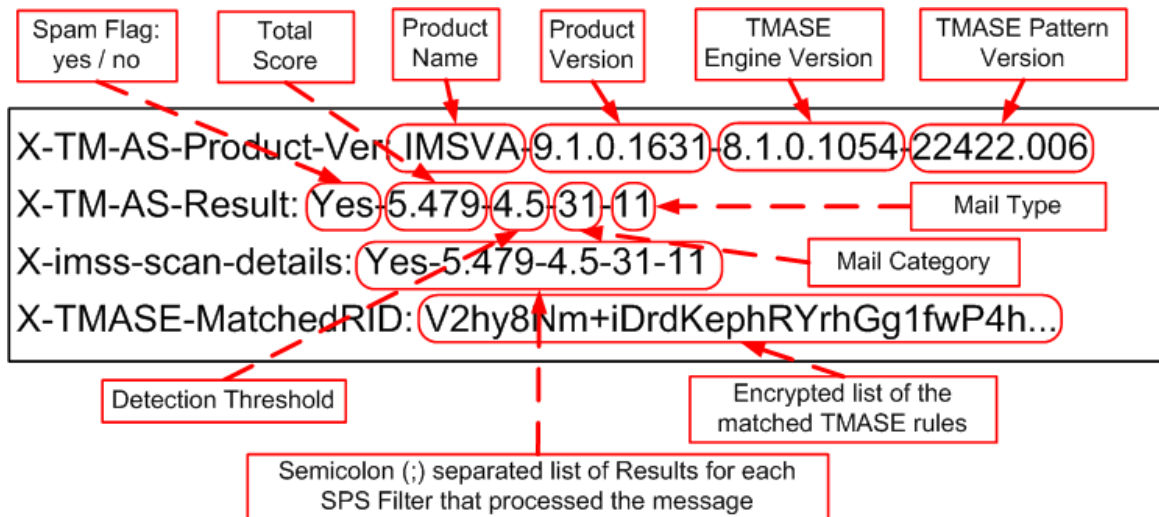
If there is DDAn integration, administrators may configure IMSVA to submit EXE files to DDAn for further analysis.

Refer to 5.1.6 on how to submit files to DDAn. Administrators may also refer to [KB 1114112](#) for details.

5.7 > Others

5.7.1 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 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.

Spam Catch Rate	Spam Catch Rate ID	Detection Threshold
High	1	4.5
Medium	2	5
Low	3	7.0
Specific rate	4	3.0-10.0

Figure 4. Detection Threshold folder

The calculated Trend Score is compared with the Detection Threshold. If the Trend Score is higher or equal, the email is classified as spam:

```
Trend_Score >= Detection_Threshold
```

Figure 5. Detection threshold score

Depending on the email characteristics coming into the environment, the spam thresholds will have to be adjusted on the Administration Console settings. If a header result is similar to the one above and it seems the email message is not spam, the spam threshold can be changed to Low, or specify a threshold of 6 in order for the message to get through.

5.7.2 White Listing

To receive email messages that are being tagged as spam by IMSVA, the sender of these messages can be added to the Approved Senders list in the Spam Rule. This will prevent future messages from this sender from being tagged as spam.

X-TM-AS-USER-Approved-Sender: Yes

5.7.3 Submitting Samples to Trend Micro


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), these samples must be submitted to Trend Micro. This will help enhance the anti-spam engine rules. See [KB 1036079](#) to learn how to submit samples to Trend Micro.

5.7.4 EUQ SMTP Authentication

The classic End User Quarantine with LDAP authentication comes with some limitations. The one most noticeable is that it only supports 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.


Select SMTP-AUTH in the Admin UI 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 **User Quarantine Access**



Enable EUQ Feature

☒ Enable End-User Quarantine Save

☐ Use LDAP for EUQ authentication 

☒ Use SMTP Server for EUQ authentication

Specify recipient domains and SMTP server addresses.

 Add  Delete 1-3 of 3 Page 1

<input type="checkbox"/>	Domain	Server/Port
<input type="checkbox"/>	domain1.com	1.2.3.4:25
<input type="checkbox"/>	domain2.com	1.2.3.5:25
<input type="checkbox"/>	*.subdomain1.com	1.2.3.6:25

15 per page

Figure 6. User Quarantine screenshot

When end-users enter the EUQ web console, they would type their email address and password. IMSVA will then connect to the corresponding MTA, greet with EHLO and when AUTH is available, it will try with the given credentials. When successful, it will close the SMTP connection and open the EUQ.

Below are some limitations when using SMTP authentication:

- As of this writing, IMSVA 9.1 GM only supports PLAN & LOGIN
- Aliases are not recognized (relies on LDAP). For each quarantined message, the EUQ will create a unique index in the imsseuq DB.
- The recently added support for Distribution Lists is not available with SMTP-AUTH as it relies on LDAP.

5.7.5 Rule Samples

Creating “Global White List” for Inbound Mails

Refer to section 5.2.5 for details.

Insert disclaimer for outgoing email messages

Email disclaimers have been practiced as a standard in corporate email messaging systems.

Administrators may generate disclaimers using the following steps.

1. On IMSVA web console, click **Policy > Stamps**, add a “Disclaimer” stamp.
2. Click **Policy > Policy List**, then add a new outgoing rule (other type), from internal domain to anyone.
3. Leave the “Scanning Conditions” setting blank.
4. For the “Action” part, select **Do not intercept messages** and **Insert stamp in body**, and use **Disclaimer** as stamp.



<input checked="" type="checkbox"/>	Insert stamp in body	Disclaimer	Edit
-------------------------------------	----------------------	------------	------

5. Save the rule with the name Disclaimer. Below is the rule summary info chart:

Rule

Notes

☒ Enable

Rule Name:

Order Number:

If recipients and senders are

outgoing

to Anyone

AND

from *@corelab.cn

And scanning conditions match

Then action is

Insert stamp in body

7. Perform some testing to make sure the rule works fine.

Blocking executable files

Administrators can use either true file type or file extensions to block executable files.

Please refer to [KB 1099617](#) for details.

Chapter 6: Backup and Disaster Recovery

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

6.1 > Backup and Restore from the GUI

6.1.1 Backup

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

6.1.2 Restore

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

6.2 > 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. The imss and imsseuq database can be backed up for recovery at a later time. Below is the procedure. Change all instances of imss to imsseuq if working on the EUQ database.

6.2.1 Backup

The `pg_dump` command can be used to back up 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@imsva90 ~]# /opt/trend/imss/PostgreSQL/bin/pg_dump -U sa -f /tmp/imss_dump.sql imss
[root@imsva90 ~]#
```

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

```
[root@imsva90 ~]# /opt/trend/imss/PostgreSQL/bin/pg_dump imss -U sa | gzip >
```

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

```
[root@imsva90 ~]# /opt/trend/imss/PostgreSQL/bin/pg_dump imsseuq -U sa | gzip >
```

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

```
[root@imsva90 ~]# /opt/trend/imss/PostgreSQL/bin/pg_dump -U sa -f /tmp/imsseuq_dump.sql imsseuq
[root@imsva90 ~]#
```

6.2.2 Recovery

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

Use the rcImss script to stop the IMSVA software:

```
[root@ims90 ~]# /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
```

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

```
[root@imsva90 ~]# /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@imsva90 ~]# /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@imsva90 ~]# /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@imsva90 ~]# /opt/trend/imss/PostgreSQL/bin/createlang -h 127.0.0.1 -U sa -d imss plpgsql
```

```
[root@imsva90 ~]#
```

Restore the database from the backup:

```
[root@imsva90 ~]# /opt/trend/imss/PostgreSQL/bin/psql imss sa < /tmp/imss_dump.sql >
/dev/null
```

```
ERROR: language "plpgsql" already exists
[root@imsva90 ~]#
```

Restore the database from the backup compressed file:

```
[root@imsva90 ~]# /usr/bin/gunzip -c /tmp/imss_dump.gz | psql imss -u sa
[root@imsva90 ~]#
```


6.2.3 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:

```
[root@imsva90 ~]# /opt/trend/imss/PostgreSQL/bin/psql imss sa -c "update tb_administrator set
md5_digest='bdd725fd5707063fd845b763b5237600' where admin_name='admin';"

UPDATE 1

[root@imsva90 ~]#
```

The next time logging in the GUI, the password will be reset to the default password, “imsva”.

6.3 > Backing up and Restoring Cloud Pre-filter account settings

6.3.1 Whole IMSVA configuration file

The IMSVA configuration file contains Pre-Filter account info. This is also the most convenient way to backup & restore entire IMSVA settings that include Pre-Filter account settings.

From IMSVA web console, navigate to **Administration > Import/Export**. The administrator can then export & import configuration files.

6.3.2 Backup Cloud Pre-Filter Account

1. On the 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, the account name info is found. Click **Export Key File** to export the key.
3. Save the key file with the filename contains account name, such as Pre-Filter_AccountName.key.

6.3.3 Restore Cloud Pre-Filter Account

Administrators may register a new Pre-Filter account or restore an existing one 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**.
Note that all of the Pre-Filter related settings are stored in the cloud. Restoring previous backup info will not restore Pre-Filter settings.

Chapter 7: References

7.1 > Communication Ports

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

The tables below are lists of communication ports used by different IMSVA components when communicating with each other.

IMSVA Component	Port	-Remote IMSVA Component to connect to -When to open?
Scanner Server	TCP/UDP 53 (DNS port)	-Central Controller Server -open this port when using IP-Profiler
	TCP 15505	-Central Controller Server & EUQ Server -open all the time
	TCP 5432 (Postgres)	-IMSVA Admin Database -open all the time
	TCP 25 (SMTP)	-Upstream and Downstream MTA servers -open all the time
	TCP 110 (POP3)	-Upstream POP3 servers and POP3 clients -open this port when POP3 scanning is enabled.
	TCP 5060	-Policy Server -open all the time
	TCP 163 (SNMP)	-SNMP server -open this port when using SNMP Notification
	TCP 10030	-Delivery Policy Server -Open all the time
	TCP 389 or 3268 (LDAP)	-Directory Server -open this port when LDAP is enabled
	TCP/UDP 53 (DNS port)	-Network DNS server Note: for performance reason, Trend recommends using a DNS Server only a hop away from the Scan Server. -open this port when using NRS
	TCP 443/80	-TMCM Server and WRS Note: WRS uses port 80 -open this port when CM-Agent is enabled
	UDP 10323 (HTTPS/HTTP)	-TMCM Server -open this port when CM-Agent is enabled

IMSVA Component	Port	-Remote IMSVA Component to connect to -When to open?
Central Controller	TCP 15505	-Scanner Server -open all the time
	TCP 5432 (Postgres)	-IMSVA Admin Database -open all the time
	TCP 389 or 3268 (LDAP)	-Directory Server -open this port when LDAP is enabled
	TCP 8445	-hosts that need to access IMSVA Web Admin Console -open all the time
	UDP 10323 (HTTPS/HTTP)	-TMCN Server -open this port when CM-Agent is enabled
	TCP 443/80 (HTTPS/HTTP)	- TMCN Server -open this port when CM-Agent is enabled
	TCP 9000	- Cloud Pre-Filter -open this port when using Cloud Pre-Filter is enabled

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

IMSVA Component	Port	-Remote IMSVA Component to connect to -When to open?
Secondary EUQ Server	TCP 8446	-Primary EUQ Server -open all the time
	TCP 15505	-Scanner Server -open all the time
	TCP 389 or 3268 (LDAP)	-Directory Server -open this port when LDAP is enabled

IMSVA Component	Port	-Remote IMSVA Component to connect to -When to open?
ALL IMSVA	TCP 5432 (Postgres)	- Postgres Database server -open all the time

NOTE 📄 If the LDAP server is an MS AD Global Catalog Server, the LDAP port can be port 3268 instead of port 389. IMSVA parent or all-in-one appliance will use the internal IP for Postgres so it is not necessary to open that port for outside use.

7.2 > ERS Portal

The ERS part of the IP-Filter module has an online configuration console where administrative tasks necessary to implement ERS effectively are:

<https://ers.trendmicro.com>

Since ERS is an online database shared by other users, there will be situations where ERS settings need to be tweaked to fit the environment. Below are some of the common settings that can be changed.

- Dynamic Settings

The Dynamic (database) is used, there will be isolated situations where in some emails, to reach the network, will temporarily be blocked if the sender's IP is in the Dynamic database. It is because an automated system, which is comprised of "catch servers" and spam analyzers, is used 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 selection of the level of aggressiveness fit for the environment. Select Level 3 to start with then adjust if necessary.

- Policy Settings (Policy | Settings)

An IP address will end up in the database only if spam mails are received from it, or the investigation showed that it is a known spammer. If there is a need to receive emails from an IP address, regardless if it is sending spams or not, it is recommended to use the Approved and Blocked lists instead of submitting an IP-Removal request.

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

The following can be performed 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 Micro 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 a couple of guidelines before Trend Micro 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 following URL to know which block list the IP is included:

<https://ers.trendmicro.com/reputations>

7.3 > TLS (Transport Layer Security) Settings

IMSVA 9.1 has default TLS certificate files included, and administrators can also generate a new certificate through the UI or use their own certificate to replicate the default one.

IMSVA 9.1 SMTP TLS support v1.0, v1.1 and v1.2. In opportunistic mode, it will always try to use the higher TLS version to communicate with sending or receiving MTA.

If the sending or receiving MTA only supports TLS 1.0, IMSVA 9.1 will use TLS 1.0 to communicate with the sending or receiving MTA.

➞ Refer to IMSVA 9.1 administration's guide "Chapter 13: Configuring Transport Layer Security Settings" for more detailed information.

➞ Refer to [KB 1118390](#) to check supported MTA's TLS version.

7.4 > Product Updates

It is strongly recommended to keep the product up-to-date at all times. Check the link below for the latest Service Pack or Patch for IMSVA 9.1

<http://www.trendmicro.com/download/>

7.5 > Upgrade/Migration

IMSVa 9.1 supports:

- Inline upgrade from IMSVa 9.0 Patch1.
- Migrate from:
 - IMSVa 9.0 Patch 1
 - IMSVa 8.5 SP1 Patch 1
 - IMSVa 8.2 SP2 Patch 1
 - IMSVa 8.0 Patch 2
 - IMSS 7.5 Windows
 - IMSS 7.1 Windows Patch 3
 - IMSS 7.1 Linux SP2
 - IMSS 7.0 Solaris SP1 Patch 4

See Chapter 5, “Upgrading from Previous Versions”, of the Trend Micro InterScan Messaging Security Virtual Appliance v9.1 Installation Guide.