



# 12.0 ScanMail™ for Microsoft™ Exchange

Service Pack 1

Best Practices Guide

Securing your Exchange environment



Messaging Security



## Table of Contents

ScanMail for Microsoft Exchange 12 Service Pack 1 Best Practice Guide	1
About this Guide.....	9
Chapter 1 Product Overview .....	15
1.1 ScanMail for Microsoft Exchange Overview.....	15
1.2 ScanMail for Microsoft Exchange Editions .....	18
1.3 Release History.....	20
1.4 What's New in SMEX 12 .....	21
1.4.1 Things You Must Know .....	21
1.4.2 Exchange Server 2016 Support.....	22
1.4.3 SQL Server 2014 Express Service Pack 1 Support.....	22
1.4.4 AlwaysOn Availability Groups Support for SQL server ...	22
1.4.5 Support Windows Authentication for Remote SQL Server	23
1.4.6 Continuous Protection with SQL Server unavailable.....	23
1.5 What's New in SMEX 12 Patch 1 .....	27
1.5.1 Ransomware Detection Visibility.....	27
1.5.2 Sender Approved List for Virtual Analyzer configuration	30
1.5.3 Bypass malware protection for resending message .....	31
1.5.4 Save message subject and body to reuse later .....	31
1.5.5 Support for monitoring advanced threats.....	32
1.5.6 Spam log .....	34

1.6	What's New in SMEX 12 SP1 .....	35
1.6.1	Things You Must Know .....	35
1.6.2	URL Analysis.....	36
1.7	Performance Report .....	39
1.7.1	SMEX12.0 SP1 performance impact on Exchange 2016 with default setting .....	39
1.7.2	SMEX 12.0 SP1 filters performance impact on Exchange 2016	42
Chapter 2	Deployment .....	45
2.1	System Requirement .....	45
2.2	Exchange Integration.....	45
2.2.1	Exchange 2010 Integration.....	45
2.2.2	Exchange 2013 Integration.....	50
2.2.3	Exchange 2016 Integration.....	51
2.3	Cluster Integration.....	52
Chapter 3	Setup and migration .....	59
3.1	Installation.....	59
3.1.1	Fresh install ScanMail prerequisite on Microsoft Exchange 2013/2016 .....	59
3.1.2	Installation Verification .....	61
3.2	Upgrade .....	65
3.2.1	Upgrade Overview .....	65
3.2.2	ScanMail Settings modification during upgrade .....	66
3.2.3	Upgrade Verification .....	67

3.3	Silent Installation .....	69
3.3.1	Silent Installation Limitations .....	69
3.3.2	Performing Silent Installation .....	69
3.3.3	Silent Installation setup switches .....	70
3.4	Uninstallation .....	73
Chapter 4	Product Management.....	75
4.1	GUI Configuration.....	75
4.1.1	Recommended Scan Settings for Different Server Roles	76
4.1.2	Attachment Blocking Policies .....	77
4.1.3	Content Filtering Active Directly Integrated.....	79
4.1.4	Data Loss Prevention Policy.....	79
4.1.5	Optimizing Web Reputation .....	87
4.2	Search & Destroy Best Practices.....	89
4.2.1	Search & Destroy Prerequisites.....	89
4.2.2	Using Search & Destroy in Mixed Exchange Environments	90
4.2.3	Preparing Exchange Server 2013/2016 for Mixed Exchange Environment.....	91
4.2.4	Configuring Search & Destroy in a Multiple Data Center Environment .....	92
4.2.5	Optimizing Search Criteria.....	92
4.2.6	Optimizing Mailbox Searches .....	94
4.2.7	Deleting Mailbox Searches .....	94
4.2.8	Exchange Management Shell Commands .....	95

Chapter 5	Central Management.....	99
5.1	ScanMail Server Management .....	99
5.1.1	Replicate Settings to Remote Servers .....	100
5.1.2	Central Log Query via SMEX Management Console.....	101
5.1.3	Central Quarantine Query via SMEX Management Console	101
5.1.4	Single Sign On .....	102
5.2	MOM/SCOM Integration .....	104
5.3	Control Manager Integration .....	110
5.3.1	Replicate SMEX Configuration via TMCM Console.....	112
5.3.2	Central Log Query via TMCM Console.....	114
5.3.3	Central Deployment and Scanning .....	118
5.3.4	License Management .....	120
Chapter 6	Virtual Analyzer Integration .....	121
6.1	Register to DDAn .....	121
6.2	Recommend Settings.....	123
6.2.1	Virtual Analyzer Mode.....	123
6.2.2	Recommended Attachment Types:.....	124
6.3	Verify Submission .....	126
Chapter 7	Recommend SMEX Configurations.....	127
7.1	Best Practice Configuration and Prevention for Spam .....	127
7.1.1	Email Reputation Service.....	127
7.1.2	Content Scanning.....	129
7.1.3	Detect New Spam source .....	130

7.1.4	Phishing Mail .....	132
7.2	Best Practice Configuration and Prevention for Ransomware 133	
Chapter 8	Troubleshooting Guide .....	139
8.1	Installation process “Installing SQL Server Express” does not finish causing a failure in ScanMail for Exchange (SMEX) installation 139	
8.2	Updating the Scan Engine Manually.....	143
8.3	Updating the Pattern File (lpt\$vpn.xxx) Manually .....	144
Chapter 9	SMEX Register Hidden Key .....	147
Chapter 10	Frequently Asked Questions.....	153
10.1	FAQ on SMEX 12 and 12 SP1 .....	153



# About this Guide

## 1. Preface

Welcome to the **Trend Micro ScanMail for Microsoft Exchange 12.0 Service Pack 1 Best Practice Guide**. This document serves as a guideline to help customers develop a set of best practices when deploying and managing ScanMail for Microsoft Exchange (SMEX).

This document provides in-depth information about ScanMail architecture, configuration and deployment process as well as troubleshooting and performance tuning. SMEX 12.0 Service Pack 1 includes all fixes resolved in SMEX 12.0, and introduces new features and enhancements. All the updates are covered in this document.

This document should be read in conjunction with the *Trend Micro ScanMail for Microsoft Exchange 12.0 and 12.0 Service Pack 1 Administrator's Guide* and *Installation and Upgrade Guide*.

## 2. Authors

This **Best Practice Guide** is written by Nickel Xu and Marc Liu, and edited by Raja Nabeel Ashraf. Additional information was provided by the members of SMEX Engineering groups, including:

- David Ruan
- Andy Jia
- Kelley Wang

### 3. Pre-requisites

This Best Practice Guide does not cover details of basic Systems Administration for Windows, Microsoft Exchange or the common technologies used in SMEX. It assumes that the book audience has a basic knowledge of the following concepts:

- Windows 2008 & 2012 Operating System
- Microsoft Exchange, 2010, 2013 and 2016 concepts
- Internet Information Server (IIS) Web Server
- Simple Mail Transport Protocol (SMTP)
- Exchange Transport Mechanism
- SQL Server Administration

### 4. Abbreviations and Terms

This Best Practice Guide uses the following abbreviations and terms:

Term	Description
SMEX	Trend Micro™ScanMail™for Microsoft™ Exchange; the all-in-one malware and malicious content protection for Microsoft Exchange messaging environments.
SMEX Server	The ScanMail for Microsoft Exchange Server; the target server where both SMEX and Microsoft Exchange run.
<SMEX program directory>	The folder where the SMEX program files are installed. By default, this directory is located under %ProgramFiles%\Trend Micro\Smex.

---

Term	Description
AC	Activation Code
AD	Active Directory
APT	Advanced Persistent Threat
AS	Anti-Spam
AU	ActiveUpdate
CCCA	Command & Control Contact Alert
CCFR	Cloud-Client File Reputation
CCWR	Cloud-Client Web Reputation
CF	Content Filter
DAG	Database Availability Group
DLP	Data Loss Prevention
DTAS	Dynamic Threat Analysis System
EUQ	End User Quarantine

Term	Description
FQDN	Fully Qualified Domain Name
IDP	Integrated Defense Protection
IRM	Information Rights Management
MCP	Management and Configuration Protocol
MOM	Microsoft Operations Manager
OPP	Outbreak Prevention Policy
PR	Product Registration
RBAC	Role Based Access Control
RBS	Remote BLOB Storage
SCM	sCloud Manager (TMCM 6.0)
SCOM	System Center Operations Manager
SPN	Smart Protection Network
SSO	Single Sign On

Term	Description
TIM	Threat Intelligence Manager
TMASE	Trend Micro Anti-Spam Engine
TMCM	Trend Micro Control Manager
WRS	Web Reputation Service
WTP	Web Threat Protection

## 1. Conventions

The following conventions are used in this Best Practice Guide:

Convention	Description
monospace	Registry, logs, configuration file parameters, commands, syntax, file names, and folder names
Tip ✓	Recommended configuration/actions
NOTE 📄	Brief comment or explanation
Refer to	References to other documents or sections of this Support Track
<u>Warning</u>	Critical actions or configurations



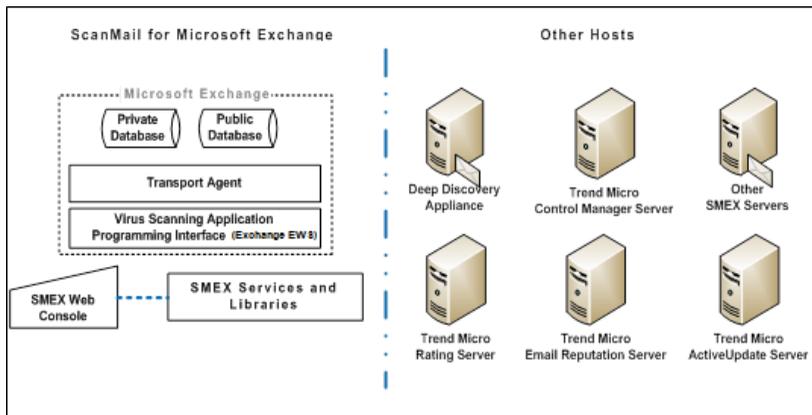
# Chapter 1

## Product Overview

This chapter provides an overview regarding the product functionalities, enhancements as well as new features introduced in this new version.

### 1.1 ScanMail for Microsoft Exchange Overview

Trend Micro ScanMail for Microsoft Exchange (SMEX) is a plug-in security solution to Microsoft Exchange Messaging System. This solution provides an integrated protection against multiple threats and data compromises in the Exchange environment. It protects the Exchange Server from malware, spyware, spam, phishing, data leakage, unwanted content and Advance Persistent Threats (APT).



In order to hook messages and its corresponding attachments processed by Microsoft Exchange, SMEX relies on the following three components:

- Transport Agents
- MS VSAPI (used in Microsoft Exchange 2010)
- EWS (Exchange Web Services) for Exchange 2013/2016

The acquired messages and selected attachments using SMEX scanners and filters are implemented as a collection of Windows Services and libraries.

The following table provides the summary of the different Exchange environments that SMEX 12 can protect and their corresponding message/attachment hooks:

Processor	Operating System	Exchange	Hook(s)
64-bit	Windows Server 2008	Exchange 2010	Transport Agent VSAPI 2.6
64-bit	Windows Server 2008 Windows Server 2012	Exchange 2013	Transport Agent EWS (Exchange Web Service)
64-bit	Windows Server 2012	Exchange 2016	Transport Agent EWS (Exchange Web Service)

**NOTE** 

In the previous version of SMEX 11, Exchange 2007, 2010 and 2013 are supported. With this release SMEX12, the support for Exchange 2007 has been dropped and Exchange 2016 has been added.

SMEX 12 has the ability to integrate with DDAn or Deep Discovery Appliance, which is a sandbox hypervisor that provides analysis to exploits and heuristic files identified as Advanced Persistent Threats (APTs). This is while retaining its feature of integrating with other hosts machines and services, such as:

- Trend Micro Control Manager Server – provides centralized licensing management, update and configuration management
- Trend Micro Rating Server – provides rating or risk assessment of the URL found in the email message
- Trend Micro Email Reputation Server – provides reputation on the email messages source if its legitimate or malicious
- Trend Micro ActiveUpdate Server – connects and provides the latest threat updates to the components licensed and activated in SMEX
- Other SMEX Servers – the ability to manage other SMEX hosts for purposes of management

**Scanning Methods**

SMEX provides the following scanning methods:

- Real-time scan
- Manual scan
- Scheduled scan

**Filters**

SMEX currently provides the following filtering methods:

- Spam Prevention
- Web Reputation
- Content Filtering
- Attachment Blocking
- Data Loss Prevention
- Deep Discovery Advisor (DDAn) filter module - Filter module used by ATSE to analyze files and confirm if the file is malicious
- Security Risk Scan - for malware & spyware detection

### **Communication Links**

A SMEX Server can communicate with any of the following hosts:

- Other SMEX Servers - for replicating product configuration
- Trend Micro Control Manager - for purposes of remote management
- Rating Server - for retrieving URL rating when Web Reputation Service is enabled
- Email Reputation Service - for retrieving the IP address reputation when Email Reputation Service is enabled
- ActiveUpdate Server - for downloading updated components
- Deep Discovery Appliance - for analyzing APT (Advanced Persistent threats)

## **1.2 ScanMail for Microsoft Exchange Editions**

There are two editions of ScanMail for Microsoft Exchange based on the Activation Code used:

- **Suite:** provides Standard protection plus Content Scanning, Web Reputation and Content Filtering (AC starts with SS)
- **Suite with DLP:** Provides Suite protection plus Data Loss Prevention and Search & Destroy (AC starts with SZ)

The differences between **Suite** and **Suite with DLP** editions are mainly in the area of available scanning filters as shown in the following table:

Features	Suite	Suite with DLP
SpamPrevention-EmailReputation		✓
SpamPrevention-ContentScanning	✓	✓
WebReputation	✓	✓
ContentFiltering	✓	✓
AttachmentBlocking	✓	✓
SecurityRiskScan	✓	✓
Advanced Threats Scan Engine	✓	✓
EndUserQuarantine	✓	✓
Search & Destroy	✓	✓
Deep Discovery Advisor	✓	✓
Manual/Scheduled Scan	✓	✓
ActiveUpdate	✓	✓
Logs and Reports	✓	✓
Quarantine Manager	✓	✓

Features	Suite	Suite with DLP
<b>Control Manager integration</b>	✓	✓

Tip ✓ Additional details about Product Registration are available in the Administration Chapter.

## 1.3 Release History

Version	Release time
ScanMail 12.0 for Microsoft Exchange (SMEX 12)	March 2016
ScanMail 12.0 for Microsoft Exchange Patch 1 (SMEX 12 Patch 1)	July 2016
ScanMail 12.0 for Microsoft Exchange Service Pack 1 (SMEX 12 SP1)	Nov 2016

SMEX 12 SP1 is the latest release which includes all fixes resolved in SMEX 12, and it also includes several new features and enhancements. See **What's New** under topic 1.4.

Administrators currently running SMEX 12 or 12 Patch 1 should install this Service Pack.

**NOTE** 

Download SMEX 12 Service Pack 1 from:

<http://files.trendmicro.com/products/scanmail/SMEX-12.0-SP1-1464.exe>

Download ScanMail for Microsoft Exchange 12 Service Pack 1 relative documents from:

Administrator's Guide:

<http://files.trendmicro.com/products/scanmail/SMEX-12.0%20SP1-GM-1464-AG.pdf>

Installation and Upgrade Guide:

<http://files.trendmicro.com/products/scanmail/SMEX-12.0%20SP1-GM-1464-IUG.pdf>

Service Pack1 ReadMe:

<http://files.trendmicro.com/products/scanmail/SMEX-12.0%20SP1-readme.txt>

## 1.4 What's New in SMEX 12

This section discusses the new features and enhancements introduced in ScanMail for Microsoft Exchange 12.

### 1.4.1 Things You Must Know

- SMEX 12 supports Exchange 2010 SP3 or above, Exchange 2013 SP1 or above, and Exchange 2016
- SMEX 12 only supports upgrade installation from SMEX 11 SP1 for customer using Exchange 2010 SP3 or above.

## 1.4.2 Exchange Server 2016 Support

SMEX 12 provides complete support for Exchange Server 2016. However, the EUQ function for Exchange Server 2016 is not supported because Microsoft has discontinued supporting MAPI/CDO on Exchange 2016.

SMEX 12 can be installed on the following 2 server roles in Exchange 2016:

- Mailbox Server
- Edge Transport Server

## 1.4.3 SQL Server 2014 Express Service Pack 1 Support

By default, if a remote SQL server is not selected during installation, SQL Server 2014 Express Service Pack 1 will be installed in the ScanMail server.

**NOTE** 📖 SQL Server 2014 Express Service Pack 1 can only be installed on Windows 2008 R2 or above.

## 1.4.4 AlwaysOn Availability Groups Support for SQL server

The Microsoft SQL Server AlwaysOn Availability Group is the new high-availability (HA) solution that combines both clustering and mirroring. This SQL function was initially

introduced in SQL Server 2012. And now SMEX 12 supports this new SQL HA technology for remote SQL server installation.

### **1.4.5 Support Windows Authentication for Remote SQL Server**

SMEX 12 supports both SQL Server account and Windows account to access remote SQL server during installation. To use a Windows account accessing remote SQL server, the minimum privileges required of this account are:

- Domain user
- Local Administrator
- Exchange Applicationimpersonation role
- Exchange Public Folder Engagement role

**NOTE** 📖 In SMEX 11, it only supports SQL Server account to access remote SQL server during installation.

### **1.4.6 Continuous Protection with SQL Server unavailable**

The ability of ScanMail to scan email messages depends on a healthy database. It needs to read each filter's configuration to determine whether the target email message triggers any policy, thus, implement the corresponding action.

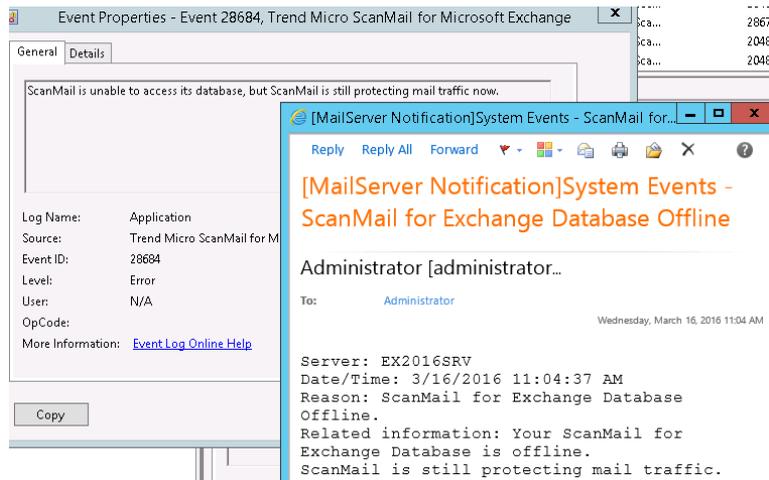
This version of ScanMail provides a high availability solution to provide continuous protection for up to 48 hours after the database connection is lost.

While the database is offline, the ScanMail administrator **MUST NOT** restart/stop ScanMail Master Service.

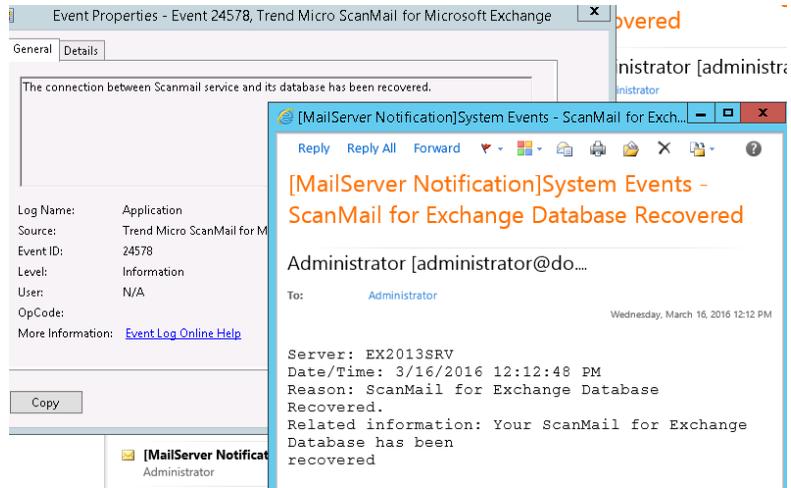
**NOTE** 📄 If ScanMail service stopped while the database is offline, ScanMail cannot perform scanning and cannot start anymore.

When ScanMail detects the database is unavailable, ScanMail will send out one alert email messages per hour to the configured database administrator's email address. This will be of advantage to the database administrator to fix the issue immediately. ScanMail will also log the database unavailable event to the Windows event log.

- Sample email notification and Windows event log for offline SMEX database



- Sample email notification and Windows event log of SMEX database recovery



While the database is offline, TMCM policy deployment will fail, and ScanMail scheduled tasks listed below will not be executed.

- Schedule Update
- Schedule Scan
- Schedule License Update
- Schedule Report
- Schedule Log/Quarantine Maintenance
- World Virus Tracking

In addition, ScanMail management console will not be able to log on. An alert message will display on the logon page.



**LOGIN**

 **The Database is currently off-line. ScanMail is still protecting mail traffic now.**

Please type your User name and Password to access the product console.

**User name:**

**Password:**

© Copyright 1998-2016 Trend Micro Incorporated. All rights reserved.

While the database is offline, ScanMail uses a local cache of policies to perform scans. And the log and report data will be saved to local files under ScanMail installation directory by default.

Scanning results and logs will be saved under %SMEX\_Home%\PUSH\HA\LOG.

Report data will be saved under %SMEX\_Home%\PUSH\HA\REPORT.

**NOTE**  The path %SMEX\_HOME%\PUSH\HA can be changed via a hidden key SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion\HADBCmdPushPath of type REG\_SZ.

Once the database connection is recovered, ScanMail uploads local logs and reports to the database periodically. If any logs cannot be uploaded to database, ScanMail sends out an alert email message to the configured administrator's email address after exceeding the maximum retry times.

## 1.5 What's New in SMEX 12 Patch 1

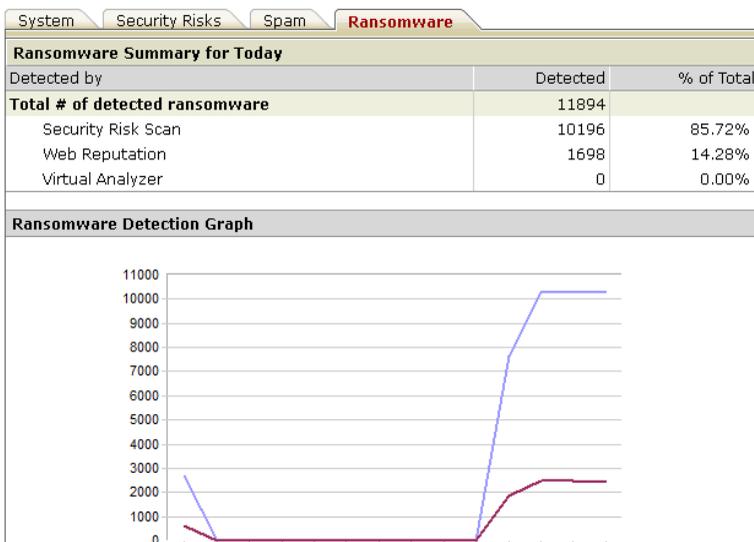
This section discusses the new features and enhancements introduced in ScanMail for Microsoft Exchange 12 Patch 1.

### 1.5.1 Ransomware Detection Visibility

ScanMail utilizes Advanced Threat Scan Engine and VSAPI engine and Web Reputation filter to detect ransomware. In previous version of ScanMail, ransomware detection is categorized as security risk with other malware/virus detection. In ScanMail 12 Patch 1, ransomware detection is re-categorized, and log query and report generation for ransomware detection are also enhanced.

A separated page is added on ScanMail management console summary page to highlight ransomware detections by ScanMail. It makes the ransomware detection more visible for administrators.

- Ransomware tab on summary page



- New category for file type ransomware detection under Security Risk Scan

**Log Query**

Criteria	
Dates:	9/7/2016 14:56 to 9/8/2016 14:56 MM/dd/yyyy hh mm MM/dd/yyyy hh mm
Type:	Security Risk Scan <b>Ransomware</b>
Found in:	All Virus/Malware Advanced threats Spyware/Grayware <b>Ransomware</b>
Sender:	
Recipient:	
Subject:	
Attachment:	
Sort by:	Scan Time Ascending Descending
Display:	15 per page
Query target(s):	Local server [EX2016MBX] Remote server(s)
<input type="button" value="Display Logs"/>	

- New category for URL type ransomware detection under Web Reputation

### Log Query

Criteria	
Dates:	9/7/2016  14 ▼ 56 ▼ to 9/8/2016  14 ▼ 56 ▼ MM/dd/yyyy hh mm MM/dd/yyyy hh mm
Type:	Web Reputation ▼ Ransomware ▼
Sender:	All
Recipient:	Ransomware
Subject:	Advanced threats
Sort by:	Scan Time ▼ <input type="radio"/> Ascending <input checked="" type="radio"/> Descending
Display:	15 per page
Query target(s):	<input checked="" type="radio"/> Local server [EX2016MBX] <input type="radio"/> Remote server(s) 
<input type="button" value="Display Logs"/>	

- New report for ransomware detection

Content	
<input type="checkbox"/> Scan status summary	
<input type="checkbox"/> Security risk scan report  Show details	
<input type="checkbox"/> Ransomware report  Hide details	
<input type="checkbox"/> Ransomware detection summary	
<input type="checkbox"/> Top ransomware senders	10
<input type="checkbox"/> Top ransomware recipients	10
<input type="checkbox"/> Top ransomware threat name	10
<input type="checkbox"/> Top ransomware file name	10
<input type="checkbox"/> Top ransomware-hosting domain/URL	10
<input type="checkbox"/> Attachment blocking report  Show details	

## 1.5.2 Sender Approved List for Virtual Analyzer configuration

This version of ScanMail provides the ability to create sender approved list on Virtual Analyzer configuration screen. Messages from senders in the approved list will not be analyzed by Trend Micro Deep Discovery Analyzer server.

Note: Suspicious file or URLs contains in the email message will bypass the scan and email message recipient will receive all the message contents.

The screenshot displays the 'Message Scan Criteria' configuration window. The 'Traffic Direction' section is set to 'All messages'. The 'Message Sender Approved List' section is highlighted with a red box. It includes options for 'Analyze messages sent from:' with 'Exclude specific accounts' selected. Below this is a search box for AD users/groups/contacts and a search button. There are also checkboxes for 'Users', 'Groups', and 'Contacts', all of which are checked. At the bottom, there are two empty list boxes: 'Available Account(s)' and 'Selected Account(s)', with 'Add >>' and '<< Remove' buttons between them. A note on the right side of the interface provides instructions on how to view or edit special groups.

**Message Scan Criteria** ⓘ

**Traffic Direction**

Analyze the following message traffic:

Inbound messages only

All messages

**Message Sender Approved List**

Analyze messages sent from:

Anyone

Exclude specific accounts ⓘ Hide details

Search for AD users/groups/contacts

Browse from special groups

Search

Search in:

Users  Groups  Contacts

Available Account(s)

Selected Account(s)

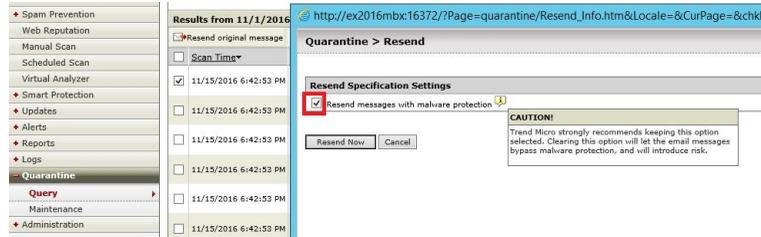
Add >>

<< Remove

Note: To view or edit special groups, navigate to **Administration > Special Group Settings** or select **Browse from special groups** and click a special group.

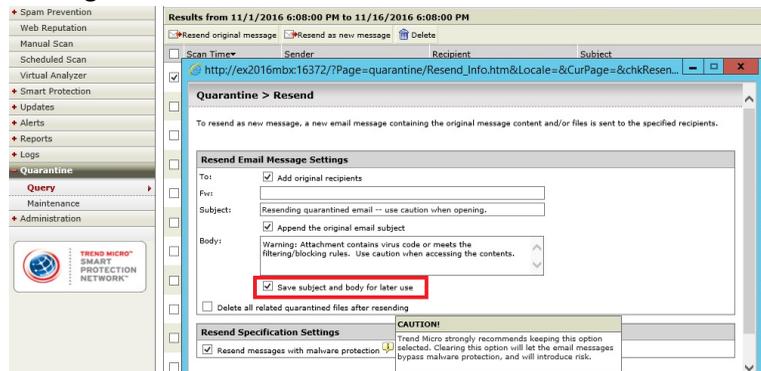
## 1.5.3 Bypass malware protection for resending message

This version of ScanMail allows administrators to resend messages without ScanMail malware protection.



## 1.5.4 Save message subject and body to reuse later

This version of ScanMail provides the ability to save the subject and body while resending a quarantined message as new. You can reuse the saved message subject and body to send messages later.



## 1.5.5 Support for monitoring advanced threats

This version of ScanMail allows administrator to monitor advanced threats scanning without affecting email traffic. These advanced threats detected by Trend Micro Deep Discovery Analyzer server can be viewed in logs on ScanMail management console.

There are two working modes for virtual analyzer. The **Monitor mode** is the new feature to allow administrator monitor advanced threats scanning.

The monitor mode is better for POC to evaluate DDAn integration without email flow impact.

Using monitor mode in production environment improves email throughput, but also increases the risk of virus leakage.

### Virtual Analyzer

Submit email messages to Virtual Analyzer 

#### Virtual Analyzer Settings

##### Virtual Analyzer Mode

Select a working mode for virtual analyzer: 

Inline mode

Monitor mode

##### Virtual Analyzer Working Modes

Inline mode: Email will be quarantined temporarily when submitting files or unrated URLs to Virtual Analyzer server for further analysis.

Monitor mode: Email will not be temporarily quarantined and only the suspicious files or unrated URLs will be submitted to Virtual Analyzer server for further analysis.

##### Virtual Analyzer Server Settings

IP address\*:

Port\*:

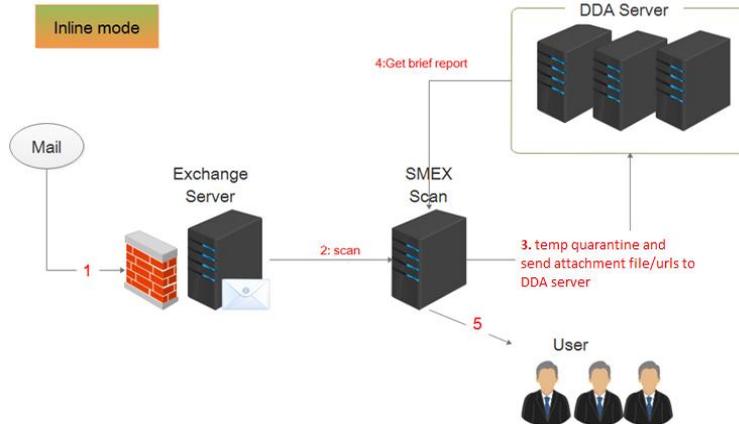
API key\*:

Use a proxy server to connect to Virtual Analyzer 

### Inline mode instruction

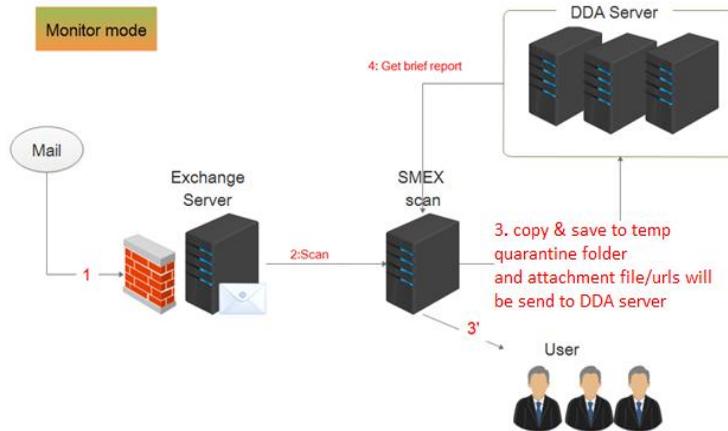
- Inline mode will intercept email flow
- Email message will be temporarily quarantined and attachment file or URLs will be sent to DDAn server for further analysis

- SMEX will take action set in VS/WTP filter base on the DDAn result and security level setting in VA page



#### Monitor mode introduction

- Monitor mode will not intercept email flow, user will receive email message immediately
- Email message will be copied under temporary quarantine folder and sent to DDAN for further analysis
- SMEX will update scan result log after receiving result from DDAn server

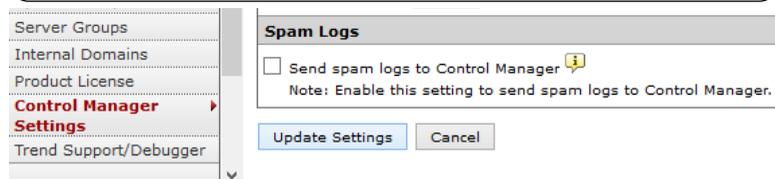


## 1.5.6 Spam log

This version of ScanMail supports sending its spam logs to Trend Micro Control Manager.

Once ScanMail is registered to Control Manager, administrator can choose to upload spam logs.

**Important:** This feature is not enabled by default. Administrator needs to pay attention that large amount of spam will cause Control Manger database grow quickly, which will affect the database performance



**NOTE** □ Spam logs section is not available on ScanMail management console on the following server roles or uses limited license:

- Standard Activation Code
- Trial Expired Activation Code
- Exchange 2010 Mailbox only server role.

**NOTE** 📄 Since the spam logs are huge in numbers, ScanMail will not save them in database for a long time. By default, sample logs older than 12 hours will be purged. This purge time can be customized via a hidden key.

SOFTWARE\\TrendMicro\\ScanMail for Exchange\\CurrentVersion\\SpamMaintenanceInterval of type REG\_DWORD.

The frequency in hours that ScanMail cleans spam logs from the database, supports any value from 1 to 24, the default value is "12".

## 1.6 What's New in SMEX 12 SP1

This section discusses the new features and enhancements introduced in ScanMail for Microsoft Exchange 12 SP1.

SMEX 12 SP1 merged all the new features and enhancement from SMEX 12 Patch 1. URL Analysis is the major new feature in this release.

### 1.6.1 Things You Must Know

- SMEX 12 SP1 supports Exchange 2010 SP3 or above, Exchange 2013 SP1 or above, and Exchange 2016.

- SMEX 12 SP1 can be upgraded from SMEX 12.0 GM build and SMEX 12.0 Patch 1 release

## 1.6.2 URL Analysis

In ScanMail 12 SP1, the ability to submit the URLs that have not been assessed by Trend Micro Web Reputation Service to Virtual Analyzer server for further analysis.

**NOTE** 

URL Analysis is also known as URL Sandboxing in other documents.

A new section URL Analysis is added under Web Reputation configuration page.

**Web Reputation**

Enable Web Reputation

---

**Target**   **Action**   **Notification**

**Security Level**

High: Blocks a greater number of web threats but increases the risk of false positives.

Medium: Blocks most web threats while keeping the false positive count low.

Low: Blocks fewer web threats but reduces the risk of false positives.

---

If you believe a URL is misclassified, please use the following link to notify Trend Micro:  
> <http://reclassify.wrs.trendmicro.com>

**Attachment Scanning**

Scan the content of message attachments for suspicious URLs  
Note: Web reputation scans the subject and contents of email messages by default.

**URL Analysis**

If you want to send URLs that have not been assessed by Trend Micro Web Reputation to Virtual Analyzer server, enable "URL Analysis" on the following link:  
> [Enable URL Analysis](#)

**Approved URL List**

Bypass internal domain URLs. Click the following link to check the Internal Domain List: [Administration > Internal Domains](#)

Enable approved URL list

Enter approved URL:

Approved URL 

Note: This will approve all subsites.

**NOTE**  Bypass Internal domain URLs setting is enable by default

Click on **Enable URL Analysis**. It directs to Virtual Analyzer configuration page and URL Analysis can be enabled here. The Virtual Analyzer settings, such as Virtual Analyzer mode, traffic direction, message sender approved list, target recipients and security level settings are still applicable to URL Analysis feature.

The screenshot displays the configuration interface for the Virtual Analyzer. On the left, a navigation menu lists various security features, with 'Virtual Analyzer' currently selected. The main panel is divided into several sections: 'Message Scan Criteria', 'Traffic Direction', 'Message Sender Approved List', 'Message Target Recipients', 'Attachment Types', and 'URL Analysis'. The 'URL Analysis' section is highlighted with a red border and contains the following text and controls:

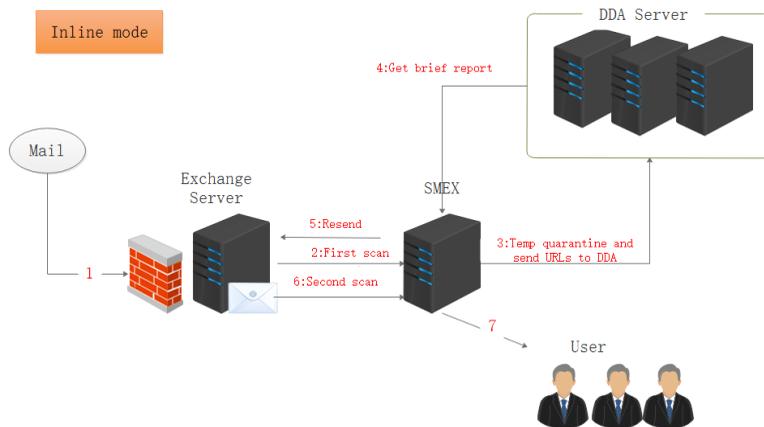
**URL Analysis**  
 Analyze message with the suspicious URLs that have not been assessed by Trend Micro Web Reputation service not:  
  
 Enable URL Analysis

**NOTE** 📄 To enable URL Analysis, it requires Deed Discovery Analyzer 5.5 or above.

## URL Analysis workflow

### Inline mode

- Email messages with unrated URL in subject/body/attachment will be temporarily quarantined
- The temporarily quarantined email messages will be replayed after the analysis result is returned or exception occurs.



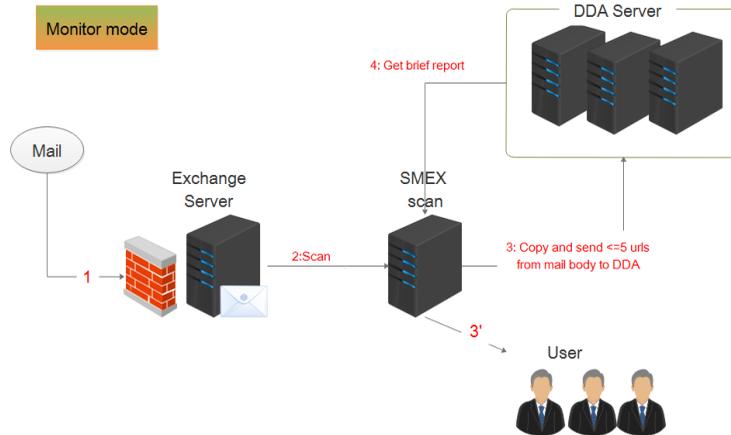
- Final action

WRS Result	DDAn Result	Final Action
Unrated	Clean	Pass
Unrated	High Risk	Web Reputation filter action configuration + Virtual Analysis security level settings
Unrated	Medium Risk	Web Reputation filter action configuration + Virtual Analysis security level settings
Unrated	Low Risk	Web Reputation filter action configuration + Virtual Analysis security level settings
Unrated	Timeout/Exception	Action on the unanalyzed risk

**NOTE** 📄 For unanalyzed URLs, the default action is Pass.ss

### Monitor mode

- Email message will be copied and saved under temporary quarantine folder and send to DDAn sandbox
- User will receive the original email message
- SMEX will update log after get result from DDAN server



## 1.7 Performance Report

### 1.7.1 SMEX12.0 SP1 performance impact on Exchange 2016 with default setting

The performance test is executed on Microsoft Exchange 2016 CU3 and Windows 2012 R2. ScanMail is designed to provide real-time and on demand protection by scanning messages, so the performance test of SMEX 12 SP1 only cover transport level real-time scan on Exchange 2016 CU3.

In the test, the multi-users-connection to Exchange server at the same time is simulated, sending SMTP email message to Exchange server concurrently, and receiving external email messages after scanning. Windows performance monitor tool gets the performance indexes information about throughput and system resource usage.

To guarantee the reasonable result, these test process is executed for several times and the average data is used in the final result.

#### Data Collection

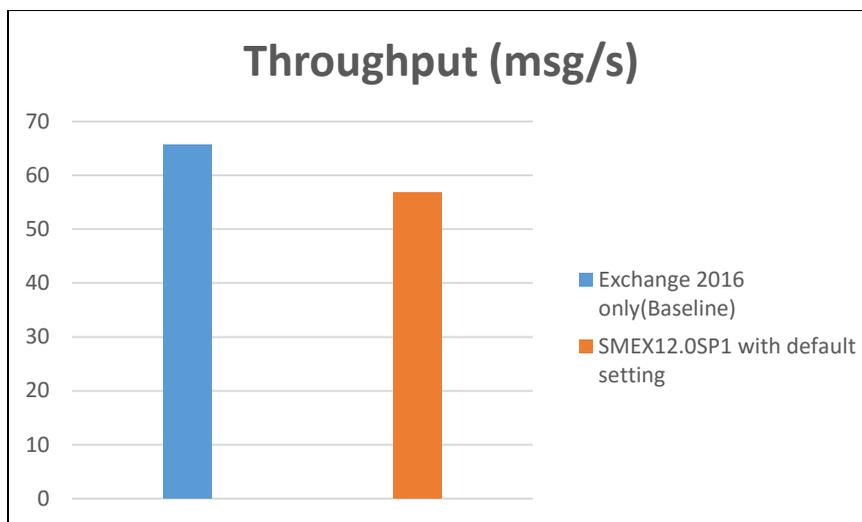
Performance indices information about throughput and system resource usage are analyzed based on Windows Performance Monitor Tool.

<b>Performance object</b>	<b>Counter</b>	<b>Instances</b>
<b>CPU usage</b>		
Processor	Processor Time	_Total
Process	Processor Time	SMEX_Master
Process	Processor Time	EdgeTransport
Process	Processor Time	Store.worker
<b>Memory usage</b>		
Process	Private Bytes	SMEX_Master
<b>Throughput</b>		
MSExchangeTransport SmtpReceive	Messages Received/sec	_Total

MSExchangeIS Mailbox	Messages Delivered/sec	_Total
MSExchangeIS	Virus Scan Messages Processed/sec	_Total

Testing result with SMEX 12 SP1 default setting

	<b>Exchange 2016 only(Baseline)</b>	<b>SMEX12 SP1 default setting</b>
<b>Processor Utilization (_Total)</b>	65.334%	64.261%
<b>Processor Utilization (SMEX)</b>	N/A	6.61%
<b>Processor Utilization (EdgeTransport)</b>	15.77%	16.46%
<b>Processor(Store.worker)</b>	8.06%	7.57%
<b>Private Bytes (MB) (SMEX)</b>	N/A	688.33
<b>Throughput (msg/s)</b>	65.603	56.943
<b>Throughput Difference (%)</b>		13.2 % downgrade



## 1.7.2 SMEX 12.0 SP1 filters performance impact on Exchange 2016

### Testing scenario

- Leverage to the similar Processor Utilization ( $\_Total=50\%\sim 60\%$ ), compare the throughput between Exchange 2016 CU3 only (baseline) and SMEX 12.0 SP1 enable different filters.
- Each time enables one filter, and the setting refers to the description in 3.4.3.
- Test data collected after every 2 hours.

### Report Summary

For SMEX default setting performance data

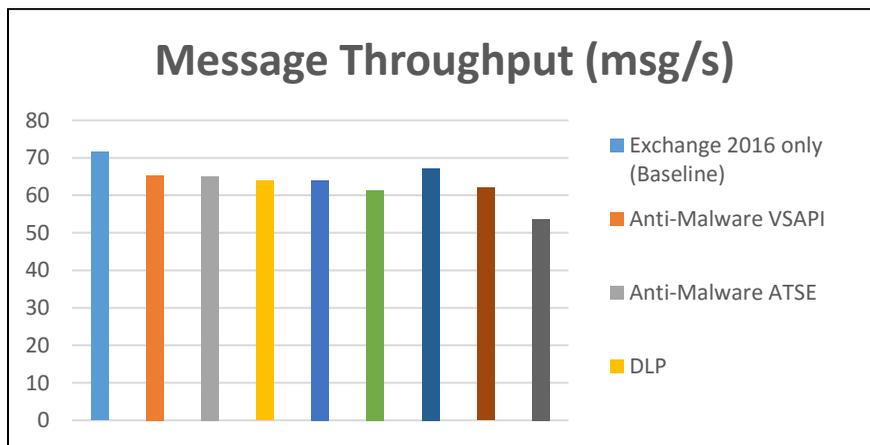
- Leverage to the similar Processor Utilization (\_Total about 60%~70%), SMEX can process about 56.943 messages/second (msg/s) with default setting, which enable anti-malware scanning, Spam Prevention, and Web Reputation.
- Throughput downgrade is about 13.2%, which is similar as previous version.

For different filter performance data

- Under similar CPU utilization circumstances, if not enabled DDAn for further scan, filter performance impact is AS>Web Reputation>DLP>CF>VS>AB. This behavior is the same as in version 12.0.
- When enable web reputation scan with URL sandboxing, throughput downgrade is about 25.13% comparing the Exchange only base line. SMEX uses more resources for doing these during scan process: temporarily quarantine email messages, upload URL samples to DDAn, wait for result, and put email messages to Exchange reply folders.

	Exchange 2016 only (Baseline)	Anti-Malware VSAPI	Anti-Malware ATSE	DLP	CF	AS	AB	Web Reputation	Web Reputation & URL sandboxing
Processor Utilization (_Total)	56.334%	56.568%	56.390%	56.508%	56.112%	56.180%	56.365%	56.242%	54.296%
Processor Utilization (SMEX_Master)	N/A	5.87%	5.93%	6.12%	4.43%	2.78%	1.85%	3.67%	4.93%
Processor Utilization	10.77%	10.37%	10.78%	10.48%	10.64%	9.01%	10.05%	9.64%	10.43%

<b>(EdgeTransport)</b>									
<b>Processor(Store.worker)</b>	9.6%	8.58%	8.96%	8.56%	8.37%	7.89%	8.44%	8.25%	8.15%
<b>Private Bytes (MB) (SMEX_Master)</b>	N/A	646.44	648.422	655.69	616.5	575.47	548.26	586.04	1151.84
<b>Throughput (msg/s)</b>	71.603	65.339	65.068	63.894	63.942	61.292	67.262	62.079	53.612
<b>Throughput downgrade (%)</b>		8.75%	9.13%	10.77%	10.69%	14.4%	6.06%	13.3%	25.13%



# Chapter 2

## Deployment

This Chapter discusses the deployment options for ScanMail for Microsoft Exchange 12 and 12 SP1.

### 2.1 System Requirement

For detailed system requirement, please see ScanMail for Microsoft Exchange 12 SP1 Administrator Guide, page 1-2, Chapter 1.

**NOTE** 

Administrator's Guide: <http://files.trendmicro.com/products/scanmail/SMEX-12.0%20SP1-GM-1464-AG.pdf>

### 2.2 Exchange Integration

#### 2.2.1 Exchange 2010 Integration

SMEX 12 only supports upgrade installation from SMEX 11 SP1 for customer using Exchange 2010 SP3 or above.

SMEX 12 can be installed on the following server roles exist in an Exchange 2010 deployment.

- Edge Transport Server (EDGE)
- Hub Transport Server (HUB)
- Client Access Server (CAS)
- Mailbox Server (MBX)

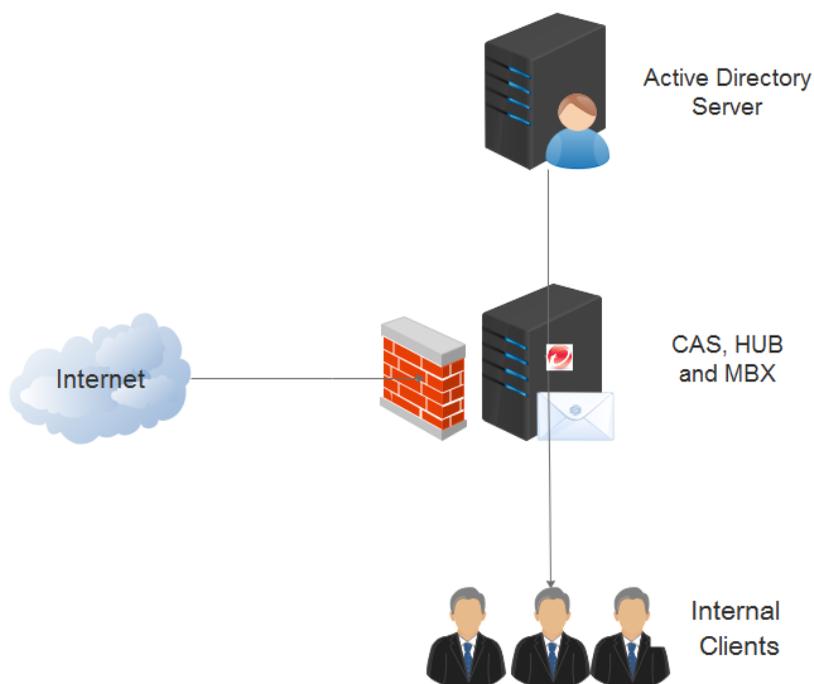
This section provides two sample SMEX deployments in Exchange 2010 environment:

- Combo Server
- Distributed Server Roles

### **Combo Server**

A Combo Server in Exchange 2010 only one physical machine is involved. There are several Exchange roles installed on the machine, particularly the CAS, HUB and MBX.

During product setup, SMEX detects if the target server has more than one role. This results to the installation of modules necessary to provide both Transport and Store Level Scanning.



## Distributed Server Roles

The available server roles in Exchange 2010 can be distributed to multiple servers. In this kind of scenario, SMEX may need to perform different types of filtering depending on the server role.

The table below summarizes the possible scan setting combinations based on their server role:

Server Role	Performance	Security
EDGE	Spam Prevention	Spam Prevention Web Reputation

Server Role	Performance	Security
(Transport Level Scanning)	Web Reputation	Security Risk Scan [Optional] Content Filtering
HUB (Transport Level Scanning)	Scheduled Scan	Content Filtering Attachment Blocking Security Risk Scan [Optional] Spam Prevention Web Reputation
MBX (Store Level Scanning)	Scheduled Scan	Security Risk Scan Scheduled Scan [Optional] Content Filtering Attachment Blocking

**NOTE** 📄 Spam Prevention in the above table refers to Email Reputation and Content Scanning

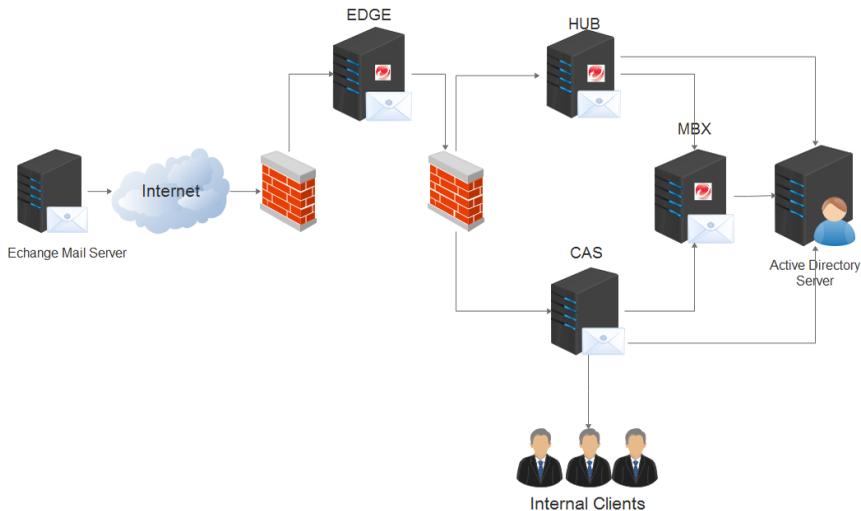
Since performance is the main deployment concern in an Exchange environment, SMEX can be enabled to deploy different kinds of protection for different server roles. Spam email message which can include malicious links, tends to have a higher amount of incidence in Edge Transport Servers hence it is logical to have Spam Prevention and Web Reputation enabled in this server role.

This translated to lesser number of email messages that needs to be processed by other server roles. Other real-time protection such as Security Risk Scan or Content Filtering is enabled on Hub Transport

Server since all email messages not tagged as spam passes through this server. Consequently, scheduled scan together with regular pattern update is sufficient to protect the Mailbox Server since protection at this level only focuses on email message storage and other threats that are undetected by existing pattern.

If security is the main deployment concern, the recommendation is to enable Security Risk Scan on all server roles. The same principle applies for the Edge Transport Server which has Spam Prevention and Web Reputation enabled. With security in mind, the Hub Transport Server is where the primary protection and policy enforcement takes place. This result in recommending all available protection enabled on this server with Spam Prevention and Web Reputation as an optional setting.

The below figure illustrates a sample deployment with distributed server roles.



## 2.2.2 Exchange 2013 Integration

The multi-role server architecture has been consolidated in Exchange Server 2013.

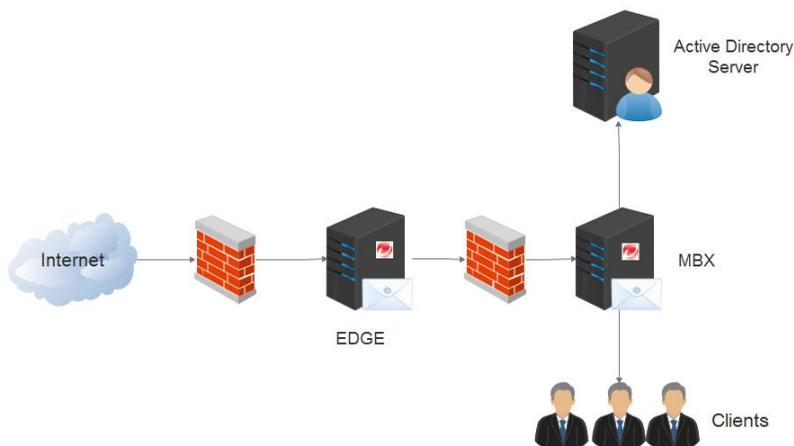
SMEX 12 can be installed on the following server roles exist in an Exchange 2013 deployment.

- Mailbox server (MBX)
- Edge Transport Server (EDGE)

**NOTE** Edge Transport Server is available in Microsoft Exchange Server 2013 Service Pack 1 (SP1).

And SMEX 12 cannot be installed on an Exchange 2013 server with only Client Access Server role.

This section provides a sample SMEX deployments in Exchange 2013 environment:



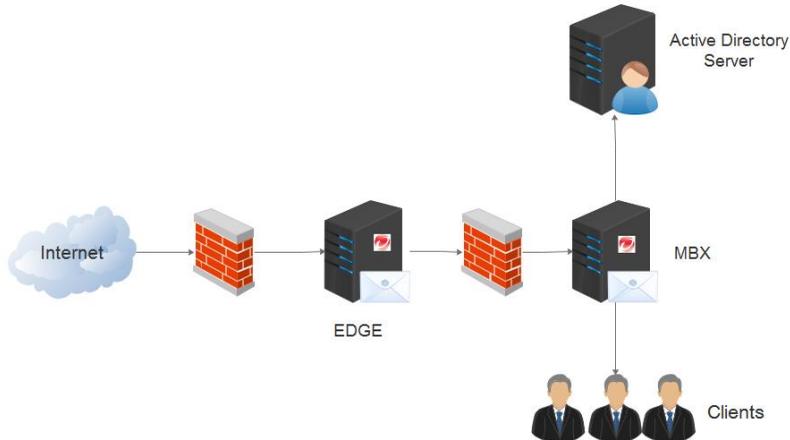
## 2.2.3 Exchange 2016 Integration

There are only 2 server roles exist in an Exchange 2016 deployment.

- Mailbox server (MBX)
- Edge Transport Server (EDGE)

**NOTE** 📄 Client Access Server role, which was previously available in Exchange 2013, has been removed and replaced by Client Access service. In addition to the server roles above, MAPI/CDO are not fully supported by Exchange 2016. Hence, the EUQ feature cannot work on Exchange 2016.

This section provides a sample SMEX deployments in Exchange 2013 environment:



## 2.3 Cluster Integration

Exchange provides high availability and fault tolerance with the use of cluster technology. The below table summarizes the different cluster models that are supported by ScanMail for Microsoft Exchange 12:

Exchange	Cluster Model
Exchange 2007 (supported only in SMEX 11)	<p>SCR (Standby Continuous Replication)</p> <p>Windows 2003: Majority Node Set, Local Quorum</p> <p>Windows 2008: Node Majority, Node and File Share Majority</p> <p>SCC (Single Copy Cluster) Windows</p> <p>2003: Standard Quorum</p> <p>Windows 2008: Node and Disk Majority</p> <p>Note: SMEX 10.0 can be installed on a Majority Node Set model on Windows</p> <p>2003 but it is not officially supported (testing conducted was limited)</p> <p>CCR (Cluster Continuous Replication)</p> <p>Windows 2003: Standard Quorum, Majority Node Set</p> <p>Windows 2008: Node and Disk Majority, Node and File Share Majority</p>

Exchange	Cluster Model
	VERITAS Cluster 5.0 R1 VERITAS Cluster 5.1
Exchange 2010	DAG (Database Availability Group) VERITAS Cluster 5.1 SP2
Exchange 2013/2016	DAG (Database Availability Group)

**NOTE**  For information and comparison purposes, other cluster model supported only in SMEX 11 was mentioned above.

When installing the previous version of SMEX on a clustered Exchange Servers, the administrator can input the name of the cluster, any EVS (Exchange Virtual Server) or any node. The SMEX setup program is responsible for detecting the whole cluster environment and will add other EVS or nodes on the list of target servers as necessary.

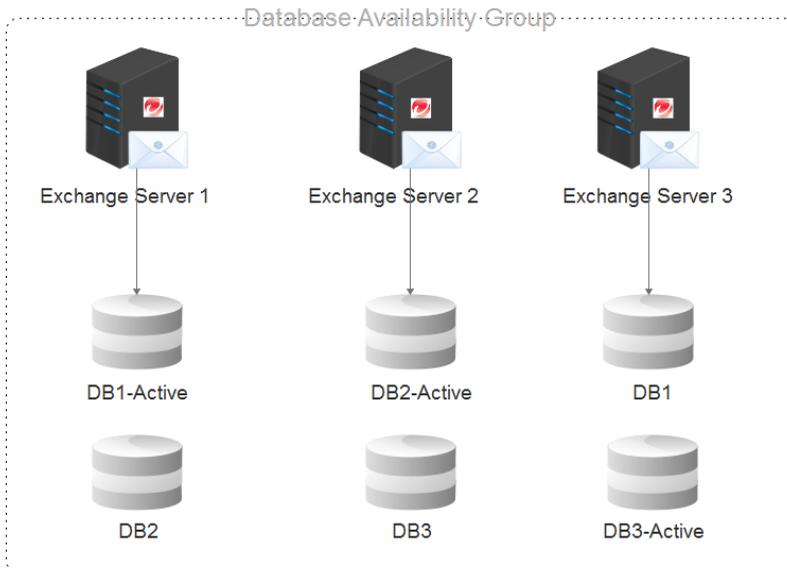
With the currently supported cluster environment, it requires the administrator to select all members of the DAG or VERITAS cluster during installation.

### **Database Available Group support**

DAG relies on continuous replication as well as a subset of Windows failover clustering to ensure that mailboxes are always available. It can support up to 16 Mailbox Servers wherein any member server can host

a copy of a mailbox database from any other server in the group. These member servers monitor each other for failures that affect mailbox databases such as disk or server failure.

As illustrated in below figure, a mailbox database from one Exchange Server can be replicated to one or more member servers in the group. In the event that the active copy fails (due to a disk or a server problem), the member which has a copy of the failed database facilitates an automatic recovery.



Regarding SMEX support for this environment, a Database Availability Group is treated just like a stand-alone server. As a result, SMEX needs to be installed on all member servers to provide complete protection to the group.

Only the active databases are scanned by SMEX and passive copies are skipped. To determine which databases are active, SMEX uses Get-

MailboxDatabaseCopyStatus, a PowerShell command that returns either Mounted for an active copy or Healthy for a passive copy. The settings used for scanning operation depend on the configuration of the current host.

### **VERITAS Cluster Support**

VERITAS Cluster is only available for version 5.1 SP2 on Exchange 2010. A VERITAS Cluster can be managed using either the Cluster Manager or via the command line interface. Its configurations are not saved in the registry but in the following files instead:

- Main.cf – contains resource group and resources
- Types.cf – contains resource types

The SMEX 12 installation on VERITAS is similar to the other cluster configurations.

ScanMail does not automatically install VERITAS cluster nodes. ScanMail will only install on the nodes that you configure on the Select Target Servers screen. Manually add all the nodes to the target server on the Select Target Server screen during installation.

Important: Exchange does not recognize a VERITAS Cluster configuration. It treats the said environment just like a stand-alone server

VERITAS provides two solutions:

HA (High Availability) Solution – this solution is similar to Microsoft SCC environment. A cluster is comprised of one or more virtual servers in a single site with all of them sharing a disk resource. In the event of a fail-over, the disk gets assigned to the online node. In this environment

when no virtual server is online, all Exchange related services are off. Once a virtual server becomes online, the following events occur:

- Computer name is changed – this occurs once the Lanman resource becomes online
- Registries are replicated – this occurs once the RegRep resource becomes online
- Exchange services are started – this occurs once the ExchService and ExchProtocol resources becomes online

DR (Disaster Recovery) Solution – this solution can be viewed as an HA hybrid. A DR solution is comprised of several sites with each site having a High Availability implementation. In this environment, each site will have its own set of shared resources.

The SMEX implementation for VERITAS depends on the solution used. In a High Availability environment, SMEX resources are only created for the online nodes. Database and binaries are installed on both offline and online nodes. When all the nodes are finished with the installation, a remote task is automatically launched to cluster resources for the SMEX (dependency list in below table).

In a Disaster Recovery environment, SMEX resources are also created on remote offline cluster nodes. To do this, the following tasks are performed by SMEX:

1. Get remote cluster IP from Main.cf
2. Analyze the remote cluster to enumerate the remote nodes
3. Detect the remote offline nodes for each virtual server
4. Select the remote offline nodes when creating the SMEX resources

In order to identify whether a virtual server is online or offline, what SMEX does is it executes the GetComputerName() function and tries to get a Lanman resource. If this is successful, then the virtual server is online. Otherwise, it is offline.

This table shows the dependencies for each resource:

Resource Name	Resource Type	Dependencies
<b>ScanMail_RegRep</b>	RegRep	Shared Disk Resource
<b>ScanMail_Master</b>	GenericService	ExchangeIS ScanMail_RegRep
<b>ScanMail_SystemWatcher</b>	GenericService	Lanman ScanMail_RegRep
<b>ScanMail_RemoteConfig</b>	GenericService	ScanMail_Master
<b>EUQ_Monitor</b>	GenericService	ExchangeIS ScanMail_RegRep

VERITAS cluster resources dependencies



VERITAS cluster resource

# Chapter 3

## Setup and migration

### 3.1 Installation

#### 3.1.1 Fresh install ScanMail prerequisite on Microsoft Exchange 2013/2016

In this section, it will highlight the important items before and after installing ScanMail. The detailed system requirement will not be introduced. See system requirement from ScanMail 12 and 12 SP1 installation and upgrade guide.

During installation, the administrator is required to provide the needed parameters before and after the target server is analyzed. These parameters are summarized in the following table:

Before Server Analysis	After Server Analysis
<ol style="list-style-type: none"><li>1. Action (Install, Upgrade or Uninstall)</li><li>2. Server Version<ul style="list-style-type: none"><li>• Exchange 2013/2016<ul style="list-style-type: none"><li>○ Mailbox Server</li><li>○ Edge Transport Server</li></ul></li></ul></li><li>3. Target Server</li></ol>	<ol style="list-style-type: none"><li>1. SQL Configuration</li><li>2. Proxy Settings</li><li>3. Product Activation</li><li>4. World Virus Tracking Program</li><li>5. Spam Prevention Settings</li><li>6. Control Manager Server Settings</li></ol>

Before Server Analysis	After Server Analysis
<ul style="list-style-type: none"> <li>4. Logon Credentials</li> <li>5. Target and Shared Directory</li> <li>6. Web Server Information</li> </ul>	<ul style="list-style-type: none"> <li>7. Management Group Selection</li> </ul>

To prevent permission issues when installing SMEX, the accounts used should have the following privileges:

ScanMail Database Option	Setup Account Privileges	Database Access Account Privileges
Local Database	Local Administrator Domain User Exchange Organization Management Group  Note: Activate End User Quarantine setup account should be the Domain Administrator	
Remote SQL Server with SQL Windows Authentication	Local Administrator Domain User Exchange Organization Management Group  Note: Activate End User Quarantine setup account should be the Domain Administrator	dbcreator role plus the following privileges: Local Administrator Exchange Organization Management Group Exchange Application Impersonation role Note: Activate End User Quarantine setup account should be the Domain Administrator

ScanMail Database Option	Setup Account Privileges	Database Access Account Privileges
Remote SQL Server with SQL Authentication	Local Administrator Domain User Exchange Organization Management Group  Note: Activate End User Quarantine setup account should be the Domain Administrator	dbcreator role

**NOTE**  If choose to use Remote SQL Server Windows Authentication option, it is a best practice to use same domain account for Setup Account

### 3.1.2 Installation Verification

- The <SMEX program directory> is created. By default, its located in %Program Files%\Trend\Smex:
  - For stand-alone environment, this contains both the SMEX binary and data files
  - For cluster environment, the program directory only contains the binary files. The data files are located in the shared disk. These are:
    - ActiveUpdate components – engine and pattern files for the virtual servers
    - Configuration files – stores the configuration for virtual servers including dbconf\_conf.xml
    - Database files – MDB files for configuration, log and report

- EUQ related configuration
- Storage – archive, backup and quarantine folders
- CM Agent configuration

2. The following services or cluster resources are created:

Services

- ScanMail EUQ Monitor (This service is disabled for Exchange Server 2016)
- ScanMail for Microsoft Exchange Master Service
- ScanMail for Microsoft Exchange Remote Configuration Server (except on Transport Server)
- ScanMail for Microsoft Exchange Systems Watcher

Cluster Resources

- Veritas – Scanmail\_RegRep

3. The following registries are created:

Registry Group	Registry Entries
Product Registry	HKLM\SW\TrendMicro\ScanMail for Exchange HKLM\SW\Wow6432Node\TrendMicro\ScanMail for Exchange
Services Registry	HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_Master HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_RemoteConfig HKLM\SYSTEM\CurrentControlSet\Services\ScanMail_SystemWatcher HKLM\SYSTEM\CurrentControlSet\Services\EUQ_Monitor
Main VirusScan Registry	HKLM\SYSTEM\CurrentControlSet\Services\MSExchangeIS\VirusScan (Hub Transport with Mailbox/Mailbox Servers)
VirusScan registry	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\ <server-name>\Private-</server-name>

Registry Group	Registry Entries
for private and public store	<p>&lt;MDB-GUID&gt;\VirusScanEnabled            HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<server-name&gt;\private-&lt;mdb-guid&gt;\virusscanbackgroundscanning </server-name&gt;\private-&lt;mdb-guid&gt;\virusscanbackgroundscanning            HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<server-name&gt;\public-&lt;mdb-guid&gt;\virusscanenabled </server-name&gt;\public-&lt;mdb-guid&gt;\virusscanenabled            HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeIS\<server-name&gt;\public-&lt;mdb-guid&gt;\virusscanbackgroundscanning< p=""> </server-name&gt;\public-&lt;mdb-guid&gt;\virusscanbackgroundscanning<></p>
Cluster Registry	<p>HKLM\SW\TrendMicro\ScanMail for Exchange\CurrentVersion            HKLM\Cluster\SW\TrendMicro\ScanMail for Exchange            *ClusterQuorumNode where 1 is sharedisk/SCC and 2 is CCR            *IsCluster where 0 is non-cluster and 1 is cluster</p>

4. SMEX management console can be access using one of the URL listed below:

Web Server	URL
Virtual Web Server	http://<Server IP or hostname>:<port>/smex/
Default Web Server	http://<Server IP or hostname>/smex

5. On the Edge or Mailbox Server, two transport agents are installed:
- ScanMail SMTP Receive Agent
  - ScanMail Routing Agent

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

Identity                                     Enabled      Priority
-----
ScanMail Routing Agent                     True         1
ScanMail SMTP Receive Agent                True         2
Transport Rule Agent                       True         3
DLP Policy Agent                           True         4
Malware Agent                              False        5
Text Messaging Routing Agent               True         6
Text Messaging Delivery Agent              True         7
System Probe Drop Smtg Agent               True         8
System Probe Drop Routing Agent            True         9

PS C:\Windows\system32>_
```

6. To record the installation, the following log files are created in the Windows Temp directory (C:\Windows\Temp):
- InstSetupHelper.log
  - MsiExec.log
  - RIFRemoteInstallAgent.log
  - Setup.log
  - SMEX\_MsiInstall-SMEX.log
  - SqlSetup.log
  - SqlSetup\_Local.log

**NOTE** Information about the database created is created under SMEXInstallDir>\SMEX\_DatabaseCreation.log. By default, C:\Program Files\Trend Micro\Smex\SMEX\_DatabaseCreation.log)

## 3.2 Upgrade

In this section, it will highlight the important items when upgrade from SMEX 11 SP1 to SMEX 12.

### 3.2.1 Upgrade Overview

Upgrade occurs when a previous of SMEX is present in the target machine and the latest version is run on top of it. The key items to remember for a successful upgrade are:

- The current SMEX version should be included in the supported migration path. For SMEX 12, the supported migration path is ScanMail 11.0 with Service Pack 1.
- At the Exchange platform end, upgrade can only be done on Exchange 2010.

When the upgrade process is run, it uses the same permissions utilized during fresh installation. The slight difference is the parameters used. For reference, see the list showed below:

Before Server Analysis	After Server Analysis
<ol style="list-style-type: none"> <li>1. License Agreement</li> <li>2. Action (Install, Upgrade or Uninstall)</li> <li>3. Server Version               <ul style="list-style-type: none"> <li>• Exchange 2010                   <ul style="list-style-type: none"> <li>○ Hub Transport/Mailbox</li> <li>○ Edge Transport</li> </ul> </li> <li>• Exchange 2013/2016                   <ul style="list-style-type: none"> <li>○ Mailbox Server</li> <li>○ Edge Transport</li> </ul> </li> </ul> </li> </ol>	<ol style="list-style-type: none"> <li>1. Activation Code</li> <li>2. World Virus Tracking Program</li> <li>3. Spam Prevention Settings</li> <li>4. Control Manager Server Settings</li> <li>5. Management Group Selection</li> </ol>

Before Server Analysis	After Server Analysis
<ol style="list-style-type: none"><li>4. Target Server</li><li>5. Logon Credentials</li><li>6. Target and Shared Directory</li><li>7. Web Server Information</li></ol>	

**NOTE** 

- If the user selected a mix of target servers (composed of both fresh installation as well as for upgrade), the hidden pages will still be displayed. However, the input provided is ignored for the upgraded servers.
- The inputs provided for the other setup parameters during upgrade (Web Server Information, Activation Code, Spam Prevention Settings, Control Manager Server Settings and Product Console Administrator Account), will replace the target server current configuration.
- The upgrade process keeps all the settings from the previous whenever possible. For the new settings, SMEX will use the default values

## 3.2.2 ScanMail Settings modification during upgrade

### Spam Prevention Setting

Spam Prevention Settings can be changed during upgrade depending on the user's selection. SMEX ensures that all previous data are kept following the basic premise that EUQ approved sender list gets migrated to Junk email safe sender list and vice-versa.

The following table summarizes the different upgrade scenarios for Spam Prevention Settings and the expected behavior for SMEX:

---

Upgraded Scenario	Result
SMEX 11 SP1 (EUQ) > SMEX 12 (Junk Email)	EUQ related resources are deleted Convert approved senders list to safe senders list
SMEX 11 SP1 (Junk Email) > SMEX 12 (EUQ)	Convert safe senders list to approved senders list

### Control Manager Setting

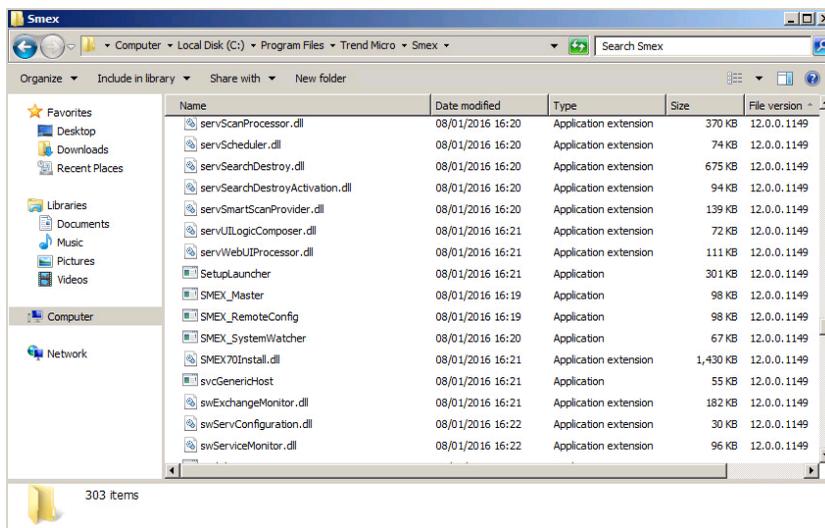
The table shows the upgrade scenario for SMEX Control Manager Agent:

Upgrade Scenarios	Results
SMEX 11 SP1 > SMEX 12	<ul style="list-style-type: none"> <li>• Unregister from original CM Server</li> <li>• Uninstall CM Agent</li> <li>• Remove all CM Agent information from the database</li> </ul>

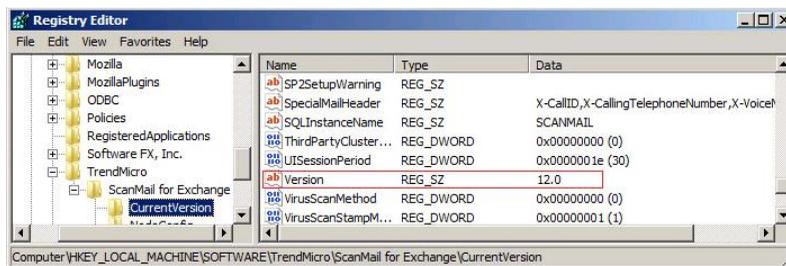
### 3.2.3 Upgrade Verification

After an upgrade has completed, the following items are need to be verified:

1. The <SMEX program directory> of the previous version was not changed. However, the files under the directory now have a file version of 12.0.1149 as shown in below Figure



2. The registry value Version located under [HKLM\SW\TrendMicro\ScanMail for Exchange CurrentVersion] now reflects to 12.0.



3. When accessing the SMEX management console, the following items can be verified:
  - About page shows Version: 12.0
  - SMEX settings from the previous version have been carried over
  - Links from new product features are now available.

## 3.3 Silent Installation

### 3.3.1 Silent Installation Limitations

The following lists the limitations for silent installation:

- Silent installation is only supported on local computers.
- Generate the preconfigured file by using recording mode the first time. Then modify settings in the preconfigured file. However, do not modify settings in the Do not edit sections.
- For version upgrades, record settings using the new package. Silent installation will keep the previous settings when an upgrade is performed.
- Record settings separately for target servers with different languages. Do not apply preconfigured files recorded on an English operating system to a target server with a German operating system.

### 3.3.2 Performing Silent Installation

#### Procedure

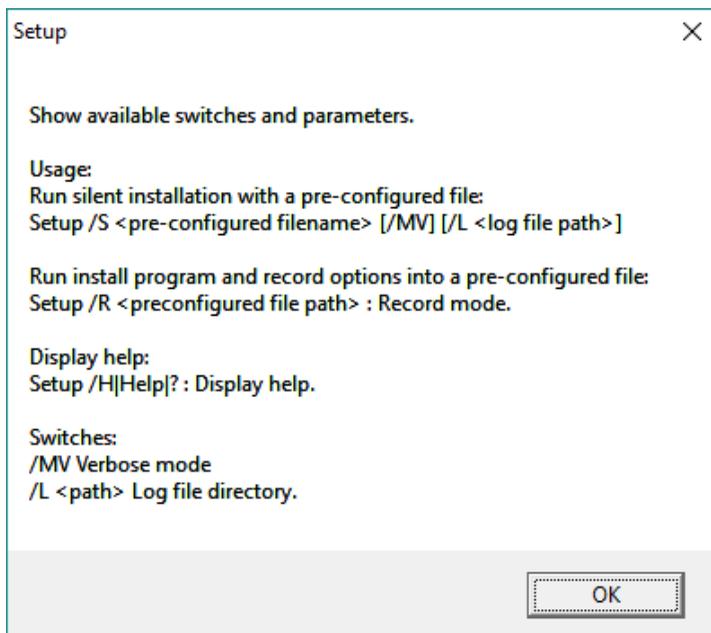
- 1 Launch Windows Command prompt.
- 2 Locate the ScanMail for Microsoft Exchange directory.
- 3 Type Setup /R to start recording mode
- 4 Copy the preconfigured file (setup-xxx.iss) to the ScanMail for Microsoft Exchange directory when the recording completes.
- 5 Type Setup /S <preconfigured filename> to perform silent installation.

### 3.3.3 Silent Installation setup switches

#### Help Switch

To invoke the help menu, the following commands can be used to trigger it:

- setup /h
- setup /help
- setup /?



## Recording Switch

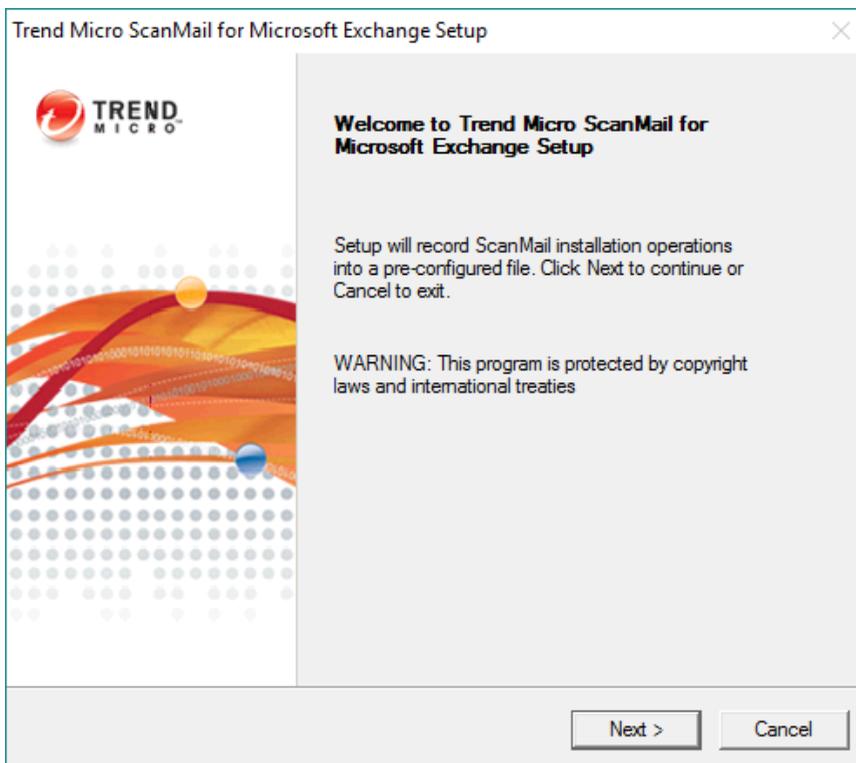
The recording mode is triggered by running `setup /r <preconfigured file path>`. It generates an ISS file that contains the settings used for silent installation/upgrade of SMEX. The name of the file corresponds to the target Exchange Server and cannot be changed during the recording:

Exchange Version	Description
Exchange 2010 (Hub/Mailbox)	setup-e2k7-hubmbx.iss
Exchange 2010 (Edge Transport)	setup-e2k7-edge.iss
Exchange 2013/2016 (Mailbox/Edge Transport)	Setup-e15.iss

The `<preconfigured file path>` is an optional parameter that refer to the directory where the ISS file is saved. The directory needs to exists before it can be used with the `/r` option. By default, the path is set to `C:\Windows`.

**NOTE**  This switch does not accept `<directory>/<filename>` for a parameter (An example is `c:\config.iss`). An error occurs if the parameter is used: The directory specified after `/R` does not exist. Should the use wish to change the name of the ISS file, it can manually modify it after the recording is completed.

When using the recording switch, the Welcome page displays a message reminding you that ScanMail records the installation process into a preconfigured file.



### Installation/Upgrade Switch

After the configuration file has been created and modified, setup.exe is triggered using the installation/upgrade switch. The available parameters are as follows:

```
Setup /s <pre-configured filename> [/MV] [/L <log file path>]
```

- setup /s <pre-configured filename> - performs the silent installation/upgrade using the settings defined in the preconfigured file. The <pre-configured filename> is a required parameter and can contain the path and the name of the

configuration file. If no path is provided, setup.exe will automatically search for the configuration file on the same directory as setup.exe.

- /L <log file path> - an optional parameter that allows the user to record all the tasks performed during the silent installation/upgrade to a file. This is in addition to the logs that are automatically generated by the setup program. The name of the file is hard-coded installlog.log but the path can be modified. The default path is the same directory where the setup.exe is located.

**NOTE** 📖 a new installlog.log is created every time. If the same directory path is specified for each installation attempt, the debug log is overwritten.

- /MV - an optional parameter that performs the silent installation/upgrade in verbose mode. When this is used, the installation status is displayed on the command prompt where setup /s <pre-configured filename> is invoked. Enabling this switch also records additional information to installlog.log.

## 3.4 Uninstallation

There are 3 different ways to uninstall ScanMail from your Exchange server.

- Using the Setup Program
- Using the Windows Control Panel
- Manually removing ScanMail

**Tip** ✓ Additional details on uninstallation are located in the ScanMail 12.0 Installation and Upgrade Guide, Chapter 6 Removing ScanMail.



# Chapter 4

## Product Management

This chapter provides the ways to grasp the ScanMail configuration well.

You can change the ScanMail configuration in the following ways:

- Via the GUI
- Via the Registry
- Via the database
- Via local configuration files (INI files)

Changes made in the GUI are stored in the database. We do not recommend changing the settings directly via the database or in the INI file unless instructed by the support professional handling your case. You should always use the GUI to make changes to ScanMail. Some settings require you to add, edit, or modify the registry to take effect.

This section provides recommendations and important notes on key settings that will help you make the necessary configuration changes based on your security requirements. Additional information is also included for some items to assist customers in configuring ScanMail according to best practices.

### 4.1 GUI Configuration

SMEX provides a GUI (Graphical User Interface) that can be accessed either locally from the same server or remotely. This is by using a web browser (Microsoft Internet Explorer or Mozilla Firefox). The verification for the browser version is performed when displaying the login page. SMEX UI

requires the installation of JVM (Java Virtual Machine) with a minimum version of 1.6. If JVM is not installed, SMEX management console prohibits any login attempt.

By default, SMEX management console is configured to accept the following requests:

- HTTP requests on port 16372
- HTTPS requests on port 16373

**NOTE** 

In SMEX 12 SP1, the HTTP access will be removed if SMEX website is installed on IIS virtual web site when both HTTP and HTTPS are bound.

## 4.1.1 Recommended Scan Settings for Different Server Roles

The following table lists the recommended settings for different server roles.

Server Role	Performance	Security
EDGE (Transport Level Scanning)	Spam Prevention Web Reputation	Spam Prevention Web Reputation Security Risk Scan  [Optional] Content Filtering
HUB (Transport Level Scanning)	Scheduled Scan	Content Filtering Attachment Blocking Security Risk Scan  [Optional] Spam Prevention Web Reputation
		Security Risk Scan Scheduled Scan

MBX (Store Level Scanning)	Scheduled Scan	[Optional] Content Filtering Attachment Blocking
----------------------------------	----------------	--

## 4.1.2 Attachment Blocking Policies

The following table lists the recommended attachment blocking settings.

SERVER ROLE	SETTING
Edge server	Disable
Transport Level Real-time Scan	Enable
Store Level Real-time Scan	Disable

Exception Rule Replication: this can be used by Server Management console, below table show the Attachment Blocking Exception Rule Limitations:

RESOURCE	LIMITATIONS
Platform	<p>Exceptions are only supported for:</p> <ul style="list-style-type: none"> <li>Exchange Server 2016</li> <li>Exchange Server 2013 SP1 or above</li> <li>Exchange Server 2010 SP3 or above.</li> </ul>
Server roles	<ul style="list-style-type: none"> <li>In Edge server, ScanMail cannot obtain sufficient information from Windows Active Directory to implement attachment blocking policies.</li> <li>Exception rules will not be applied in Store Level real time scan, manual scan, and scheduled scan.</li> <li>Exception rules only display on the Summary screen for transport level real time scan.</li> <li>On store level scan and edge servers, only the global policy is applied.</li> </ul>

## Sample Usage Scenarios

### Scenario:

The company policy is to prevent all users from receiving Sound attachment types, but allow users that belong to the Music Club receive mp3 files.

### Solution:

1. Configure the Global rule to **Block specified >Sound**.
2. Create an exception rule that applies to **Music Club**.
3. Configure the exception rule target to mp3.
4. Typical User scenario II (AB Exception)

### Scenario:

The company policy is to block .mp3, .doc, and .exe files. However, allow the Music Club to receive .mp3 files and allow ScanMail to receive .exe files.

### Solution:

1. Set the Global policy to block .mp3, .doc, and .exe files.
2. Create an exception rule named **Music Club** and configure it to pass .mp3 files and set the priority to 1.
3. Create an exception rule named ScanMail and configure it to pass .exe files and set the priority to 2.

### Known Issue:

If a user belongs to both the Music Club and ScanMail groups, when an email message includes .mp3, .doc, 38 and .exe files, the user will receive the .doc and .exe files.

### 4.1.3 Content Filtering Active Directly Integrated

The following table lists the recommended content filtering setting

SERVER ROLE	SETTING
Edge server	Disable
Transport Level real-time scan	Enable
Store Level real-time scan	Disable

Content Filtering Policy Replication which can use Server Management to replicate settings between different exchange servers. Only replicate the settings between same server roles.

RESOURCE	LIMITATIONS
Platform	Policies are only supported for: <ul style="list-style-type: none"> <li>• Exchange Server 2016</li> <li>• Exchange Server 2013 SP1 or above</li> <li>• Exchange Server 2010 SP3 or above.</li> </ul>
Server roles	<ul style="list-style-type: none"> <li>• Content filtering policies only apply for Transport level real time scan</li> <li>• Store level scan and edge server only apply the global policy.</li> </ul>

### 4.1.4 Data Loss Prevention Policy

The following table lists the recommended Data Loss Prevention settings for real-time

scans.

SERVER ROLE	SETTING
-------------	---------

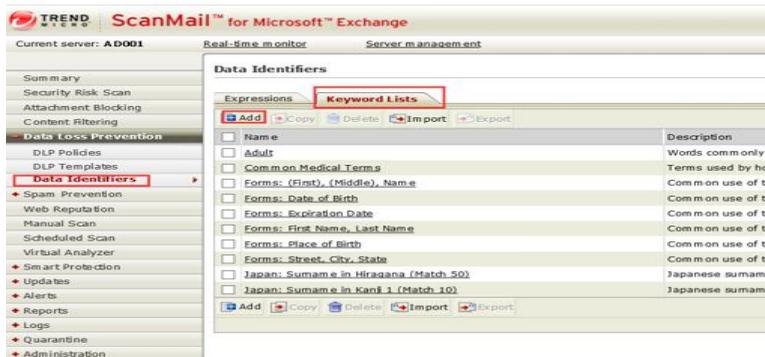
Hub server	Apply policies to "Outbound messages"
Edge server	Disable

**NOTE** 

When Data Loss Prevention policies only apply to outbound messages, no policy violations trigger for the internal domains. This will highly improve the real-time scan performance of Data Loss Prevention.

Steps to deploy a DLP Policy:

1. Define an DLP Identifier: (Two kinds of data identifier in DLP)
  - Keyword
  - Regular expression
2. Define “Keyword” Identifier
  - i. SMEX management console. Go to **Data Loss Prevention > DLP Identifiers >Click Keyword List**



- ii. Input keyword in **Keyword** field and click **Add**. One or more keyword can be created. Can being defined to meet **any, all keywords** or **All keywords within <x> characters**

## Add Keyword List



Keyword List: New keyword list

**Properties**

Name\*: A Sample Keyword  
 Description:  
 Criteria: All keywords

**Keyword**

Keyword:  **Add**  
 Case-sensitive

**List**

Delete 1 - 1 of 1 Page 1 of 1

<input type="checkbox"/>	Keyword	Case-sensitive
<input type="checkbox"/>	Trend Micro	No

Delete 1 - 1 of 1 Page 1 of 1  
 Rows per page: 10

Save Cancel

- iii. After keyword is all added, click **Save** to finish the keyword data identifier creation

Expressions **Keyword Lists**

Add Copy Delete Import Export 21 - 27 of 27 Page 3 of 3

<input type="checkbox"/>	Name	Description	Type	Template Instances
<input type="checkbox"/>	Source Code: VB	Common source code functions/commands used in Visual Basic	Pre-defined	2
<input type="checkbox"/>	US: HCFA (CMS) 1500 Form	Standard claim form used by health care professionals and...	Pre-defined	2
<input type="checkbox"/>	US: SOX(Sarbanes-Oxley) Confidentiality Terms	Terms commonly used to describe confidential information	Pre-defined	1
<input type="checkbox"/>	US: SOX(Sarbanes-Oxley) Financial Terms	Terms commonly used in financial and accounting data	Pre-defined	1
<input type="checkbox"/>	US: UB-04 Form	A universal billing form that simplifies and standardizes...	Pre-defined	2
<input type="checkbox"/>	Weapons	Words that describe implements of violence	Pre-defined	0
<input type="checkbox"/>	A Sample Keyword		User Defined	1

Add Copy Delete Import Export 21 - 27 of 27 Page 3 of 3  
 Rows per page: 10

3. Define “Regular Expression” Data Identifier  
 Go to **Data Loss Prevention > DLP Identifiers > Click the Expression tab > Click Add**



## Go to **Data Loss Prevention > DLP Templates** and click **Add**

**Add Data Loss Prevention Template** [Help](#)

Data Loss Prevention Templates: New template

**Name and Description**

Name\*:

Description:

**Condition Statement**

For detailed instructions on defining DLP templates, click [here](#).

Expressions  Occurrences:

**Template Definition**

1	<input type="text" value="A Sample Keyword"/>	<input type="button" value="Up"/>
2	<input type="text" value="A Sample Expression (1)"/> <input type="button" value="Or"/>	<input type="button" value="Down"/>

8. click **Save**. A compliance template is created

**Data Loss Prevention Templates** [Help](#)

231 - 233 of 233   24 of 24

<input type="checkbox"/>	Name	Description	Type	Policy Instances
<input type="checkbox"/>	US: UB-04 Form	A universal billing form that simplifies and standardizes...	Pre-defined	0
<input type="checkbox"/>	United Arab Emirates: International Bank Account Number	An international standard for identifying bank accounts w...	Pre-defined	0
<input type="checkbox"/>	A Sample Template		User Defined	0

231 - 233 of 233   24 of 24

Rows per page:

9. Define an DLP Policy

## Go to **Data Loss Prevention > Click Enable transport level Data Loss Prevention** to enable DLP service

**Data Loss Prevention Policies** [Help](#)

Enable transport level Data Loss Prevention

Apply policies to

Digital asset discovery in

1 - 8 of 8   1 of 1

<input type="checkbox"/>	Policy	Accounts	Action	Priority	Status
<input type="checkbox"/>	test1	Anyone	Quarantine entire message	1	<input type="button" value="X"/>
<input type="checkbox"/>	Data Loss Prevention (GLBA)	Anyone	Quarantine entire message	2	<input type="button" value="X"/>
<input type="checkbox"/>	Data Loss Prevention (HIPAA)	Anyone	Pass message part	3	<input type="button" value="X"/>
<input type="checkbox"/>	Data Loss Prevention (PCI-DSS)	Anyone	Pass message part	4	<input type="button" value="X"/>
<input type="checkbox"/>	Data Loss Prevention (SB-1386)	Anyone	Pass message part	5	<input type="button" value="X"/>
<input type="checkbox"/>	Data Loss Prevention (US PII)	Anyone	Pass message part	6	<input type="button" value="X"/>
<input type="checkbox"/>	Source Code	Anyone	Pass message part	7	<input type="button" value="X"/>
<input type="checkbox"/>	A Sample Policy	Anyone	Quarantine entire message	8	<input checked="" type="button" value="X"/>

1 - 8 of 8   1 of 1

Rows per page:

10. Go to **Data Loss Prevention > Add**. Select account type which you want to monitor

Data Loss Prevention: Add Policy Help

Policy List > New policy

Step 1: Select Accounts >>> Step 2 >>> Step 3 >>> Step 4 >>> Step 5

**Select Accounts**

From any sender to any recipient  
 From specific sender(s) to any recipient  
 From any sender to specific recipient(s)  
 From specific sender(s) to specific recipient(s)

< Back Next > Cancel

### 11. Choose the email message parts to monitor

Data Loss Prevention: Add Policy Help

Policy List > New policy

Step 1 >>> Step 2: Specify Rule >>> Step 3 >>> Step 4 >>> Step 5

**Target**

Header (  from  To  Cc )  
 Subject  
 Body  
 Attachment

**Templates**

Available DLP Template(s)  
 US: HIPAA (Health Insurance Portability and Acc...  
 US: HIPAA (HIPAA) ELDI Form  
 US: HICA (Health Insurance Claim Number)  
 US: HIEBA (Health Insurance Portability and Acc...  
 US: NPI (National Provider Identifier)  
 US: OII (Personally Identifiable Information)  
 US: Phone Number  
 US: SSN (Social Security Number)  
 US: SB (SBI)  
 US: Sarbanes-Oxley Act  
 US: U4 Form  
 United Arab Emirates: International Bank Accou...

Match any selected template

Selected DLP Template(s)

A Sample Template

Description:

Notes: Double-click a template name to edit it.

< Back Next > Cancel

### 12. Select the action when violation happens

Data Loss Prevention: Add Policy Help

Policy List > New policy

Step 1 >>> Step 2 >>> Step 3: Specify Action >>> Step 4 >>> Step 5

**Action Settings**

Replace with text/file  
 Quarantine entire message  
 Quarantine message part  
 Delete entire message  
 Backup  
 Pass message part

**AND**

Forward to sender's manager  
 Forward to specific email address(es):

Use semi-colon (;) to separate addresses

**AND**

Notify  
 Do not notify

**Advanced Options**

Quarantine and Backup Settings  
 Replacement Settings  
 Forward Email Message Settings

< Back Next > Cancel

### 13. Click Next to specify notification setting

Data Loss Prevention: Add Policy Help

Policy List > New policy

Step 1 >>> Step 2 >>> Step 3 >>> **Step 4: Specify Notification** >>> Step 5

**People to Notify**

Notify administrator Show details

Notify sender Show details

Notify recipient(s) Show details

**Advanced Notifications**

SNMP Show details

Write to Windows event log

< Back   Next >   Cancel

## 14. Click Next to specify Name and Priority setting

Data Loss Prevention: Add Policy Help

Policy List > New policy

Step 1 >>> Step 2 >>> Step 3 >>> Step 4 >>> **Step 5: Name and Priority**

**Name and Priority**

Enable this policy

Policy name\*:

Priority\*:

Review the existing policies below to determine the priority of this new policy

Policy	Accounts	Action	Priority	Status
test1	Anyone	Quarantine entire message	1	
Data Loss Prevention (GLBA)	Anyone	Quarantine entire message	2	
Data Loss Prevention (HIPAA)	Anyone	Pass message part	3	
Data Loss Prevention (PCI-DSS)	Anyone	Pass message part	4	
Data Loss Prevention (SB-1386)	Anyone	Pass message part	5	
Data Loss Prevention (US PII)	Anyone	Pass message part	6	
Source Code	Anyone	Pass message part	7	

< Back   Finish   Cancel

### Reference:

- The quarantine file is created when a violation happens under quarantine folder.

Local Disk (C:) > Program Files > Trend Micro > Smex > storage > quarantine

elp

ry > Share with > New folder

Name ^	Date modified	Type	Size
Advanced threats	1/6/2016 2:18 PM	File folder	
AD001_57e21aa33_DLP.xlsx_	9/21/2016 1:29 PM	XLSX_File	9 KB
AD001_57e21aa44.eml	9/21/2016 1:29 PM	EML File	24 KB
AD001_57e21abf5_DLP.xlsx_	9/21/2016 1:29 PM	XLSX_File	9 KB

- SMEX send notification to users or the administrator when a DLP violation happens

**[MailServer Notification]Data Loss Prevention Notification**

Administrator <administrator@do.not.reply>

📧 Extra line breaks in this message were removed.

Sent: Mon 10/10/2016 3:43 PM

To: corpad001@corpad.com

Digital assets found in the attached email message triggered a Data Loss Prevention policy incident. This email message triggered the A Sample Policy policy, and the Quarantine entire message action was performed on 10/10/2016 3:42:52 PM.

Message details:

Server: AD001

Found in: SMTP

Sender: [corpad001@corpad.com](mailto:corpad001@corpad.com);

Recipient: [corpad001@corpad.com](mailto:corpad001@corpad.com);

Subject: Trend Micro

Tip ✓

1. If multiple policies are defined for a user, all policies will take effect according to the priority.
2. The smaller the policy number is, the higher the priority is. We can change the policy priority by editing the priority number.
3. For email message detection, all the header, subject, body, and attachments are regarded as an entire part to match a template only when set Digital assert discovery in “Multiple message parts”.
4. Short length keyword terms like “anal” might cause violation when match to word “analysis” which is not adult sensitive word.

## 4.1.5 Optimizing Web Reputation

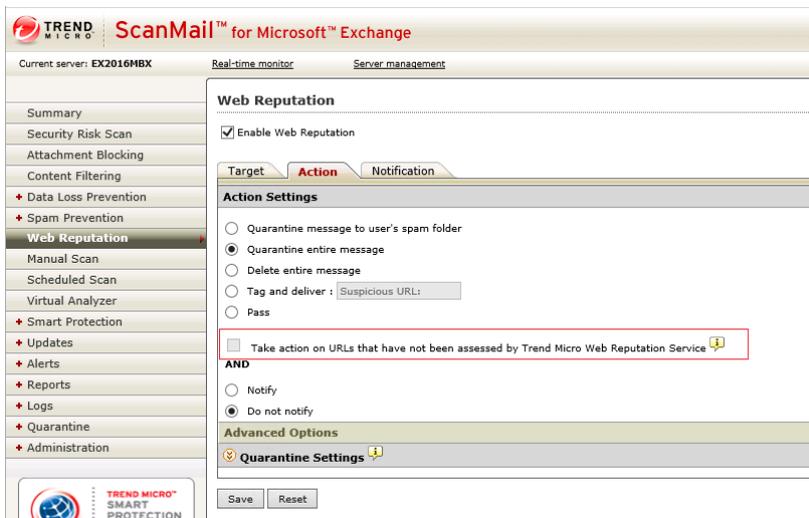
You can optimize the performance of the web reputation scanning by configuring your settings in several different ways. Consider implementing the following web reputation

settings to optimize network and scanning performance:

- Add your company's internal URL to the "Approved URL List". This will allow ScanMail to bypass messages containing internal URLs, which will reduce network bandwidth usage and improve performance.
- Use a Smart Protection Server to reduce network bandwidth usage. Web reputation services sends URL queries to the external Smart Protection Network or to the local Smart Protection Server. Networks can suffer a performance impact with a slow Internet connection when querying the Smart Protection Network. Configure a Smart Protection Server using the management console and change the web reputation source by clicking Smart Protection > Scan Service Settings.
- To optimize Smart Protection Server performance, consider a dedicated Smart Protection Server for ScanMail. If your Smart Protection Server is providing services to both ScanMail and OfficeScan, for example, server performance could suffer.
- Scanning attachments for URLs can introduce a performance impact to your system. If you are already using content filtering or Data Loss Prevention policies with attachment scanning, the URL scanning in attachments should introduce a limited impact to your system. If you are not using content filtering or Data Loss Prevention policies with attachment scanning, using the URL scanning in attachments can noticeably affect performance.

Things You Must Know:

1. "Take action on URLs that have not been assessed by Trend Micro Web Reputation Service" check box will be unchecked and grey if enable URL Analysis.



- Email message with unrated URLs which need to be sent to Virtual Analyzer will be temporarily quarantined to a local sub-folder "SuspiciousURLs" under the default advanced threat quarantine directory. The directory also can be customized on Web Reputation settings page.



## 4.2 Search & Destroy Best Practices

Take note of the following best practices when configuring the Search & Destroy feature.

- Search & Destroy Prerequisites
- Configuring Search & Destroy in a Multiple Data Center Environment
- Using Search & Destroy in Mixed Exchange Environments
- Optimizing Search Criteria
- Optimizing Mailbox Searches
- Deleting Mailbox Searches
- Exchange Management Shell Commands
- Exchange Server 2013/2016 Throttling Policy Settings

### 4.2.1 Search & Destroy Prerequisites

Before using Search & Destroy in the Exchange environment, take note of the following

prerequisite knowledge.

FEATURE	DESCRIPTION
Service account	<p>This account performs the backend searches in the Exchange environment. Only one service account is necessary for the entire organization. Configure the service account as follows:</p> <ul style="list-style-type: none"> <li>• Ensure that the account is a member of the Exchange discoverymanagement group</li> <li>• Ensure that the account never expires</li> <li>• Ensure that the account is a member of the Exchange Mailbox Import Export role to export search results to a .pst file</li> <li>• Create a mailbox for this account (Exchange Server</li> </ul>

	2013/2016 only)
Discovery mailbox	<p>This mailbox stores the search result messages. ScanMail copies messages from the end user’s mailboxes into the discovery mailbox.</p> <p>Configure the discovery mailbox(es) as follows:</p> <ul style="list-style-type: none"> <li>• Ensure that the discovery management group has full access permission to each discovery mailbox</li> <li>• Assign at least one discovery mailbox to each data center in the organization</li> </ul> <p>Note</p> <p>Trend Micro recommends that administrators do not place the discovery mailbox in Data Availability Groups (DAG) solutions.</p> <p>The discovery mailbox consumes more database space when used in a DAG solution.</p>
Exchange Server 2013/2016 Throttling Policy	<p>Exchange Server 2013/2016 utilizes a throttling policy to limit the number of concurrent mailbox searches and the number of specified mailboxes each search can search.</p> <p>Administrators must reconfigure the throttling policy to optimize Search &amp; Destroy mailbox searches.</p>

## 4.2.2 Using Search & Destroy in Mixed Exchange Environments

The Search & Destroy feature can only search and take action on mailboxes in Exchange environments that are the same version as the Exchange environment associated with the ScanMail installation. For administrators with multiple ScanMail servers that manage multiple Exchange versions, Search & Destroy tasks must be run separately on each ScanMail server.

For example:

A ScanMail server installed in an Exchange 2010 environment cannot perform Search & Destroy tasks on an Exchange 2013 database. To search both Exchange 2010 and Exchange 2013 databases, administrators must perform a Search & Destroy search task from the ScanMail server installed on Exchange 2010 and then run a separate Search & Destroy task from the ScanMail server installed on Exchange 2013.

**NOTE** 

ScanMail can perform Search & Destroy tasks on multiple Exchange servers if the Exchange Server versions are the same as the Exchange Server version the ScanMail server is associated with.

### 4.2.3 Preparing Exchange Server 2013/2016 for Mixed Exchange Environment

Exchange Server 2013/2016 requires that the SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} mailbox exists on the Exchange server before starting a search in a mixed Exchange environment. If the mailbox does not exist on Exchange Server 2013/2016, configure the mailbox using Exchange Management Shell Commands.

Procedures:

1. Execute the command: `Get-Mailbox -Arbitration` retrieves the current system mailbox information.
2. Execute the command: `Get-Mailbox -Arbitration "SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}" | New-MoveRequest -Targetdatabase "Exchange2013/2016 DB Name"` Moves the SystemMailbox{e0dc1c29-89c3-

4034-b678-e6c29d823ed9} mailbox to the Exchange Server 2013/2016 mailbox database.

3. Execute the command: Get-MoveRequest Checks the status of the move operation.

## **4.2.4 Configuring Search & Destroy in a Multiple Data Center Environment**

1. Select a dedicated Exchange mailbox server to perform all Search & Destroy tasks across all data centers.
2. Configure a Search & Destroy administrator using the ScanMail management console.
3. Prepare one service account to manage all Search & Destroy tasks.
4. Prepare a separate discovery mailbox for each data center in the organization.
5. Activate Search & Destroy and assign the most used discovery mailbox as the default mailbox.
6. For each data center, create a search task and only search mailboxes that reside in a single data center.
7. For each search task, select a discovery mailbox that resides at the same level as the target mailboxes.

## **4.2.5 Optimizing Search Criteria**

When performing mailbox searches, attempt to narrow the search scope by defining the following search criteria.

- Search in message subject, body, or attachment:
  - For Exchange Server 2010, administrators can use AQS to search for text that only resides in specific message parts. The following examples display some simple AQS search strings:
    - Example 1: To search for messages containing the word “test” in the message subject, type `subject:test`.
    - Example 2: To search for messages containing the attachment “test.xlsx”, type `attachment:test.xlsx`.

**NOTE** 

For details on AQS, see <http://msdn.microsoft.com/en-us/library/bb266512.aspx>.

- For Exchange Server 2013/2016, administrators can use KQL to search for text that only resides in specific message parts. The following examples display some simple KQL search strings:
  - Example 1: To search for messages containing the word “test” in the message subject, type `Subject:test`.
  - Example 2: To search for messages containing the attachment “test.xlsx”, type `attachment:test.xlsx`.

**NOTE** 

For details on KQL, see <http://msdn.microsoft.com/en-us/library/ee558911.aspx>.

- Search for users in specific mailbox servers:

ScanMail does not provide a direct way to search specific mailbox servers. Administrators can, however, create a distribution group that contains all users on a specific mailbox server and then perform a search on that distribution group.

## 4.2.6 Optimizing Mailbox Searches

During a mailbox search, the service account copies messages from the end user mailbox to the Exchange discovery mailbox and then parses the search results to the ScanMail database. This is a time-consuming and resource-intensive task. Trend Micro recommends performing an estimate of the search results before performing the actual search.

Performing an estimate of the search results does not require the service account to copy any messages and has a limited impact on the Exchange server. After performing an estimate, administrators can optimize the search criteria before performing the actual search.

If administrators think a mailbox search may affect the performance of the Exchange server, Trend Micro recommends scheduling the search to run at off-peak hours using the Search Later function.

## 4.2.7 Deleting Mailbox Searches

- To delete search result messages from end users' mailboxes without deleting the search criteria:  
Go to the search results screen and manually select the messages to delete from end users' mailboxes. This also deletes the selected search results stored in the Exchange server discovery mailbox and the ScanMail database.

### NOTE

Administrators can use the Exchange management shell commands to manually delete Exchange search tasks.

- When using the Delete task only function:  
ScanMail only deletes the search criteria, task name, and search results from the ScanMail database. The Exchange search task still exists along

with all search results stored in the discovery mailbox ScanMail does not delete any messages in the end users' mailboxes

**NOTE**

Use Delete task only to retain the search results for archival purposes.

## 4.2.8 Exchange Management Shell Commands

Administrators can use Exchange Management Shell Commands to perform a variety of tasks on the Exchange server. Trend Micro recommends noting the following prerequisite and useful tasks:

- Service Account Settings on page
- Discovery Mailbox Settings on page
- Exchange Server 2013/2016 Throttling Policy Settings on page
- Backend Search Tasks on page

### Service Account Settings

An Exchange service account is necessary to perform the backend searches in the Exchange environment. Administrators can use the following Exchange Management Shell Commands to configure the service account:

Command	Description
<code>Add-RoleGroupMember -Identity "Discovery Management" -Member "SERVICE_ACCOUNT_NAME"</code>	Adds the "SERVICE_ACCOUNT_NAME" account to the Exchange Discovery Management group
<code>New-ManagementRoleAssignment -Role "mailbox import export" -User "SERVICE_ACCOUNT_NAME"</code>	Adds the "SERVICE_ACCOUNT_NAME" account to the Exchange Mailbox Import Export role

## Discovery Mailbox Settings

An Exchange discovery mailbox is necessary to store the mailbox search result messages. Administrators can use the following Exchange Management Shell Commands to configure the discovery mailbox:

Command	Description
<code>Get-Mailbox -Filter {RecipientTypeDetails -eq "DiscoveryMailbox"}</code>	Returns all discovery mailboxes that exist on the Exchange server
<code>New-Mailbox "NEW_DISCOVERY_MAILBOX_NAME" -Discovery -database "MAILBOX_DATABASE_NAME"</code>	Creates a new discovery mailbox named "NEW_DISCOVERY_MAILBOX_NAME" in the database named "MAILBOX_DATABASE_NAME"
<code>Add-MailboxPermission -Identity "DISCOVERY_MAILBOX_NAME" -user "Discovery Management" -AccessRights FullAccess</code>	Assigns the Exchange Discovery Management group full access permission to the "DISCOVERY_MAILBOX_NAME"

## Exchange Server 2013/2016 Throttling Policy Settings

Exchange Server 2013/2016 utilizes a throttling policy to limit the number of concurrent mailbox searches and the number of specified mailboxes each search can search. By default, Exchange Server 2013/2016 only allows 2 mailbox searches to run concurrently with a maximum of 50 specified mailboxes per search.

To optimize the Search & Destroy feature, Trend Micro recommends using Exchange

Management Shell Commands to configure the following Exchange Server 2013/2016

### Settings

Command	Description
<code>Get-ThrottlingPolicy  fl *discovery*</code>	Returns the current policy settings

<pre>New-ThrottlingPolicy -Name [<i>policy_name</i>] - DiscoveryMaxConcurrency 10 - DiscoveryMaxMailboxes 500 - ThrottlingPolicyScope organization</pre>	<p>This command creates the new policy “[<i>policy_name</i>]” and sets the following:</p> <ul style="list-style-type: none"> <li>• Maximum number of concurrent searches: 10</li> <li>• Maximum number of specified mailboxes per search: 500</li> </ul>
--	--

### Backend Search Tasks

When administrators create a mailbox search, ScanMail creates an Exchange search task to perform the backend search. This Exchange search task name implements the following format:

[*task\_name*][*server\_name*][*time\_stamp*]

For example, for the mailbox search “task1” performed on “serverA” at 4:30 am on September 12, 2012, the Exchange search task name is:

task1serverA20120912043000

Administrators can use the following shell commands to perform actions on the backend search tasks:

Exchange Version	Command	Description
Exchange Server 2010	Get-mailboxSearch-identity [ <i>task_name</i> ][ <i>server_name</i> ]*	Returns the full search task name and the task status
Exchange Server 2013/2016	get-mailboxsearch  fl name	Returns the full search task name
	get-mailboxsearch -identity [ <i>task_name</i> ]  fl	Returns the task status
Exchange Server 2010/2013/2016	remove-mailboxSearch-identity [ <i>task_name</i> ]	Removes the mailbox search from the Exchange server and all associated search results from the discovery mailbox



# Chapter 5

## Central Management

### 5.1 ScanMail Server Management

The ScanMail Server Management console allows you to view all of the ScanMail servers on a network. You will only see server with the same type of Activation Code. View all ScanMail servers in a forest when you install ScanMail with Exchange 2016, 2013 or 2010.

Tip ✓ Additional details on Server Management are located in the ScanMail 12 Administrator's Guide, Chapter 4 Managing ScanMail.

To manage other SMEX Servers, it is a requirement for a SMEX Server to have a valid AC (Activation Code). It follows the following behavior outline below:

- If the local server has no AC, Server Management only shows the local server (it displays itself on the list)
- Server Management only displays SMEX Servers with the same AC type (a SMEX server with Suite license can only manage servers with Suite licenses as well)
- Server Management is not supported for Edge Transport Servers. Consequently, it is not listed in the Server Management page.

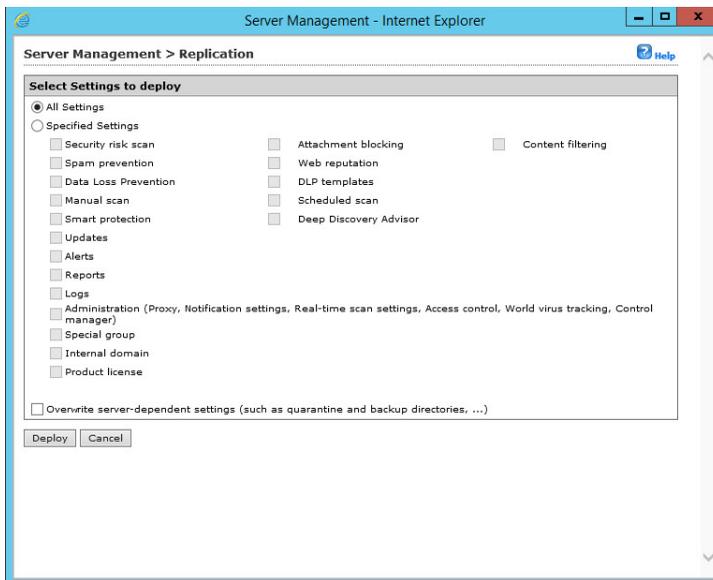
## 5.1.1 Replicate Settings to Remote Servers

You can use Server Management to replicate any or all of your configurations from one ScanMail server to another. Replicating servers in this way is much faster and easier than configuring each server separately. In addition, it ensures that all ScanMail servers that provide the same kind of protection share the same configuration.

- SMEX Management Console → Server Management



- Select the target SMEX servers, then click “Replicate”



## 5.1.2 Central Log Query via SMEX Management Console

On one single SMEX management console, you can query logs from multiple SMEX servers by selecting the query target(s) as Remote server(s).

- SMEX Management Console → logs → Query

**Log Query**

**Criteria**

Dates: 12/4/2016 12 05 to 12/5/2016 12 05  
MM/dd/yyyy hh mm MM/dd/yyyy hh mm

Type: Security Risk Scan | All

Found in:

Sender:

Recipient:

Subject:

Attachment:

Sort by: Scan Time  Ascending  Descending

Display: 15 per page

Query target(s):  Local server [ENW2012R2]  Remote server(s)

Server Group: All servers  
Mailbox servers  
Transport servers

Available Servers: ENW2012R2

Selected Server(s)

Add >>  
Add All >>  
<< Remove  
<< Remove All

## 5.1.3 Central Quarantine Query via SMEX Management Console

On one single SMEX server management console, you can query quarantine logs from multiple SMEX servers by selecting the query target(s) as Remote server(s)

## SMEX Management Console → Quarantine → Query

### Quarantine Query

**Criteria**

Dates:    to

Reasons:  All reasons  
 Specified reasons  
 Security risk scan  Attachment blocking  Content filtering  Data Loss Prevention  
 Unscannable message parts  Web Reputation

Resend Status:  Never been resent  
 Resent at least once  
 Any status

Sender:

Recipient:

Subject:

Sort by:   Ascending  Descending

Display:  per page

Query target(s):  Local server [ENW2012R2]  
 Remote server(s)

Server Group:

Selected Server(s):

Tip ✓ You can resend the quarantined message even it is quarantined on a remote server.

## 5.1.4 Single Sign On

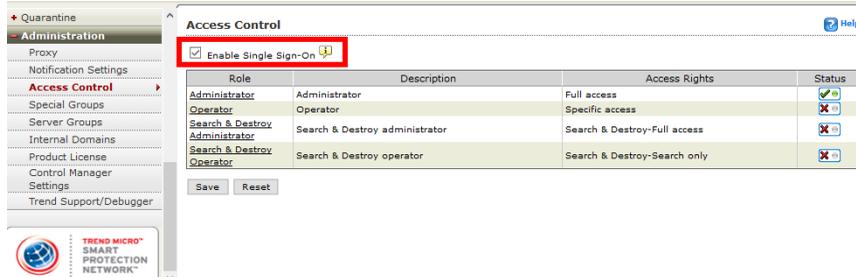
SSO (Single Sign On) is a feature introduced in SMEX 10.0 and continued in the later versions of SMEX. This allows a user to access the management console without the need to provide their logon credentials (username and password). The basic premise of SSO is that

it uses the logon credentials of the account currently logged on to the machine where SMEX management console is being accessed.

Tip ✓ SSO only supports Microsoft Internet Explorer. Since it is also dependent to Active Directory, support for Edge Transport Server Is not available

SMEX implementation of SSO relies on the IIS (Internet Information Server) SSO mechanism. The kind of configuration used is Integrated Windows Authentication using Kerberos. Under this setting, as long as a user has logged on to a local computer as a domain user, no authentication will be required when accessing another computer in the same domain. Consequently, IE and IIS will be able to automatically negotiate and perform authentication without any interaction with SMEX.

To enable SSO for a specific user with Administrator role, click the checkbox located under the Access Control page.



The screenshot shows the 'Access Control' page in the SMEX Administration console. The 'Enable Single Sign-On' checkbox is checked and highlighted with a red box. Below it is a table listing roles and their access rights.

Role	Description	Access Rights	Status
Administrator	Administrator	Full access	
Operator	Operator	Specific access	
Search & Destroy Administrator	Search & Destroy administrator	Search & Destroy-Full access	
Search & Destroy Operator	Search & Destroy operator	Search & Destroy-Search only	

Buttons: Save, Reset

The result is an additional button in the login page “Log on with domain credentials”.



The screenshot shows the login page for ScanMail for Microsoft Exchange. At the top left is the Trend Micro logo. To its right, the text "ScanMail™ for Microsoft™ Exchange" is displayed in a large, bold, red font. Below this is a "LOGIN" section with a light gray background. It contains the instruction "Please type your User name and Password to access the product console." followed by two input fields: "User name:" and "Password:". To the right of the password field is a "Log On" button. Below these fields is a button labeled "Log on with domain credentials" with a small yellow information icon to its right. At the bottom of the login area, a copyright notice reads: "© Copyright 1998-2013 Trend Micro Incorporated. All rights reserved."

When enabled, both Administrator and Operator accounts can login to the management console without the need to input their credentials and wait for verification.

**NOTE** ⓘ for information regarding Kerberos, refer to its website which is <http://web.mit.edu/Kerberos/>

## 5.2 MOM/SCOM Integration

Microsoft SCOM (Systems Center Operations Manager) is a third-party application that uses a client-server model to provide centralized monitoring of application installed on a remote system. This product is mainly used in enterprise environments to enable IT administrators to manage end to end service management of their Microsoft platforms and applications.

**NOTE** ⓘ MOM or Microsoft Operations Manager is the previous name of SCOM. Starting in version 2007, Microsoft changed its name to SCOM. In this Support Track, both terms are interchangeable

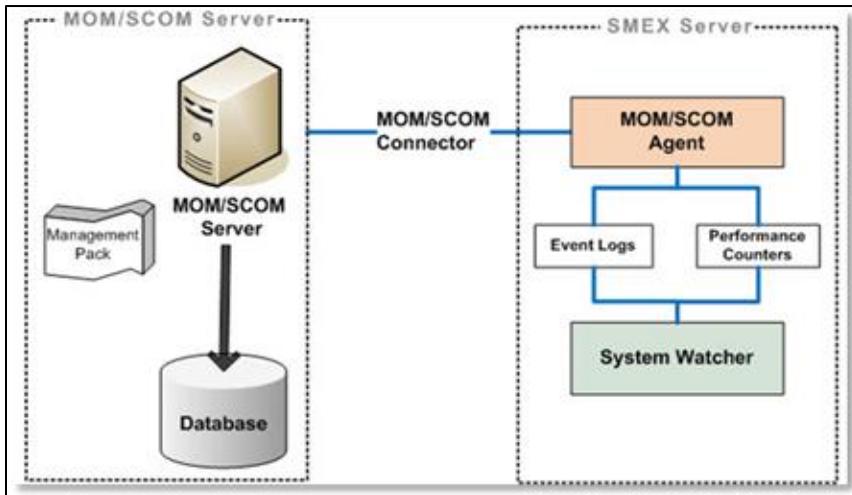
To establish communication between SCOM server and the client machine, the agent needs to be installed on the latter. This particular agent monitors various data sources on the client (typical examples are performance counters and Windows Event Log) for selected events or alerts generated by monitored applications. Information about these specific events and alerts are sent to the server.

The MOM/SCOM has an interface where these events and alerts are viewed. Specific actions such as sending an email notification, generating a support ticket or monitoring a package update can be done depending on the nature of the event or alert. Aside from monitoring applications, MOM/SCOM can generate reports based on data acquired from remote systems.

ScanMail for Exchange leverages this monitoring and reporting capability by supporting the following MOM/SCOM versions:

- SCOM 2007 SP1
- SCOM 2007 R2
- SCOM 2012
- SCOM 2012 SP1

To illustrate how SMEX integrates with MOM/SCOM, refer to the following figure:



To explain the diagram above, SMEX uses the Systems Watcher libraries (InSWServiceMonitor.dll and InSWOutbreakAnalysis.dll) to write supported alerts and performance counters to event logs and performance counters. The MOM/SCOM agent in return, collects these data.

**NOTE**  for reference regarding both event logs and performance counters, check the following resources:

- Event Viewer
- Performance Counters

To establish connection, do the following steps:

1. On the MOM/SCOM server, run the installation program for SMEX MP (Management Pack). This is the Trend Micro ScanMail for Microsoft Exchange Management Pack.msi which

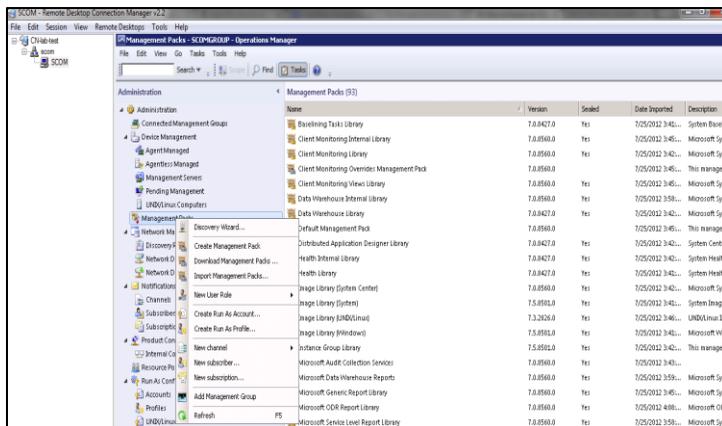
is included in the SMEX setup package and located under the Management Pack folder.

2. This extracts the available MPs for SMEX to the folder %ProgramFiles%\System Center Management Packs\Trend Micro ScanMail for Microsoft Exchange MP:

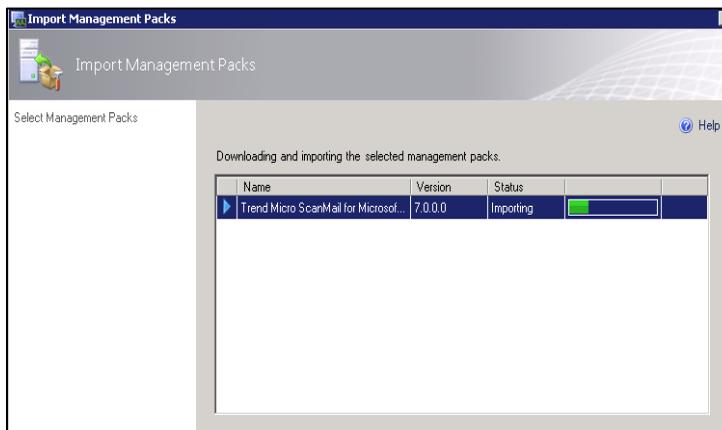
MOM/SCOM version	Description
System Center Operations Manager (SCOM) 2007 SP1	Trend.Micro.ScanMail.for.Microsoft.Exchange.xml
System Center Operations Manager (SCOM) 2007 R2	
System Center Operations Manager (SCOM) 2012	
System Center Operations Manager (SCOM) 2012 SP1	

**NOTE**  Management packs define filtering rules specific to a monitored application. It determines what data are acquired from the monitored application and stored in the MOM/SCOM database.

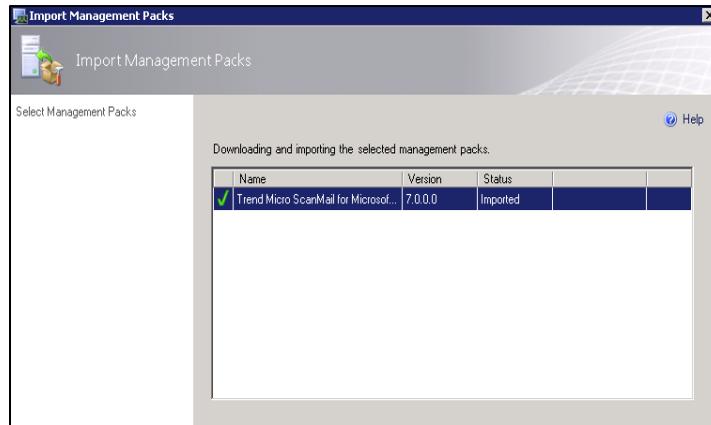
3. Import the management pack to the MOM/SCOM Server. The following are the steps to import it on a SCOM 2012 Server:
  - Launch the SCOM Server: Click Start > Programs > Microsoft System Center 2012 > Operation Manager > Operation Console
  - In the Operations console, click Administration, right click Management Packs > Import Management Packs



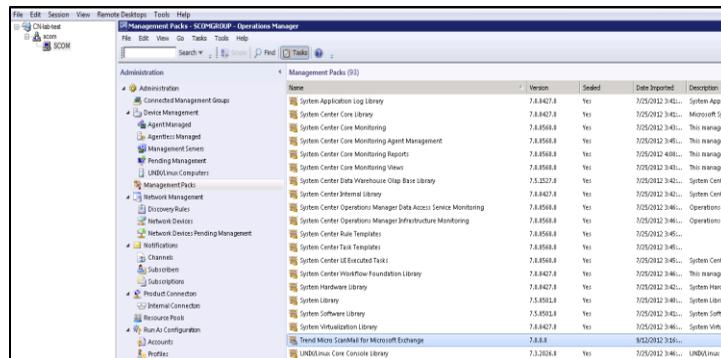
- Click Add > Add from Disk > Add Trend.Micro.ScanMail.for.Microsoft.Exchange > Click Open. This will update the Import List with the Name: Trend Micro ScanMail for Microsoft Exchange with the Version Column of 7.0.0.0. Click Install Button



- Once Management Pack importation completed, Click Close.



- To verify if the Trend Micro ScanMail for Exchange Management Pack, browse in the Management Packs Pane located under Administration > Management Packs.



4. Install the corresponding MOM/SCOM agent on the machine where SMEX is installed.

**NOTE** Management pack upgrade is also required when SMEX is upgraded to the latest version

## 5.3 Control Manager Integration

TMCM or Trend Micro Control Manger is a software management and reporting solution which controls Trend Micro antivirus and security programs from a central location. It provides an integrated and simplified administration interface for the following operations:

- Product configuration and status monitoring
- On-demand product control
- Component update and deployment
- Report generation

Tip ✓ Additional details on Trend Micro Control Manager are located in the ScanMail 12 Administrator's Guide, Appendix A: Introducing Trend Micro Control Manager.

Steps to register SMEX to TMCM:

1. Open SMEX Management Console .Negative to Administration→Control Manager Settings



2. On the left panel, check the option: Enable communication between the ScanMail MCP agent and Control Manager.

#### Control Manager Settings

Configure the settings for communication between the ScanMail MCP agent and the Control Manager server.

- Enable communication between the ScanMail MCP agent and Control Manager.

3. Fill the TCMC server IP and Port (e.g. 80 or 443):

**Connection Settings**

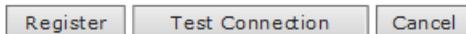
Entity display name\*: AD001\_SMEX

**Control Manager Server Settings**

Server FQDN or IP address\*: 192.168.54.154

Port\*: 443  Connect using HTTPS

4. Click "Register" at the bottom of the page.



## 5.3.1 Replicate SMEX Configuration via TCM Console

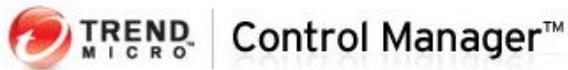
The integration with Control Manager Server allows the Administrator to access SMEX management console (using SSO) and configure replication using the TCM console.

Steps to replicate SMEX settings via TCM console.

- Directories → Products → Select one SMEX server as source server (that you want to replicate the settings from) → Click on **Configure**, and select **Configuration Replication**



- Select the target SMEX servers in Step 2 → Click **Replicate**



## Configuration Settings

Step 1 >>> **Step 2: Select Target Machines**

### Source Machine

Source:ENW2012R2\_8MEX

### Target Machines

Target(s):



< Previous

Replicate

Cancel

- Click **OK** to process settings replication



Tip ✓ Unlike ScanMail Server Management Console, TMCM will NOT replicate below items settings:

- Activation Code
- Backup and Quarantine Settings (folder locations)
- Database selection in Manual or Scheduled Scan
- Scan status in Manual or Scheduled Scan
- Spam Maintenance Information
- Last maintenance time for logs and quarantine manager
- Trend Support/Debugger settings
- All information in the Summary page
- Special policies with specific sender or recipient added from Active Directory

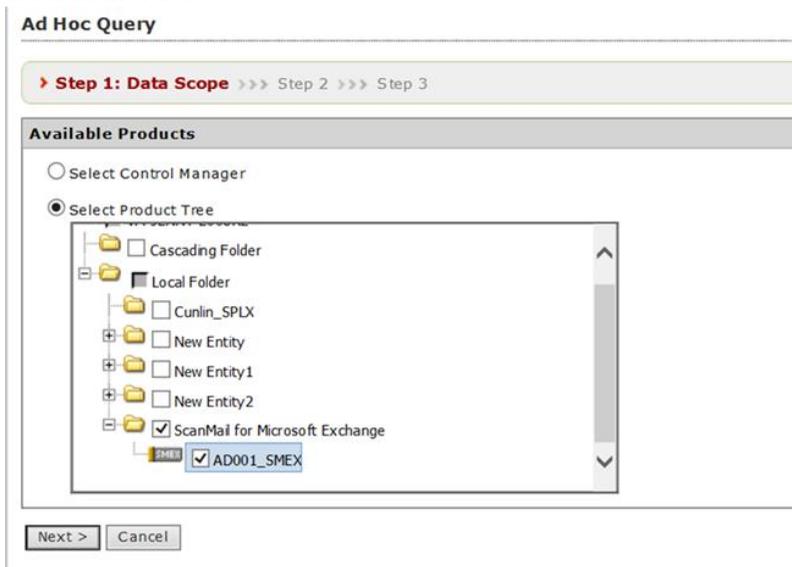
### 5.3.2 Central Log Query via TMCM Console

By default, when you register a ScanMail for Exchange server to Control Manager, the logs will be sent to the Control Manager. In the latest build SMEXX 12.0 SP1 (build 1350) – there is a capability to also send the spam logs to the control Manager. This will have the benefit of collecting logs for Health across all servers in one place and allowing a single search for investigation in single database rather than searching

across a number of servers for a particular event or action taken on an email message.

Steps to query SMEX logs from TCMC console:

1. Login TCMC console : Logs→New Ad Hoc Query.
2. Select Product Tree, and choose ScanMail server(s) in the product tree. Click Next.



3. Select the required log type under Available Data Views, and click Next.

## Ad Hoc Query

Step 1 >>> **Step 2: Data View** >>> Step 3

**Available Data Views**

Select the data view:

- Product Information
  - Managed Product Information
  - Component Information
- Security Threat Information
  - Virus/Malware Information
    - Overall Virus/Malware Summary
    - Virus/Malware Source Summary
    - Virus/Malware Endpoint Summary
    - Virus/Malware Detection Over Time Summary
  - Summary Information
- Date/Time

< Back   Next >   Cancel

- On Criteria Settings section, define the time range:

**Ad Hoc Query**

Step 1 >>> Step 2 >>> **Step 3: Query Criteria**

**Result Display Settings**

Selected View: Overall Virus/Malware Summary   Change column display

**Criteria Settings**

**Required criteria**

Date/Time   is between   %last7days%   and   %now%

**Custom criteria**

Match: All of the criteria

Note: Columns marked with asterisk (\*) can be selected to filter data only once.

\* Product   is equal to   ScanMail for Microsoft Exchange

**Save Query Settings**

Save this query to the saved Ad Hoc Queries list.

Query Name: Overall Virus/Malware Summary\_2016\_11

< Back   Query   Cancel

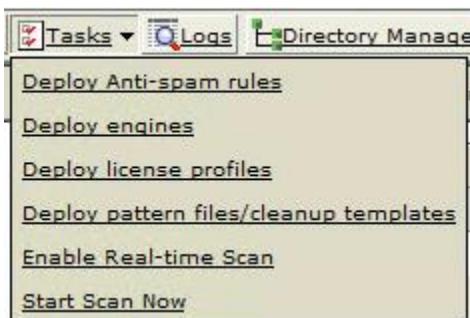
- Click Query → then the query results window will appear:



### 5.3.3 Central Deployment and Scanning

Once ScanMail is registered to TCMC, then administrator can deploy the following scan components to its target entity (SMEX server) through the SMEX CMAgent.

On TCMC console, administrator can perform deploy task.



- Anti-spam rules
- Engines
- License Profiles
- Pattern files/cleanup templates

For scanning, TCMC triggers two operations which are:

- Enable Real-Time Scan
- Start Scan Now

**NOTE** 

SMEX AU download source will be automatically changed to TCMC server temporarily if any AU deploy command distributed from TCMC.

There's no need to manual configure the Download Source to TCMC from SMEX management console.

Additionally, once ScanMail is registered to TMCM, the TMCM server can be configured as an alternative update source for ScanMail servers, this would be a solution for customer has strict network access policy that only allow some specific servers to have internet access.

1. Open SMEX Management Console .Negative to Administration→Updates.



2. Go to Download Source page.
3. Select “Other update source” and fill in the TMCM server info:

### Download Source

**Source**

Trend Micro ActiveUpdate server

Intranet location containing a copy of the current file

UNC path:   
IPv4 example: \\fileserver\pattern\_folder  
IPv6 example: \\fe80--1.ipv6-literal.net\pattern\_folder\

User name:   
For example: domain\user name

Password:

Other update source

IPv4 example: http://fileserver:port\_number/pattern\_folder/  
IPv6 example: http://[fe80::1]:port\_number/pattern\_folder/

Allow other servers to download updates from this server

4. Click “Save”

## 5.3.4 License Management

Starting in TMCM 5.0, Control Manager introduces the feature of storing multiple Activation Codes. This enables TMCM to deploy new or updated Activation Codes to the products it manages.

License Management feature is used in the following instances:

- When a new Activation Code is entered in the TMCM console, the Administrator can decide to automatically deploy the new AC with the license profile to the target SMEX Server.
- A renewed Activation Code (whose expiration date had been extended) together with its license profile can be deployed either manually or automatically:
  - Manual redeployment can be initiated by the Administrator from the TMCM management console to the SMEX Server.
  - A license profile update takes place every 12:00 AM with the TMCM Server connecting to the Product Registration Server to renew its Activation Code that expired. If the licensed is renewed, TMCM automatically deploys the updated profile to the relevant product.

Administration → License Management → Managed Product

The screenshot shows the Trend Micro Control Manager Administration console. The top navigation bar includes: Dashboard, Directories, Policies, Logs, Reports, Updates, and Administration. The Administration menu is expanded, showing options: Account Management, Managed Servers, Command Tracking, Event Center, License Management, Settings, Suspicious Objects, Indicators of Compromise, and Tools. The License Management menu item is highlighted with a red box, and its sub-menu is also visible, showing Control Manager and Managed Product, with Managed Product also highlighted by a red box. Below the navigation bar, the License Management section is active, displaying a table with columns for Activation Code, Note, Products, and Status. The table contains one row with a redacted activation code and a status of 'Active'. Action buttons for 'Add and Deploy', 'Re-Deploy', and 'Delete' are visible above and below the table.

# Chapter 6

## Virtual Analyzer Integration

SMEX 12 has the ability to integrate with DDAn or Deep Discovery Appliance which is a sandbox hypervisor that provides analysis to exploits and heuristic files identified as APTs (Advanced Persistent Threats).

### 6.1 Register to DDAn

Follow below steps to register to DDAn

1. Go to SMEX management console → Click Security Risk Scan → On Target tab, check “ Enable Advanced Threat Scan Engine”.



2. Go to SMEX management console → Virtual Analyzer.  
Fulfill these info: IP address, Port and API Key of the DDAn server  
Click **Register**

Note: Select “Use a proxy server to connect to Virtual Analyzer” if the DDAn is reachable only through proxy.

**Virtual Analyzer**

Submit email messages to Virtual Analyzer ⓘ

**Virtual Analyzer Settings**

**Virtual Analyzer Mode**

Select a working mode for virtual analyzer: ⓘ

Inline mode

Monitor mode

**Virtual Analyzer Sever Settings**

IP address\*:

Port\*:

API key\*:

Use a proxy server to connect to Virtual Analyzer ⓘ

**NOTE** ⓘ

API key is available on the Deep Discovery Analyzer management console, in **Help** → **About**.

Click **Register** to complete registering to Vritual Analyzer.

**Connecting to Virtual Analyzer**

**This step is registering to Virtual Analyzer. Registration takes a few minutes.**

- ✓ Verifying Virtual Analyzer connection
- ✓ Registering to the Virtual Analyzer



Start time: 12/12/2016 2:20:17 PM  
 Elapsed time: 3 sec

## 6.2 Recommend Settings

### 6.2.1 Virtual Analyzer Mode

In SMEX 12 SP1, SMEX supports 2 modes: Inline mode and Monitor Mode.

**Virtual Analyzer**

Submit email messages to Virtual Analyzer ⓘ

---

**Virtual Analyzer Settings**

**Virtual Analyzer Mode**

Select a working mode for virtual analyzer: ⓘ

Inline mode  
 Monitor mode

**Virtual Analyzer Sever Settings**

IP address\*: 10.204.166.  
 Port\*: 543  
 API key\*: 5EFBB869-D51A-46A1-8434-1AB85A6

Use a proxy server to connect to Virtual Analyzer ⓘ

UnRegister Test Connection

**Virtual Analyzer Working Modes**

Inline mode: Email will be quarantined temporarily when submitting files or unrated URLs to Virtual Analyzer server for further analysis.  
 Monitor mode: Email will not be temporarily quarantined and only the suspicious files or unrated URLs will be submitted to Virtual Analyzer server for further analysis.

- **Inline Mode:** It will intercept email message flow, the email message will be temporarily quarantined and attachment file or unrated URLs will be send to DDAn server for further analysis, then SMEX will take action set in VS/WTP filter base on the DDAn result and security level setting in Virtual Analyzer page.
- **Monitor Mode:** It will not intercept email message flow and user will receive email message immediately. And Administrator can judge the system stability and observe messages health status in this model. Additionally, this mode is better used in POC stage, virtual analyzer pressure testing and settings modification can be done in this mode without impact the messaging environment before switching to inline mode.

## 6.2.2 Recommended Attachment Types:

In a production environment, only “Highly recommendable file types” is recommended. None of the “Specified file types” is recommended. By the default selection, SMEX will trust ATSE first. If ATSE take it as suspicious, then it’s necessary to send to DDAn for further analysis.

**Attachment Types**

Analyze messages with the following attachment types:

- Highly recommendable file types 
- Suspicious files detected by Advanced Threat Scan Engine (ATSE)
- Microsoft Office files with macros
- Scripts (such as JavaScript and others)
- Microsoft Windows executable files (.exe)
- Specific file types 

In Monitor mode, administrator can select **Specific file types** that necessary send to DDAn for further analysis.

Please pay attention that the “Highly recommendable file types” is selected by default.

### Attachment Types

Analyze messages with the following attachment types:

- Highly recommendable file types 
  - Suspicious files detected by Advanced Threat Scan Engine (ATSE)
  - Microsoft Office files with macros
  - Scripts (such as JavaScript and others)
  - Microsoft Windows executable files (.exe)

- Specific file types 
  - Applications and executable files 
  - Documents 
  - Images 
  - Videos 
  - Sounds 
  - Compressed files 
  - Specify file extensions (use ; to separate entries):

<input type="text"/>	Add
<input type="text"/>	Delete

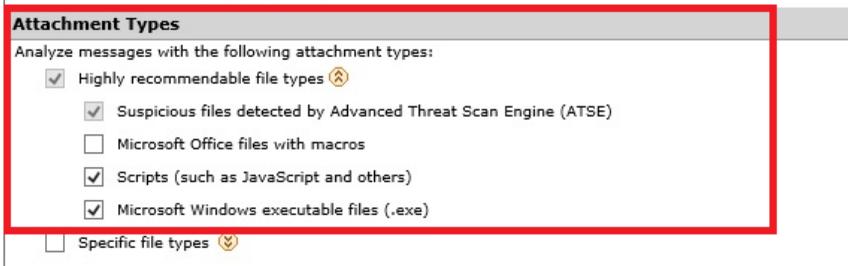
Tip ✓

**Never check the complete “Documents” or “Images” categories as this will bypass heuristic analysis and will submit all these files into sandbox with potential **massive overload of Virtual Analyzer****

Things You Must Know:

When upgrade from SMEX 12.0 with Virtual Analyzer integrated and hidden key

HEUR\_HAS\_MACRO enabled, then “Microsoft office files with macros” will be checked as default under Attachment Types



## 6.3 Verify Submission

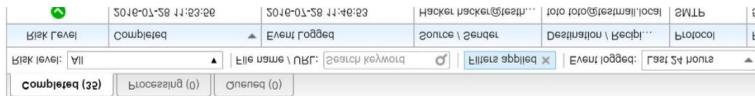
To test Virtual Analyzer submission, you can create non-dangerous file that will match submission criteria which is allowed by the antispam gateway

Example with VBS file:

1. Create file  
Filename: test.vbs  
Content: WScript.Echo "test"
2. Send it to a test Exchange Mailbox from outside mailbox
3. Verify submission on SMEX log: LogQuery-Type:VA Submission



4. Verify submission on DDAn console: Virtual Analyzer -> Submissions



# Chapter 7

## Recommend SMEX Configurations

### 7.1 Best Practice Configuration and Prevention for Spam

SMEX provides 2 main features to prevent Spam: Email Reputation and Content Scanning . Phishing detection and new spam sources detection are available options you can enable within Content Scanning.

#### 7.1.1 Email Reputation Service

Email reputation blocks IP addresses of known spam senders that Trend Micro maintains in a central database. There are two possible service levels:

- Standard is a DNS single-query-based service. Your designated email server makes a DNS query to the standard reputation database server whenever an incoming email message is received from an unknown host. If the host is listed in the standard reputation database, Email reputation reports that email message as spam.
- Advanced is a dynamic, real-time antispam solution. To provide this service, Trend Micro continuously monitors network and traffic patterns and immediately updates the dynamic reputation database as new spam sources emerge, often within minutes of the first sign of spam. As evidence of spam activity

ceases, the dynamic reputation database is updated accordingly.

Like Email reputation: Standard, Email reputation: Advanced is a DNS query-based service, but two queries can be made to two different databases - the standard reputation database and the dynamic reputation database (a database updated dynamically in real time). These two databases have distinct entries (no overlapping IP addresses), allowing Trend Micro to maintain a very efficient and effective database that can quickly respond to highly dynamic sources of spam. Email reputation: Advanced has blocked more than 80% of total incoming connections (all were malicious) in customer networks. Results will vary depending on how much of your incoming email stream is spam. The more spam you receive, the higher the percentage of blocked connections you will see.

To enable this:

1. Go to the Email Reputation screen by navigating to **Spam Prevention > Email Reputation**.
2. Select **Enable Email Reputation**.
3. Click **Save**.

The screenshot displays the Trend Micro Smart Protection Network management console. On the left is a navigation menu with options like Summary, Security Risk Scan, Attachment Blocking, Content Filtering, Data Loss Prevention, Spam Prevention (highlighted), Email Reputation (selected), Content Scanning, Web Reputation, Manual Scan, Scheduled Scan, Virtual Analyzer, Smart Protection, Updates, Alerts, Reports, Logs, Quarantine, and Administration. The main content area is titled 'Email Reputation' and includes a description: 'Email Reputation Services verifies IP addresses of incoming email messages using one of and botnets as they first emerge.' There is a checked checkbox for 'Enable Email Reputation'. Below this are tabs for 'Target' and 'Action'. The 'Service Portal' section contains the text 'View global spam information and configure advanced email reputation service settings a' and a link for 'Smart Protection Network portal'. The 'Approved IP Address' section has a text input field for adding an IP address, an 'Add' button, and examples for IPv4 (192.168.0.31 or 192.168.0.0/24) and IPv6 (2620:101:4002:759::139:161 or 2620:101:4002:759::0/96). There is also a list for 'Approved IP Addresses' with a 'Remove' button. At the bottom are 'Save' and 'Reset' buttons.

## 7.1.2 Content Scanning

Content Scanning uses detection technology based on sophisticated content processing and statistical analysis. Unlike other approaches to identifying spam, content analysis provides high performance, real-time detection that is highly adaptable, even as spammers change their techniques.

To enable and configure this:

1. Go to the Content Scanning screen by navigating to **Spam Prevention > Content Scanning**.
2. Select **Enable content scanning**.

3. Click the **Target** tab.
4. Select a detection level:
  - High: This is the most rigorous level of spam detection. ScanMail monitors all email messages for suspicious files or text, but there is greater chance of false positives. False positives are those email messages that ScanMail filters as spam when they are actually legitimate email messages.
  - Medium: ScanMail monitors at a high level of spam detection with a moderate chance of filtering false positives.
  - Low: This is the default setting. This is most lenient level of spam detection. ScanMail will only filter the most obvious and common spam messages, but there is a very low chance that it will filter false positives.
5. Add addresses to the list of Approved Senders and Blocked Senders.
6. Click the **Action** tab and select action for Spam messages.
7. Click **Save**.

### 7.1.3 Detect New Spam source

This feature is proven to be effective especially when preventing spam and malicious emails. Web Reputation Service (WRS) and Email Reputation Service (ERS) information is used to scan email messages with URLs unknown by Trend Micro.

Content Scanning can identify new spam sources in conjunction with Web Reputation Services. After enabling detect new spam sources, ScanMail performs the following actions after receiving an email message containing a URL:

- Web Reputation Services determines the reputation score of the URL.
- ScanMail uses the configured internal gateway MX record or IP address lists to determine the sender IP address of the email message.
- Email Reputation Services determines the reputation score of the sender IP address.

Content Scanning uses the reputation scores of both the URL contained in the email message and the sender IP address to determine the risk level of the email message. Enabling Web Reputation Services allows detection of new spam sources.

To enable and configure:

1. Go to the Content Scanning screen by navigating to **Spam Prevention > Content Scanning**.
2. Select Detect new spam sources to scan email messages containing URLs that may be new spam sources. You must enable Web Reputation Services to detect new spam sources.
3. Identify your Organizational MX records or your Organizational email gateway IP addresses:
  - a. Identify your company's Organizational MX records and add the MX records to the list.

- b. Identify your company's Organizational email gateway IP addresses and add the IP addresses to the list.
4. Click **Save**.

To learn more about this feature, refer to KB 1108290 (<https://success.trendmicro.com/solution/1108290>)

### New Spam Sources

Detect new spam sources

Organizational MX records 

Add an organizational MX record FQDN:  
(for example: domain.com)

Organizational MX record FQDN(s):

Organizational mail gateway IP addresses 

## 7.1.4 Phishing Mail

Phishing email feature is part of Spam Prevention Solution. Phishing is a form of identity theft in which a scammer uses an authentic-looking email from a legitimate business to trick recipients into giving out sensitive personal information, such as a credit card, bank account, Social Security numbers or other sensitive personal information. The spoofed email message urges the recipient to click on a link to update

their personal profile or carry out some transaction. The link then takes the victim to a fake website where any personal or financial information entered is routed directly to the scammer.

To enable and configure:

1. Go to the Content Scanning screen by navigating to **Spam Prevention > Content Scanning**.
2. Select Detect phishing to scan for phishing email messages.
3. Click the **Action** tab and select action for Phishing messages.
4. Click **Save**.



## 7.2 Best Practice Configuration and Prevention for Ransomware

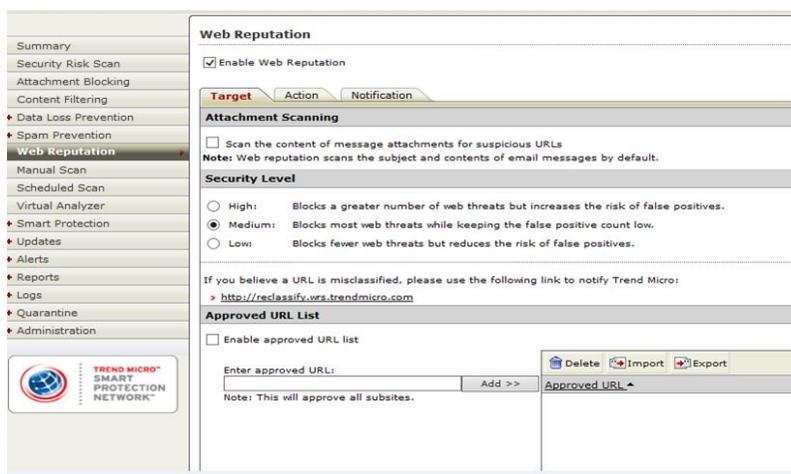
Ransomware can enter an organization through many vectors, such as email spam, phishing attacks, or malicious web downloads. For highest level of protection, organizations are encouraged to deploy multiple layers of protection on endpoint, gateway, and email servers.

In order to prevent ransomware on email server, please follow chapter 7.1 to enable **Spam Prevent**. Additionally, Trend Micro **Web Reputation** technology helps break the infection chain by assigning websites a “reputation” based on an assessment of the trustworthiness of an URL, derived from an analysis of the domain. Web reputation protects

against web-based threats including zero-day attacks, before they reach the network. Trend Micro web reputation technology tracks the lifecycle of hundreds of millions of web domains, extending proven Trend Micro anti-spam protection to the Internet.

To enable **Web Reputation** Services:

1. On the SMEX management console, go to the Web Reputation screen by navigating to Web Reputation from the main menu.



2. Select **Enable Web Reputation**.
3. Click **Save**.

To enable Macro Scan:

1. On the SMEX management console go to **Security Risk Scan > Action**.
2. Navigate to **Advanced Options** and check **Enable advanced macro scan**.

Target **Action** Notification

ActiveAction and

Selecting ActiveAction uses Trend Micro recommended settings

Customized action for detected threats:

Enable action on mass-mailing behavior. (This overwrites all other actions.)

Type	Action	Notification
Mass-mailing behavior	Delete entire mes:	Do not notify

**Detected Threats**

All security risks

Type	Action	Notification
All security risks	Clean	Notify

Specify action per detected security risk

Type	Action	Notification
Viruses	Clean	Notify
Worms/Trojans	Replace with text/l	Notify
Advanced threats	Quarantine entire	Notify
Packed files	Quarantine entire	Notify
Other malicious code	Clean	Notify
Spyware/Grayware	Quarantine entire	Notify

**Uncleanable files** Quarantine entire message

Backup infected file before performing action

Do not clean infected compressed files to optimize performance.

**Advanced Options**

**Macros**

Enable advanced macro scan

Heuristic level: 2 - Default filtering

Delete all macros detected by advanced macro scan

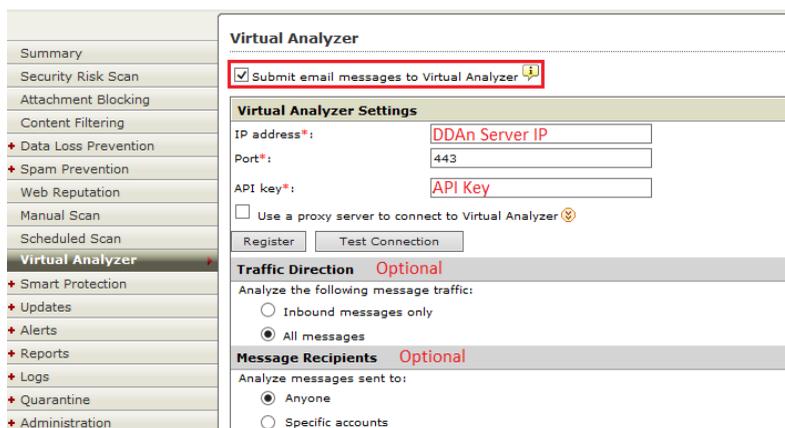
Quarantine and Backup Settings

Replacement Settings

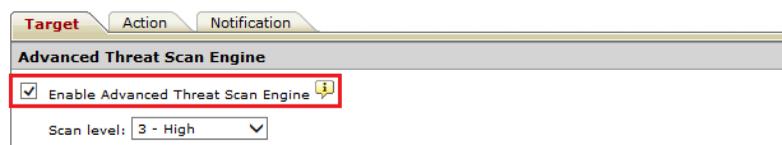
Unscannable Message Parts

To Configure SMEX with Sandbox integration in Deep Discovery Analyzer (DDAN):

1. Register to DDAN: SMEX management console > **Virtual Analyzer**.



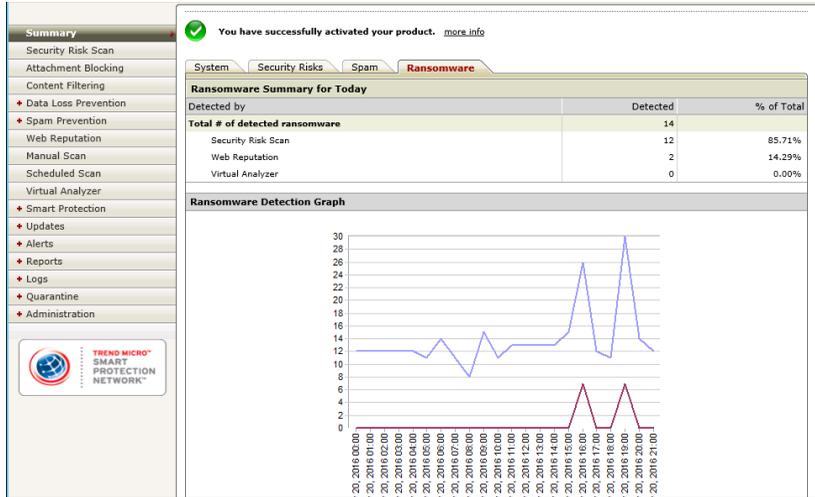
2. On the SMEX management console go to **Security Risk Scan > Target** then check **Advanced Threat Scan Engine**.



Email is one of the major vectors for ransomware attacks. Even though SMEX already blocks most emails with ransomware links or attachments, there is no dedicated ransomware category in previous versions and customers may have no awareness how much work SMEX has done to block emails with ransomware. In this patch, SMEX has enhanced the ransomware visibility so that customers will know how many ransomware emails SMEX has blocked.

To view the result of the Ransomware Prevention, on the SMEX

management console go to **Summary > Ransomware**.



To generate the report for Ransomware Prevention, on the SMEX management console go to **Report > One-time reports/ Schedule reports > The Ransomware report >Generate**.

**Content**

- Scan status summary
- Security risk scan report [Show details](#)
- Ransomware report [Hide details](#)
  - Ransomware detection summary
  - Top ransomware senders 10
  - Top ransomware recipients 10
  - Top ransomware threat name 10
  - Top ransomware file name 10
  - Top ransomware-hosting domain/URL 10
- Attachment Blocking report [Show details](#)

**NOTE**

ScanMail Ransomware visibility change (only applicable in SMEX 12.0 Patch 1 and SP1)



# Chapter 8

## Troubleshooting Guide

### 8.1 Installation process “Installing SQL Server Express” does not finish causing a failure in ScanMail for Exchange (SMEX) installation

In some environment, the SQL Server Express installation may take longer time to complete causing an installation failure in SMEX. Once the SMEX installation progress exceeds the timeout threshold (3 hours), the installation process fails. The progress halts on the step, “Installing SQL Server Express” before the failure message occurs.

This issue could be relative to the server environment that leads longer installation time of SQL Server Express.

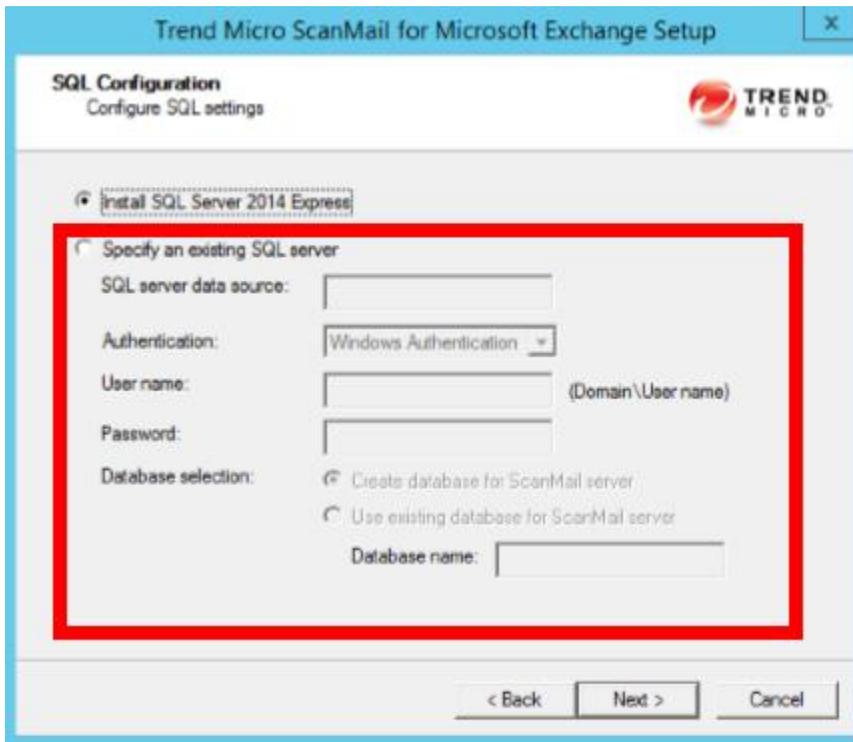
#### NOTE

When performing a fresh installation of SMEX 11 or 12, an SQL Server Express will be installed if a remote SQL Server is not selected during installation.

- ScanMail for Microsoft Exchange 11 will install SQL Server 2008 Express
- ScanMail for Microsoft Exchange 12 will install SQL Server 2014 Express

**Recommendation 1: Installing SMEX by configuring a remote SQL Server :**

For SMEX 12.0, select "Specify an existing SQL Server" to use an existing database server. It is recommended to select Windows Authentication when using an existing SQL Server.



### Recommendation 2: SQL Server Express manual installation

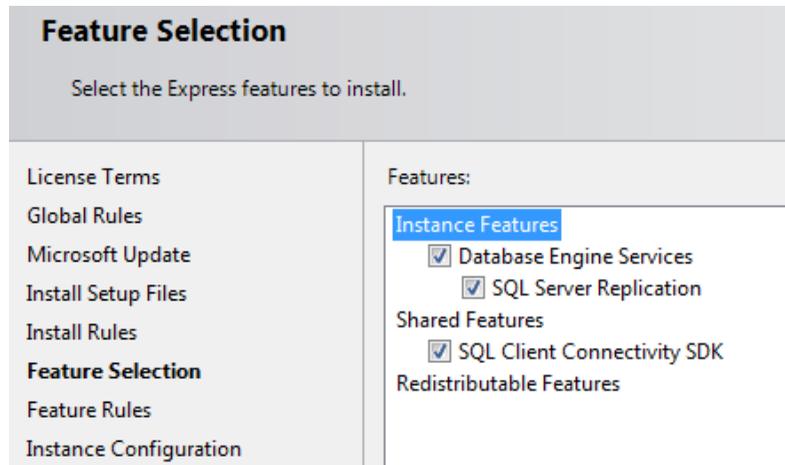
You may also perform manual installation of the SQL Server Express to verify whether it can be installed on your Exchange server.

1. Extract SMEX 12.0 installation package.

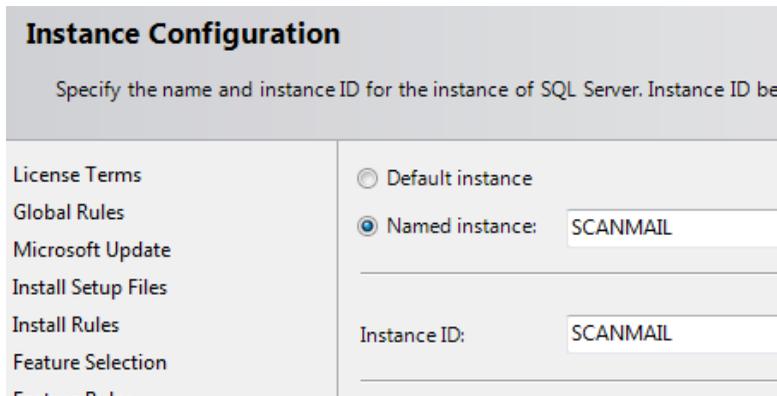
**NOTE** 

Download SMEX 12.0 installation package [here](#).

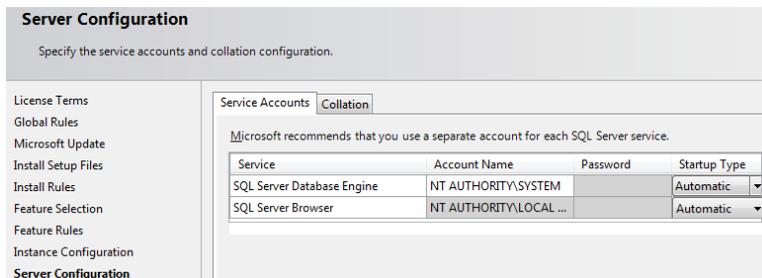
2. Find the SQL Express install package from SMEX-12.0-GM-1220\Smex\package\SQL2014SP1Express
  - a. Double-click SQLEXPRESS.exe.
  - b. On the step Feature Selection, choose at least Database Engine Services.



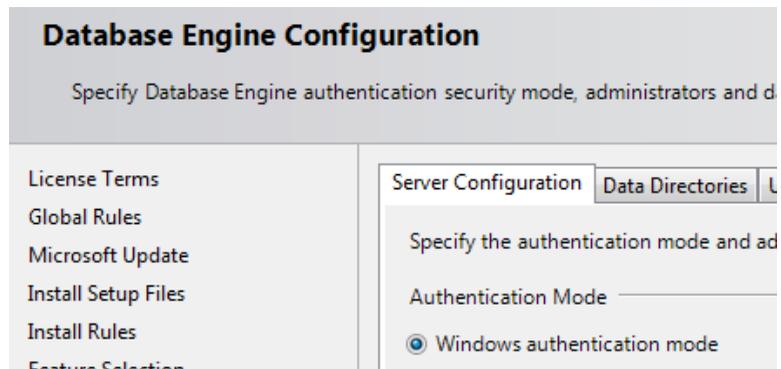
- c. For Instance Configuration, input SCANMAIL in Named instance.



- d. For Server Configuration, under Service Accounts tab select NT AUTHORITY\SYSTEM as Account Name for SQL Server Database Engine service. Set SQL Server Database Engine as Automatic for startup type.



- e. For Database Engine Configuration, under Account Provisioning tab, select "Windows authentication mode" for Authentication mode.



- f. Continue with the installation using default settings.
3. Install SMEX by double-clicking setup.exe from SMEX installation package.

## 8.2 Updating the Scan Engine Manually

Although Trend Micro recommends that you schedule ScanMail to perform automatic

updates of the scan engine, you can do it manually, as shown below.

### Procedure

1. Download the latest scan engine from the Trend Micro website.

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

2. Extract the contents of the engv\_x64dll\_v####-####.zip file to a temporary directory.

3. Stop the following ScanMail services by clicking the Windows Start button and navigating to Programs > Administrative Tools > Services:

- ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail\_RemoteConfig)
- ScanMail for Microsoft Exchange Master Service (ScanMail\_Master)

4. Back up the following scan engine file:

\Program Files\Trend Micro\Smex\engine\vsapi\latest\vsapi64.dll

5. Extract the new scan engine files from their temporary directory to:

\Program Files\Trend Micro\Smex\engine\vsapi\latest\

6. Start the ScanMail services:

- a. Click the Windows Start button, then Programs > Administrative Tools > Services.
- b. Right click each of the following ScanMail scan services and select Start in the pop-up menu that appears.
  - ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail\_RemoteConfig)
  - ScanMail for Microsoft Exchange Master Service (ScanMail\_Master)

## 8.3 Updating the Pattern File (lpt\$vpn.xxx) Manually

Procedure:

1. Download the latest pattern file from the Trend Micro website.

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

2. Download and save to a temporary directory on the ScanMail server:

- The following latest Official Pattern Release (OPR) file:

Enterprise Pattern - Windows

- The following Controlled Pattern Release (CPR) file:

Enterprise Pattern – CPR

**NOTE** 

A Controlled Pattern File Release (CPR) is an early release of the virus pattern file. It has been fully tested, and is intended to provide customers with advanced protection against burgeoning security risks.

3. Click the Windows Start button, then Programs > Administrative Tools > Services to stop all ScanMail services.
4. Extract the contents of the compressed file you downloaded to following folder: \Program Files\Trend Micro\Smex\engine\vsapi\latest
5. Restart all the ScanMail services, then refresh the ScanMail management console.



# Chapter 9

## SMEX Register Hidden Key

The following keys are under the path:

HKEY\_LOCAL\_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\ CurrentVersion\

### Key: AntiSpamSkipScanning

- Type: REG\_SZ
- Value: Email message content-type. Use semicolon (;) as separator.
- Purpose: When an email message passes through the Anti-spam filter, ScanMail will update the email message header. In some environment, this action might corrupt some email messages. We can use this registry key to specifically TNEF binary email messages.

### Key: MaxAllowedVsapiMessageSize

- Type: REG\_DWORD
- Value: 33554432 (= 32\*1024\*1024, 32 MB)
- Purpose: This sets the allowed scan size.

### Key: StoreLevelTrustScan

- Type: REG\_DWORD
- Value: 0
- Purpose: This disables Trust Scan between transport and store level. Add hidden key to all Transport Level SMEX. Restarting the ScanMail\_Master service is required for this key to take effect.

- Value: 1 (default value and mean enable), 0 (disable)
- Purpose: This indicates trust scan result at transport level and is enabled by default. When the hidden is enabled it will add VS stamp at transport level, then store level will trust it and not scan. Customer may disable it and the email message will be scanned at recipient mailbox. The key will then take effect for the next email message.

Key: SkipQuarantinedSpamMail

- Value: 0
- Type: DWORD
- Purpose: When the key "SkipQuarantinedSpamMail = 0" is not applied, once an email messages is detected as a spam, ScanMail delivers it to the spam folder directly without performing any scanning.

Key: EnableSpamMailAttachmentBlocking

- Type: REG\_DWORD
- Data value: "1" = ScanMail (for Microsoft Exchange) performs attachment blocking scans on quarantined spam email messages
- Purpose: This performs attachment blocking scans on quarantined spam email messages.

Key: RemoveSuspiciousURLTag

- Type: DWORD
- Value: 1
- Purpose: When the URL triggers WTP filter and the action is Quarantine to User Spam Folder, SMEX will add "Suspicious URL" tag to notify customer that the email message has suspicious URL. It is an SMEX default behavior. This hidden key can remove this tag.

Key: SkipBackupEncryptPwd

- Type: DWORD
- Value: 1
- Purpose: This hidden key can skip the email message backup.

Key: MaxAllowedBytesPerEntityHeader

- Type: DWORD
- Value: 2048000 (Decimal)
- Purpose: This exceeds the allowed scan length of the email message header.

Key: SkipBlockingFilesInsideOffice2007Files

- Type: REG\_DWORD
- Value: 1
- Purpose: This skips Office 2007 files, as they are considered compressed files in Attachment Blocking.

Key: DLPTreatBodyAsPlainText

- Type: REG\_DWORD
- Value: 1
- Purpose: the DLP filter in ScanMail (for Microsoft Exchange) extracts and scans plain text from the HTML contents of messages
- Data value: 0
- Purpose: the DLP filter in ScanMail (for Microsoft Exchange) scans the original HTML content of messages

Key: EnableTLSQuery

- Type: REG\_DWORD
- Value: 1
- Purpose: This queries remote server logs or quarantined records using the Transport Layer Security (TLS) protocol.

Key: DisableLocalAdminHasFullPermission

- Type: REG\_DWORD
- Value: 1
- Purpose: ScanMail (for Microsoft Exchange) doesn't allow local and domain administrators to log on to the management console.

Key: AUFromHTTPSServer

- Type: REG\_DWORD
- Value: 1
- Purpose: This updates pattern and engine files through the HTTPS server when it is set to use "Trend Micro ActiveUpdate Server" as download source.

Key: EnableMacroRule

- Type: REG\_DWORD
- Value: 1
- Purpose: This allows users to enable the "HEUR\_HAS\_MACRO" ATSE rule which is used to detect if an email messages file attachment contains macros.

Key: TransportLevelTrustScan

- Type: REG\_DWORD
- Value: 1
- Purpose: The TrustScan in Transport level is disabled by default. Add this key to enable it. Transport Trust Scan is applicable only for Spam Prevention, Web Reputation and Security Risk Scan filters. Results from both Content Filtering and Attachment Blocking etc. will not be trusted.

Key: PassMalformedMail

- Type: REG\_DWORD
- Values:
  - 1 = SMEX does not scan malformed email messages
  - 0 = SMEX quarantines malformed email messages
- Purpose: This skips scanning emails which will otherwise trigger “Malformed message” feature.
- Note: Disabling this feature may cause virus leak as the email message is not scanned.



# Chapter 10

## Frequently Asked Questions

### 10.1 FAQ on SMEX 12 and 12 SP1

1. Do I have the latest pattern file or Service Pack?

Depending on which modules you have installed, ScanMail may use the following updatable files:

- Virus Pattern • Anti-spam Pattern
- Spyware Pattern • Anti-spam Engine
- IntelliTrap Pattern • URL Filtering Engine
- IntelliTrap Exception Pattern • Smart Scan Agent Pattern
- Virus Scan Engine • Advanced Threat Scan Engine

To find the latest available patterns, open a web browser to the Trend Micro Update Center.

Locating the ScanMail Version:

- a. From the main ScanMail menu, click Summary.
  - b. A list of installed components, the current ScanMail version, and update schedules appears.
2. Is "Public Folder Scan" supported only on Exchange 2013 and Exchange 2016?
- This option is only supported on Exchange Server 2013 and Exchange Server 2016. Exchange Server 2010 public folders are based in the database system. To enable public folder scanning on Exchange Server 2010, select the Public Folder Database option in

the Database Selection section when performing Manual and Scheduled Scans.

3. What is a compression ratio?

The compression ratio is the uncompressed file size / compressed file size. The following table contains compression ratio examples

FILE SIZE (NOT COMPRESSED)	FILE SIZE (COMPRESSED)
500 KB	10 KB (ratio is 50:1)
1000 KB	10 KB (ratio is 100:1)
1001 KB	10 KB (ratio exceeds 100:1)
2000 KB	10 KB (ratio is 200:1)

4. Are UNC paths supports for quarantine and backup folders:  
ScanMail supports the usage of Universal Naming Convention (UNC) paths when configuring the quarantine and backup folders (for example, [\\fileservers\directory](#)).

Important Comments:

- UNC paths are not supported on Exchange Edge servers
- UNC paths cannot contain blank spaces.
- For clustered environments, computer accounts can only select cluster nodes, not virtual server names.

5. How do I update newly installed ScanMail servers to the Server Groups list?

Click the **Refresh** button the first time that you go to the **Server Groups** screen. This

automatically polls the network and returns a list of all available ScanMail servers. If you

do not click **Refresh** when opening the screen, each group will take some time to populate when opening each separately.

After upgrading an existing ScanMail server, click **Refresh** again to update the lists.

6. How long will be spam log kept in local database?  
By default, spam logs older than 12 hours will be purged.
7. What's the final action for URL sandboxing in inline mode:  
Please see below chart:

WRS Result	DDA Result	Final Action
Unrated	Clean	Pass
Unrated	High Risk	Web Reputation filter action config + Virtual Analysis security level settings
Unrated	Medium Risk	Web Reputation filter action config + Virtual Analysis security level settings
Unrated	Low Risk	Web Reputation filter action config + Virtual Analysis security level settings
Unrated	Timeout/Exception	Action on the unanalyzed risk

8. If the suspicious was sent to DDAn for further analysis, next time, when SMEX detect the same file, can the file be sent to DDAn again?  
NO, It will not. DDAn will compare with the existing SHA-1 in Cache.
9. How Can I query the quarantine email message logs for multiple servers?

Quarantined logs only can be query via SMEX management console, if you want to query the quarantine logs for the remote SMEX server, use "remote server" feature.





**TREND MICRO INCORPORATED**

225 E. John Carpenter Freeway, Suite 1500  
Irving, Texas 75062 U.S.A.  
Phone: +1 (817) 569-8900, Toll-free: (888) 762-8736  
Email: support@trendmicro.com

[www.trendmicro.com](http://www.trendmicro.com)

Item Code: SMEM127724/170216