TREND MICRO™

11.0 ScanMail™ for Microsoft™ Exchange

Service Pack 1

Administrator's Guide

Securing your Exchange environment

Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/en-us/enterprise/scanmail-for-microsoft-exchange.aspx

Trend Micro, the Trend Micro t-ball logo, Control Manager, eManager, and ScanMail are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2015. Trend Micro Incorporated. All rights reserved.

Document Part No. SMEM116853/150119

Release Date: February 2015

Document Version No.: 1.0

Product Name and Version No.: ScanMail™ *for Microsoft*™ *Exchange* 11.0 SP1

Protected by U.S. Patent No.: 5,951,698

The user documentation for Trend Micro ScanMail *for Microsoft Exchange* 11.0 SP1 is intended to introduce the main features of the software and installation instructions for your production environment. You should read through it prior to installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the Knowledge Base at Trend Micro Web site.

Trend Micro is always seeking to improve its documentation. Your feedback is always welcome. Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Table of Contents

Preface

Preface xi
ScanMail Documentation xii
Audience xii
Document Conventions xiii

Part I: Introducing ScanMail and Getting Started

Chapter 1: Introducing Trend Micro ScanMail for Microsoft Exchange

System Requirements 1-2
What's New 1-7
Features and Benefits 1-10
Version Comparison 1-19
How ScanMail Protects the Microsoft Exchange Environment 1-20
About Uncleanable Files 1-23
ScanMail Technology 1-24

Chapter 2: Getting Started with ScanMail

Getting Started 2-2
Understanding the Product Console 2-2
ScanMail Registration 2-9
ScanMail Activation 2-11
About ScanMail Updates 2-16

Chapter 3: Establishing and Maintaining Security for Your Exchange Servers

Establishing a Security Baseline 3-2
Maintaining Security 3-3
Managing Outbreak Situations 3-4

Chapter 4: Managing ScanMail

Understanding Real-time Monitor 4-2
Understanding the Server Management Console 4-4
Manually Creating a ScanMail Resource for Virtual Servers 4-10
Starting and Stopping the Services 4-14
Understanding ScanMail Icons 4-14

Part II: Configuring Scans and Scan Filters

Chapter 5: Understanding Smart Protection

About Trend Micro Smart Protection 5-2
Configuring Local Sources 5-7
Scan Service Settings 5-8

Chapter 6: Configuring Scans

About Scans 6-2
Compressed File Handling 6-7
About ScanMail Actions 6-10
Notifications 6-23

Chapter 7: Configuring Security Risk Scans

About Security Risk Scans 7-2

ScanMail Scan Hierarchy 7-3
Security Risk Scan Actions 7-5
Enabling Real-time Security Risk Scan 7-6
Configuring Security Risk Scan Targets 7-6
Configuring Security Risk Scan Actions 7-8
Configuring Security Risk Scan Notifications 7-12

Chapter 8: Configuring Attachment Blocking

About Attachment Blocking 8-2
Enabling Real-time Attachment Blocking 8-3
About the Attachment Blocking Global Policy 8-3
Adding an Exception to the Attachment Blocking Global Policy 8-6
Editing an Attachment Blocking Exception 8-8

Chapter 9: Configuring Content Filtering

About Content Filtering 9-2
Enabling Real-time Content Filtering 9-3
Global Settings 9-4
Configuring Content Filtering Policies 9-4
Configuring a Content Filtering Exception 9-13
Editing a Content Filtering Policy 9-14

Chapter 10: Configuring Data Loss Prevention

About Data Loss Prevention (DLP) 10-2
Data Identifier Types 10-2
About Data Loss Prevention Templates 10-12
About Data Loss Prevention Policies 10-17

Chapter 11: Configuring Spam Prevention

About Spam Prevention 11-2
About Email Reputation 11-3
About Content Scanning 11-6

Chapter 12: Configuring Web Reputation

About Web Reputation Services 12-2
Configuring the Web Reputation Scan Service 12-3
Enabling Web Reputation 12-4
Configuring Web Reputation Targets 12-5
Configuring Web Reputation Actions 12-6
Configuring Web Reputation Notifications 12-7

Chapter 13: Configuring Search & Destroy

About Search & Destroy 13-2
Configuring Search & Destroy Access Accounts 13-2
Activating Search & Destroy 13-4
About Mailbox Searches 13-6
Configuring a Mailbox Search 13-13
Configuring Search & Destroy Settings 13-20
Viewing Search & Destroy Event Logs 13-21
Troubleshooting Search & Destroy 13-22

Chapter 14: Configuring Virtual Analyzer

About Virtual Analyzer 14-2
Configuring Virtual Analyzer Settings 14-2

Part III: Managing ScanMail

Chapter 15: Managing the Quarantine Area

About the Quarantine 15-2
Configuring the Quarantine Folder/Directory 15-2
Performing a Quarantine Query 15-3
Scheduling Automatic Quarantine Maintenance 15-4
Manually Performing Quarantine Maintenance 15-5
Resending Quarantined Messages 15-5

Chapter 16: Monitoring ScanMail

Viewing the Summary Screen 16-2
About Alerts 16-5
About Reports 16-11
About Logs 16-15

Chapter 17: Performing Administrative Tasks

Configuring Proxy Settings 17-2
Global Notification Settings 17-2
Configuring Spam Maintenance 17-4
Configuring Real-time Scan Settings 17-5
About Access Control 17-6
About Special Groups 17-8
About Server Groups 17-9
About Internal Domains 17-10
Product License 17-11
World Virus Tracking Program 17-12
About Trend Micro Control Manager 17-13
Using Trend Support / System Debugger 17-16

Part IV: Getting Help

Chapter 18: Understanding Security Risks

Understanding the Terms 18-2
About Internet Security Risks 18-2
About Spyware/Grayware 18-13

Chapter 19: Frequently Asked Questions

Scanning and Updating 19-2
Expressions and Keywords 19-3
File Handling 19-13
Quarantine and Log Management 19-15
Logs, Quarantine Records, and Server Groups 19-17
Logging On and Registration 19-18
Security Threats 19-21

Chapter 20: Troubleshooting

Updating the Scan Engine Manually 20-2
Updating the Pattern File (lpt$vpn.xxx) Manually 20-3
Known Issues 20-3

Chapter 21: Contacting Trend Micro

Contacting Technical Support 21-2
Speeding Up Your Support Call 21-3
Using the Support Portal 21-3
Security Information Site 21-4

Appendix A: Introducing Trend Micro Control Manager

Control Manager Standard and Advanced A-3

Introducing Control Manager Features A-3

Control Manager Architecture A-5

Registering ScanMail to Control Manager A-8

Understanding User Access A-9
- Control Manager User Access with ScanMail User Access A-11
- MCP Heartbeat A-11

Understanding the Product Directory A-15
- Product Directory Structure Recommendations A-17
- Accessing the Product Directory A-21
- Manually Deploying Components Using the Product Directory A-22
- Viewing Status Summaries for Managed Products A-23
- Configuring Managed Products A-24
- Issuing Tasks to Managed Products A-25
- Querying and Viewing Managed Product Logs A-26
- About Recovering Managed Products Removed From the Product Directory A-30
- Searching for Managed Products, Product Directory Folders, or Computers A-32
- Searching for a Folder or Managed Product A-32
- Refreshing the Product Directory A-33
- Understanding the Directory Management Screen A-33

Downloading and Deploying New Components A-39
- Manually Downloading Components A-41
- Understanding Scheduled Download Exceptions A-48
- Configuring Scheduled Downloads A-49
- Configuring Scheduled Download Settings A-57
- Configuring Scheduled Download Automatic Deployment Settings A-59
- Understanding Deployment Plans A-61
- Configuring Proxy Settings A-62
- Configuring Update/Deployment Settings A-63
- Setting "Log on as batch job" Policy A-65

Using Logs A-65
- Understanding Managed Product Logs A-66
- Querying Log Data A-67

Understanding Reports A-69
Understanding Control Manager Report Templates A-69
Adding One-time Reports A-82
Adding Scheduled Reports A-88

Appendix B: ScanMail Windows Event Log Codes

Appendix C: Database Schema for 64-bit Operating Systems

Log Database Schema C-2

Log View Database Schema C-17

Report Database Schema C-30

Appendix D: Best Practices

Real-time Scan Settings for Server Roles D-2

Attachment Blocking Policies D-3
Exception Rule Replication D-3
Sample Usage Scenarios D-4

Content Filtering Active Directory Integrated Policies D-5
Content Filtering Policy Replication D-5

Data Loss Prevention Policies D-6
Data Identifiers and Template Creation D-6
Data Loss Prevention Policy Replication D-7
Data Loss Prevention: Hidden Keys D-7

Optimizing Web Reputation D-8
Troubleshooting Web Reputation Performance Issues D-9

Search & Destroy Best Practices D-10
Search & Destroy Prerequisites D-10
Using Search & Destroy in Mixed Exchange Environments D-12
Configuring Search & Destroy in a Multiple Data Center Environment D-13
Optimizing Search Criteria D-14
Optimizing Mailbox Searches D-15

Deleting Mailbox Searches D-15
Exchange Management Shell Commands D-16
Virtual Analyzer - Integration Pre-requisites D-19
Internal Domains D-20
Recommended Settings D-20

Index

Index IN-1

Preface

Preface

Welcome to the Trend Micro™ ScanMail™ *for Microsoft™ Exchange* Administrator's Guide. This book contains basic information about the tasks you need to perform to manage ScanMail to protect your Exchange servers. It is intended for novice and advanced users of ScanMail who want to manage ScanMail.

This preface discusses the following topics:

- *ScanMail Documentation on page xii*
- *Audience on page xii*
- *Document Conventions on page xiii*

ScanMail Documentation

The product documentation consists of the following:

- **Online Help**: Web-based documentation that is accessible from the product console

  The Online Help contains explanations about ScanMail features.

- **Installation and Upgrade Guide**: PDF documentation that discusses requirements and procedures for installing and upgrading the product

- **Administrator's Guide**: PDF documentation that discusses getting started information and product management

- **Readme File**: Contains late-breaking product information that might not be found in the other documentation. Topics include a description of features, installation tips, known issues, and product release history.

- **Knowledge Base**: Contains the latest information about all Trend Micro products. Other inquiries that were already answered area also posted and a dynamic list of the most frequently asked question is also displayed.

  http://esupport.trendmicro.com

Note

Trend Micro recommends checking the corresponding link from the Update Center (http://docs.trendmicro.com/en-us/enterprise/scanmail-for-microsoft-exchange.aspx) for updates to the documentation.

Audience

The ScanMail documentation assumes a basic knowledge of security systems, including:

- Antivirus and content security protection

- Spam protection

- Network concepts (such as IP address, netmask, topology, LAN settings)
- Various network topologies
- Microsoft Exchange Server administration
- Microsoft Exchange Server 2013, 2010, and 2007 server role configurations
- Various message formats

Document Conventions

The documentation uses the following conventions.

TABLE 1. Document Conventions

CONVENTION	DESCRIPTION
UPPER CASE	Acronyms, abbreviations, and names of certain commands and keys on the keyboard
Bold	Menus and menu commands, command buttons, tabs, and options
Italics	References to other documents
`Monospace`	Sample command lines, program code, web URLs, file names, and program output
Navigation > **Path**	The navigation path to reach a particular screen For example, **File** > **Save** means, click **File** and then click **Save** on the interface
Note	Configuration notes
Tip	Recommendations or suggestions

Convention	Description
Important	Information regarding required or default configuration settings and product limitations
WARNING!	Critical actions and configuration options

Part I

Introducing ScanMail and Getting Started

Chapter 1

Introducing Trend Micro ScanMail *for Microsoft Exchange*

Trend Micro™ ScanMail™ *for Microsoft™ Exchange* protects your Exchange mail servers. Once installed, ScanMail can protect your servers from viruses/malware, Trojans, worms, spyware/grayware and malicious URLs. ScanMail also sustains business and network integrity by filtering spam messages and messages containing undesirable or unwanted content. ScanMail notifications send timely alerts to administrators or other designated individuals whenever significant system events or outbreak activities occur.

Topics include the following:

- *System Requirements on page 1-2*
- *What's New on page 1-7*
- *Features and Benefits on page 1-10*
- *Version Comparison on page 1-19*
- *How ScanMail Protects the Microsoft Exchange Environment on page 1-20*
- *About Uncleanable Files on page 1-23*
- *ScanMail Technology on page 1-24*

System Requirements

The following lists the system requirements for running Trend Micro™ ScanMail™ *for Microsoft™ Exchange* .

ScanMail with Exchange Server 2013

The following table lists the system requirements for running ScanMail with Exchange Server 2013 and Exchange Server 2013 Service Pack 1.

TABLE 1-1. System Requirements for Installation with Exchange Server 2013

RESOURCE	REQUIREMENTS
Processor	• x64 architecture-based processor that supports Intel™ 64 architecture (formally known as Intel EM64T) • x64 architecture-based computer with AMD™ 64-bit processor that supports AMD64 platform
Memory	1GB RAM exclusively for ScanMail (2GB RAM recommended)
Disk space	2GB free disk space
Operating System	• Microsoft™ Windows Server™ 2012 R2 Standard or Datacenter (64-bit) • Microsoft™ Windows Server™ 2012 Standard or Datacenter (64-bit) • Microsoft™ Windows Server™ 2008 R2 Standard with Service Pack 1 or above (64-bit) • Microsoft™ Windows Server™ 2008 R2 Enterprise with Service Pack 1 or above (64-bit) • Microsoft™ Windows Server™ 2008 R2 Datacenter RTM or above (64-bit)
Mail Server	Microsoft Exchange Server 2013

RESOURCE	REQUIREMENTS
Web Server	• Microsoft Internet Information Services (IIS) 8.5 • Microsoft Internet Information Services (IIS) 8.0 • Microsoft Internet Information Services (IIS) 7.5
Browser	• Microsoft™ Internet Explorer™ 6.0 or above • Mozilla Firefox™ 3.0 or above
MSXML	4.0 Service Pack 2 or above
.NET framework	3.5 Service Pack 1

ScanMail with Exchange Server 2010

The following table lists the system requirements for running ScanMail with Exchange Server 2010.

TABLE 1-2. System Requirements for Installation with Exchange Server 2010

RESOURCE	REQUIREMENTS
Processor	• x64 architecture-based processor that supports Intel™ Extended Memory 64 Technology (Intel EM64T) • x64 architecture-based computer with AMD™ 64-bit processor that supports AMD64 platform
Memory	1GB RAM exclusively for ScanMail (2GB RAM recommended)
Disk space	2GB free disk space

RESOURCE	REQUIREMENTS
Operating System	• Microsoft™ Windows Server™ 2012 Standard or Datacenter (64-bit) • Microsoft Windows Server 2008 R2 or above (64-bit) • Microsoft Windows Server 2008 with Service Pack 2 or above (64-bit) • Microsoft Small Business Server (SBS) 2011 **Note** Microsoft Small Business Server (SBS) 2011 received limited compatibility testing with this version of ScanMail. The installation recommendation is to uninstall Microsoft ForeFront prior to installing ScanMail from Microsoft Small Business Server (SBS) 2011.
Mail Server	Microsoft Exchange Server 2010 or above
Web Server	• Microsoft Internet Information Services (IIS) 8.0 • Microsoft Internet Information Services (IIS) 7.5 • Microsoft Internet Information Services (IIS) 7.0
Browser	• Microsoft™ Internet Explorer™ 6.0 or above • Mozilla Firefox™ 3.0 or above
MSXML	4.0 Service Pack 2 or above
.NET framework	3.5 Service Pack 1

ScanMail with Exchange Server 2007

The following table lists the system requirements for running ScanMail with Exchange Server 2007.

TABLE 1-3. System Requirements for Installation with Exchange Server 2007

RESOURCE	REQUIREMENTS
Processor	• x64 architecture-based processor that supports Intel™ Extended Memory 64 Technology (Intel EM64T) • x64 architecture-based computer with AMD™ 64-bit processor that supports AMD64 platform
Memory	1GB RAM exclusively for ScanMail (2GB RAM recommended)
Disk space	2GB free disk space
Operating System	• Microsoft Windows Server 2008 R2 or above (64 bit) • Microsoft Windows Server 2008 with Service Pack 2 or above (64-bit) • Microsoft Small Business Server 2008 **Note** Microsoft Small Business Server (SBS) 2008 received limited compatibility testing with this version of ScanMail. The installation recommendation is to uninstall Microsoft ForeFront prior to installing ScanMail from Microsoft Small Business Server (SBS) 2008. • Microsoft Windows Server 2003 R2 with Service Pack 2 (64-bit) • Microsoft Windows Server 2003 with Service Pack 2 (64-bit)
Mail Server	Microsoft Exchange Server 2007 with Service Pack 1 or above
Web Server	• Microsoft Internet Information Services (IIS) 7.5 • Microsoft Internet Information Services (IIS) 7.0 • Microsoft Internet Information Services (IIS) 6.0

Resource	Requirements
Browser	• Microsoft Internet Explorer 6.0 or above • Mozilla Firefox 3.0 or above
MSXML	4.0 Service Pack 2 or above
.NET framework	3.5 Service Pack 1

Cluster Installations

The following lists supported cluster environments:

- Exchange Server 2013 with Database Availability Group (DAG) model
- Exchange Server 2010 with VERITAS Cluster 5.1 SP2
- Exchange Server 2010 with Database Availability Group (DAG) model
- Exchange Server 2007 with VERITAS Cluster 5.1 SP2
- Exchange Server 2007 with Single Copy Cluster (SCC) model
- Exchange Server 2007 with Cluster Continuous Replication (CCR) model
- Exchange Server 2007 with Standby Continuous Replication (SCR) model

ScanMail Integration with Trend Micro Products

You can optionally integrate ScanMail with other Trend Micro products. The following table outlines the supported products and versions.

Table 1-4. Integrated Trend Micro Product Support

Trend Micro Product	Supported Versions
Control Manager™	• 6.0 or above • 5.5 with Service Pack 1 • 5.0 with Patch 7 and Hotfix 2108

Trend Micro Product	Supported Versions
Smart Protection Server	• 3.0 • 2.5 • 2.1 • 2.0 • OfficeScan Server Integrated Smart Protection Server
Deep Discovery Advisor	2.92 or later
Deep Discovery Analyzer	5.0

What's New

The following new features are available in this version of ScanMail.

Table 1-5. New Features in 11.0 SP1

Feature	Description
Server Groups	Create server groups to easily manage and monitor multiple Exchange servers.
New spam source detection	Content Scanning provides scanning for new sources of spam messages when used in conjunction with Web Reputation Services.
Centralized reports, logs, and quarantine queries	Using the Server Groups feature, you can centrally monitor multiple ScanMail servers by: • Creating reports • Querying logs and quarantined messages
Automated End User Quarantine folder deletion	After disabling the End User Quarantine, ScanMail can automatically delete the spam folder for all client accounts.

Feature	Description
Advanced Threat Scan Engine scan levels	Advanced Threat Scan Engine scanning includes a "Scan level" that allows you to specify how "aggressively" ScanMail examines messages and files for advanced threats.
Manual and Scheduled Scans enhancements	Manual and Scheduled Scans include: • The option of disabling the "Public folder" scan (Exchange Server 2013 only) • Enhanced reporting on detections found on specific databases
Data Loss Prevention enhancements	Data Loss Prevention includes: • Digital Asset Discovery in single or multiple message parts • An updated sender and recipient selection process
"Pass" action support	ScanMail supports the "Pass" action for the following scan types: • Web Reputation • Content Scanning
Attachment Blocking target enhancements	Attachment Blocking allows you to create filters based on specific senders and specific recipients.
UNC directory support	ScanMail supports UNC shared directories for the quarantine, backup, and archive directories.

Table 1-6. New Features in 11.0 Repack

Feature	Description
Platform support	ScanMail provides full support for Exchange Server 2013 Service Pack 1 environments and full support for Exchange Server 2013 with the Edge Transport role. For details on system requirements, see *System Requirements on page 1-2*.

TABLE 1-7. New Features in 11.0

FEATURE	DESCRIPTION
Platform support	ScanMail provides full support for Windows Server 2012, Windows Server 2012 R2, and Exchange Server 2013 environments. For details on system requirements, see *System Requirements on page 1-2*.
Search & Destroy enhancements	Search & Destroy Operator: Administrators can assign users the Search & Destroy Operator role which permits the searching of mailboxes, and the viewing and copying of search results. For details, see *Configuring Search & Destroy Access Accounts on page 13-2*. Exporting search results to PST files: ScanMail allows administrators to generate, copy, export, and delete PST copies of matched search results. For details, see *Viewing Mailbox Search Results on page 13-18*. Automatic deletion of matches during mailbox searches: For companies with high-level security concerns, ScanMail allows administrators to configure the automatic deletion of mailbox components when a mailbox search finds a match. For details, see *Mailbox Search Options on page 13-9*.
Command & Control (C&C) Contact Alert detections	Web Reputation Services has been enhanced to provide detection capabilities for C&C callbacks. Administrators can use the Global Intelligence list or integrate a Smart Protection Server with Deep Discovery Advisor to make use of the Virtual Analyzer C&C server list. The Virtual Analyzer generates this list based on data received from connected Trend Micro products ensuring very company-specific protection. For details. see *Command & Control Contact Alert Services on page 12-2*.

Features and Benefits

ScanMail provides the following features and benefits.

Web-based Product Console

Use SSL to access remote servers through a secure product console.

Installation and Support

TABLE 1-8. Installation and Support

FEATURE	BENEFITS
Fast and Simple Installation	• Install to a single or multiple Microsoft Exchange servers using a single installation program. • Install to cluster environments.

FEATURE	BENEFITS

Cluster Support	Cluster Support
	• Exchange 2013:
	  • Database Availability Group (DAG)
	• Exchange 2010:
	  • Database Availability Group (DAG)
	  • VERITAS Cluster 5.1 SP2
	• Exchange 2007
	  • Single Copy Cluster (SCC)
	  • Cluster Continuous Replication (CCR)
	  • Standby Continuous Replication (SCR) models
	  • VERITAS Cluster 5.1 SP2
	ScanMail uses the Exchange Virtual Servers (EVS) management model for managing clusters. Each virtual server owns independent ScanMail configuration information and keeps the data consistent even when performing a failover to another node.

Antivirus Features and Scan Types

TABLE 1-9. Antivirus Features and Scan Types

FEATURE	BENEFIT
Powerful and Creative Antivirus Features	• SMTP scanning (Transport scanning) and store level scanning. • Leverage Microsoft Virus Scanning API to scan messages at a low-level in the Exchange store. • Quickly scan messages using multi-threaded in-memory scanning. • Detect and take action against viruses/malware, Trojans, and worms. • Detect and take action against spyware/grayware. • Use true file type recognition to detect falsely labeled files. • Use Trend Micro recommended actions or customize actions against viruses/malware. • Detect all macro viruses/malware and remove them or use heuristic rules to remove them.
• Advanced Threat Scan Engine (ATSE)	The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.
• IntelliTrap	This version of ScanMail incorporates IntelliTrap technology. Use IntelliTrap to scan for packing algorithms to detect packed files. Enabling IntelliTrap allows ScanMail to take user-defined actions on infected attachments and to send notifications to senders, recipients, or administrators.

FEATURE	BENEFIT
• Trust Scan	Real-time scan can skip scanning email messages at the store level when the message has been scanned by ScanMail at the Hub Transport Level. Once ScanMail scans a message on an Edge or Hub Transport server, ScanMail adds scan information to the message. When the message reaches the Mailbox, ScanMail evaluates the scan information to prevent redundant use of resources. ScanMail only scans the message if the message was scanned with an older scan engine or pattern file or if ScanMail has not previously scanned the message.
• A Category for Unscannable Message Parts	ScanMail separates the unscannable message count from the virus/malware count. Unscannable files can be files that fall outside of the **Scan Restriction Criteria**, encrypted files, or password protected files.
Manual Scan and Scheduled Scan	ActiveUpdate does not interrupt Manual Scan or Scheduled Scan. For Exchange Server 2010 and 2007, the Manual Scan and Scheduled Scan pages only appear on Combo Server (Hub Transport and Mailbox server role) and Mailbox server roles. For Exchange Server 2013, these pages appear only for Mailbox server roles. ScanMail provides three incremental scan options: • Scan messages delivered during a time period • Scan messages with attachments • Scan messages that have not been scanned by ScanMail

FEATURE	BENEFIT
Smart Scan	Smart scan moves security capabilities from the server to the cloud. An integral part of the Trend Micro Smart Protection Network, Smart Scan provides the following benefits: • Fast, real-time security status lookup capabilities in the cloud • Reduces the overall time it takes to deliver protection against emerging threats • Lowers memory consumption on endpoints
Updates	• Receive scheduled or on-demand component updates and customize your update source.

Multiple Scan Filters

TABLE 1-10. Multiple Scan Filters

FEATURE	BENEFITS
Attachment Blocking	• Block named attachments or block attachments by true file type, file extension, or file name. • Active Directory integrated exception rules
Content Filtering	• Use rule-based filters to screen out message content deemed to be offensive or otherwise objectionable. • Active Directory integrated policies • Content Filtering Logs This version of ScanMail displays the keyword in content filtering logs when there is a match. **Note** If the keyword or regular expression is too long to display, logs display truncated information.

FEATURE	BENEFITS
Data Loss Prevention	• Use rule-based filters to detect, filter, and mask sensitive data before it transmits out of the network. • Select from over 100 predefined templates and data identifiers, or create customized expressions and keyword lists to meet company-specific mandates. • Create customized rules to block, mask, log, and delete sensitive data transmitting across the network. • Create Data Loss Prevention policies and deploy to ScanMail servers from Control Manager 6.0 to ensure that company-wide policies remain consistent across all servers.
Spam Prevention Rules	• Use spam prevention filters with adjustable sensitivity levels to screen out spam while reducing falsely identified messages. • End User Quarantine (EUQ) with Spam Confidence Level (SCL) This version of ScanMail provides "Integrate with Outlook Junk E-mail" and "Integrate with End User Quarantine" solutions. You can select either solution during installation. • Junk E-Mail folder In this version of ScanMail, you can select to send detected Spam messages to the standard Outlook folder. The creation of a separate Spam folder is no longer necessary.

FEATURE	BENEFITS
Web Reputation	• This version of ScanMail leverages Web Reputation technology, which evaluates the integrity of all requested web pages. • Web Reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. • Web Reputation blocks web pages based on their reputation ratings. It queries Trend Micro servers for these ratings, which are correlated from multiple sources, including web page links, domain and IP address relationships, spam sources, and links in spam messages. By obtaining ratings online, Web Reputation uses the latest available information to block harmful pages. • Web Reputation helps deter users from following malicious URLs when the feature is enabled. Web reputation queries Trend Micro servers for the reputation rating when an email message with a URL in the message body or message attachment is received. Depending on the configuration, Web Reputation can quarantine, delete, or tag the email message with URLs.
Search & Destroy	Search & Destroy provides administrators the ability to search and remove mailbox components (for example, email messages, meetings, tasks) containing undesirable content from Exchange mailbox servers. **Note** • The Search & Destroy feature only provides support for mailbox servers running Exchange 2010 Service Pack 1 or above, or Exchange 2013. • The Search & Destroy menu only appears after configuring the Search & Destroy Administrator or Search & Destroy Operator roles.

Feature	Benefits
Virtual Analyzer integration	Administrators can leverage the Virtual Analyzer in Deep Discovery Advisor or Deep Discovery Analyzer to evaluate messages and files in which Advanced Threat Scan Engine detects suspicious behavior. ScanMail sends the suspect files to Virtual Analyzer which then performs content simulation and analysis in an isolated virtual environment to identify characteristics commonly associated with many types of malware. After Virtual Analyzer completes the analyses, ScanMail receives a report indicating the risk level of the message or file. Administrators can configure ScanMail to perform specific actions on analyzed files based on the company's security level policy.

Informative Monitoring Tools

TABLE 1-11. Informative Monitoring Tools

FEATURE	BENEFITS
Notifications	ScanMail can automatically send notifications when it does the following: • Detects and takes action against a virus or other threat detected in an email message • Blocks an infected attachment • Detects suspicious URLs • Filters out undesirable content from an email message • Detects a significant system event • Detects virus/malware outbreak conditions • ScanMail can notify designated individuals during real-time, manual, or scheduled scanning. **Note** For correct resolution of ScanMail notifications with Simple Network Management Protocol (SNMP), you can import the Management Information Base (MIB) file to your network management tools from the following path in the ScanMail installation directory: trend_smex_v2.mib.
Informative and Timely Reports and Logs	• Keep up-to-date using activity logs that detail significant events • Send or print graphical reports
Quarantine	• Set ScanMail to quarantine suspicious email messages • Query logs for quarantine events and resend quarantined messages when you decide they are safe

Version Comparison

The following table lists versions of ScanMail and the features for each:

TABLE 1-12. ScanMail Version Comparison

SUPPORT	SCANMAIL 10.X	SCANMAIL 11.X
Operating system version	• Microsoft™ Windows™ Server 2003 with Service Pack 2, or R2 with Service Pack 2 (32-bit or 64-bit) • Microsoft™ Windows Server™ 2008 with Service Pack 1 or above (64-bit) • Microsoft™ Windows Server™ 2008 R2 (64-bit)	• Microsoft™ Windows Server™ 2008 R2 Standard with Service Pack 1 or above (64-bit) • Microsoft™ Windows Server™ 2008 R2 Enterprise with Service Pack 1 or above (64-bit) • Microsoft™ Windows Server™ 2008 R2 Datacenter RTM or above (64-bit) • Microsoft™ Windows Server™ 2012 Standard or Datacenter (64-bit)
Minimum Exchange Version	• Microsoft™ Exchange Server 2003 with Service Pack 2 • Microsoft™ Exchange Server 2007 with Service Pack 1 • Microsoft™ Exchange Server 2010	• Microsoft™ Exchange Server 2007 with Service Pack 1 • Microsoft™ Exchange Server 2010 • Microsoft™ Exchange Server 2013
Scan mechanism	• VSAPI 2.5 • VSAPI 2.6	• VSAPI 2.5 • VSAPI 2.6
Exchange Information Store scanning	Yes	Yes

SUPPORT	SCANMAIL 10.X	SCANMAIL 11.X
SMTP (Transport) scanning	Yes	Yes
Quarantine Manager	Yes	Yes
Active Message Filter	Integrated as delete function for inbound and outbound messages	Integrated as delete function for inbound and outbound messages
Notification	• Collaborative Data Object • Collaborative Data Object EX • Exchange Web Service	• Collaborative Data Object • Collaborative Data Object EX • Exchange Web Service

Note

Previous versions of ScanMail offered eManager™ as a separate module add-on. ScanMail has integrated eManager features so that it is no longer necessary to install eManager separately from version 7.0 on.

How ScanMail Protects the Microsoft Exchange Environment

Trend Micro recognizes the unique dangers posed by security threats to Microsoft Exchange servers. Trend Micro designed ScanMail to protect Exchange from these numerous and diverse security risks. ScanMail uses a filtering strategy to protect Exchange. ScanMail subjects the email message to each filter in the following order:

- Spam Prevention
- Data Loss Prevention
- Content Filtering
- Attachment Blocking

- Security Risk Scan (advanced threat scan)
- Virtual Analyzer
- Web Reputation

In addition, ScanMail provides notifications and log queries to assist administrators to monitor and react to security risks.

TABLE 1-13. How ScanMail Protects the Microsoft Exchange Environment

FEATURE	DESCRIPTION
Spam Prevention	**Email Reputation** ScanMail includes Email Reputation, which allows you to block spam messages before they enter the network. **Content Scanning** ScanMail uses the Trend Micro spam engine and spam pattern file to screen out spam messages before they are delivered to the Information Store. Administrators can create approved and blocked senders lists if End User Quarantine is enabled. If End User Quarantine is enabled, end users can create their own lists of approved senders.
Data Loss Prevention	ScanMail can filter content for sensitive information in different message parts based on policies set by the administrator. ScanMail filters outgoing email messages and can perform specific actions on email messages that contain sensitive information.
Content Filtering	ScanMail can filter content in a message header, subject, body, and/or attachment based on policies set by the administrator. ScanMail filters incoming and outgoing email messages and can perform specific actions on email messages that contain undesirable content in the message body or attachments.
Attachment Blocking	ScanMail can block undesirable attachments according to administrator-defined types or specific names. During scanning, ScanMail can replace the detected file with a text message and then deliver the message to the intended recipient.

Feature	Description
Security Risk Scan	Security risk scan employs one of the following scan engines: • Security risk scan uses the latest version of the Trend Micro VSAPI scan engine to detect viruses/malware, spyware/grayware, worms, Trojans, and other malicious code. The Trend Micro scan engine uses pattern recognition and rule-based technologies to scan all incoming and outgoing messages for viruses/malware and other security risks in real time or on-demand. • Security risk scan uses the Advanced Threat Scan Engine (ATSE) which employs a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks. Administrators can configure ScanMail to send suspicious files to Virtual Analyzer for further analysis.
Web Reputation	ScanMail queries Trend Micro rating servers for the reputation rating when an email message with a URL in the message subject, body, or attachment arrives, before delivery to the information store. However, administrators can enable approved list to avoid scanning trusted URLs.
Real-time Scan	ScanMail guards possible virus/malware entry points with real-time scanning of all incoming and outgoing messages, SMTP messages, documents posted on public folders, and files replicated from other Microsoft Exchange servers. During real time scanning, ScanMail takes actions against security risks according to the administrator's configurations.

FEATURE	DESCRIPTION
Manual/Scheduled Scans	ScanMail performs manual and scheduled scanning on demand according to a manual prompt or schedule. On demand scanning eliminates viruses/malware from inside the Information Store databases, eradicates old virus/malware infections, and minimizes the possibility of reinfection. When performing a manual or scheduled scan, ScanMail takes actions against security risks depending on the administrator's configurations. ScanMail allows the selection of individual Stores for scanning. For example, you can use this option to provide security risk scan and content security for a particular storage groups' databases, rather than for all storage groups.
Alerts and notifications	ScanMail can send alerts about outbreaks and significant system events. Outbreak alerts notify administrators when the number of detected security risks exceeds a set number. This enables administrators to react quickly to security breaches in their Exchange environment.
Reports and logs	ScanMail provides logs and reports to keep administrators informed about the latest security risks and system status. ScanMail logs significant events such as component updates and scan actions. Administrators can query these events to create log reports providing current and detailed information about the security of the Exchange environment. ScanMail can generate reports for system analysis that can be printed or exported.

About Uncleanable Files

When ScanMail cannot successfully clean a file, it labels the file "uncleanable" and performs the user-configured action for uncleanable files. The default action is "Replace with text/file". ScanMail records all viruses/malware events and associated courses of action in the log file.

Some common reasons why ScanMail cannot perform the clean action are as follows:

- The file contains a Trojan, worm, or other executable program. To stop an executable from executing, ScanMail must completely remove it.
- ScanMail does not support the compression format used to compress the file. The scan engine only cleans files compressed using pkzip and only when the infection is in the first layer of compression.
- An unexpected problem prevents ScanMail from cleaning.

ScanMail Technology

The Trend Micro scan engine and spam engine detect viruses/malware and other security threats and screen out spam messages. These engines rely on the latest pattern files supplied by TrendLabs℠ and delivered through ActiveUpdate servers or a user-configured update source.

Trend Micro Scan Technology

ScanMail allows administrators to choose the level of malware detection that is appropriate for the company's security policy. Administrators configure the security level ScanMail provides by configuring the scan engine and any further analyses necessary.

The following table outlines the scanning technology available in ScanMail.

TABLE 1-14. Scanning Technology

SCAN TECHNOLOGY	DESCRIPTION
Virus Scan Engine	The standard malware scan engine available in ScanMail. The Virus Scan Engine employs pattern matching and heuristic scanning technology to identify threats before malware can infect a system.

SCAN TECHNOLOGY	DESCRIPTION
Advanced Threat Scan Engine (ATSE)	Advanced Threat Scan Engine performs aggressive heuristic scanning to check files for less conventional threats, including document exploits. Some detected files may be safe and should be further observed and analyzed in a virtual environment. Advanced Threat Scan Engine enhances the features provided by the Virus Scan Engine. For more information on Advanced Threat Scan Engine configuration, see *Configuring Security Risk Scan Targets on page 7-6*.
Virtual Analyzer	Virtual Analyzer performs content simulation and analysis in an isolated virtual environment to identify characteristics commonly associated with many types of malware. In particular, Virtual Analyzer checks if files attached to messages contain exploit code. Although many files do not include executable data, attackers find ways to cause such files to exploit vulnerabilities in programs and operating systems that run them. Because of this, sending malicious files to target users has become an effective way for attackers to compromise systems. **Note** Virtual Analyzer is a separately licensed product that provides unique security visibility based on Trend Micro's proprietary threat analysis and recommendation engines. ScanMail integrates with the Virtual Analyzer in Deep Discovery Advisor and Deep Discovery Analyzer. For more information on Virtual Analyzer settings, see *Configuring Virtual Analyzer on page 14-1*.

The Trend Micro Virus Scan Engine

At the heart of all Trend Micro antivirus products lies a proprietary scan engine. This engine has a long history in the industry and has proven to be one of the fastest.

The ScanMail scan engine is designed to work closely with the Virus Scanning Application Programming Interface (VSAPI) 2.6 and 2.5 available from Microsoft Exchange.

- VSAPI provides a virus-scanning implementation with high performance so that scanning occurs before a client can access a message or attachment. This low-level access facilitates the elimination of viruses/malware that file-level scanners cannot eliminate.
- VSAPI enables message scanning once before delivery, rather than multiple times as determined by the number of intended recipients, reducing processing time. This single-instance scanning also prevents re-scanning when a user copies a message.

The scan engine provides:

- Real-time multi-threaded scanning

  ScanMail performs all scanning in memory and is capable of processing multiple scan requests. When it receives multiple scan requests, it prioritizes and queues the requests that it cannot run immediately and runs the requests when resources become available. When a manual or scheduled scan is running and a client attempts to access a scannable object, ScanMail performs an immediate real-time scan.

  ScanMail supports SMTP real time email message scans.

- Non-redundant scanning

  When ScanMail completes a scan of an object, it logs the object as scanned. If you access the object again, ScanMail checks to see if it has already been scanned and does not scan it a second time.

Scan Engine Updates

Trend Micro periodically makes new scan engine versions available. New engines are released, for example, when:

- Trend Micro incorporates new detection technologies into the software
- A new, potentially harmful, virus/malware is discovered that cannot be handled by the current engine

- Scanning performance is enhanced
- Support is added for additional file formats, scripting languages, encoding, and/or compression formats

To view the version number for the most current version of the scan engine, visit:

http://www.trendmicro.com

To view the version of the scan engine that ScanMail is currently using, open the product console and view **Summary** > **System**.

Tip

Trend Micro recommends frequently updating your scan engine. Scheduled updates can be used to conveniently and regularly update ScanMail components.

The Trend Micro Pattern Files

The Trend Micro scan engine uses an external data file, called the virus pattern file, to identify the latest security risks.

You can view the most current version, release date, and a list of all the new definitions included in the file from the following website:

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

To view the version of the pattern file that ScanMail is currently using on your ScanMail server, open the product console and view **Summary** > **System**.

Tip

Trend Micro recommends frequently updating your pattern files. Scheduled updates can be used to conveniently and regularly update ScanMail components.

Pattern File Numbering

To allow you to compare the current pattern file in your software products to the most current pattern file available from Trend Micro, pattern files have a version number.

The pattern file numbering system uses 7 digits, in the format xx.xxx.xx.

For the pattern file number 1.786.01:

- The first digit (1) indicates the new numbering system. (The second of two digits in this segment of the pattern file identifier will not be utilized until the number increases from 9 to 10.)
- The next three digits (786) represent the traditional pattern file number.
- The last two digits (01) provide additional information about the pattern file release.

How the Scan Engine Works with the Pattern File

The scan engine works together with the pattern file to perform the first level of detection, using a process called pattern matching. When the engine finds a match, it sends a notification through an email message to the system administrator.

Note

The scan engine includes an automatic cleanup routine for old pattern files (to help manage disk space).

About ActiveUpdate

ActiveUpdate provides the latest downloads of all ScanMail components over the Internet.

ActiveUpdate does not interrupt network services, or require you to reboot your computers. ScanMail can receive updates on a regularly scheduled interval or through manual updates.

Incremental Updates of the Pattern File

ActiveUpdate supports incremental updates of the pattern file. Rather than download the entire pattern file each time, ActiveUpdate can download only the portion of the file that is new, and append it to the existing pattern file. This efficient update method can substantially reduce the bandwidth needed to update your antivirus software.

Configure ScanMail to use ActiveUpdate and incremental updates to decrease the time spent updating.

Using ActiveUpdate with ScanMail

You can configure ScanMail to use the ActiveUpdate server as a source for manual and scheduled component updates. When it is time for the component update, ScanMail polls the ActiveUpdate server directly. ActiveUpdate determines if an update is available, and ScanMail downloads the updates if they are available.

Tip

For a more efficient download in a multi-server environment, configure ScanMail to allow other servers to download updates from it. This makes ScanMail a virtual ActiveUpdate server for other servers in your environment that receive incremental updates.

IntelliScan™

IntelliScan optimizes scanning performance by examining file headers using true file type identification and scanning only file types associated with malware risks. With true file type identification, IntelliScan identifies files disguised using false extension types.

IntelliScan provides the following benefits:

- **Performance optimization**: Using minimal system resources, IntelliScan does not affect the performance of crucial applications running on the host.
- **Shorter scanning period**: Using true file type identification, IntelliScan only scans files vulnerable to infection, significantly reducing scan times.

IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering the network by blocking real-time compressed executable files and pairing them with other malware characteristics. Because IntelliTrap identifies such files as security risks and may incorrectly block safe files, consider quarantining (not deleting or cleaning) files after

enabling IntelliTrap. If users regularly exchange real-time compressed executable files, disable IntelliTrap.

IntelliTrap uses the following components:

- Virus Scan Engine
- IntelliTrap Pattern
- IntelliTrap Exception Pattern

Trend Micro ActiveAction™

ActiveAction identifies virus/malware types and recommends actions based on how each type invades a computer system or environment. ActiveAction categorizes malicious code, replication, and payload types as viruses/malware. When a scan detects a virus or malware threat, it takes the recommended action on the virus/malware type to protect the environment's vulnerable points.

Tip

Trend Micro recommends using ActiveAction for users who are not familiar with the available scan actions or are not sure which scan action is suitable for a certain type of virus/malware.

Using ActiveAction provides the following benefits:

- **Time saving and easy to maintain**: ActiveAction uses scan actions recommended by Trend Micro. Users do not have to spend time configuring the scan actions.
- **Updateable scan actions**: Virus/malware writers constantly change the way viruses/malware attack computers. Trend Micro updates ActiveAction settings in each new pattern file to protect clients against the latest threats and the latest methods of virus/malware attacks.

About Hot Fixes, Patches, and Service Packs

After an official product release, Trend Micro often develops hot fixes, patches, and service packs to address outstanding issues, enhance product performance, and add new features.

The following is a summary of the items Trend Micro may release:

- **Hot Fix**: a work-around or solution to customer-reported issues.
- **Patch**: a group of security patches suitable for deployment to all customers.
- **Service Pack**: significant feature enhancements that upgrade the product.

Your vendor or support provider may contact you when these items become available. Check the Trend Micro website for information on new hot fix, patch, and service pack releases:

http://www.trendmicro.com/download

All releases include a readme file that contains installation, deployment, and configuration information. Read the readme file carefully before performing installation.

Enterprise Protection Strategy

Trend Micro Enterprise Protection Strategy (EPS) was designed to help you manage all aspects of an outbreak life cycle, beginning with assessing a potential vulnerability and ending with restoration of systems after a threat is cleaned from your environment.

The Enterprise Protection Strategy is available for customers running Microsoft Windows.

Note

For the additional information on the Enterprise Protection Strategy, visit the Trend Micro website at:

http://www.trendmicro.com

Outbreak Prevention Services

Outbreak Prevention Services (OPS) are Trend Micro services that you can take advantage of using Control Manager. It allows enterprises to take proactive steps against new security risks before the necessary virus pattern files are available. By bridging the gap between threat notification and virus pattern delivery, enterprises can quickly contain virus outbreaks, minimize system damage, and prevent undue downtime.

OPS is a key component of the Trend Micro Enterprise Protection Strategy (EPS) - the culmination of a research initiative that identified best practices for preventing or deflecting potentially damaging virus attacks. This study was brought on by the apparent failure of conventional security measures to defend against new generation security risks, such as CodeRed and Nimda.

Trend Micro created Outbreak Prevention Services to address concerns at each stage of the life cycle. OPS harnesses the three core strengths of Trend Micro:

- Enterprise-class antivirus and content security products
- TrendLabs, the Trend Micro ISO-certified virus research and technical support center
- Partnerships with best-of-breed network security vendors and brings them together in a single powerful interface: Trend Micro Control Manager. With OPS, Control Manager provides answers to the following key security questions:
    - Am I under attack?
    - Can my system handle the attack?
    - How should I respond to the attack?

Chapter 2

Getting Started with ScanMail

This chapter explains how to register and activate ScanMail and describes the update process.

Topics include:

- *Getting Started on page 2-2*
- *Understanding the Product Console on page 2-2*
- *ScanMail Registration on page 2-9*
- *ScanMail Activation on page 2-11*
- *About ScanMail Updates on page 2-16*

Getting Started

After installing ScanMail, there are a number of tasks administrators can perform to ensure that everything is set up and working properly.

Procedure

1. Open the ScanMail product console.
2. Configure ScanMail to recognize an existing proxy server (if not completed during Setup).
3. Activate other ScanMail installed modules.
4. Register ScanMail to work with Trend Micro Control Manager™ (if not completed during Setup).
5. Perform an immediate update of ScanMail pattern files and scan engines.
6. Schedule automatic pattern file and scan engine updates.
7. Obtain the EICAR test file to confirm that the installation is working.

Understanding the Product Console

Access and control ScanMail through the intuitive product console. Use the product console to manage multiple Exchange servers and remote servers from any endpoint on the network. The ScanMail product console is password protected, ensuring that only

authorized administrators can modify ScanMail settings. Administrators can view the product console from any endpoint on the network that is running a supported browser.

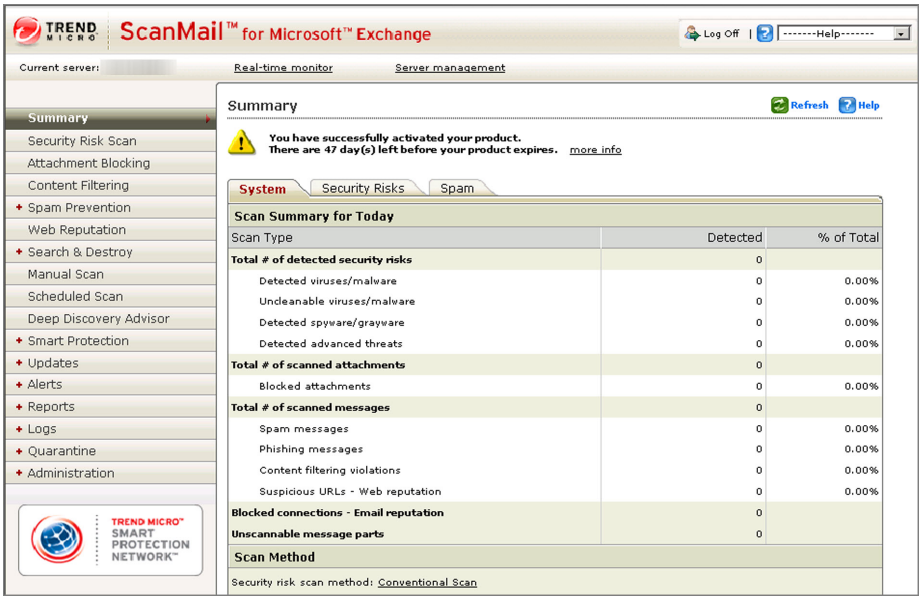


FIGURE 2-1. The product console

Viewing the Product Console on a Local Server

Procedure

1. Click **Start** > **Programs** > **Trend Micro ScanMail for Microsoft Exchange** > **ScanMail Management Console**.

   Note

   On Windows 2012 platforms, only a desktop shortcut is available.

2. Type the user name and password.

3. Click **Log on**.

Note

Use the account that belongs to **Management Group** configured during Setup to log on the ScanMail installations.

Viewing the Product Console from a Remote Server

Procedure

1. Use a supported browser to access:

   <http OR https>://<servername>:<portnumber>/smex

   Where "servername" is the name of the server with the ScanMail installation and "port number" is the port number used to access the server.

   Note

   By default, HTTP uses port 16372 and HTTPS uses port 16373.

2. Type the user name and password.
3. Click **Log on**.

Product Console Main View

The ScanMail web console has an intuitive user interface that provides easy access to all the functions needed to configure and manage ScanMail.

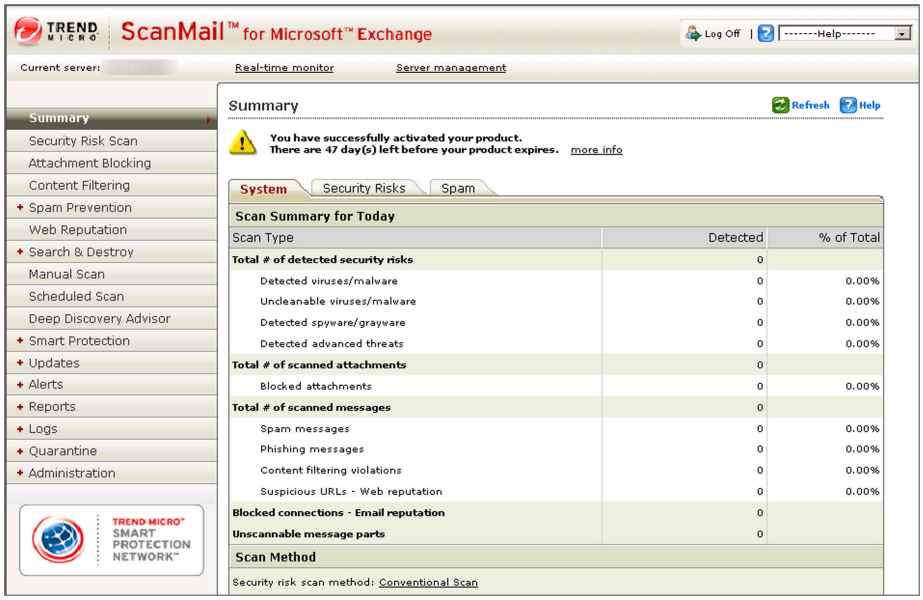


FIGURE 2-2. The product console

Product Console Elements

Banner

The banner identifies and describes the product and provides access to Trend Micro support.

FIGURE 2-3. Product console banner

The banner displays the following:

- **Current server**: The server you manage from this console
- **Real-time monitor**: Click to access the **Real-time Monitor**

  For more information, see *Understanding Real-time Monitor on page 4-2*.
- **Server management**: Click to access the **Server management** console

  For more information, see *Understanding the Server Management Console on page 4-4*.
- **Log Off**: Click to end your session and close the product console

  Note

  Logging off the product console prevents unauthorized users from modifying the settings.

- **Help**: Get support by selecting an option from the drop-down list

  Help options include:

  - **Contents and Index**: Opens the online help table of contents and index
  - **Knowledge Base**: Access the Knowledge Base to get the latest information about product troubleshooting and frequently asked questions
  - **Security Info**: Visit the Trend Micro Security Information page to read about the latest security risks
  - **Sales**: View the Trend Micro web page to find resellers and service providers in your area
  - **Support**: Access the Trend Micro technical support website
  - **About**: View ScanMail and component version numbers and ScanMail system information

Side Menu

The side menu provides access to the main menu items for ScanMail.

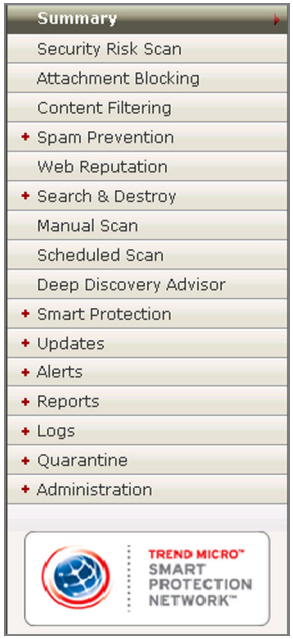


FIGURE 2-4. Product console side menu

Configuration Area

The configuration area allows administrators to configure and modify all ScanMail configurations and options.

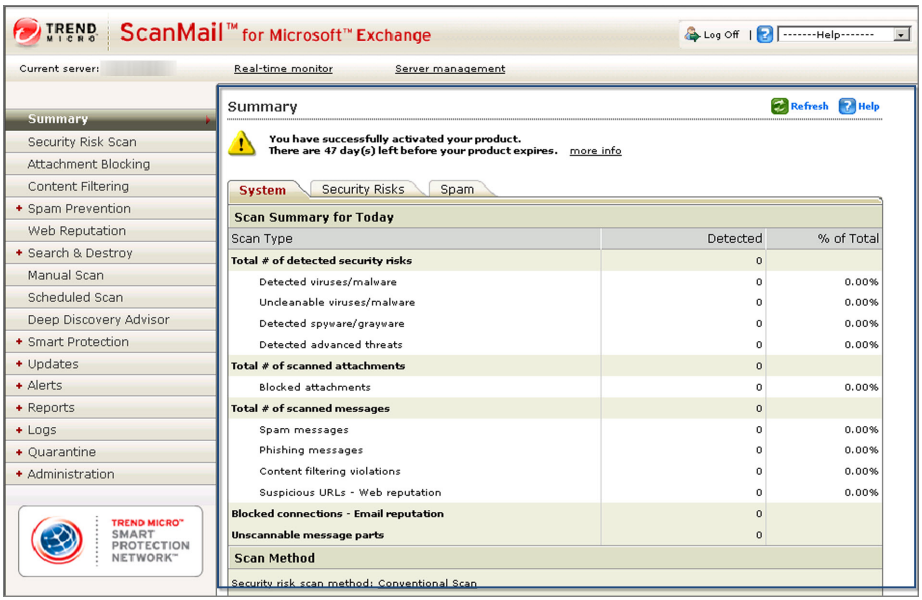


FIGURE 2-5. Product console configuration area

Getting Help While Using the ScanMail Product Console

ScanMail offers the following types of help:

Procedure

- To get help using ScanMail features, read the context-sensitive help. Access context-sensitive help by clicking the help icon (Help) or open the Table of Contents by selecting **Contents and Index** from the **Help** drop-down list in the banner area.

- To access troubleshooting and FAQ information, select **Knowledge Base** from the drop-down list in the banner area.
- To access general information about computer security threats and alerts, select **Security Info** from the drop-down list in the banner area.
- To get information about how to contact Trend Micro sales representatives or service providers, select **Sales** from the drop-down list in the banner area.

ScanMail Registration

The product package or Trend Micro reseller provides a Registration Key for ScanMail. Registering ScanMail entitles administrators to standard support and telephone and online technical support. The length of the maintenance agreement depends on the contract arranged with the Trend Micro representative, but is usually 12 months.

Administrators must register and activate ScanMail to enable updates (even when using an evaluation-version Activation Code).

Online Purchase

After completing an online purchase, Trend Micro sends licensing and registration information, including a number that is used during the product registration process. The number needed for registration is either a Serial Number or a Registration Key.

A Serial Number is 24 characters in length, including hyphens, in the following format:

XXXX-XXXX-XXXX-XXXX-XXXX

A Registration Key is 22 characters in length, including hyphens, in the following format:

XX-XXXX-XXXX-XXXX-XXXX

Most Trend Micro products use a Registration Key. When ready to register, go to the following Trend Micro website:

http://olr.trendmicro.com

Reseller Purchase

When you purchase ScanMail from a reseller, you receive a Registration Key with your product package or from your Trend Micro reseller. Registering ScanMail entitles you to standard support, which consists of pattern file updates, product version upgrades, and telephone and online technical support. The length of the maintenance agreement depends on the contract you arrange with your Trend Micro representative.

When you register, you receive an Activation Code that you can use to activate ScanMail.

Registering ScanMail

Use one of the following methods to register:

Procedure

- During installation

  The installation program prompts for an online registration using the Registration Key. Follow the link to the Trend Micro website, register the product, and then return to the installation program to complete the installation process.

- Online

  Visit the following Trend Micro website to register online and receive an Activation Code:

  http://olr.trendmicro.com

- Contact Trend Micro directly

  Provide a Trend Micro representative with the Registration Key to receive an Activation Code. Trend Micro maintains a list of North American contacts at:

  http://www.trendmicro.com/buy/us/enterprise.asp

Note

For maintenance renewal, contact Trend Micro sales or your reseller. Click **Update License** to manually update the maintenance expiration date on the **Product License** screen.

For more information, see *Contacting Technical Support on page 21-2*.

ScanMail Activation

The following conditions require activation.

- Installing ScanMail for the first time

  For example, after purchasing a product version from a Trend Micro reseller and using the registration key to obtain an Activation Code.

- Changing the version type

  For example, after obtaining a new Activation Code from a Trend Micro representative and using the product console to activate the new version.

Note

The evaluation version is fully functional for 30 days, after which ScanMail tasks continue to run, but no updates occur.

Activate ScanMail during installation or using the product console.

Activating ScanMail During Installation

Procedure

1. Run the installation program.
2. Type the Activation Code on the **Product Activation** screen.

3. Complete the installation to activate ScanMail.

Activating ScanMail Using the Product Console

Procedure

1. Click **Administration** > **Product License**.
2. Click **Upgrade Instruction** to register ScanMail.

   The Trend Micro website opens which allows online registration. Register online to obtain an Activation Code.
3. Click **New Activation Code** on the **Product License** screen.
4. Type the Activation Code in the space provided.
5. Click **Activate**.

Activation Codes

ScanMail has two types of Activation Code: standard and suite. Both of these have two types of maintenance agreements: evaluation and full. When you register ScanMail, you receive one Activation Code depending on whether you chose Standard or Suite and the evaluation or fully licensed version.

Note

Trend Micro recommends obtaining a new Activation Code before the expiry date to allow uninterrupted protection for your Exchange server(s). Contact a Trend Micro representative to renew your license agreement.

For example: You choose ScanMail Suite and decide to install the evaluation version. You download ScanMail Suite, register, and receive a suite evaluation Activation Code. When you provide the Activation Code, ScanMail suite evaluation service begins.

Tip

Run a pilot installation in a test environment using an evaluation version of ScanMail. When you decide to install the fully licensed version, use the experience gained from this cost-free evaluation.

Standard Activation Code

Using the standard Activation Code activates ScanMail.

TABLE 2-1. Standard Activation Code Features

MAINTENANCE AGREEMENT	STANDARD FEATURES
Evaluation	Using the evaluation Activation Code allows administrators to implement all ScanMail functions for a limited duration.
Fully licensed	A fully licensed Activation Code entitles administrators to the standard maintenance agreement and implements all ScanMail functions available for standard activations. ScanMail provides a warning when the license agreement is close to expiration.

Suite Activation Code

Using the suite Activation Code activates all the functions of the ScanMail Standard Activation Code plus content filtering, spam prevention, and End User Quarantine functions. In addition to scan engine and pattern file updates, you also receive spam engine and spam pattern file updates. Content filtering screens out undesirable content from email messages arriving at the Exchange server. The spam engine and spam pattern file work to prevent the delivery of spam messages to Exchange client mailboxes.

TABLE 2-2. Suite Activation Code Features

MAINTENANCE AGREEMENT	SUITE FEATURES
Evaluation	Using the evaluation Activation Code allows you to use ScanMail functions for a limited duration. During the evaluation period, ScanMail performs security risk scan, attachment blocking, content filtering, spam prevention, End User Quarantine, and web reputation functions, as well as scan engine and pattern file updates. Once such a code expires, you cannot reuse it. The expiring code disables any rules or other configuration settings that were created while it was in use. The expiration of one Activation Code does not affect another. For instance, if you are evaluating a product that has separate licensing for spam prevention, expiration of one license does not affect the other.
Fully licensed	A fully licensed Activation Code entitles you to standard maintenance agreement and allows you to implement the full functions of ScanMail. ScanMail warns you when your license agreement is close to expiration. When a full-version Activation Code expires, you can no longer download engine or pattern file updates. However, unlike an evaluation-version Activation Code, when a full-version Activation Code expires, all existing configurations and other settings remain in force. This provision maintains a level of protection in case you accidentally allow your license to expire.

Suite Activation Code with Additional Features

You can purchase or use a trial version of suite Activation Codes that provide additional licensing for features in ScanMail. These additional features are:

- **Email Reputation**: ScanMail provides Email Reputation features as a part of spam prevention. As the first line of defense, Trend Micro Email Reputation helps stop spam before it can flood your network and burden your system resources.
- **Data Loss Prevention**: Trend Micro Data Loss Prevention is a comprehensive software solution that helps organizations protect information from accidental disclosure and intentional theft. Through use of fully customizable, company-

specific policy creation, and pre-packaged regulatory templates, Data Loss Prevention helps companies manage, control, and monitor their sensitive information.

Activation Code Comparison

The following table illustrates the features available for each type of Activation Code.

TABLE 2-3. Features Available for Each Type of Activation Code

FEATURE	SUITE AC		STANDARD AC	
	FULL	TRIAL	FULL	TRIAL
Product console	Yes	Yes	Yes	Yes
Spam prevention, content filtering, and web reputation items on reports, logs, and quarantine manager	Yes	Yes	No	No
Security Risk Scan	Yes	Yes	Yes	Yes
Advanced Threat Scan Engine	Yes	Yes	Yes	Yes
Attachment Blocking	Yes	Yes	Yes	Yes
Spam Prevention: Content Scanning	Yes	Yes	No	No
Data Loss Prevention	Yes	Yes	No	No
Spam Prevention: Email Reputation	Yes	Yes	No	No
Content Filtering	Yes	Yes	No	No
Web Reputation	Yes	Yes	No	No
Manual Scan / Scheduled Scan	Yes	Yes	Yes	Yes
Smart Protection	Yes	Yes	Yes	Yes
ActiveUpdate	Yes	Yes	Yes	Yes
End User Quarantine	Yes	Yes	No	No
Control Manager Support	Yes	Yes	Yes	Yes

Feature	Suite AC		Standard AC	
	Full	Trial	Full	Trial
Search & Destroy	Yes	Yes	No	No
Virtual Analyzer	Yes	Yes	Yes	Yes

Reactivating ScanMail

Administrators may need to reactivate ScanMail when changing the product version. Reactivating involves changing the Activation Code from one number to another. After clicking **New Activation Code**, type the new Activation Code to receive all the benefits of the new ScanMail version.

Procedure

1. Click **Administration** > **Product License**.

   The **Product License** screen appears.

2. Click **New Activation Code**.

   The **Product License > New Activation Code** screen appears.

3. Type or paste the new Activation Code.

4. Click **Activate**.

   This activates the new version of ScanMail and enables all the functions available according to that license.

About ScanMail Updates

Security software can only be effective if it is using the latest technology. Since new viruses/malware and other malicious codes are constantly being released, it is crucial that you regularly update your ScanMail components to protect against new security threats.

ScanMail components available for updating are:

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

To find out if you have the latest components, view the ScanMail **Summary** screen from the product console. It shows your current version and lists the latest version available for download.

Updating ScanMail - Prerequisite Tasks

Procedure

1. Register your software.
2. If a proxy server handles Internet traffic on your network, you must set the proxy server information.
3. Configure your update method and source.
   - Methods include **Manual Update** and **Scheduled Update**.
   - Sources include the ActiveUpdate server, the Internet, the intranet UNC PATH, and Control Manager.

Updating Components on Clusters

You must install and configure ScanMail separately for each node of a cluster. All virtual servers on a node share the same components and update source. When a virtual server from one node has a failover to another node, then ScanMail will compare the components' versions and retain the most recent one. For this reason, when you check

the **Summary** screen for the component version after a failover, it may show a more recent update than before the failover happened.

Configuring Proxy Settings

Proxy servers are used for added security and more efficient use of bandwidth. If your network uses a proxy server, configure the proxy settings to connect to the Internet, download the updated components necessary to keep ScanMail updated, and check the license status online.

The following features use proxy servers:

- Smart Protection Network
- ActiveUpdate
- Product registration
- Web reputation
- World Virus Tracking

Procedure

1. Click **Administration** > **Proxy**.
2. Select **Use a proxy server for Web Reputation, updates, and product license notifications**. Select this check box to use a proxy server for web reputation queries to Trend Micro reputation servers, updates, and product license notifications.
3. Type the proxy server name or IP address.
4. Type the **Port**.
5. (Optional) Select **Use SOCKS 5 proxy protocol**.
6. If the proxy server requires authentication, specify the user name and password.

Configuring Manual Updates

Trend Micro recommends manually updating your scan engines and pattern files immediately after installing ScanMail or whenever there is an outbreak.

Procedure

1. Click **Updates** > **Manual**.
2. Select the component(s) that you want to update.
3. Click **Update**.

   ScanMail begins downloading the components and displays a progress bar that shows you the elapsed time and the percentage of the download remaining. ScanMail downloads the current components from the specified source.

Configuring Scheduled Update

Configure ScanMail to regularly check the update server and automatically download any available components. During a scheduled update, ScanMail checks the user specified download source for the latest components.

Tip

During times of outbreaks, Trend Micro responds quickly to update pattern files (updates can be issued more than once each week). Trend Micro also regularly updates the scan engine and other components. Trend Micro recommends updating components daily - or even more frequently in times of outbreaks - to help ensure ScanMail has the latest components.

Procedure

1. Select a source from which your updates will be downloaded.

   a. Click **Updates** > **Download Source**.

      The **Download Source** screen appears.

b. Select a download source.

c. Click **Save**.

2. Set up your schedule.

a. Click **Updates** > **Scheduled**.

b. Click **Enable schedule updates** to have ScanMail begin to update according to your schedule.

c. Set the **Update Schedule**.

i. Select an update frequency: by minutes, by hours, by days, or weekly.

ii. Set the start time for the schedule by selecting the hour and minute. Each time the update occurs, the download begins at this time.

3. Select the components for downloading from the update source.

a. Select the components that ScanMail downloads during each scheduled update.

Tip

When you select the check box at the top of the table, all components are selected.

b. Click **Save**.

ScanMail will begin downloading the selected components according to your schedule.

Configuring the Download Source

To keep ScanMail updated, you need to download the latest components. Use this page to set the source where ScanMail receives the latest components. The default location is the Trend Micro ActiveUpdate server. During manual or scheduled downloads, ScanMail checks the location you specify here, and downloads the latest components from that source.

Procedure

- **Trend Micro ActiveUpdate server**: Select this option to download from the default update server.

  Trend Micro uploads new components to the ActiveUpdate server as soon as they are available. Select the ActiveUpdate server as a source if you require frequent and timely updates.

- **Intranet location containing a copy of the current file**: Select this option to download from an Intranet location.

  Download components from an Intranet source that receives updated components.

  Type the Universal Naming Convention (UNC) path of another server on your network.

  Note

  Setting one or more centralized Intranet locations can greatly reduce network traffic and update time. This option is also useful when you do not want to connect an email server directly to the Internet. Instead, you can connect a front-end server to the Trend Micro ActiveUpdate server on the Internet and then set your back-end servers to receive updates from the front-end server.

- **Other update source**: Select this option to specify an update source different from the default. The update source must begin with "http://".

  Download components from an Internet or other source.

  You might choose to receive updates from a special server during testing. For example, when customers participate in Trend Micro beta testing, they type the name of the designated test server.

- **Allow other servers to download updates from this server**: Select this option to allow other ScanMail servers to download updates from this server.

  Click **Allow other servers to download updates from this server** to set ScanMail to create a duplicate copy of the update package on the current server. Normally, ScanMail only downloads components that the user has set it to download or the increments of the components that it needs. When you set ScanMail to duplicate

the update package, it will download all the components that are available for downloading.

For example: There are two Exchange servers (a and b) and each one has ScanMail installed. ScanMail is set up to update server "a" daily and download all components. ScanMail is set to update server "b" every week and download only the spam pattern component. Both servers receive updates from the Trend Micro ActiveUpdate server as required. Therefore, the components on these servers are not always identical and they require different incremental updates when they poll the ActiveUpdate server. Another, more efficient, way to configure your servers would be to set up server "a" to duplicate the update package. Then, you could set server "a" as the source for downloads for server "b", and server "b" could receive incremental updates from server "a" just as if server "a" was the ActiveUpdate server.

Note

You must duplicate the update package to clusters. That is, this option is grayed-out so that you must reproduce the components from one virtual server across all virtual servers on that node by default.

Rolling Back a Component Update

If ScanMail has downloaded the current components, but you want to use a previous component, you can manually roll back the component update.

Procedure

1. Stop the following ScanMail services:
   - ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail_RemoteConfig)
   - ScanMail for Microsoft Exchange Master Service (ScanMail_Master)
2. Delete all the files in the following folders:

   <Installation folder>\AU_Data\AU_Cache\

<Installation folder>\AU_Data\AU_Temp\

<Installation folder>\AU_Data\AU_Storage\

<Installation folder>\web\activeupdate\

3. Roll back the Smart Scan Agent pattern file, Virus pattern file, Spyware pattern file, IntelliTrap pattern file, and the IntelliTrap exception pattern file.

   a. Remove the most recently downloaded pattern files from this location:

      <Installation folder>\engine\vsapi\latest\pattern

   b. Remove the following files. Verify that ScanMail has already downloaded an older version of these files to which you can roll back.

      - The Smart Scan Agent pattern file:

        ex:icrc$oth.xxx

      - The Virus pattern file:

        ex:lpt$vpn.xxx

      - The Spyware pattern file:

        ex:ssaptn.xxx

      - The IntelliTrap pattern file:

        tmblack.xxx

      - The IntelliTrap exception file:

        tmwhite.xxx

      Where "xxx" refers to the latest pattern file download.

      For example: If you have recently downloaded Virus pattern file ex:lpt$vpn.345 and you want to roll back to a previous download pattern, ex:lpt$vpn.344, then delete ex:lpt$vpn.345 and ScanMail will begin to use ex:lpt$vpn.344.

   c. Delete all files in the following folders:

      <Installation folder\engine\vsapi\primary\pattern\

<Installation folder\engine\vsapi\secondary\pattern\

4. To roll back the anti-spam pattern file:

   a. Remove the latest pattern from following folder:

      <Installation folder>\engine\TMASE\latest\rule

      ex:tmxxxxxx.*

      "xxxxxx" means the latest version.

   b. Delete all files in the following folders:

      <Installation folder>\engine\TMASE\primary

      <Installation folder>\engine\TMASE\secondary

      <Installation folder>\engine\TMASE\latest\rule

      <Installation folder>\engine\TMASE\latest\cache

5. Restart the following ScanMail services:

   - ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail_RemoteConfig)
   - ScanMail for Microsoft Exchange Master Service (ScanMail_Master)

Rolling Back a Component Update in Cluster Environments

If ScanMail has downloaded the current components, but you want to use a previous component, you can manually roll back the component update.

Procedure

1. Take the ScanMail resource offline using the cluster management console.
2. Stop the following ScanMail services:

- ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail_RemoteConfig)
- ScanMail for Microsoft Exchange Master Service (ScanMail_Master)

3. Delete all the files in the following folders:

<Installation folder>\AU_Data\AU_Cache\

<Installation folder>\AU_Data\AU_Temp\

<Installation folder>\AU_Data\AU_Storage\

<Installation folder>\web\activeupdate\

4. Roll back the Smart Scan Agent pattern file, Virus pattern file, Spyware pattern file, IntelliTrap pattern file, and the IntelliTrap exception pattern file.

a. Remove the most recently downloaded pattern files from this location:

<Installation folder>\engine\vsapi\latest\pattern

b. Remove the following files. Verify that ScanMail has already downloaded an older version of these files to which you can roll back.

- The Smart Scan Agent pattern file:

  ex:icrc$oth.xxx

- The Virus pattern file:

  ex:lpt$vpn.xxx

- The Spyware pattern file:

  ex:ssaptn.xxx

- The IntelliTrap pattern file:

  tmblack.xxx

- The IntelliTrap exception file:

  tmwhite.xxx

Where "xxx" refers to the latest pattern file download.

For example: If you have recently downloaded Virus pattern file ex:lpt$vpn.345 and you want to roll back to a previous download pattern, ex:lpt$vpn.344, then delete ex:lpt$vpn.345 and ScanMail will begin to use ex:lpt$vpn.344.

c. Delete all files in the following folders:

<Installation folder\engine\vsapi\primary\pattern\

<Installation folder\engine\vsapi\secondary\pattern\

5. To roll back the anti-spam pattern file:

a. Remove the latest pattern from following folder:

<Installation folder>\engine\TMASE\latest\rule

ex:tmxxxxxx.*

"xxxxxx" means the latest version.

b. Delete all files in the following folders:

<Installation folder>\engine\TMASE\primary

<Installation folder>\engine\TMASE\secondary

<Installation folder>\engine\TMASE\latest\rule

<Installation folder>\engine\TMASE\latest\cache

6. Restart the following ScanMail services:

- ScanMail for Microsoft Exchange Remote Configuration Server (ScanMail_RemoteConfig)
- ScanMail for Microsoft Exchange Master Service (ScanMail_Master)

7. Repeat steps 2 to 6 for each server in the cluster.

8. Bring the ScanMail resource online using the PowerShell command below, or using the GUI. Right-click **"<SMEX_Resource_Name>"** then click **Bring this resource online**:

```
cluster.exe group <ClusteredMailboxServer_Group_Name> /
online
```

Chapter 3

Establishing and Maintaining Security for Your Exchange Servers

ScanMail was designed to provide comprehensive security for your complete Exchange environment. The following information gives an overview of the major security features of ScanMail and describes how to quickly establish and maintain a security baseline.

Topics include:

- *Establishing a Security Baseline on page 3-2*
- *Maintaining Security on page 3-3*
- *Managing Outbreak Situations on page 3-4*

Establishing a Security Baseline

When you have registered and activated ScanMail, you are ready to configure ScanMail features. Trend Micro recommends the following steps to establish a security baseline for your Exchange servers.

Procedure

1. Update ScanMail.

   When ScanMail is released it contains a Smart Scan Agent pattern file, scan engine, virus pattern file, spam engine, and spam pattern file that was available at the time. However, Trend Micro continuously updates pattern files and engines. Update these components immediately following installation to gain optimal protection for ScanMail. See *About ScanMail Updates on page 2-16*.

2. Verify that ScanMail is running and functioning correctly.

   From the web management console, click **Real-time monitor**. The Real-time monitor page opens and shows ScanMail activities in real time. When you can read **Real-time scan has been running since**, then you know ScanMail is running. See *Understanding Real-time Monitor on page 4-2*.

3. Perform a manual scan of your entire Information Store.

   Trend Micro recommends performing a manual scan of your entire Information Store following installation. When ScanMail detects viruses/malware or other malicious code it takes action against them according to Trend Micro defaults. The Trend Micro default action for viruses/malware is **clean**, or **quarantine** when it is unable to **clean**.

When the manual scan is complete, you have established a security baseline for your Exchange environment and you can start to focus on maintaining a secure environment.

Note

After installation and activation, ScanMail begins to protect your Exchange servers. ScanMail uses Trend Micro default values to filter undesirable content, block potentially harmful attachments, and scan for viruses/malware and other security threats in real time. When you are ready, customize ScanMail configurations to gain the optimal protection and efficiency for your network.

Maintaining Security

To maintain security on your Exchange servers, Trend Micro recommends the following:

TABLE 3-1. Maintaining Security

ACTION	BENEFIT
Scheduled updates	To ensure that ScanMail is always up-to-date, regularly update ScanMail components. To facilitate this, ScanMail allows you to configure scheduled updates. Scheduled updates check the Trend Micro update server according to the schedule you set and automatically download any available components.
Scheduled scans	Viruses/malware and other security threats can attack your Exchange servers from unexpected sources such as local unprotected computers and servers or by bypassing too lenient configurations. Run regular scheduled scans to significantly reduce this risk.
Enable action on mass-mailing behavior	Select **Enable action on mass-mailing behavior** from the Security Risk Scan Action screen to provide early warning of outbreaks.
Outbreak Alerts	When an attack occurs, it is vital that administrators receive early warning to prevent the attack from spreading. Trend Micro recommends setting ScanMail to send alerts to key network security professionals when outbreak conditions threaten your network. You can use Outbreak Alert to set ScanMail to automatically notify designated individuals.

ACTION	BENEFIT
Consider your overall security	ScanMail *for Microsoft Exchange* is designed to guard your Exchange mail servers. ScanMail does not provide protection to non-Exchange mail servers, file servers, desktops, or gateway devices. ScanMail protection is enhanced when used together with other Trend Micro products such as Trend Micro OfficeScan™ to protect your file servers and desktops, and Trend Micro InterScan VirusWall™ or InterScan™ Messaging Security Suite to protect your network perimeter. Visit the Trend Micro website for a more comprehensive list of solutions for all your network security needs. http://www.trendmicro.com/us/business/index.html
Exclude ScanMail folders from scans	File-based antivirus software usually allows you to set up folders to exclude from scanning. Trend Micro recommends setting up the following folders to exclude from scanning when using ScanMail with other antivirus software: • SMEX/storage/ • SMEX/temp • SMEX/debug **Note** These folder names are the names that ScanMail uses by default when it installs.

Managing Outbreak Situations

Outbreaks happen when viruses/malware, Trojans, worms, or other spyware/grayware suddenly attack many Exchange servers or personal computers on your network. There are many reasons why an attack might occur such as out-of-date components, poor configuration of anti-virus software, or a new malware arising for which there is not yet a pattern file. Outbreaks are a critical time when administrators must endure a chaotic, time-consuming process of communication, often to global and decentralized groups within their organizations.

The actions that administrators take when outbreaks happen can be broken down into four general stages:

1. Confirming that the security incident is a legitimate problem and not a false alarm
2. Responding to the security incident
3. Analyzing the security incident
4. Recovering the Exchange servers and mailboxes

ScanMail has some very useful features that can assist administrators in every stage of an outbreak. Consider the following features when an outbreak threatens:

1. To confirm that the security incident is truly a malware outbreak:
   - Check the Trend Micro website for virus/malware alerts and the latest security advisory information.

     http://www.trendmicro.com/vinfo/
   - Check ScanMail notifications. ScanMail can be configured to automatically send alerts when outbreak conditions exist. In addition, ScanMail can be configured to notify administrators or other designated individuals when ScanMail takes actions against detected threats.
   - For a quick analysis of the security incident, view the ScanMail **Summary** screen or create a one-time report. For more detailed information about the security incident, query ScanMail logs.
2. Responding
   - Manually update components to immediately download the latest ScanMail components.
   - Follow-up the update with a manual scan of the entire information store. Use the Trend Micro recommended defaults such as IntelliScan and ActiveAction or set even more aggressive scanning filters. If you know exactly what you are scanning for, select **Specified files** from the **Security Risk Scan** screen and type the name of the file for ScanMail to detect.
3. Analyzing

- Perform a Log Query to discover information about the attack. The log contains such useful information as the time and date, sender and receiver, and infected attachment names.
- If you need assistance to help analyze the security problem, send your virus/malware case to the Trend Micro Virus Response Service.

  http://www.trendmicro.com/us/enterprise/consulting-support-services/technical-account-management/index.html
- If you need more assistance, contact Trend Micro support. See *Contacting Technical Support on page 21-2*.

4. Recovering

   - When you have restored your Exchange environment, consider changing your configurations and security policies. Consider the following points:
     - Set ScanMail to back up files before taking action and then set very aggressive configurations. This allows ScanMail to detect and eliminate many threats without taking irreversible actions.
     - Monitor the results using the real-time monitor or by generating logs and reports.
     - Use the Server Management tool to quickly and easily replicate configurations from one secure and tested ScanMail server to another.

Chapter 4

Managing ScanMail

This chapter describes how to open and use the product console, and how to manage your ScanMail servers.

Topics include:

- *Understanding Real-time Monitor on page 4-2*
- *Understanding the Server Management Console on page 4-4*
- *Manually Creating a ScanMail Resource for Virtual Servers on page 4-10*
- *Starting and Stopping the Services on page 4-14*
- *Understanding ScanMail Icons on page 4-14*

Understanding Real-time Monitor

The Real-time monitor displays information about one Exchange server in real time. Administrators can view ScanMail scanning messages and the current count of any security risks detected on the server.

Use Real-time Monitor to monitor the local server, or any server connected to the network. This allows administrators to manage ScanMail servers from a centralized location.

Note

Details may be different depending on the Exchange version, server role, and license version.

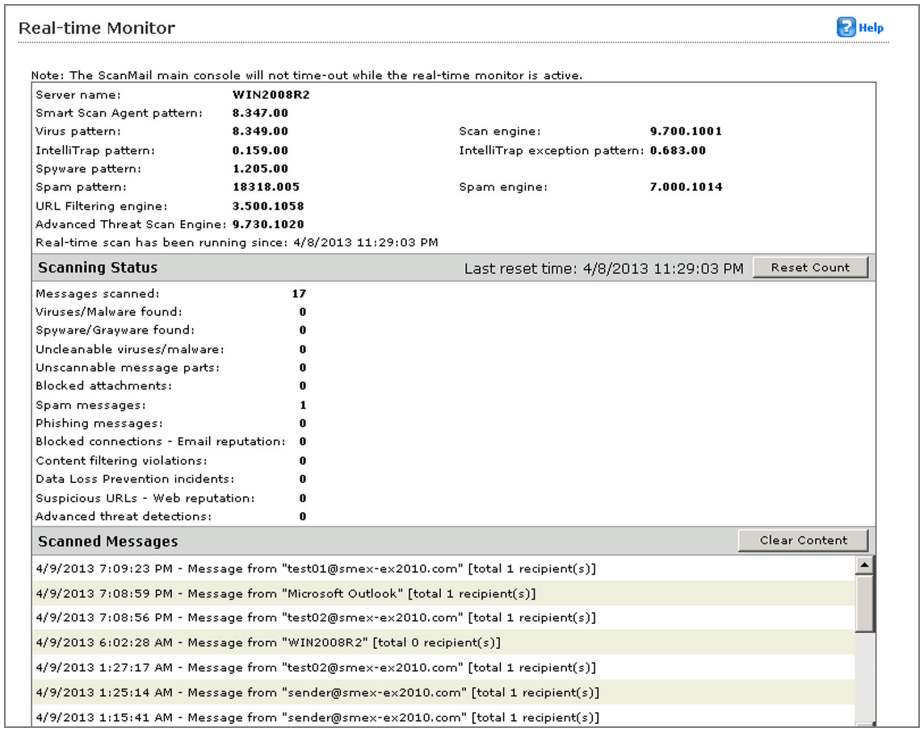


FIGURE 4-1. Real-time Monitor

A brief description of the options is available below.

- **Reset Count**: Resets all **Scanning Status** counts and messages scanned to zero and clears **Message Scanned** information
- **Clear Content**: Clears **Scanned Messages** information
- **Close**: Closes the screen

Viewing Real-time Monitor for a Remote Server

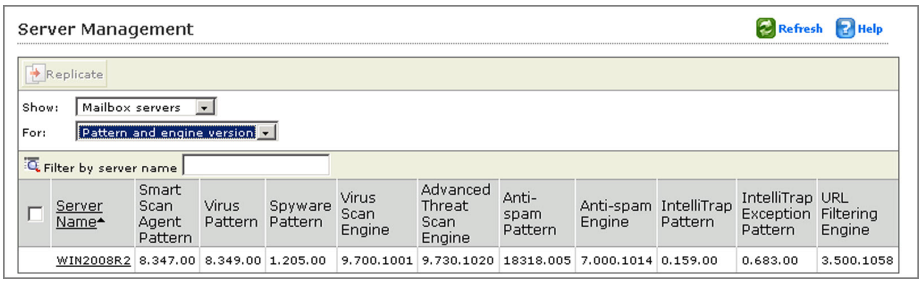
Procedure

1. Access the remote server using the product console.
2. Click **Real-time monitor** in the banner.

   The **Real-time Monitor** screen opens displaying information about the remote server.

Understanding the Server Management Console

The ScanMail Server Management console allows you to view all of the ScanMail servers on a network. You will only see servers with the same type of Activation Code. View all ScanMail servers in a forest when you install ScanMail with Exchange 2013, 2010, or 2007.



Server Name	Smart Scan Agent Pattern	Virus Pattern	Spyware Pattern	Virus Scan Engine	Advanced Threat Scan Engine	Anti-spam Pattern	Anti-spam Engine	IntelliTrap Pattern	IntelliTrap Exception Pattern	URL Filtering Engine
WIN2008R2	8.347.00	8.349.00	1.205.00	9.700.1001	9.730.1020	18318.005	7.000.1014	0.159.00	0.683.00	3.500.1058

FIGURE 4-2. The Server Management console

Activating Server Management

The **Server Management** console displays remote server status and allows you to replicate settings to remote servers. If you did not activate Server management during

the ScanMail installation process, you need to activate Server management before you use the Server management console.

Procedure

1. Log on the ScanMail server using an account with local administrator privileges.
2. Click the **Server management** link at the top of the product console.
3. Specify an existing group in Active Directory and the activation wizard prompts you through the steps required to activate Server Management.

Using the Server Management Console

Use the **Server Management** console to do the following:

TABLE 4-1. Server Management Console Features

FEATURE	DESCRIPTION
View pattern and engine version	View information about current scan engine, virus pattern file, spyware pattern, IntelliTrap pattern, IntelliTrap exception pattern, spam engine, URL Filtering engine, spam pattern, and Smart Scan Agent pattern files for remote ScanMail servers.
View scan results	View information about the total messages scanned and the scan results for remote ScanMail servers. Scanning results also shows the number of detected: • Security risks • Uncleanable Virus/ Malware • Advanced Threats • Blocked attachments • Spam • Data Loss Prevention • Content violations • Suspicious URLs • Messages Scanned • Unscannable message parts

Feature	Description
View scan status	Indicates whether the scan type is enabled or disabled. View the following scan status types for remote ScanMail servers: • Store security risk scan • Transport security risk scan • Store attachment blocking • Transport attachment blocking • Store content filtering • Transport content filtering • Spam prevention • Data Loss Prevention • Web reputation • Virtual Analyzer
View last replication	View the server name, status, and duration of the last replication.

FEATURE	DESCRIPTION
Replicate settings to remote servers	Replicate settings to one or multiple remote servers in the list. Administrators can choose to replicate All Settings, Overwrite server-dependent settings (such as quarantine and back up directories), or select from the Specified Settings below: • Security risk scan • Spam prevention • Data Loss Prevention • Manual scan • Smart Protection • Updates • Alerts • Reports • Logs • Administration (Proxy, Notification settings, Access Control, World Virus Tracking, Control Manager) • Special group • Internal domain • Product license • Attachment blocking • Web reputation • Data Loss Prevention templates • Scheduled scan • Virtual Analyzer • Content filtering
View Smart Protection status	View information about your Smart scan servers including the server name, scan service, scan setting, smart protection source, and server status.

Viewing Servers from the Product Console

You can administer one server at a time using the ScanMail product console.

Note

Use an account with local administrator privileges and/or an account that belongs to the ScanMail administrative group. Administrators can use an account that is part of the Active Directory group or any Active Directory group that is part of the Exchange forest that was used to activate Server Management.

Procedure

- From a local server:

  a. Click **Start** > **Programs** > **Trend Micro ScanMail for Microsoft Exchange** > **ScanMail Management Console**.

  > **Note**
  > On Windows 2012 platforms, only a desktop shortcut is available.

  b. Type your user name and password.

  c. Click **Enter**.

- From a remote server:

  Use a Java-enabled web browser that supports frames and access one of the following:

  http://<servername>:<portnumber>/smex

  https://<servername>:<portnumber>/smex

  Where:

  - `servername` is the name of the server on which you installed ScanMail
  - `port number` is the port number you use to access that computer

  > **Note**
  > By default, HTTP uses port 16372 and HTTPS uses port 16373.

Viewing Virtual Servers on a Cluster

Each Exchange virtual server is an independent management unit and must have its own configuration and log storage, no matter how many virtual servers are on one single cluster node. The product console should use the network name/IP address associated with the specified Exchange virtual server to control ScanMail operations on that server.

Each node has a ScanMail shortcut to allow you to view all virtual servers links. Click **All programs** > **Trend Micro ScanMail for Microsoft Exchange** > **ScanMail Management Console** to view all virtual servers.

Note

The virtual server links are not updated when you create or delete the ScanMail resource manually. At times components might appear out of date when viewing servers through the **Server Management** console. This is caused by a synchronization delay between the product console and the **Server Management** console. Wait a moment and the component version will refresh.

Using Server Management to Replicate Configurations

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.

Procedure

1. Click **Server management** to open the **Server Management** screen.
2. Select target servers.
3. Click **Replicate**.

   The **Replication Settings** screen appears.
4. Select the settings that you want to replicate:
   - Click **All settings** to replicate all the configurations to the target server(s)
   - Click **Specified settings** to set each configuration that you want to replicate individually

   Note

   The server on which you are currently logged on is the source for the replication.

5. Select the check box to overwrite server-dependent settings. When this check box is selected, ScanMail can copy directory paths that you have set for such folders as the quarantine and backup folders.

6. Click **Deploy**.

   A screen appears showing a progress bar and the ongoing status of the replication.

Manually Creating a ScanMail Resource for Virtual Servers

You can install ScanMail to virtual servers on clusters during installation. Once the installation is complete, you cannot install ScanMail on more servers using the Setup program. ScanMail does not support build upgrades in the cluster environment.

If you want to add virtual servers to a cluster and have the servers protected by ScanMail after the initial installation, you must first manually create a ScanMail resource for the new virtual servers.

Creating a Resource for Windows Server 2003

Procedure

1. Create a ScanMail resource by selecting the correct resource type:
   - Microsoft Exchange Server 2007 SCC: ScanMail for Exchange Cluster Agent for Single Copy Cluster
   - Microsoft Exchange Server 2007 CCR: ScanMail for Exchange Cluster Agent for MNS Cluster
2. Create a ScanMail resource on the server group for the target virtual server. The new resources will have a dependency on resource types. Refer to the following list of the ScanMail resource dependencies:
   - Microsoft Exchange Server 2007 SCC: Physical/Mount-point disk, network name, and Microsoft Exchange Information store

- Microsoft Exchange Server 2007 CCR: Network name and Microsoft Exchange Information Store

3. Disable the **Affect the group** option in the ScanMail resource properties.

   a. Right-click the ScanMail resource and then click **Properties** > **Advanced**.

   b. Clear the **Affect the group** check box.

4. Create a virtual directory using an Internet Information Services (IIS) web server to view reports about the target server on each node.

   Note

   The target virtual server must be on the current node.

   a. Navigate to **[computer name] SMEX Web Site** > **SMEX** > **[virtual directory]** to open the IIS.

   b. Create the virtual directory. Type the path directory as follows:

   <Shared Drive on the target server>:\SMEX\data\report

5. Create an account and mailbox for EUQ functions:

   EUQ_<Virtual Server Name>

Creating a Resource for Windows Server 2008, Exchange 2007 SCC Cluster

Procedure

1. Verify that the cluster resource type already exists or is registered by running the following PowerShell command:

   ```
   cluster restype
   ```

   You should see this resource type:

   ```
   ScanMail for Exchange Cluster Agent for Single Copy Cluster
   ```

2. Add the data path for ScanMail by running the command:

```
cluster.exe res "<SMEX_Resource_Name>" /create /
group:"<ClusteredMailboxServer_Group_Name>" /
type:"clusRDLL" /priv
SMEX_DATA_PATH="<share_disk_Data_path>"
```

3. Once the resource group has been successfully created, select and right-click the new **<SMEX_Resource_Name>** then click **Properties** > **Policies**.

4. Disable the **If restart is unsuccessful, fail over all resources in this service or application** option.

5. Add the dependencies for ScanMail using the PowerShell command, or using the graphics user interface (GUI) by right-clicking **"<SMEX_Resource_Name>"** then go to **Properties** > **Dependencies** > **Inserts**:

```
cluster.exe res "<SMEX_Resource_Name>" /
adddep:"<Network_Name>"
```

```
cluster.exe res "<SMEX_Resource_Name>" /
adddep:"<Share_Disk>"
```

```
cluster.exe res "<SMEX_Resource_Name>" /
adddep:"<Exchange_Information_Store_Instance>"
```

6. Bring the ScanMail resource online using the PowerShell command below, or using the GUI. Right-click **"<SMEX_Resource_Name>"** then click **Bring this resource online**:

```
cluster.exe group <ClusteredMailboxServer_Group_Name> /
online
```

Creating a Resource for Windows Server 2008, Exchange 2007 CCR Cluster

Procedure

1. Verify that the cluster resource type already exists or is registered by running the following in the command prompt:

```
cluster restype
```

You should see this resource type:

```
ScanMail for Exchange Cluster Agent for MNS Cluster
```

2. Create the ScanMail resource using this command:

```
cluster.exe res "SMEX-<EVS Name>" /create /group:"<EVS
Name>" /type:"clusRDLLCCR" /priv SMEX_DATA_PATH="C:\Program
Files\Trend Micro\Smex\CCRVSDB\<EVS Name>"
```

3. Add the resource dependency.

```
cluster.exe res "SMEX-<EVS Name>" /adddep:"Exchange
Information Store Instance (<EVS Name>)"
```

```
cluster.exe res "SMEX-<EVS Name>" /adddep:"Network Name
(<EVS Name>)"
```

4. Clear the **Affect the group** check box.

```
cluster.exe res "SMEX-<EVS Name>" /prop RestartAction=1
```

Creating a Resource for Exchange 2007 SCR Cluster

Procedure

1. Verify that the cluster resource type already exists or is registered by running the following in the command prompt:

```
cluster restype
```

You should see this resource type:

```
ScanMail for Exchange Cluster Agent for Single Copy Cluster
```

2. Create the ScanMail resource using this command:

```
cluster.exe res "SMEX-<EVS Name>" /create /group:"<EVS
Group>"/type:"clusRDLL" /priv SMEX_DATA_PATH="C:\Program
Files\Trend Micro\Smex"
```

3. Add the resource dependency.

```
cluster.exe res "SMEX-<EVS Name>" /adddep:"Exchange
Information Store Instance (<EVS Name>)"
```

```
cluster.exe res "SMEX-<EVS Name>" /adddep:"Network Name
<EVS Name>
```

4. Clear the **Affect the group** check box.

```
cluster resource "SMEX-<EVS Name>" /prop restartaction=1
```

Starting and Stopping the Services

ScanMail services may need to be started or stopped for procedures such as a manual rollback. You can start and stop services from the Microsoft Services console.

ScanMail adds the following services:

- **ScanMail for Microsoft Exchange Master Services**: The main ScanMail service
- **ScanMail for Exchange Remote Configuration Server**: For remote configuration

  Note

  This service is not added for ScanMail with Exchange Server 2013, 2010, and 2007 Edge Transport server roles.

- **ScanMail for Microsoft Exchange System Watcher**: Monitors logs for system events
- **ScanMail EUQ Monitor**: ScanMail adds this service if **End User Quarantine** was selected during installation

Understanding ScanMail Icons

The following table displays ScanMail icons.

TABLE 4-2. ScanMail Icons

ICON	DESCRIPTION
( ) Help	Click to view the ScanMail Help.
( ) Enabled	Click to disable a rule or policy. When this icon displays, the rule or policy is currently enabled.
( ) Disabled	Click to enable a rule or policy. When this icon displays, the rule or policy is currently disabled.
( ) Refresh	Click to refresh the information on the screen.
( ) Warning	This indicates a warning status.
( ) Enabled	This indicates an enabled status.
( ) Disabled	This indicates a disabled status.
( ) Delete	Click to delete a template.
( ) Tooltip	Mouse over this icon to see helpful information about a feature.
( ) Show details	Click to expand the drop-down.
( ) Hide details	Click to collapse the drop-down.

Part II

Configuring Scans and Scan Filters

Chapter 5

Understanding Smart Protection

This chapter discusses Trend Micro smart protection solutions and describes how to set up the environment required to use the solutions.

Topics include:

- *About Trend Micro Smart Protection on page 5-2*
- *Configuring Local Sources on page 5-7*
- *Scan Service Settings on page 5-8*

About Trend Micro Smart Protection

Trend Micro™ smart protection is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both local and hosted solutions to protect users whether they are on the network, at home, or on the go, using light-weight agents to access its unique in-the-cloud correlation of email, web and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services, and users access the network, creating a real-time neighborhood watch protection service for its users.

By incorporating in-the-cloud reputation, scanning, and correlation technologies, the Trend Micro smart protection solutions reduce reliance on conventional pattern file downloads and eliminate the delays commonly associated with desktop updates.

The Need for a New Solution

In the current approach to file-based threat handling, patterns (or definitions) required to protect endpoints are, for the most part, delivered on a scheduled basis. Patterns are delivered in batches from Trend Micro to agents. When a new update is received, the virus/malware prevention software on the agent reloads this batch of pattern definitions for new virus/malware risks into memory. If a new virus/malware risk emerges, this pattern once again needs to be updated partially or fully and reloaded on the agent to ensure continued protection.

Over time, there has been a significant increase in the volume of unique emerging threats. The increase in the volume of threats is projected to grow at a near-exponential rate over the coming years. This amounts to a growth rate that far outnumbers the volume of currently known security risks. Going forward, the volume of security risks represents a new type of security risk. The volume of security risks can impact server and workstation performance, network bandwidth usage, and, in general, the overall time it takes to deliver quality protection - or "time to protect".

A new approach to handling the volume of threats has been pioneered by Trend Micro that aims to make Trend Micro customers immune to the threat of virus/malware volume. The technology and architecture used in this pioneering effort leverages technology that off-loads the storage of virus/malware signatures and patterns to the cloud. By off-loading the storage of these virus/malware signatures to the cloud, Trend

Micro is able to provide better protection to customers against the future volume of emerging security risks.

Smart Protection Services

Smart protection includes services that provide anti-malware signatures, web reputations, and threat databases that are stored in-the-cloud.

Smart protection services include:

- **File Reputation Services**: File Reputation Services off-loads a large number of anti-malware signatures that were previously stored on agent computers to smart protection sources.

  For details, see *File Reputation Services on page 5-3*.

- **Web Reputation Services**: Web Reputation Services allows local smart protection sources to host URL reputation data that were previously hosted solely by Trend Micro. Both technologies ensure smaller bandwidth consumption when updating patterns or checking a URL's validity.

  For details, see *Web Reputation Services on page 5-3*.

File Reputation Services

File Reputation Services checks the reputation of each file against an extensive in-the-cloud database. Since the malware information is stored in the cloud, it is available instantly to all users. High performance content delivery networks and local caching servers ensure minimum latency during the checking process. The cloud-agent architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall agent footprint.

ScanMail must be in smart scan mode to use File Reputation Services.

Web Reputation Services

With one of the largest domain-reputation databases in the world, Trend Micro web reputation technology tracks the credibility of web domains by assigning a reputation

score based on factors such as a website's age, historical location changes and indications of suspicious activities discovered through malware behavior analysis. Web reputation then continues to scan sites and block users from accessing infected ones. Web reputation features help ensure that the pages that users access are safe and free from web threats, such as malware, spyware, and phishing scams that are designed to trick users into providing personal information. To increase accuracy and reduce false positives, Trend Micro Web reputation technology assigns reputation scores to specific pages or links within sites instead of classifying or blocking entire sites, since often, only portions of legitimate sites are hacked and reputations can change dynamically over time.

Web reputation helps deter users from following malicious URLs when the feature is enabled. Web reputation queries the assigned web reputation server for the reputation rating upon receipt of an email message with a URL in the message body or attachment. Depending on the configuration, Web Reputation can quarantine, delete, or tag the email message with URLs.

Tip

To save network bandwidth, Trend Micro recommends adding the enterprise internal web sites to the web reputation approved URL list. To save network bandwidth, Trend Micro recommends adding the enterprise internal web sites to the web reputation approved URL list.

Smart Protection Sources

Trend Micro delivers File Reputation Services and Web Reputation Services to ScanMail and smart protection sources.

Smart protection sources provide File Reputation Services by hosting the majority of the virus/malware pattern definitions. OfficeScan agents host the remaining definitions. The agent sends scan queries to smart protection sources if its own pattern definitions cannot determine the risk of the file. Smart protection sources determine the risk using identification information.

Smart protection sources provide Web Reputation Services by hosting web reputation data previously available only through Trend Micro hosted servers. The agent sends web reputation queries to smart protection sources to check the reputation of websites that a user is attempting to access. The agent correlates a website's reputation with the specific

web reputation policy enforced on the endpoint to determine whether access to the site will be allowed or blocked.

Trend Micro™ Smart Protection Network™

The Trend Micro™ Smart Protection Network™ is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. Smart Protection Network uses lighter-weight agents to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Smart Protection Server

The Smart Protection Server retains a repository of file reputation virus/malware threats and verified web reputation threats. The implementation of a Smart Protection Server reduces bandwidth usage and provides a higher level of privacy for companies. Smart Protection Servers verify all queries against their local reputation data.

There are two types of Smart Protection Servers:

- **Integrated Smart Protection Server**: An integrated Smart Protection Server installs alongside other Trend Micro products. ScanMail can leverage these pre-existing server resources without the need to expend further resources.
- **Standalone Smart Protection Server**: A standalone Smart Protection Server installs on a VMware or Hyper-V server. The standalone server has a separate management console and the ScanMail web console does not manage it.

Smart Protection Sources Compared

The following table highlights the differences between Smart Protection Network and Smart Protection Server.

TABLE 5-1. Smart Protection Sources Compared

BASIS OF COMPARISON	SMART PROTECTION SERVER	TREND MICRO SMART PROTECTION NETWORK
Availability	Available for internal agents, which are agents that meet the location criteria specified on the ScanMail web console	Available mainly for external agents, which are agents that do not meet the location criteria specified on the ScanMail web console
Purpose	Designed and intended to localize smart protection services to the corporate network to optimize efficiency	A globally scaled, Internet-based infrastructure that provides smart protection services to agents who do not have immediate access to their corporate network
Administration	ScanMail administrators install and manage these smart protection sources	Trend Micro maintains this source
Pattern update source	Trend Micro ActiveUpdate server	Trend Micro ActiveUpdate server
Agent connection protocols	HTTP and HTTPS	HTTPS

Smart Protection Pattern Files

File Reputation Services and Web Reputation Services use the smart protection pattern files. Trend Micro releases these pattern files through the Trend Micro ActiveUpdate server.

TABLE 5-2. Smart Protection Pattern Files

PATTERN FILE	DESCRIPTION
Smart Scan Agent Pattern	ScanMail downloads the daily updates to the Smart Scan Agent Pattern. When in smart scan mode, ScanMail uses the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, ScanMail leverages another pattern, called the Smart Scan Pattern.
Smart Scan Pattern	Smart protection sources download the hourly updates to the Smart Scan Pattern. ScanMail verifies potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources.
Web Blocking List	Smart protection sources download the Web Blocking List. ScanMail verifies a website's reputation against the Web Blocking List by sending web reputation queries to a smart protection source. ScanMail correlates the reputation data received from the smart protection source with the web reputation policy enforced on the computer. Depending on the policy, ScanMail will either allow or block access to the site.

Configuring Local Sources

Configure the local sources settings to use smart scan in Security Risk Scans.

Procedure

1. Click **Smart Protection** > **Local Sources** from the main menu.

   The **Local Sources** screen displays.

2. Click **Add**.

   The **Add Smart Protection Server** screen appears.

3. Type the **Server name or address** for the server you want to add.

4. Select **File Reputation service port** and type the port number for the Smart Protection Server providing file reputation services. Select **Web Reputation service port** and type the port number for the Smart Protection server providing web reputation services.

> **Tip**
>
> You can locate the port numbers of the Smart Protection Server by opening the server's web console and viewing the **Reputation Services Summary** screen.

5. For a Smart Protection Server providing file reputation services, optionally select to enable Secure Sockets Layer (**SSL**) protocol.
6. Click the appropriate test connection button to verify a successful connection to the server.
7. Click **Add**.

   The Smart Protection Server displays at the bottom of the Smart Protection Server List.
8. Specify the **Query order**:
   - **As listed**: Select to query the servers by priority.

     Specify the priority of the Smart Protection Servers by clicking the up and down arrows. ScanMail will send queries to the Smart Protection Servers based on the priority in this list.
   - **Random**: Select to query the servers randomly.
9. Click **Proxy Settings** and configure proxy settings if ScanMail requires a proxy for server communication with Smart Protection Server.
10. Click **Save**.

Scan Service Settings

A brief description of the Scan Service Settings (**Smart Protection** > **Scan Service Settings**) is available below.

TABLE 5-3. Scan Service Settings

SCAN TYPE	OPTIONS
Security Risk Scan	• **Conventional Scan**: Select the scan method used in previous ScanMail versions. All components used for security risk scans are stored locally on the ScanMail server. • **Smart Scan - File Reputation service**: Select the next-generation, in-the-cloud protection solution. At the core of this solution is an advanced scanning architecture that leverages threat signatures that are stored in the cloud. Install Smart Protection Servers on your network to further increase scan efficiency.

Web Reputation Services	• **Smart Protection Network**: Sends all web reputation queries to Trend Micro servers for verification.
	• **Smart Protection Server**: Verifies all web reputation queries locally. If the local server cannot verify the queries, the server sends them to Trend Micro servers for further analyses.
	  • **Do not make external queries to Smart Protection Network**: Restricts the local server from sending web reputation queries to Trend Micro servers.
	  Note
	  For Smart Protection Servers version 2.5 (or later), querying the Smart Protection Network is disabled. These Smart Protection Servers operate in Privacy mode. For details, see the *Smart Protection Server Administrator's Guide*.

Chapter 6

Configuring Scans

This chapter explains how to configure Real-time, Manual, and Scheduled scans to protect your Exchange environment.

Topics include:

- *About Scans on page 6-2*
- *Compressed File Handling on page 6-7*
- *About ScanMail Actions on page 6-10*
- *Notifications on page 6-23*

About Scans

ScanMail has three types of scans: real-time scans, manual scans, and scheduled scans. To protect your Exchange environment, ScanMail scans messages and their attached files, searching for security risks and undesirable data. When ScanMail makes a detection, ScanMail automatically takes action against the detection according to your configurations.

You can configure ScanMail to scan specific targets and configure actions for ScanMail to take when it discovers a security risk or undesirable data in the targeted messages or files. You can also configure ScanMail to send notifications when it takes actions against security risks and undesirable data.

You can configure ScanMail to backup a file to the Backup folder before taking action on it. This is a safety precaution designed to protect the original file from damage.

Note

Trend Micro recommends deleting backed up files once you have determined that the original file was not damaged and that it is usable after ScanMail has executed an action on it. If the file becomes damaged or unusable, send it to Trend Micro for further analysis.

Even if ScanMail has completely cleaned and removed the virus itself, some viruses damage the original file code beyond repair.

By default, ScanMail scans all scannable outgoing, incoming, and stored messages in your Exchange environment. Scannable files are all files except files that are encrypted, password protected, or exceed user-configured scanning restrictions. Scanning all files provides the maximum security possible. However, scanning every message requires a lot of time and resources and might be redundant in some situations. Therefore, consider limiting the files ScanMail includes in scans.

Real-time Scan

ScanMail scans the following in real time:

- All incoming and outgoing email messages

- SMTP messages arriving at Exchange from the Internet
- Public-folder postings
- All server-to-server replications

Trust Scan

Real-time scan can skip scanning email messages at the store level when the message has been scanned by ScanMail at the Hub Transport Level. This feature is available for ScanMail with Exchange Server 2010 and 2007.

Once ScanMail scans a message on an Edge or Hub Transport server, ScanMail adds scan information to the message. When the message reaches the Mailbox, ScanMail evaluates the scan information to prevent redundant use of resources. ScanMail only scans the message if the message was scanned with an older scan engine or pattern file or if ScanMail has not previously scanned the message.

Manual Scan

You can run a manual scan to ensure that ScanMail scans all messages in the Information Store once. Completely scanning the Information Store in this way minimizes the chance of infections from unexpected sources such as unprotected mail servers or improper configurations. Manual scanning scans the entire Information Store by default; however, you can configure ScanMail to scan any of the Mailbox Stores and Public Folder Stores. For clusters, ScanMail can scan each virtual server or all virtual servers on one node.

Note

If you have more than one storage group, you may want to disable scanning the replicated databases. Go to **Manual Scan** and change the databases selected for scanning.

You can perform security risk scan, attachment blocking, and content filtering through manual scanning. These filters are similar to those used during real-time scan, except some actions are not available during manual or scheduled scans.

You can specify the store database that belongs to a current virtual server. If manual scan is in progress, you cannot start a new Manual Scan process and ActiveUpdate does

not interrupt Manual Scan. However, if a Scheduled Scan is in progress, starting a Manual Scan stops the scheduled scan. Scheduled scan resumes according to its schedule.

Scheduled Scan

Scheduled Scan runs automatically on the appointed date and time. Use Scheduled Scan to automate routine scansand improve scan management efficiency.

Starting another scheduled scan does not interrupt the scheduled scan that is already in progress. ActiveUpdate does not interrupt a scheduled scan.

Scheduled Scan List

A brief description of the options is available below.

- **Add**: Click to add a new scheduled scan to the list.
- **Delete**: Click to delete scheduled scan tasks selected from the list.
- **Stop All Schedules**: Click to stop all scheduled scans whether they are currently running or in queue.
- **Enable**: Click to enable/disable a scheduled scan.

Note

When you use ScanMail with Exchange Server 2010 and 2007, Scheduled Scan is only available for clustered Mailbox servers, Combo Servers (Hub Transport and Mailbox server roles), and Mailbox server roles.

About Manual Scans and Scheduled Scans on Cluster Servers

Node-based Scanning

The Manual and Scheduled Scans are node based. This means, only one manual or scheduled scan can be run on one node at the same time.

Example: Virtual servers A and B are on node1; if one scanning task is running on A, then B cannot run a background scan at the same time.

Scans During a Failover or Following a Real-time Scan Change

During a failover period on clusters, the database of the Information Store will be unmounted and mounted by another node. After failover, manual or scheduled scan tasks stop. This is also true when the real-time scan status changes on the same node (as a result of enabling or disabling virus scanning, attachment blocking, or content filtering).

Example 1: Virtual servers A and B are on node1. If server A has a failover to node 2, the scan task running on server B will stop.

Example 2: Virtual servers A and B are on node1. If server A turns off real-time scanning (that is, disables all filters), the scan task running on server B will stop.

Manual and Scheduled Scan Settings

A brief description of the options is available below.

TABLE 6-1. Manual and Scheduled Scan Settings

SECTION	SETTINGS
Schedule **Note** Only available for Scheduled Scans.	Scan every: • **Day**: Select to perform a scan every day at a specific time. • **Week on**: Select to perform a scan every week on a specific day and time. • **Month on day**: Select to perform a scan every month on a specific date and time.

Section	Settings
Database Selection	• **All databases**: Select this to scan all databases including any databases you add after this setting is configured. • **Specific databases**: Select this to scan databases you specify. • **Refresh**: Click to display the latest Mailbox databases.
Public Folders **Note** Only available on Exchange 2013 servers.	• **Enable public folder scan**: Select this to scan the public folders on Exchange 2013 servers.
Scan Type Selection	• **Security risk scan**: Select this to scan for viruses/ malware and advanced threats, based on the configured settings. • **Attachment blocking**: Select this to perform a scan based on the attachment blocking settings. • **Content filtering**: Select this to perform a scan based on the content filtering settings. • **Data Loss Prevention**: Select this to perform a scan based on the Data Loss Prevention settings.

SECTION	SETTINGS
Incremental Scan Options: Selecting multiple check boxes creates "AND" relationships between those check boxes.	**Note** If all check boxes are clear, all messages in the database(s) you specify are scanned. • **Scan messages delivered**: Select this to scan messages delivered during a time period. • **Scan messages with attachments**: Select this to only scan messages with attachments. • **Scan messages that have not been scanned**: Select this to only scan messages that have not been previously scanned by ScanMail. **Note** When you use ScanMail with Exchange Server 2010 and 2007, Manual Scan is only available for clustered Mailbox servers, Combo Servers (Hub Transport and Mailbox server roles), and Mailbox server roles.
CPU Usage: This feature allows you to manage performance by limiting the resources that manual and scheduled scans use.	• **Enable CPU usage limitation**: Select to limit CPU usage and specify the maximum CPU percentage used.

Compressed File Handling

Compressed files provide a number of special security concerns. Compressed files can be password-protected or encrypted, can harbor so-called “zip-of-death” security risks, and can contain numerous layers of compression.

Compression Types

The ScanMail scan engine can extract and scan files compressed using any of the most popular compression types (listed below). ScanMail can also check for viruses/malware being "smuggled" within nested compressions, for example, an infected file that is zipped, ARJ-compressed, MS-compressed, and zipped again.

The maximum number of recursive scan layers is 20. You can configure this limit from **Security Risk Scan** > **Target** > **Scan Restriction Criteria**.

TABLE 6-2. Supported Compression Types

- Archive created by LHA (.lzh)
- Archive created by Pkzip (.zip)
- Archive created by RAR (.rar)
- Archive created by Tar (.tar)
- ARJ Compressed archive (.arj)
- BINHEX (.hqx)
- GNU Zip (.gz; .gzip)
- LZW/Compressed 16bits (.Z)
- MacBinary (.bin)
- Microsoft Cabinet (.cab)
- Microsoft Compressed/MSCOMP
- MIME (.eml; .mht)
- Teledisk format (.td0)
- Unix BZ2 Bzip compressed file (.bz2)
- UUEncode (.u)
- WinAce (.ace)

Blocking All Compressed Attachments

Consider configuring ScanMail to block all compressed files sent to clients. Users can be notified through their mail client that ScanMail blocked the attached file.

Procedure

1. Go to the Attachment Blocking Target tab.
   - For Manual or Scheduled Scans:

     [Scan type] > **Attachment Blocking** > **Target**
   - For Real-time Scans:

Attachment Blocking > **Global Policy** > **Target**

2. Click **Specific attachments**, then click **Attachment types** and expand the category.
3. Click **Compressed files**.
4. Click **Action** and select an action.
5. Click **Notification** and select a notification method.

Security Risk Scan Compressed File Restrictions

The following tables describes the compressed file restrictions available in ScanMail.

TABLE 6-3. Security Risk Scan Compressed File Restrictions

SETTING	DESCRIPTION
Decompressed file count exceeds	Type a number to configure a restriction for the number of decompressed files that ScanMail will scan. When the amount of decompressed files within the compressed file exceeds this number, then ScanMail only scans files up to the limit set by this option.
Size of decompressed files exceeds	Type a number that represents the size limit in MB. ScanMail only scans compressed files that are smaller or equal to this size after decompression.
Number of layers of compression exceeds	Type a number from 1-20. ScanMail only scans compressed files that have less than or equal to the specified layers of compression. For example, if you set the limit to 5 layers of compression, then ScanMail will scan the first 5 layers of compressed files, but not scan files compressed to 6 or more layers.

SETTING	DESCRIPTION
Size of decompressed file is "x" times the size of compressed file	ScanMail only scans compressed files when the ratio of the size of the decompressed file compared to the size of the compressed file is less than or equal to this number. This function prevents ScanMail from scanning a compressed file that might cause a Denial-of-Service (DoS) attack. A Denial-of-Service (DoS) attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing ScanMail from scanning files that decompress into very large files helps prevent this problem from happening.

About ScanMail Actions

The actions that ScanMail takes when scans detect viruses/malware, suspicious URLs, or undesirable content can include the following:

Note

Not all actions are available for every type of scan. For details about the actions available for a specific scan, refer to the configuration settings for the scan or refer to *Scan Actions by Scan Settings on page 6-13*.

TABLE 6-4. ScanMail Actions

ACTION	DESCRIPTION
Clean	Removes viral code from infected message bodies and attachments. The remaining email message text, any uninfected files, and the cleaned files are delivered to the intended recipient(s). **Tip** Trend Micro recommends using the default scan action "clean" for viruses/malware. Under some conditions, ScanMail cannot clean a file. These files are referred to as uncleanable. You can configure ScanMail to take a special action against these files when they are detected. During a manual or scheduled scan, ScanMail updates the Information Store and replaces the file with the cleaned one.
Replace with text/file	ScanMail deletes the attachment, infected, malicious, or undesirable content and replaces it with text or a file. The email message is delivered to the intended recipient, but the text replacement informs them that the original content was infected and was replaced. **Note** For Data Loss Prevention and content filtering, ScanMail does not perform this action in Transport level scans when the violation is in the header/subject of the email message.
Quarantine entire message	ScanMail moves the email message to a restricted access folder, removing it as a security risk to the Exchange environment. This option is not available in manual and scheduled scanning.

Action	Description
Quarantine message part	ScanMail moves the email message body or attachment to a restricted access folder, removing it as a security risk to the Exchange environment. ScanMail replaces the message part with the text/file you specify. **Note** For Data Loss Prevention and content filtering, ScanMail does not perform this action in Transport level scans when the violation is in the header/subject of the email message.
Backup	ScanMail backs up the message, delivers, and records the detection in logs. **Note** This action behaves the same as archive in previous versions of ScanMail.
Delete entire message	During real-time scanning, ScanMail deletes the entire email message.
Pass	ScanMail records the detection in a log and delivers the message unchanged.
Pass entire message	ScanMail records the detection in a log and delivers the message unchanged.
Pass message part	ScanMail records the detection in a log and delivers the message unchanged. **Note** For Data Loss Prevention and content filtering, this does not apply to low priority policies.

Action	Description
Tag and deliver	ScanMail adds a tag to the header information of the email message that identifies it as spam and then delivers it to the intended recipient.
Quarantine message to user's spam folder	ScanMail moves the email message to the Spam Mail folder located on the server-side of the Information Store.
Forward to sender's manager	Forward the email message to the sender's manager.
Forward to specific email address(es)	Forward the email message to the specific email address(es).

Scan Actions by Scan Settings

The following table lists the scan actions available for each scan filter type.

Table 6-5. Scan Actions by Scan Settings

Scan Setting	Available Actions
Security Risk Scan	
• ActiveAction	• Do not notify • Notify • Notify when uncleanable

Scan Setting	Available Actions
• Mass-mailing behavior	• Clean • Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part
• All security risks	• Clean • Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part

Scan Setting	Available Actions
• Viruses	• Clean • Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part
• Worms/Trojans	• Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part

Scan Setting	Available Actions
• Advanced Threats	• Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Replace with text/file **Note** Only available for Manual and Scheduled Scans. • Quarantine message part **Note** Only available for Manual and Scheduled Scans.
• Packed files	• Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part

Scan Setting	Available Actions
• Other malicious code	• Clean • Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part
• Spyware/ Grayware	• Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part
• Uncleanable files	• Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Pass • Quarantine message part

Scan Setting	Available Actions
Attachment Blocking	• Replace attachment with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Quarantine message part • Delete entire message • Notify • Do not notify

Scan Setting	Available Actions
Content Filtering	• Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Quarantine message part • Delete entire message • Backup • Pass message part • Pass entire message **Note** Only available for “Match all conditions” policies. • Forward to sender’s manager **Note** Not available for Manual and Scheduled Scans. • Forward to specific email address(es) **Note** Not available for Manual and Scheduled Scans. • Notify • Do not notify

Scan Setting	Available Actions
Data Loss Prevention	• Replace with text/file • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Quarantine message part • Delete entire message • Backup • Pass message part • Forward to sender's manager **Note** Not available for Manual and Scheduled Scans. • Forward to specific email address(es) **Note** Not available for Manual and Scheduled Scans. • Notify • Do not notify
Spam Prevention	
• Content Scanning: Spam	• Quarantine message to user's spam folder • Delete entire message • Tag and deliver • Pass

Scan Setting	Available Actions
• Content Scanning: Phishing Incident	• Quarantine message to user's spam folder • Delete entire message • Tag and deliver • Pass
Web Reputation	• Quarantine message to user's spam folder • Quarantine entire message **Note** Not available for Manual and Scheduled Scans. • Delete entire message • Tag and deliver • Pass • Notify • Do not notify

Advanced Scan Action Options

Configure advanced options to specify directories, message options, and further scanning.

TABLE 6-6. Scan Actions: Advanced Options

SETTING	DESCRIPTION

Macros	Advanced macro scanning supplements regular virus scanning. It uses heuristic scanning to detect macro viruses/ malware or strips all detected macro codes. Heuristic scanning is an evaluative method of detecting viruses that uses pattern recognition and rules-based technologies to search for malicious macro code.
	• **Heuristic level**
	  • Level 1 uses the most specific criteria, but detects the least macro codes.
	  • Level 4 detects the most macro codes, but uses the least specific criteria and may falsely identify safe macro code as harboring malicious macro code.
	• **Delete all macros detected by advanced macro scan**: ScanMail deletes all of the macro codes that it detects

Quarantine Settings / Quarantine Directory	The directory where ScanMail will save quarantined messages **Note** • ScanMail supports UNC paths (except on Exchange Edge servers) when configuring directory settings. The logged on user account must have full control permissions for the UNC path specified. • For security risk scans, configure the **Advanced threat quarantine directory** to specifically manage possible targeted attack threats.

SETTING	DESCRIPTION
Backup Settings / Backup Directory	The directory where ScanMail will save backup messages **Note** ScanMail supports UNC paths (except on Exchange Edge servers) when configuring directory settings. The logged on user account must have full control permissions for the UNC path specified.
Replacement Settings	The **Replacement file name** and **Replacement text** that ScanMail will use when a violation or incident occurs. ScanMail will replace the file/text with the replacement settings that you configure.
Forward Email Message Settings	The email address(es) and email message content that ScanMail forwards after detecting a violation or incident
Unscannable Message Parts	• Actions for encrypted and password protected files and files not in the scan restriction criteria • The **Replacement file name** and **Replacement text** that ScanMail will use when an unscannable message arrives. ScanMail will replace the file/text with the replacement settings that you configure.

Notifications

Administrators can configure ScanMail to send a notification by email message or SNMP when ScanMail takes action against security risks. Administrators can also automatically record notifications in the Windows Event Log.

Send notifications to:

- Warn the original user that their email message was altered
- Notify an administrator or other network security professional of a security risk
- Display information to the user about security risks and the actions taken

ScanMail gives you the option to append additional ScanMail fields to the default message or to create customized messages.

Tip

For correct resolution of ScanMail notifications with SNMP, you can import the Management Information Base (MIB) file to your network management tools from the following path in ScanMail Package: tool\admin\trend.mib.

Notification Settings

TABLE 6-7. Notification Settings

SETTING	DETAILS
Notify administrator	• **To**: Type the email address for the administrator. • **Subject**: Type the subject of the message to send to the administrator. • **Message**: Click on a message element and add it to the notification. Example: Click **[Time]** and add it to the message list. The notification message will contain the time when ScanMail took the action. • **Send consolidated notifications periodically**: ScanMail sends an email message that consolidates all the notifications for a period of time. Specify the period of time by typing a number in the box and selecting hour(s) or day(s). • **Send consolidated notifications by occurrences**: ScanMail sends an email message that consolidates notifications for a set number of filtering actions. Specify the number of security risk occurrences by typing a number in the box. • **Send individual notifications**: ScanMail sends an email message notification every time ScanMail performs a filtering action.

SETTING	DETAILS
Notify sender	• **Do not notify external sender(s)**: ScanMail will not send an email message notification to senders outside of the company network. • **Disable sender notification for spoofing mails**: ScanMail will not send an email message notification when the scan detects a spoofing message. **Note** This option is available for Security Risk Scan notifications only. • **Subject**: Type the subject of the message to send to the email message sender. • **Message**: Click on a message element and add it to the notification. Example: Click **[Time]** and add it to the message list. The notification message will contain the time when ScanMail took the action. • **Same notification that the internal senders receive**: Select when the message ScanMail sends to external senders is the same as the message it sends to internal senders. ScanMail sends a message just like the one customized for internal senders. • **Specify different notification below**: Select when you want to send a different customized message to an external sender. Then click on a message element and add it to the notification.

SETTING	DETAILS
Notify recipient(s)	• **Do not notify external recipient(s)**: ScanMail will not send an email message notification to senders outside of the company network. • **Subject**: Type the subject of the message to send to the recipient(s). • **Message**: Click on a message element and add it to the notification. Example: Click **Show details** and add it to the message list. The notification message will contain the time when ScanMail took action. • **Same notification that the internal recipients receive**: Select when the message ScanMail sends to external senders is the same as the message it sends to internal senders. ScanMail sends a message just like the one customized for internal senders. • **Specify different notification below**: Select when you want to send a different customized message to an external sender. Then click on a message element and add it to the notification.
SNMP	Select to send notifications by SNMP. Click to customize the SNMP message. • **IP address**: Type an IP address. • **Community**: Type the Community Name (Public or Private). • **Message**: Click on a message element and add it to the notification.
Write to Windows event log	Select to record the notification to a Windows event log.

Chapter 7

Configuring Security Risk Scans

This chapter explains how to configure Security Risk Scans to protect your Exchange environment.

Topics include:

- *About Security Risk Scans on page 7-2*
- *ScanMail Scan Hierarchy on page 7-3*
- *Security Risk Scan Actions on page 7-5*
- *Enabling Real-time Security Risk Scan on page 7-6*
- *Configuring Security Risk Scan Targets on page 7-6*
- *Configuring Security Risk Scan Actions on page 7-8*
- *Configuring Security Risk Scan Notifications on page 7-12*

About Security Risk Scans

ScanMail protects your Exchange environment by performing scans on all incoming and outgoing email messages. You can accept the Trend Micro default values set by the installation program or you can customize scanning by setting a number of configurations described in this chapter. You can configure ScanMail to run scans on-demand (manual scanning), according to a schedule (scheduled scanning), or in an ongoing and persistent manner (real-time scanning). You configure scans using the **Security Risk Scan** screen, accessible from the sidebar, or from the **Manual Scan** and **Scheduled Scan** screens.

The following describes the key characteristics of security risk scans:

TABLE 7-1. Security Risk Scan Characteristics

TYPE OF SCAN	CHARACTERISTICS
Scan method	There are two methods for security risk scans: • Conventional Scan • Smart Scan Configure the scan method on the **Scan Service Settings** screen (**Smart Protection** > **Scan Service Settings**). For details on scan methods, see *Scan Service Settings on page 5-8*.
Real-time scan	ScanMail scans the following in real time: • All incoming and outgoing email messages • Public-folder postings • All server-to-server replications

TYPE OF SCAN	CHARACTERISTICS
Manual scan and scheduled scan	During manual and scheduled scans, ScanMail scans messages stored in the mailbox and public folder stores. Starting another scheduled scan does not interrupt the scheduled scan that is already in progress. ActiveUpdate does not interrupt a scheduled scan. On cluster servers: Each virtual server has a scan task list. You can specify the store database that belongs to the current virtual server. When there is a running scheduled scan task, new tasks are queued. When another task is triggered at the same time, then the task will be queued and finished eventually.

ScanMail Scan Hierarchy

Administrators can configure security risk scans in ScanMail to provide varying levels of security. Enabling the Advanced Threat Scan Engine in conjunction with Virtual Analyzer assists in discovering and preventing targeted attacks by suspected malware threats.

The following table provides an overview of the scan engine hierarchy in ScanMail.

TABLE 7-2. Scan Engine Hierarchy

SCAN ENGINE	DESCRIPTION
Virus Scan Engine scanning	The Virus Scan Engine provides pattern-based and heuristic scanning for traditional malware threats.

Scan Engine	Description
ATSE scanning	ATSE enhances the traditional malware threat protection offered by the Virus Scan Engine. ATSE performs an aggressive scan using heuristic algorithms to identify possible targeted attacks, such as document exploits. For scan configurations that enable ATSE without sending files to Virtual Analyzer, ScanMail performs the action configured for **Advanced threats** on any suspicious messages and files detected as an advanced threat by ATSE. **Note** Some detected files may be safe. Trend Micro recommends selecting the **Quarantine entire message** action for suspected threats detected by ATSE. Perform an evaluation on files not sent to Virtual Analyzer to determine the actual threat of the quarantined files.
ATSE and Virtual Analyzer	After ATSE detects a suspected malware threat, ScanMail sends the message to Virtual Analyzer for further analysis. Virtual Analyzer assesses the risk level of the message in an isolated virtual environment and returns the threat rating to the ScanMail server. ScanMail then performs the action configured for **Advanced threats** if the security rating violates the configured security level for suspected threats.

About Advanced Threat Scan Engine

The Advanced Threat Scan Engine (ATSE) uses a combination of pattern-based scanning and heuristic scanning to detect document exploits and other threats used in targeted attacks.

Major features include:

- Detection of zero-day threats
- Detection of embedded exploit code
- Detection rules for known vulnerabilities

- Enhanced parsers for handling file deformities

Important

Because ATSE identifies both known and unknown advanced threats, enabling ATSE may increase the possibility of legitimate files being flagged as malicious.

Security Risk Scan Actions

ScanMail provides two basic settings for security risk scan: using ActiveAction or setting a customized action according to security risk type.

TABLE 7-3. Security Risk Scan Actions

SETTING	DESCRIPTION
ActiveAction	Select **ActiveAction** to have ScanMail perform Trend Micro recommended actions. Trend Micro recommends using ActiveAction when you are not familiar with scan actions or if you are not sure which scan action is suitable for a certain type of virus/malware.
Customized action for detected threats	Select **Customized action for detected threats** to instruct ScanMail to execute a customized action according to the type of detected threat. At the bottom of the screen, you can configure ScanMail to **Backup infected file before performing action**. This is a safety precaution designed to protect the original file from damage.

Using Customized Scan Actions

Use these actions when you want to optimize scanning for your environment.

Procedure

- When you want to protect your Exchange servers against a mass-mailing attack, select **Enable action on mass-mailing behavior** and select the action that

ScanMail executes whenever it detects a mass-mailing attack. This action overrides any other action for ScanMail. The real-time scanning default action is **Delete entire message**.

- When you want to configure ScanMail to use the same action against all detected security risks, select **All security risks** and accept the default action or select a customized action.
- When you want to configure a ScanMail action for each type of threat that ScanMail detects, select each threat type individually and configure the action ScanMail executes when it detects that threat type.

Enabling Real-time Security Risk Scan

Procedure

1. Click **Security Risk Scan** from the main menu.

   The **Security Risk Scan** screen appears.

2. Select **Enable transport level real-time security risk scan** from the **Security Risk Scan** screen.
3. For Exchange Server 2010/2007, select **Enable store level real-time security risk scan** from the **Security Risk Scan** screen.

Configuring Security Risk Scan Targets

Procedure

1. Go to the **Security Risk Scan** screen by navigating to one of the following:
   - For Real-time scans: **Security Risk Scan**
   - For Manual scans: **Manual Scan** > **Security risk scan**

- For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Security risk scan**

2. Go to the **Target** tab.

   The **Target** tab displays.

3. Select **Enable Advanced Threat Scan Engine** to allow ScanMail to perform aggressive scanning for less conventional threats and specify the **Scan level**.

   Tip

   Some detected files may be safe. Trend Micro recommends selecting the **Quarantine entire message** action for suspected threats detected by ATSE. Perform an evaluation on files not sent to Virtual Analyzer to determine the actual threat of the quarantined files. Selecting a higher scan level may result in a greater number of false positives.

4. Select one of the following for scanning:

   - **All attachment files**: ScanMail scans for viruses/malware, worms, Trojans, and other malicious code in all files except unscannable files. Unscannable files are password protected files, encrypted files, or files that exceed the user-defined scanning restrictions. Other malicious code describes previously unknown threat types for which you want to configure a ScanMail action.

   - **IntelliScan**: IntelliScan uses Trend Micro recommended settings to perform an efficient scan.

     Note

     There is one key difference between using IntelliScan and performing other scans using ScanMail true file type recognition. ScanMail true file type recognition allows users to define their own selection of files to scan, while IntelliScan always uses the Trend Micro recommended selection of files to scan.

   - **Specify file types**: Click the link to expand the list and select the files you want ScanMail to scan. These files are "true file types". The scan engine examines the file header rather than the file name to ascertain the actual file type. Or, select to create a list of file extensions by selecting **Specify file extensions**.

Note

For example: If you click **Specify file types** and then click **Application and executables** > **Executable (.exe; .dll, .vxd)** then ScanMail scans executable, DLL and VXD file types - even when the file has a false file extension name (is labeled .txt when it is actually an .exe). However, if you click **Specify file extensions** and type .exe, then ScanMail scans only .exe type files. ScanMail does not recognize falsely labeled file types.

5. To scan the message body, select **Scan message body**.
6. To use IntelliTrap technology, select **Enable IntelliTrap**.

   For details on IntelliTrap scanning, see *IntelliTrap on page 1-29*.
7. To scan for spyware/grayware, select **Select All** for **Spyware/Grayware Scan** or select from the list.
8. Click **Scan Restriction Criteria** if performance improvement is required.

   For details on compressed file restrictions, see *Security Risk Scan Compressed File Restrictions on page 6-9*.

   Tip

   Trend Micro recommends using scanning restrictions to protect against Denial-of-Service attacks. Denial-of-Service is an attack on a computer or network that causes a loss of 'service', namely a network connection. Typically, Denial-of-Service (DoS) attacks negatively affect network bandwidth or overload computer resources such as memory.
9. Click **Save**.

Configuring Security Risk Scan Actions

When ScanMail detects a file that matches your scanning configurations, it executes an action to protect your Exchange environment. The type of action it executes depends on the type of scan it is performing (real-time, manual, or scheduled), the server role in Exchange Server 2010 and 2007, and the type of actions you have configured for that scan.

Procedure

1. Go to the **Security Risk Scan** screen by navigating to one of the following:
   - For Real-time scans: **Security Risk Scan**
   - For Manual scans: **Manual Scan** > **Security risk scan**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Security risk scan**
2. Click the **Action** tab.

   The **Action** tab displays.
3. Select one of the following:
   - **ActiveAction**: Perform scan actions recommended by Trend Micro.
   - **Customized action for detected threats**: Select to perform an action over all security risks or specify an action for each threat.

   Note

   To configure the scan action that ScanMail performs on **Advanced threats**, administrators must enable the Advanced Threat Scan Engine on the **Security Risk Scan: Target** tab.

   For details on Security Risk Scan actions, see *Security Risk Scan Actions on page 7-5*.
4. To back up the infected file, select **Backup infected file before performing action**.
5. Select **Do not clean infected compressed files to optimize performance**. if performance improvement is required.
6. Configure **Advanced Options** as necessary.

   Note

   For details on advanced scan actions, see *Advanced Scan Action Options on page 6-21*.

a. Click the **Macros** heading to configure macro scan.

   i. Select **Enable advanced macro scan**.

   ii. Select one of the following:

   Select one of the following:

   - **Heuristic level**
   - **Delete all macros detected by advanced macro scan**

Note

For details on conifguring macro scanning, see *Configuring Macro Scanning on page 7-10*.

b. Click the **Unscannable Message Parts** heading to specify actions for encrypted and password protected files and files not in the scan restriction criteria.

c. Click **Quarantine and Backup Settings** to specify the directory paths.

d. Click **Replacement Settings** to configure the text or file name that replaces infected content.

7. Click **Save**.

Configuring Macro Scanning

ScanMail uses the virus pattern file to identify known malicious macro codes during regular virus scanning. ScanMail takes action against malicious macro code depending on the action that you configure from the **Security Risk Scan** screen. Use advanced macro scanning to gain additional protection against malicious macro code.

Advanced macro scanning supplements regular virus scanning. It uses heuristic scanning to detect macro viruses/malware or strips all detected macro codes. Heuristic scanning is an evaluative method of detecting viruses that uses pattern recognition and rules-based technologies to search for malicious macro code. This method excels at detecting undiscovered viruses and security risks that do not have a known virus signature. When

a malicious macro code is detected using heuristic scanning, ScanMail takes action against the malicious code based on the action that you configured from the **Security Risk Scan** screen. When you select **Delete all macros detected by advanced macro scan**, then ScanMail strips all macro code from the scanned files.

Procedure

1. Go to the **Security Risk Scan** screen by navigating to one of the following:
   - For Real-time scans: **Security Risk Scan** > **Action**
   - For Manual scans: **Manual Scan** > **Security risk scan** > **Action**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Security risk scan** > **Action**
2. Click **Advanced Options** and then click **Macros**.
3. Select **Enable advanced macro scan**.
4. Select a detection type:
   a. Select **Heuristic level** and configure a level for the heuristic rules.
      - Level 1 uses the most specific criteria, but detects the least macro codes.
      - Level 4 detects the most macro codes, but uses the least specific criteria and may falsely identify safe macro code as harboring malicious macro code.

      Tip

      Trend Micro recommends a heuristic scan level of 2. This level provides a high detection level for unknown macro viruses, a fast scanning speed, and it uses only the necessary rules to check for macro virus/malware strings. Level 2 also has a low level of falsely identifying malicious code in safe macro code.

   b. Select **Delete all macros detected by advanced macro scan** to have ScanMail delete all of the macro codes that it detects.
5. Click **Save**.

Configuring Security Risk Scan Notifications

Procedure

1. Go to the **Security Risk Scan** screen by navigating to one of the following:
   - For Real-time scans: **Security Risk Scan**
   - For Manual scans: **Manual Scan** > **Security risk scan**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Security risk scan**
2. Click the **Notification** tab.

   The **Notification** screen displays.
3. Click the check boxes corresponding to the people ScanMail will notify.
4. Click **Show details** to customize the notification for that recipient.
5. Select from the notification options.

   Refer to *Notification Settings on page 6-24* for details.
6. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
7. Click **Save**.

Chapter 8

Configuring Attachment Blocking

This chapter explains how to configure Attachment Blocking to protect your Exchange environment.

Topics include:

- *About Attachment Blocking on page 8-2*
- *Enabling Real-time Attachment Blocking on page 8-3*
- *About the Attachment Blocking Global Policy on page 8-3*
- *Adding an Exception to the Attachment Blocking Global Policy on page 8-6*
- *Editing an Attachment Blocking Exception on page 8-8*

About Attachment Blocking

Attachment blocking prevents email messages containing suspicious attachments from being delivered. ScanMail can block attachments according to the following:

- Attachment type
- Attachment name
- Attachment extension
- Suspicious URL detection

After detecting a suspicious attachment, ScanMail can then replace, quarantine, or delete all the messages that match a policy rule. Blocking can occur during real-time, manual, and scheduled scanning.

The extension of an attachment identifies the file type, for example .doc, .exe, or .dll. Many viruses/malware are closely associated with certain types of files. By configuring ScanMail to block according to file type, administrators can decrease the security risk to Exchange servers from those types of files. Similarly, specific attacks are often associated with a specific file name.

Note

Using attachment blocking is an effective way to control virus/malware outbreaks. Administrators can temporarily quarantine all high-risk file types or those with a specific name associated with a known virus/malware. After the outbreak ends, administrators can examine the quarantine folder and take action on detected files.

Recipients for messages can match one attachment blocking exception or the attachment blocking global rule based on priority. If the recipient matches an attachment blocking exception, then targets selected in the exception are excluded from attachment blocking global rule. If the recipient does not match any attachment blocking exceptions, then the attachment blocking global rule is applied.

Four types of accounts are supported for customizing specified Recipients: Active Directory users, Active Directory contacts, Active Directory distribution groups and special groups.

For each attachment blocking exception, administrators can specify selected accounts and excluded accounts. The exception applies to those accounts that belong to selected accounts but does not apply to those that belong to the excluded accounts. For example, Active Directory Group1 contains ADuser1 and ADuser2. When selected accounts includes "AD Group1", excluded accounts include "ADuser1", then the policy only applies to ADuser2.

Enabling Real-time Attachment Blocking

When attachment blocking is enabled, you can enable and disable individual attachment blocking exceptions. The green check icon ( ) indicates the exception is enabled, and the red "x" ( ) indicates the exception is disabled. Click the icon to toggle between enabled and disabled.

Note

You cannot disable the Global Policy.

Procedure

1. Click **Attachment Blocking** on the main menu.

   The **Attachment Blocking** screen displays.

2. Select **Enable transport level attachment blocking**.

3. Select **Enable store level attachment blocking** (Exchange Server 2010 and 2007).

4. Click **Save**.

About the Attachment Blocking Global Policy

The attachment blocking Global Policy applies to all incoming and outgoing email messages. You can configure the Global Policy to automatically block email messages with attachments by file type or by file name.

You can also create attachment blocking exceptions to allow specific accounts to send and receive email messages with the attachments specified in the Global Policy when certain users have different privilege requirements.

Configuring Attachment Blocking Targets

You can block attachments according to a specific name or according to an attachment type. ScanMail determines attachment type by the file name extension and true file type. Block attachments with two general strategies: either block all attachments and then exclude specified attachments or specify all the attachments to block.

Procedure

1. Go to the **Attachment Blocking** screen by navigating to one of the following:
   - For Real-time scans: **Attachment Blocking** > **Global Policy**
   - For Manual scans: **Manual Scan** > **Attachment Blocking**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Attachment Blocking**
2. Click the **Target** tab.

   The **Target** screen displays.
3. Select from one of the following:
   - **All attachments**
     - Select **Attachment types to exclude** and/or **Attachment names to exclude**. Click **Show details** to specify specific types or names.
   - **Specific attachments**
     - Select **Attachment types** and/or **Attachment names**. Click **Show details** to specify specific types or names.
4. Select **Block attachment types or names within compressed files**.
5. Click **Scan Restriction Criteria** if performance improvement is required.

- **Number of layers of compression exceeds**: Specify a number from 1 to 20 to use as the threshold for not scanning compression files. If the number of compression layers exceeds the specified number, the file is not scanned.

6. Click **Save**.

Configuring Attachment Blocking Actions

ScanMail performs an action whenever it detects an attachment that requires blocking. You configure the action ScanMail performs using this screen. Additionally, configure whether or not ScanMail sends a notification.

Procedure

1. Go to the **Attachment Blocking** screen by navigating to one of the following:
   - For Real-time scans: **Attachment Blocking** > **Global Policy**
   - For Manual scans: **Manual Scan** > **Attachment Blocking**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Attachment Blocking**
2. Click the **Action** tab.

   The **Action** screen displays.
3. Select an action for ScanMail to take when it detects undesirable content.

   For details on the available actions, see *About ScanMail Actions on page 6-10*.
4. Configure **Advanced Options** as necessary.

   For details on advanced scan actions, see *Advanced Scan Action Options on page 6-21*.
5. Click **Save**.

Configuring Attachment Blocking Notifications

Procedure

1. Go to the **Attachment Blocking** screen by navigating to one of the following:
   - For Real-time scans: **Attachment Blocking** > **Global Policy**
   - For Manual scans: **Manual Scan** > **Attachment Blocking**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Attachment Blocking**
2. Click the **Notification** tab.

   The **Notification** screen displays.
3. Click the check boxes corresponding to the people ScanMail will notify.
4. Click **Show details** to customize the notification for that recipient.
5. Select from the notification options.

   Refer to *Notification Settings on page 6-24* for details.
6. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
7. Click **Save**.

Adding an Exception to the Attachment Blocking Global Policy

Procedure

1. Click **Attachment Blocking** on the main menu.

   The **Attachment Blocking** screen displays.

2. Click **Add Exception**.

   The **Select Accounts** screen displays.

3. Select the accounts to exclude from the Global Policy.

   - **From specific sender(s) to any recipient**
   - **From any sender to specific recipient(s)**.

4. Click the **specific sender(s)** or **specific recipient(s)** link (if applicable).

5. Select one of the following:

   - **Anyone**: Apply this policy or exception to all users.
   - **Specific accounts**: Select from Active Directory groups or ScanMail special groups.

6. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list.

7. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list on the **Exclude Accounts** screen.

8. Click **Save**.

   The **Select Accounts** screen displays.

9. Click **Next >**.

   The **Specify Policy** screen displays.

10. Configure the following settings:

    - **Attachment types**: Select specific file types to exclude from the Global Policy.
    - **Attachment names**: Specify file names and/or extensions to exclude from the Global Policy.

    Note

    Click **Show details** to specify file types or names.

11. Click **Next >**.

    The **Name and Priority** screen displays.

12. Configure the following settings:

    - **Enable this exception**: Select to enable this exception.
    - **Exception name**: Type a name for this exception.

13. Type a number for the **Priority**.

14. Click **Save**.

Editing an Attachment Blocking Exception

Procedure

1. Click **Attachment Blocking** on the main menu.

   The **Attachment Blocking** screen displays.

2. Click the exception **Accounts** or **Policy** hyperlink to edit an exception.

3. Configure the following settings:

   - **Enable this exception**: Select to enable this exception.
   - **Exception name**: Type a name for this exception.

4. Click the **Accounts** tab.

   a. To change the accounts to exclude from the Global Policy, select an account type:

      - **Specific sender(s)**
      - **Specific recipient(s)**

Note

ScanMail only applies the policy to the accounts selected for the **Accounts** type. If you select accounts for a different account type, ScanMail does not apply the policy to the previous accounts selected.

b. Click the **Edit** link in the tables to change the included accounts and excepted accounts for this policy.

c. Select one of the following:

- **Anyone**: Apply this policy or exception to all users.
- **Specific accounts**: Select from Active Directory groups or ScanMail special groups.

d. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list.

e. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list on the **Exclude Accounts** screen.

f. Click **Save**.

5. To change the targeted attachment settings, click the **Target** tab.

- **Attachment types**: Select specific file types to exclude from the Global Policy.
- **Attachment names**: Specify file names and/or extensions to exclude from the Global Policy.

Note

Click **Show details** to specify file types or names.

6. Click **Save**.

Chapter 9

Configuring Content Filtering

This chapter explains how to configure Content Filtering to protect your Exchange environment.

Topics include:

- *About Content Filtering on page 9-2*
- *Enabling Real-time Content Filtering on page 9-3*
- *Global Settings on page 9-4*
- *Configuring Content Filtering Policies on page 9-4*
- *Configuring a Content Filtering Exception on page 9-13*
- *Editing a Content Filtering Policy on page 9-14*

About Content Filtering

The content filter evaluates inbound and outbound messages on the basis of user-defined policies. Each policy contains a list of keywords and phrases. Content filtering evaluates the header and/or content of messages by comparing the messages with the list of keywords. When ScanMail finds a word that matches a keyword it can take action to prevent the undesirable content from being delivered to Exchange clients. ScanMail can send notifications whenever it takes an action against undesirable content.

ScanMail applies the content filtering policies to email messages according to the order shown in the Content Filtering screen. You can configure the order in which the policies are applied. ScanMail filters all email messages according to each policy until a content violation triggers an action that prevents further scanning (such as "delete", or "quarantine"). You can change the order of these policies to optimize content filtering.

The content filter provides a means for the administrator to evaluate and control the delivery of email messages on the basis of the message text itself. It can be used to monitor inbound and outbound messages to check for the existence of offensive or otherwise objectionable message content. The content filter also provides a synonym checking feature, which allows you to extend the reach of your policies.

You can, for example, create policies to check for:

- Sexually harassing language
- Racist language
- Spam embedded in the body of an email message

Note

This feature is not available on ScanMail Standard versions.

Active Directory Integrated Policies

For Active Directory integrated policies, you can specify selected accounts and excluded accounts. The policy applies to accounts that belong to selected accounts but do not belong to excluded accounts. For example, AD Group1 contains ADuser1 and

ADuser2. When selected accounts include "AD Group1" and excluded accounts include "ADuser1", then the policy only applies to ADuser2.

Data Leakage Prevention

For convenience, ScanMail includes default content filtering data leakage prevention policies. There are 10 default data leakage prevention policies configured by region. Compared to standard content filtering policies, keywords in the data leakage prevention policies are regular expression description strings and not the actual keyword.

For example, IBAN is the description for the regular expression:

```
[^\w](([A-Z]{2}\d{2}\s?)([A-Za-z0-9]{11,27}|([A-Za-z0-9]{4}\s)
{3,6}[A-Za-z0-9]{0,3}|([A-Za-z0-9]{4}\s){2}[A-Za-z0-9]{3,4}))[^
\w]
```

Messages that contain the string "IBAN" do not trigger this policy. Strings such as "BE68 5390 0754 7034 " match the regular expression and trigger this policy.

Enabling Real-time Content Filtering

When content filtering is enabled, you can enable and disable individual content filtering policies. The green check icon ( ) indicates the policy is enabled, and the red "x" ( ) indicates the policy is disabled. Click the icon to toggle between enabled and disabled.

Procedure

1. Click **Content Filtering** from the main menu.

   The **Content Filtering** screen displays.

2. Select **Enable transport level content filtering**.

3. Select **Enable store level content filtering**. (Exchange Server 2010 and 2007)

4. Click **Save**.

Global Settings

ScanMail uses Quarantine to move actionable messages to a quarantine directory, replace the targeted files, and deliver the remaining messages to the original recipient.

You can configure ScanMail to quarantine or backup email messages when it detects a policy incident. You can set the quarantine or backup folder for each policy individually from the **Action Settings** screen, or you can specify a global directory.

When you specify a global quarantine or backup directory, ScanMail moves all files that it quarantines or backs up as a result of a policy incident to the directory that you specify.

For details on global advanced scan actions, see *Advanced Scan Action Options on page 6-21*.

To configure the Global Settings, click **Content Filtering** > **Global Settings.**

Note

You must click **Apply to All** to configure the new directories. If you click **Save**, ScanMail only saves directory paths that you typed, but they will not be applied.

Configuring Content Filtering Policies

To create a content filtering policy, a policy wizard directs you through a series of steps. At each step, you add to your policy until it is complete. After you have created your policy, ScanMail begins to filter all incoming and outgoing messages according to your policy.

You can create the policies that do the following:

TABLE 9-1. Content Filtering Policies

POLICY	DESCRIPTION
Match any or apply to all	This type of policy is capable of filtering content from any message in real-time or during a manual or scheduled scan. **Note** Active Directory integration is available for Exchange Server 2013, and 2010/2007 Hub Transport server roles.
Match all conditions	This type of policy performs an action when ScanMail detects specific details in the From, To, Cc, Subject, Size, and Attachment file name fields in email messages.
Match any condition	This type of policy scans the message content of particular email account(s). These policies are similar to general content filtering policies, except that they only filter content from specified email account(s).
Exceptions	This type of policy creates an exception for specific email account(s).

Configuring the Senders and Recipients List (Match any or apply to all)

Note

When editing a policy, you can only change the accounts for **Match any or apply to all** policies. For other policy types, the default account setting is "All accounts" .

Procedure

1. Go to the **Content Filtering** screen by navigating to **Content Filtering**.
2. Add or edit a **Match any or apply to all** policy:
   - While creating a new policy:

     Click **Add** > **Match any or apply to all**.

- While editing a policy:
  a. Click the policy name.
  b. Click the **Accounts** tab.

3. Select the senders or recipients for the policy scan.
   - While creating a new policy:
     a. Select the account type:
        - **From any sender to any recipient**
        - **From specific sender(s) to any recipient**
        - **From any sender to specific recipient(s)**.
     b. Click the **specific sender(s)** or **specific recipient(s)** link (if applicable).
   - While editing a policy:
     a. Select the account type:
        - **All**
        - **Specific sender(s)**
        - **Specific recipient(s)**

        ScanMail only applies the policy to the accounts selected for the **Accounts** type. If you select accounts for a different account type, ScanMail does not apply the policy to the previous accounts selected.
     b. Click the **Edit** link in the tables to change the included accounts and excepted accounts for this policy.
4. Select one of the following:
   - **Anyone**: Apply this policy or exception to all users.
   - **Specific accounts**: Select from Active Directory groups or ScanMail special groups.
5. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list.

6. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list on the **Exclude Accounts** screen.
7. Click **Save**.

Configuring Content Filtering Targets

Specify the content that ScanMail filters by configuring the following target settings.

Procedure

1. Go to the **Content Filtering** screen by navigating to one of the following:
   - For Real-time scans: **Content Filtering**
   - For Manual scans: **Manual Scan** > **Content filtering**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Content filtering**
2. Add or edit a policy:
   - For new policies:
     a. Click **Add** > **[Policy Type]**.
     b. Go to the **Specify Policy** screen.
   - For pre-existing policies:
     a. Click the policy name.
     b. Click the **Target** tab.
3. Specify the target settings:

TABLE 9-2. Content Filtering Target Settings

SECTION	SETTINGS
Email Account(s) (Match any condition policies)	Specify email accounts to scan for in the following fields: • **From** • **To** • **Cc**
Target	Select to scan for keywords in the following: • For **Match any or apply to all** policies: **Header**, **From**, **To**, **Cc**, **Subject**, **Body**, **Attachment** • For **Match any condition** policies: **Subject**, **Body**, **Attachment** For **Match all conditions** policies: • Specify keywords to scan for in: **From**, **To**, **Cc**, **Subject**, **Attachment file name** • **Case-sensitive**: Select to make scans for keywords case-sensitive. • **Size**: Select greater than, less than, equal to, or not equal to and specify the number of bytes.

SECTION	SETTINGS
Add Keyword(s) (Match any or apply to all, Match any condition)	• **Match**: Select **All specified keywords** or **Any specified keywords**. • **Enter keyword(s)**: Type a keyword to add to the list. • **Add**: Click to add the keyword to the list. • **Remove**: Click to remove the selected keyword from the list. • **Export**: Click to export keywords to a file. • **Import**: Click to import keywords from a file. • **Match case-sensitive**: Select to make scans for keywords case-sensitive. • **Match synonym**: Select to match synonyms. • **Show details**: Click to manage synonyms.

Imported Keyword Lists

When you import a keyword file, the imported keywords appear in the keyword list. The imported file must be a text (.txt) file. The imported keywords use the same format as they had in the text file. You can import keyword lists from previous versions of ScanMail. ScanMail imports the keywords and applies the same syntax as used in this version of ScanMail.

TABLE 9-3. Imported Text File for Content Filtering

THE IMPORTED TEXT FILE CONTAINS	THE KEYWORD LIST DISPLAYS
win cash prize	win cash prize
win cash prize	win cash prize

Note

Export keywords when the list is complete to keep a copy of keywords to use on other ScanMail servers or to import keywords in the future.

Configuring Content Filtering Actions

ScanMail performs an action whenever it detects undesirable content. You configure the action ScanMail performs using this screen. Additionally, configure whether or not ScanMail sends a notification.

Procedure

1. Go to the **Content Filtering** screen by navigating to one of the following:
   - For Real-time scans: **Content Filtering**
   - For Manual scans: **Manual Scan** > **Content filtering**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Content filtering**
2. Add or edit a policy:
   - For new policies:
     a. Click **Add** > **[Policy Type]**.
     b. Go to the **Specify Actions** screen.
   - For pre-existing policies:
     a. Click the policy name.
     b. Click the **Action** tab.
3. Select an action for ScanMail to take when it detects undesirable content.

   For details on the available actions, see *About ScanMail Actions on page 6-10*.
4. To notify specific individuals:
   - Select the check box **Forward to sender's manager**.

- Select the check box **Forward to specific email address(es)** and type the email address of the recipients.

5. Specify whether to send notifications when an action is taken by selecting **Notify** or **Do not notify**.
6. Configure **Advanced Options** as necessary.

Note

For details on advanced scan actions, see *Advanced Scan Action Options on page 6-21*.

Configuring Content Filtering Notifications

Procedure

1. Go to the **Content Filtering** screen by navigating to one of the following:
   - For Real-time scans: **Content Filtering**
   - For Manual scans: **Manual Scan** > **Content filtering**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Content filtering**
2. Add or edit a policy before configuring notification settings:
   - For new policies:
     a. Click **Add** > **[Policy Type]**.
     b. Go to the **Specify Notification** screen.
   - For pre-existing policies:
     a. Click the policy name.
     b. Click the **Notification** tab.
3. Click the check boxes corresponding to the people ScanMail will notify.
4. Click **Show details** to customize the notification for that recipient.

5. Select from the notification options.

   Refer to *Notification Settings on page 6-24* for details.

6. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.

Enabling a Content Filtering Policy

Enable individual policies and designate each policy a priority for use in scanning.

Procedure

1. Go to the **Content Filtering** screen by navigating to one of the following:
   - For Real-time scans: **Content Filtering**
   - For Manual scans: **Manual Scan** > **Content filtering**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Content filtering**
2. Add or edit a policy before enabling:
   - For new policies:
     a. Click **Add** > **[Policy Type]**.
     b. Go to the **Name and Priority** screen.
   - For pre-existing policies:

     Click the policy name.
3. Select to enable this policy or exception.
4. Type the name of your policy in the **Policy name** space.
5. Specify the priority.
   - For new policies:

     Type the priority of your policy in the **Priority** space.

- For preexisting policies:
  a. Select the check box next to the policy or exception name in the list.
  b. Click **Reorder**.
  c. Type the priority number in the **Priority** field.
  d. Click **Save Reorder**.

6. Click **Save**.

Configuring a Content Filtering Exception

Exception policies follow the same priority behavior as other content filtering policies. Exception policies specify email address exception lists for content filtering policies with a lower priority.

Note

Exception email addresses can be SMTP addresses or display name (for users in the domain where ScanMail is installed). Regular expressions can be used in exception email addresses.

Procedure

1. Go to the **Content Filtering** screen by navigating to one of the following:
   - For Real-time scans: **Content Filtering**
   - For Manual scans: **Manual Scan** > **Content filtering**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Content filtering**
2. Add or edit a policy:
   - For new policies:

     Click **Add** > **Exceptions**.

- For pre-existing policies:

  Click the policy name.

3. Type an email address under **Enter address(es)**.
4. Click **Add**.

   The email address appears in the list.
5. Save the list.

Editing a Content Filtering Policy

A brief description of the editing options is available below.

Procedure

1. Click **Content Filtering** from the main menu.

   The **Content Filtering** screen displays.
2. Click the name of the policy to edit.
3. Configure the following options:
   - **Enable this policy**: Select to enable this policy.
   - **Policy name**: Edit the policy name by typing a new name.
   - **Accounts**: View the accounts that the current policy applies to.
   - **Target**: Edit the target based on the type of policy.
   - **Action**: Edit the action by selecting from the available actions for this policy.
   - **Notification**: Edit the notifications by selection from the available options for this policy.
4. Click **Save**.

Chapter 10

Configuring Data Loss Prevention

This chapter explains how to configure Data Loss Prevention to protect the Exchange environment.

Topics include:

- *About Data Loss Prevention (DLP) on page 10-2*
- *Data Identifier Types on page 10-2*
- *About Data Loss Prevention Templates on page 10-12*
- *About Data Loss Prevention Policies on page 10-17*

About Data Loss Prevention (DLP)

With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure.

Data Loss Prevention safeguards an organization's sensitive data against accidental or deliberate leakage. Data Loss Prevention allows you to:

- Identify the sensitive information that requires protection using data identifiers
- Create policies that limit or prevent the transmission of digital assets through common transmission channels, such as email and external devices
- Enforce compliance to established privacy standards

Before you can monitor sensitive information for potential loss, you must be able to answer the following questions:

- What data needs protection from unauthorized users?
- Where does the sensitive data reside?
- How is the sensitive data transmitted?
- What users are authorized to access or transmit the sensitive data?
- What action should be taken if a security violation occurs?

This important audit typically involves multiple departments and personnel familiar with the sensitive information in your organization.

If you already defined your sensitive information and security policies, you can begin to define data identifiers and company policies.

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. Administrators can define digital assets using the following data identifiers:

- **Expressions**: Data that has a certain structure.

For details, see *Expressions on page 10-3*.

- **Keyword lists**: A list of special words or phrases.

  For details, see *Keywords on page 10-8*.

Note

Administrators cannot delete a data identifier that a DLP template is using. Delete the template before deleting the data identifier.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.

Administrators can use predefined and customized expressions.

For details, see *Predefined Expressions on page 10-3* and *Customized Expressions on page 10-3*.

Predefined Expressions

Data Loss Prevention comes with a set of predefined expressions. These expressions cannot be modified or deleted.

Data Loss Prevention verifies these expressions using pattern matching and mathematical equations. After Data Loss Prevention matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Expressions are a powerful string-matching tool. Become comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, when creating an expression that includes a date, refer to the expressions prefixed with "Date".
- Note that Data Loss Prevention follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:

  http://www.pcre.org/
- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Administrators can choose from several criteria when creating expressions. An expression must satisfy the chosen criteria before Data Loss Prevention subjects it to a DLP policy. For details about the different criteria options, see *Criteria for Customized Expressions on page 10-4*.

Criteria for Customized Expressions

TABLE 10-1. Criteria Options for Customized Expressions

CRITERIA	RULE	EXAMPLE
None	None	All - Names from US Census Bureau • Expression: [^\w]([A-Z][a-z]{1,12}(\s?,\s?|[\s]|\s([A-Z])\.\s)[A-Z][a-z]{1,12})[^\w]

Criteria	Rule	Example
Specific characters	An expression must include the characters you have specified. In addition, the number of characters in the expression must be within the minimum and maximum limits.	US - ABA Routing Number • Expression: [^\d]([0123678]\d{8})[^\d] • Characters: 0123456789 • Minimum characters: 9 • Maximum characters: 9
Suffix	Suffix refers to the last segment of an expression. A suffix must include the characters you have specified and contain a certain number of characters. In addition, the number of characters in the expression must be within the minimum and maximum limits.	All - Home Address • Expression: \D(\d+\s[a-z.]+\s([a-z]+\s){0,2} (lane|ln|street|st|avenue|ave| road|rd|place|pl|drive|dr|circle| cr|court|ct|boulevard|blvd)\.? [0-9a-z,#\s\.]{0,30}[\s|,][a-z]{2}\s\d{5}(-\d{4})?)[^\d-] • Suffix characters: 0123456789- • Number of characters: 5 • Minimum characters in the expression: 25 • Maximum characters in the expression: 80
Single- character separator	An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit.	All - Email Address • Expression: [^\w.]([\w\.]{1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z\.]{0,10})[^\w.] • Separator: @ • Minimum characters to the left: 3 • Maximum characters to the left: 15 • Maximum characters to the right: 30

Adding and Editing Expressions

Create customized expressions if none of the predefined expressions meet the company's requirements.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Expressions** tab.

3. Click **Add** or edit an expression by clicking the expression's name.

   A new screen displays.

4. Type a name for the expression.

   The name must not exceed 512 bytes in length.

5. Type a description that does not exceed 2048 bytes in length.

6. Type the expression and specify whether it is case-sensitive.

7. Type the displayed data.

   For example, when creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and does not appear elsewhere in the product.

8. Choose one of the following criteria and configure additional settings for the chosen criteria:

   - **None**
   - **Specific characters**
   - **Suffix**
   - **Single-character separator**

9. Select an additional validation method if necessary.

These additional validators were specifically designed to detect highly specialized digital assets.

10. Test the expression against an actual data.

    For example, if the expression is for a national ID, type a valid ID number in the **Test data** text box, click **Test**, and then check the result.

11. Click **Save**.

> **Tip**
>
> Save the settings only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

Importing Expressions

Administrators with a properly-formatted .dat file containing the expressions can use this option. Generate the file by exporting the expressions from either the ScanMail server on the current server or from another ScanMail server.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Expressions** tab.

3. Click **Import** and then locate the .dat file containing the expressions.

4. Click **Open**.

   A message appears, indicating the status of the import.

Note

Each expression contains a unique ID value. If an expression with the same ID already exists, ScanMail overwrites the existing expression. If an expression with the same display name already exists, ScanMail appends the suffix "Original" to the preexisting expression and adds the new expression to the list.

Keywords

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure Data Loss Prevention to block files containing these keywords.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see *Predefined Keyword Lists on page 10-8* and *Customized Keyword Lists on page 10-8*.

Predefined Keyword Lists

Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

For details about the predefined keyword lists in Data Loss Prevention, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Customized Keyword Lists

Create customized keyword lists if none of the predefined keyword lists meet your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before Data Loss Prevention subjects it to a policy. Choose one of the following criteria for each keyword list:

- **Any keyword**
- **All keywords**
- **All keywords within <x> characters**
- **Combined score for keywords exceeds threshold**

For details regarding the criteria rules, see *Customized Keyword List Criteria on page 10-9*.

Customized Keyword List Criteria

TABLE 10-2. Criteria for a Keyword List

CRITERIA	RULE
Any keyword	A file must contain at least one keyword in the keyword list.
All keywords	A file must contain all the keywords in the keyword list.

CRITERIA	RULE
All keywords within <x> characters	A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within <x> characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If Data Loss Prevention detects all keywords in the order DISK, WEB, and USB, the number of characters from the "D" (in DISK) to the "W" (in WEB) and from the "W" to the "U" (in USB) must be 20 characters or less. The following data matches the criteria: DISK####WEB############USB The following data does not match the criteria: DISK**********WEB****USB(23 characters between "D" and "W") When deciding on the number of characters, remember that a small number, such as 10, usually results in a faster scanning time but only covers a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.
Combined score for keywords exceeds threshold	A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as "salary increase" for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.

Adding and Editing Keyword Lists

Keywords are special words or phrases. Add related keywords to a keyword list to identify specific types of data. Create customized keyword lists if none of the predefined keyword lists meet the company's requirements.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Keyword Lists** tab.

3. Click **Add** or edit a keyword list by clicking the keyword list's name.

   A new screen displays.

4. Type a name for the keyword list.

   The name must not exceed 512 bytes in length.

5. Type a description that does not exceed 2048 bytes in length.

6. Choose one of the following criteria and configure additional settings for the chosen criteria:

   - **Any keyword**
   - **All keywords**
   - **All keywords within <x> characters**
   - **Combined score for keywords exceeds threshold**

7. To manually add keywords to the list:

   a. Type a keyword that is 3 to 512 bytes in length and specify whether it is case-sensitive.

   b. Click **Add**.

8. To delete keywords, select the keywords and click **Delete**.

9. Click **Save**.

Importing Expressions

Administrators with a properly-formatted .dat file containing the expressions can use this option. Generate the file by exporting the expressions from either the ScanMail server on the current server or from another ScanMail server.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **Data Identifiers**.

   A list of data identifiers appears.

2. Click the **Expressions** tab.
3. Click **Import** and then locate the .dat file containing the expressions.
4. Click **Open**.

   A message appears, indicating the status of the import.

   Note

   Each expression contains a unique ID value. If an expression with the same ID already exists, ScanMail overwrites the existing expression. If an expression with the same display name already exists, ScanMail appends the suffix "Original" to the preexisting expression and adds the new expression to the list.

About Data Loss Prevention Templates

Use Data Loss Prevention templates to tag and detect sensitive content by a set combination of data identifiers. A template combines data identifiers and operators (And, Or) in condition statements. When a set of data matches the criteria of a condition, Data Loss Prevention triggers a policy action. For example, a file containing data matching the All: Names from US Census Bureau AND US: HICN (Health Insurance Claim Number) templates, triggers the HIPAA policy.

Use Data Loss Prevention out-of-the-box templates for regulatory compliance initiatives, such as GLBA, PCI-DSS, SB-1386, US PII, and HIPAA. Companies can also create custom templates or modify existing templates to suit their business requirements. Companies that have preexisting, user-defined templates can import and export templates to maintain policy consistency throughout their organization.

Create company-specific templates after configuring DLP data identifiers or use the predefined templates.

Predefined DLP Templates

Data Loss Prevention comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified or deleted.

- **GLBA**: Gramm-Leach-Billey Act
- **HIPAA**: Health Insurance Portability and Accountability Act
- **PCI-DSS**: Payment Card Industry Data Security Standard
- **SB-1386**: US Senate Bill 1386
- **US PII**: United States Personally Identifiable Information

For a detailed list on the purposes of all predefined templates, and examples of data being protected, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Defining a Data Loss Prevention Template

Data Loss Prevention templates define an organization's sensitive data using keyword lists and expressions. Define templates to use in Data Loss Prevention policies and protect sensitive information that is company-specific. For more information on Data Loss Prevention Templates, see *About Data Loss Prevention Templates on page 10-12*.

Note

Administrators cannot modify a pre-packaged template. To use a pre-packaged template as the basis for a new template, select the check box beside the template name and click **Copy** in the Data Loss Prevention Template toolbar. This creates a new template with the suffix "Copy" at the end.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. Choose to create or modify a Data Loss Prevention Template.

   - To create a template, on the Data Loss Prevention Templates toolbar, click **Add**.
   - To modify a template, click the template name.

3. Type the **Name** of the template.

4. (Optional) Type a **Description** of the template.

5. From the drop-down box under **Condition Statement**, beside the (+) control, select the criteria **Expressions** or **Keyword Lists**.

6. Select an expression or keyword list from the drop-down box beside the selected criteria.

7. When adding **Expressions** criteria, type the number of **Occurrences** necessary for the template to trigger. This value designates the number of times an expression must be present in an email message before ScanMail triggers an action.

   Note

   The **Occurrences** amount is a required value. The value cannot be zero (0) or blank.

8. Add additional criteria by clicking the (+) control. Remove criteria by clicking the (−) control.

9. When adding more than one template definition, select the **And** or **Or** operator from the drop-down box beside the condition in the **Condition Statement** list.

10. Click **Add** to add the condition to the **Template Definition** list or click **Clear** to clear the condition statement.

11. When adding more than one condition, select the **And** or **Or** operator from the drop-down box beside the template definition in the **Template Definition** list.

12. To remove a definition from the **Template Definition** list, click the delete icon ( ) to the right of the definition.

13. Click **Save**.

    The **Data Loss Prevention Templates** screen appears with the new template at the bottom of the Data Loss Prevention templates list.

Deleting a Data Loss Prevention Template

Note

Administrators cannot delete a pre-packaged DLP template or any templates associated with a company policy. Remove the template from all policies before deleting the template.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. Select the check box beside the template that you want to delete.

3. On the Data Loss Prevention Templates toolbar, click **Delete**.

Importing a Data Loss Prevention Template

Administrators can import Data Loss Prevention templates from other ScanMail servers or other Trend Micro products to keep predefined rules consistent throughout the organization.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. On the Data Loss Prevention Templates toolbar, click **Import**.

   Note

   Each template contains a unique ID value. If a template with the same ID already exists, ScanMail overwrites the existing template. If a template with the same display name already exists, ScanMail appends the suffix "Original" to the preexisting template and adds the new template to the list.

   The **Data Loss Prevention Import Template** screen appears.

3. Click the **Browse...** button, locate, and select the template file to import. Click **Open**.

   Note

   Template files save in DAT format.

4. Click **Import** to import the template file.

Exporting a Data Loss Prevention Template

You can export templates to other ScanMail servers or other Trend Micro products to keep predefined rules consistent throughout your organization.

Procedure

1. On the left navigation bar, click **Data Loss Prevention** > **DLP Templates**.

   A list of templates appears.

2. Select the check box(es) next to the template name(s) that you want to export.

3. On the Data Loss Prevention Templates toolbar, click **Export**.

   A **File Download** dialog appears.

4. Click **Save**.

   A **Save As** dialog appears.

5. Select a name and location for the export file. Click **Save**.

> **Note**
> Template files save in DAT format.

About Data Loss Prevention Policies

Data Loss Prevention policies allow companies to monitor the flow of sensitive information over the network. Policy rules, through use of Data Loss Prevention templates, help to manage the distribution of sensitive data across the network. Administrators can scale policies to apply to the entire company, groups, or specific endpoints.

Administrators can apply policies to both outbound and inbound mail traffic, as well as to the exact message parts to monitor. Policy configurations can exempt certain groups or users from scans and define specific incident response actions.

ScanMail integrates Data Loss Prevention policy management with Control Manager 6.0. Administrators can create and manage the company's Data Loss Prevention policies from the Control Manager console and deploy the settings to all ScanMail servers registered to Control Manager.

Enabling Real-time Data Loss Prevention

When Data Loss Prevention is enabled, you can enable and disable individual Data Loss Prevention policies. The green check icon ( ) indicates the policy is enabled, and the red "x" ( ) indicates the policy is disabled. Click the icon to toggle between enabled and disabled.

Procedure

1. Click **Data Loss Prevention** > **DLP Policies** from the main menu.

   The **Data Loss Prevention Policies** screen displays.

2. Select **Enable transport level Data Loss Prevention**.

3. From the **Apply policies to** drop-down select to apply policies to **Outbound messages** only or to **All messages**.

4. From the **Digital asset discovery** drop-down, select how Data Loss Prevention matches digital assets:

   - **Single message part**: Data Loss Prevention identifies digital assets in each message part separately.

     For example, one of the triggers of the "Canada: Cardholder Information" template is the detection of 5 occurrences of credit card numbers. Selecting **Single message part** requires DLP to match 5 credit card numbers all in the same message part before triggering the policy.

   - **Multiple message parts**: Data Loss Prevention identifies digital assets spread among all selected message parts.

     For example, one of the triggers of the "Canada: Cardholder Information" template is the detection of 5 occurrences of credit card numbers. Selecting **Multiple message parts** allows DLP to match credit card numbers among all selected message parts (if 2 credit card numbers are matched in the message body and 3 in the message attachment, DLP triggers the template).

5. Click **Save**.

Global Settings

ScanMail uses Quarantine to move actionable messages to a quarantine directory, replace the targeted files, and deliver the remaining messages to the original recipient.

You can configure ScanMail to quarantine or backup email messages when it detects a policy incident. You can set the quarantine or backup folder for each policy individually from the **Action Settings** screen, or you can specify a global directory.

When you specify a global quarantine or backup directory, ScanMail moves all files that it quarantines or backs up as a result of a policy incident to the directory that you specify.

For details on global advanced scan actions, see *Advanced Scan Action Options on page 6-21*.

To configure the Global Settings, click **Data Loss Prevention** > **DLP Policies** > **Global Settings.**

Note

You must click **Apply to All** to configure the new directories. If you click **Save**, ScanMail only saves directory paths that you typed, but they will not be applied.

Configuring a Data Loss Prevention Policy

Data Loss Prevention policies govern the actions ScanMail takes when it discovers sensitive information in email messages.

Create a new policy by clicking **Data Loss Prevention** > **DLP Policies** > **Add**.

Modify an existing policy by clicking **Data Loss Prevention** > **DLP Policies** > **[DLP Policy Name]**.

Configure Data Loss Prevention policies through the following five step process:

1. *Selecting Accounts on page 10-20*
2. *Configuring DLP Targets on page 10-21*
3. *Configuring DLP Actions on page 10-22*
4. *Configuring DLP Notifications on page 10-24*
5. *Enabling a DLP Policy on page 10-25*

Selecting Accounts

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to **Data Loss Prevention** > **DLP Policies**.
2. Add or edit a policy or exception:
   - For new policies or exceptions:

     Click **Add**.
   - For preexisting policies or exceptions:
     a. Click the policy or exception name.
     b. Click the **Accounts** tab.
3. Select the senders or recipients for the policy scan.
   - While creating a new policy:
     a. Select the account type:
        - **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)**.

     b. Click the **specific sender(s)** or **specific recipient(s)** link (if applicable).
   - While editing a policy:
     a. Select the account type:
        - **All**
        - **Specific sender(s)**
        - **Specific recipient(s)**

- **Specific sender(s) and recipient(s)**

  ScanMail only applies the policy to the accounts selected for the **Accounts** type. If you select accounts for a different account type, ScanMail does not apply the policy to the previous accounts selected.

b. Click the **Edit** link in the tables to change the included accounts and excepted accounts for this policy.

4. Select one of the following:
   - **Anyone**: Apply this policy or exception to all users.
   - **Specific accounts**: Select from Active Directory groups or ScanMail special groups.
5. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list.
6. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list on the **Exclude Accounts** screen.

Configuring DLP Targets

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:
   - For Real-time scans: **Data Loss Prevention** > **DLP Policies**
   - For Manual scans: **Manual Scan** > **Data Loss Prevention**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**
2. Add or edit a policy or exception:
   - For new policies or exceptions:

     a. Click **Add**.

b. Go to the **Specify Rule** screen.

- For preexisting policies or exceptions:

  a. Click the policy or exception name.

  b. Click the **Target** tab.

3. Select the check box(es) for the target area(s) of the email message to scan.

   Available targets are:

   - **Header** (**From**, **To**, and **Cc**)
   - **Subject**
   - **Body**
   - **Attachment**

4. Select templates from the list of available templates and click **Add >>** to apply the templates to the policy.

   Note

   A Data Loss Prevention policy requires selecting at least one template before activation.

5. In the Available DLP Template(s) toolbar, click **Add** to create a new template (see *Defining a Data Loss Prevention Template on page 10-13*) or click **Import** to import a template file (see *Importing a Data Loss Prevention Template on page 10-15*).

Configuring DLP Actions

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:

   - For Real-time scans: **Data Loss Prevention** > **DLP Policies**
   - For Manual scans: **Manual Scan** > **Data Loss Prevention**

- For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**

2. Add or edit a policy or exception:
   - For new policies or exceptions:
     a. Click **Add**.
     b. Go to the **Specify Action** screen.
   - For preexisting policies or exceptions:
     a. Click the policy or exception name.
     b. Click the **Action** tab.
3. Select an action for ScanMail to take when it detects undesirable content.

   For details on the available actions, see *About ScanMail Actions on page 6-10*.
4. To notify specific individuals:
   - Select the check box **Forward to sender's manager**.
   - Select the check box **Forward to specific email address(es)** and type the email address of the recipients.
5. Specify whether to send notifications when an action is taken by selecting **Notify** or **Do not notify**.
6. Configure **Advanced Options** as necessary.

Note

For details on advanced scan actions, see *Advanced Scan Action Options on page 6-21*.

Configuring DLP Notifications

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:
   - For Real-time scans: **Data Loss Prevention** > **DLP Policies**
   - For Manual scans: **Manual Scan** > **Data Loss Prevention**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**
2. Add or edit a policy or exception:
   - For new policies or exceptions:
     a. Click **Add**.
     b. Go to the **Specify Notification** screen.
   - For preexisting policies or exceptions:
     a. Click the policy or exception name.
     b. Click the **Notification** tab.
3. Click the check boxes corresponding to the people ScanMail will notify.
4. Click **Show details** to customize the notification for that recipient.
5. Select from the notification options.

   Refer to *Notification Settings on page 6-24* for details.
6. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.

Enabling a DLP Policy

Procedure

1. Go to the **Data Loss Prevention Policies** screen by navigating to the following:
   - For Real-time scans: **Data Loss Prevention** > **DLP Policies**
   - For Manual scans: **Manual Scan** > **Data Loss Prevention**
   - For Scheduled scans: **Scheduled Scan** > **[Add or Edit]** > **Data Loss Prevention**
2. Add or edit a policy before enabling:
   - For new policies:
     a. Click **Add**.
     b. Go to the **Name and Priority** screen.
   - For pre-existing policies:

     Click the policy name.
3. Select to enable this policy or exception.
4. Type the name of your policy in the **Policy name** space.
5. Specify the priority.
   - For new policies:

     Type the priority of your policy in the **Priority** space.
   - For preexisting policies:
     a. Select the check box next to the policy or exception name in the list.
     b. Click **Reorder**.
     c. Type the priority number in the **Priority** field.
     d. Click **Save Reorder**.

6. Click **Save**.

Chapter 11

Configuring Spam Prevention

This chapter explains how to configure Spam Prevention to protect your Exchange environment.

Topics include:

- *About Spam Prevention on page 11-2*
- *About Email Reputation on page 11-3*
- *About Content Scanning on page 11-6*

About Spam Prevention

Trend Micro spam prevention service intercepts spam to prevent spam messages from reaching your email clients. Spam prevention works by:

- Comparing, in real time, incoming email messages against a list of known spam.
- Making a series of logical deductions to determine whether the mail has the characteristics of spam.

Even when senders of spam change their methods, spam prevention can distinguish spam from legitimate email messages. Trend Micro spam prevention employs patent-pending, heuristic technology that evaluates, identifies, and monitors existing and new messages using multiple email characteristics, providing highly accurate spam capture rates. False positives are kept low by the use of sophisticated behavior-evaluation algorithms, which calculate the probability that a particular message is spam.

ScanMail provides two powerful features, Email Reputation and content scanning, for filtering spam messages.

Spam Folder Configuration

- Trend Micro Spam Folder

  ScanMail creates a spam folder on all of the mailboxes on the Exchange server where you installed ScanMail. During the installation, the installation program prompted you to name this folder and it will have the name that you specified.

  After installation, you can rename the spam folder using Microsoft Outlook. Trend Micro identifies the folder by ID, not by folder name.

- Spam detection levels

  ScanMail also configures the spam detection level defaults. The spam detection level filters out spam messages arriving at the Exchange server.

  - **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.

About Email Reputation

ScanMail provides Email Reputation features as a part of spam prevention. As the first line of defense, Trend Micro Email Reputation helps stop spam before it can flood your network and burden your system resources.

When your email server accepts an initial connection from another email server, your email server records the IP address of the computer requesting the connection. Your email server then queries its DNS server, which in turn queries the Reputation database(s) to determine if there is a record for the IP address of the requesting computer. If the host is listed in a database, Email Reputation recommends an appropriate action. You can also customize actions.

Trend Micro Email Reputation Standard

This service helps block spam by validating requested IP addresses against the Trend Micro reputation database, powered by the Trend Micro Threat Prevention Network. This ever-expanding database currently contains over 1 billion IP addresses with reputation ratings based on spam activity. Trend Micro spam investigators continuously review and update these ratings to ensure accuracy.

Email Reputation Standard Service 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. You can set up your Message Transfer Agent (MTA) to take the appropriate action on that message based on the spam identification from Email Reputation.

Tip

Trend Micro recommends that you configure your Message Transfer Agent (MTA) to block, not receive, any email from an IP address that is included on the standard reputation database.

Trend Micro Email Reputation Advanced

This service identifies and stops sources of spam while they are in the process of sending millions of messages. This 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 Service 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 message stream is spam. The more spam you receive, the higher the percentage of blocked connections you will see.

Enabling Email Reputation

Email Reputation verifies IP addresses of incoming email messages using one of the world's largest, most trusted reputation databases along with a dynamic reputation database to identify new spam and phishing sources, stopping even zombies and botnets as they first emerge.

Procedure

1. Go to the Email Reputation screen by navigating to **Spam Prevention** > **Email Reputation**.

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

Configuring Email Reputation Targets

Procedure

1. Go to the **Email Reputation** screen by navigating to **Spam Prevention** > **Email Reputation**.
2. Configure the following settings:
   - **Smart Protection Network portal**: Click to view global spam information, reports, create or manage Approved and Blocked Sender IP address lists, perform administrative tasks, and configure the service from the **Trend Micro Email Reputation** website.
   - **Add**: Type an IP address and click to add the IP address to the Approved IP Address list.
3. Click **Save**.

Configuring Email Reputation Actions

If you specified **Standard** as the Service Level from the **Target** tab, only the **Standard Reputation Database Action** options display. Otherwise, if you specified **Advanced** as the Service Level from the **Target** tab, both the **Standard Reputation Database Action** and the **Dynamic Reputation Database Action** display because both databases will be used. If both action boxes display, specify separate actions for detections made with each database.

Procedure

1. Go to the **Email Reputation** screen by navigating to **Spam Prevention** > **Email Reputation**.

2. Click the **Action** tab.
3. Select one of the following for the **Standard Reputation Database Action**:
   - **Intelligent action**: Denial of connection for Standard Reputation Database matches.

     (Optional) Type an SMTP error code and type a custom error message.
   - **Close connection with no error message**: Select to close the connection.
   - **Bypass**: Select to pass without logging.
4. (Optional) Select one of the following for the **Dynamic Reputation Database Action** if **Advanced** was selected:
   - **Intelligent action**: Denial of connection for Dynamic Reputation Database matches.

     (Optional) Type an SMTP error code and type a custom error message.
   - **Close connection with no error message**: Select to close the connection.
   - **Bypass**: Select to pass without logging.
5. Click **Save**.

About Content Scanning

ScanMail uses the Trend Micro Anti-spam Engine to implement heuristic-based policies when detecting unwanted content, or blocking, or automatically allowing a message. If you chose to install the End User Quarantine tool when installing ScanMail, ScanMail creates a spam folder on all of the mailboxes on the Exchange server where you installed ScanMail.

Content Scanning uses the Approved and Blocked Sender Lists and the Spam Filter to screen messages for spam.

Spam Engine and Spam Pattern Files

ScanMail uses the Trend Micro spam engine and Trend Micro spam pattern files to detect and take action against spam messages. Trend Micro updates both the engine and pattern file frequently and makes them available for download. ScanMail can download these components through a manual or scheduled update.

The spam engine makes use of spam signatures and heuristic rules to screen email messages. It scans email messages and assigns a spam score to each one based on how closely it matches the rules and patterns from the pattern file. ScanMail compares the spam score to the user-defined spam detection level. When the spam score exceeds the detection level, ScanMail takes action against the spam. You cannot modify the method that the spam engine uses to assign spam scores, but they can adjust the detection levels used by ScanMail to decide what is spam and what is not spam.

For example: Many spammers use many exclamation marks, or more than one consecutive exclamation mark (!!!!) in their email messages. When ScanMail detects a message that uses exclamation marks this way, it increases the spam score for that email message.

End User Quarantine

During installation, you can add a folder to the server-side mailbox of each end user for Microsoft Exchange. You name the spam folder and configure the storage time limit during the installation process. Trend Micro recommends naming the spam folder "Spam Mail". When ScanMail detects spam messages, the system quarantines them in this folder according to spam filter rules predefined by ScanMail. End users can view this spam folder to open, read, or delete the suspect email messages.

End users can open email messages quarantined in the spam folder. When they open one of these messages, two buttons appear on the actual email message: **Approved Sender** and **View Approved Sender List**. When they click **Approved Sender**, ScanMail moves the message from that sender to their local Inbox, adds the address of the message to their personal Approved Sender List, and logs an entry of the event (the administrator can view this log in a report at a later time). Clicking **View Approved Sender** opens another screen that allows the end user to view and modify their list of approved senders by name or domain. When the Exchange server receives messages from the addresses on the end user's approved sender list, it delivers them to the end user's Inbox, regardless of the header or content of the message.

ScanMail also provides administrators with an Approved Senders and Blocked Senders list. ScanMail applies the administrator's approved senders and blocked senders before considering the end user list.

Approved and Blocked Sender Lists

ScanMail does not classify addresses from the Approved senders list as spam (unless it detects a phishing incident), nor does it filter messages from this list as spam. ScanMail filters addresses from Blocked senders lists and always classifies them as spam with the action depending on the rule set by the administrator.

Note

The Exchange administrator maintains a separate Approved and Blocked Senders list for the Exchange server. If an end-user creates an approved sender, but that sender is on the administrator's Blocked Senders list, then ScanMail detects messages from that blocked sender as spam and takes action against those messages.

Spam Filter

Administrators configure a spam detection rate to filter out spam. The higher the detection level, the more likely messages will be classified as spam.

The detection level determines how tolerant ScanMail is towards suspect email messages. A high detection level quarantines the most email messages as spam, but it might also falsely identify and quarantine legitimate email messages as spam, creating "false positive" spam mail. A low detection level does not rigorously screen email messages, but does not create many false positive spam messages.

New Spam Sources

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:

1. Web Reputation Services determines the reputation score of the URL.

2. ScanMail uses the configured internal gateway MX record or IP address lists to determine the sender IP address of the email message.
3. 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.

Important

You must enable Web Reputation Services to detect new spam sources.

Enabling Content Scanning

ScanMail detects spam messages in real time and takes actions to protect Exchange clients. The approved senders list has higher priority than the blocked senders list. If an email address is in both the approved and blocked senders lists, ScanMail will not classify the email message as spam.

Procedure

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

Configuring Content Scanning Targets

Procedure

1. Go to the **Content Scanning** screen by navigating to **Spam Prevention** > **Content Scanning**.
2. Click the **Target** tab.

3. 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.

4. Select **Detect new spam sources** to scan email messages containing URLs that may be new spam sources.

   Important

   You must enable Web Reputation Services to detect new spam sources. For details, see *Enabling Web Reputation on page 12-4*.

   For details about new spam sources, see *New Spam Sources on page 11-8*.

   - Identify your company's **Organizational MX records** and add the MX records to the list.
   - Identify your company's **Organizational mail gateway IP addresses** and add the IP addresses to the list.

5. Select **Detect phishing** to scan for phishing email messages.
6. Add addresses to the list of Approved Senders and Blocked Senders.
7. Click **Save**.

Configuring Content Scanning Actions

Procedure

1. Go to the **Content Scanning** screen by navigating to **Spam Prevention** > **Content Scanning**.
2. Click the **Action** tab.
3. Select one of the following actions for **Spam** messages:
   - **Quarantine message to user's spam folder**
   - **Delete entire message**
   - **Tag and deliver**
   - **Pass**

   For details on the available actions, see *About ScanMail Actions on page 6-10*.
4. Select one of the following actions for **Phishing Incident** messages:
   - **Quarantine message to user's spam folder**
   - **Delete entire message**
   - **Tag and deliver**
   - **Pass**

   For details on the available actions, see *About ScanMail Actions on page 6-10*.
5. Click **Save**.

Chapter 12

Configuring Web Reputation

This chapter explains how to configure Web Reputation Services to protect your Exchange environment.

Topics include:

- *About Web Reputation Services on page 12-2*
- *Configuring the Web Reputation Scan Service on page 12-3*
- *Enabling Web Reputation on page 12-4*
- *Configuring Web Reputation Targets on page 12-5*
- *Configuring Web Reputation Actions on page 12-6*
- *Configuring Web Reputation Notifications on page 12-7*

About Web Reputation Services

Web Reputation Services tracks the credibility of web domains by assigning a reputation score based on factors such as a website's age, historical location changes, and indications of suspicious activities discovered through malware behavior analysis. It will then continue to scan sites and block users from accessing infected ones.

In order to protect your company from possible suspicious websites, you must configure the web reputation source, target, actions, and notifications.

Command & Control Contact Alert Services

Trend Micro Command & Control (C&C) Contact Alert Services provides enhanced detection and alert capabilities to mitigate the damage caused by advanced persistent threats and targeted attacks. C&C Contact Alert Services are integrated with Web Reputation Services which determines the action taken on detected callback addresses based on the web reputation security level.

For details on configuring the Web Reputation Services security level, see *Configuring Web Reputation Targets on page 12-5*.

FEATURE	DESCRIPTION
Global Intelligence list	Trend Micro Smart Protection Network compiles the Global Intelligence list from sources all over the world and tests and evaluates the risk level of each C&C callback address. Web Reputation Services uses the Global Intelligence list in conjunction with the reputation scores for malicious websites to provide enhanced security against advanced threats. The web reputation security level determines the action taken on malicious websites or C&C servers based on assigned risk levels.

FEATURE	DESCRIPTION
Virtual Analyzer list	Trend Micro Smart Protection Network compiles the Global Intelligence list from sources all over the world and tests and evaluates the risk level of each C&C callback address. Web Reputation Services uses the Global Intelligence list in conjunction with the reputation scores for malicious websites to provide enhanced security against advanced threats. The web reputation security level determines the action taken on malicious websites or C&C servers based on assigned risk levels. Smart Protection Servers retrieve the list from Virtual Analyzer and can evaluate all possible C&C threats against both the Global Intelligence and the local Virtual Analyzer list. For details on connecting the integrated Smart Protection Server to Deep Discovery Advisor, see the *Smart Protection Server Administrator's Guide*.
C&C categories	Web Reputation Services logs display information regarding the category of detected threats. C&C Contact Alert Services uses the following categories: • **C&C Server**: Servers/Repositories that harbor command-and-control (C&C) servers and dropzones in the C&C Global Intelligence list • **Malicious Domain**: Domains that host malicious payloads; such domains cannot be reclassified • **New Domain**: Newly-detected domains (for example, throwaway domains); domains that have not been classified by Trend Micro • **C&C Server (Virtual Analyzer)**: Servers/Repositories in the C&C Virtual Analyzer server list

Configuring the Web Reputation Scan Service

ScanMail provides two server options for web reputation queries: the Smart Protection Network and Smart Protection Servers.

For a more information on Smart Protection Network and Smart Protection Servers, see *Smart Protection Sources on page 5-4*.

Procedure

1. On the left navigation pane, click **Smart Protection** > **Scan Service Settings**.

   The **Scan Service Settings** screen appears.

2. Under Web Reputation Services, select:

   a. **Smart Protection Network**: Sends all web reputation queries to Trend Micro servers for verification.

   b. **Smart Protection Server**: Verifies all web reputation queries locally. If the local server cannot verify the queries, the server sends them to Trend Micro servers for further analyses.

      - Select **Do not make external queries to Smart Protection Network** to restrict the local server from sending web reputation queries to Trend Micro servers.

      Note

      Preventing queries from transmitting to Trend Micro Smart Protection Network provides the highest level of privacy and lowest network bandwidth usage, but also restricts the web reputation security level to **Low**. Smart Protection Servers cannot maintain the vast repository of Trend Micro Smart Protection Network.

3. To configure your Local Sources settings, click the related link and refer to *Configuring Local Sources on page 5-7*.

4. Click **Save**.

Enabling Web Reputation

Procedure

1. Click **Web Reputation** from the main menu.

   The **Web Reputation** screen displays.

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

Configuring Web Reputation Targets

Procedure

1. Click **Web Reputation** from the main menu.

   The **Web Reputation** screen displays.
2. Click the **Target** tab.
3. Select **Scan the content of message attachments for suspicious URLs** to include web reputation scanning within the attachments of email messages.
4. Select one of the following security levels:
   - **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.
5. Select **Enable approved URL list** to avoid scanning URLs deemed safe under your security policy.
6. Add approved URLs to the list.
7. Add addresses to the list of **Approved Senders**.
8. Click **Save**.

Configuring Web Reputation Actions

Procedure

1. Click **Web Reputation** from the main menu.

   The **Web Reputation** screen displays.

2. Click the **Action** tab.

3. Select an action for ScanMail to take when it detects undesirable content.

   - **Quarantine message to user's spam folder**

     Note

     The **Quarantine message to user's spam folder** action only quarantines email messages from external networks when integrating with Outlook Junk E-mail. ScanMail adds the tag "Suspicious URL" to internal email messages and delivers the messages to the user's inbox.

   - **Quarantine entire message**
   - **Delete entire message**
   - **Tag and deliver**
   - **Pass**

   For details on the available actions, see *About ScanMail Actions on page 6-10*.

4. Select **Take action on URLs that have not been assessed by Trend Micro** to treat URLs that have not been classified as suspicious URLs and perform the specified action.

5. Specify whether to send notifications when an action is taken by selecting **Notify** or **Do not notify**.

6. Configure **Advanced Options** as necessary.

Note

For details on advanced scan actions, see *Advanced Scan Action Options on page 6-21*.

7. Click **Save**.

Configuring Web Reputation Notifications

Procedure

1. Click **Web Reputation** from the main menu.

   The **Web Reputation** screen displays.

2. Click the **Notification** tab.

3. Click the check boxes corresponding to the people ScanMail will notify.

4. Click **Show details** to customize the notification for that recipient.

5. Select from the notification options.

   Refer to *Notification Settings on page 6-24* for details.

6. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.

Chapter 13

Configuring Search & Destroy

This chapter explains how to configure Search and Destroy to protect your Exchange environment.

Topics include:

- *About Search & Destroy on page 13-2*
- *Configuring Search & Destroy Access Accounts on page 13-2*
- *Activating Search & Destroy on page 13-4*
- *About Mailbox Searches on page 13-6*
- *Configuring a Mailbox Search on page 13-13*
- *Configuring Search & Destroy Settings on page 13-20*
- *Viewing Search & Destroy Event Logs on page 13-21*
- *Troubleshooting Search & Destroy on page 13-22*

About Search & Destroy

Search & Destroy provides administrators the ability to search and remove mailbox components (for example, email messages, meetings, tasks) from Exchange mailbox servers. Administrators can specify detailed search criteria to focus searches on specific keyword matching, users, mailboxes, and component creation dates.

ScanMail provides administrators with **Access Control** roles specific to Search & Destroy. Only users assigned to one of the following roles can access Search & Destroy:

- **Search & Destroy Administrator**: Can search for, monitor, and delete undesirable content from both a user's mailbox and the Exchange server
- **Search & Destroy Operator**: Can search for and monitor undesirable content in both a user's mailbox and the Exchange server

Note

By default, ScanMail does not assign any users, including the **Administrator**, to the Search & Destroy administrator role. Administrators must assign users access to Search & Destroy manually. For details, see *Configuring Search & Destroy Access Accounts on page 13-2*.

Search & Destroy employs an Exchange service account that performs keyword-matching searches on mailbox components based on administrator-configured search criteria and stores copies of the matches in an Exchange discovery mailbox. Administrators can review the component matches to determine if the content is undesirable. ScanMail can then delete the undesirable search results from the discovery mailbox and the mailbox of the offending user.

Configuring Search & Destroy Access Accounts

Search & Destroy requires administrators to configure two access accounts before use: an Active Directory service account and the Search & Destroy Administrator for ScanMail.

Create the Active Directory service account and add the account to the Exchange Discovery Management group. ScanMail uses this service account to perform the backend mailbox searches.

The Search & Destroy Administrator in ScanMail is a specialized account that permits users to access all Search & Destroy features. Search & Destroy is not visible to any user (Administrator or Operator) if the user is not also a Search & Destroy administrator.

Note

The Search & Destroy feature only provides support for mailbox servers running Exchange 2010 Service Pack 1 or above, or Exchange 2013.

The Search & Destroy Operator role can only configure mailbox searches and view results.

Procedure

1. Go to **Administration** > **Access Control**.
2. Click the Search & Destroy role to configure.
3. Optionally, modify the Search & Destroy description.
4. Search for users or groups to add to the Search & Destroy role.
5. In the Available Account(s) list, select the accounts to add to the role and click **Add >>**.
6. Click **Save**.

   The **Access Control** screen appears.
7. To the right of the **Search & Destroy** role, click the Status icon to enable the role.

   The icon changes from a red x ( ) to a green check ( ).
8. Click **Save**.
9. Log off from the ScanMail console and log on using an account with a Search & Destroy role to use the feature.

The Search & Destroy menu items appear in the left navigation menu. For users with multiple roles, the Search & Destroy menu items integrate with the existing menu.

Activating Search & Destroy

Before using Search & Destroy for the first time, administrators must specify the Active Directory service account and the discovery mailbox that stores the search results.

Note

- The activation process only appears when accessing the Search & Destroy feature for the first time.
- The Search & Destroy feature only provides support for mailbox servers running Exchange 2010 Service Pack 1 or above, or Exchange 2013.

Procedure

1. Click **Search & Destroy** > **Mailbox Search** or **Search & Destroy** > **Settings**.

   The **Search & Destroy Activation** wizard appears.

2. Click **Next >**.

   The **Exchange Server Prerequisite Configurations** screen appears.

3. Read the prerequisite items carefully. Configure the prerequisite Exchange environment settings before proceeding.

   For details on configuring the Exchange environment settings, see *Search & Destroy Prerequisites on page D-10*.

4. After configuring all necessary settings, select **All Exchange Server prerequisite settings have been properly configured**.

5. Click **Next >**.

   The service account logon credentials screen appears.

6. Type the **User name** for the previously configured service account.

> **Note**
>
> The format for the service account is as follows:
>
> domain\user name

7. Type the **Password** for the service account.
8. Click **Next >**.

   The discovery mailbox selection screen appears.
9. Select a discovery mailbox that stores the Search & Destroy search results from the **Available Discovery Mailbox(es)** list.
10. Click **Next >**.

    The generate PST search results screen appears.
11. Select the **Allow Search & Destroy users to generate a .pst file containing all search results** option to configure ScanMail to create the <ScanMail installation path>\SmexSDPst folder and share the folder with the Exchange Trusted Subsystem.

> **Note**
>
> Ensure that the account is a member of the Exchange Mailbox Import Export role.

12. Click **Next >**.

    The Search & Destroy activation details screen appears.

> **Note**
>
> If the service account or discovery mailbox provided are invalid, the activation process cannot proceed. For possible reasons why Search & Destroy activation was unsuccessful, see *Troubleshooting Search & Destroy on page 13-22*.

13. Review the Search & Destroy settings and click **Finish**.

About Mailbox Searches

A mailbox search discovers email messages, mailbox components (for example, meetings or contacts), and specialized items in the Exchange environment, that contain specified keywords.

The following table lists the Search & Destroy mailbox search types.

TABLE 13-1. Mailbox Search Types

TYPE	DESCRIPTION
Estimate Matches	ScanMail searches the Exchange environment and returns an estimated count and an estimated size of the mailbox components that matched the search criteria. ScanMail does not copy the matched items to the discovery mailbox. Performing an estimate search allows administrators to evaluate the effectiveness of the search criteria before copying a large amount of data to the discovery mailbox. If an estimated search returns an excessively large number of matches, consider refining the search criteria to target more specific matches. **Tip** Trend Micro recommends performing an estimated search before performing **Search Now** or **Search Later**. Copying large amounts of data to the discovery mailbox requires more system resources and could result in reduced performance.
Search Now	ScanMail searches the Exchange environment and copies the mailbox components that match the search criteria to the specified discovery mailbox.
Search Later	Administrators can schedule mailbox searches to run at specific times to reduce the system resource usage at peak traffic times.

Syntax Used for Keyword Strings

Administrators can specify the keywords to locate using several different methods. Properly formatted keyword search strings reduce the number of matches and make

searches more efficient and productive. ScanMail allows administrators to use logical operators, wildcards, and Advanced Query Syntax (AQS) or Keyword Query Language (KQL) to narrow the scope of keyword searches.

TABLE 13-2. Keyword Syntax

TYPE OF SYNTAX	DESCRIPTION	EXAMPLES
Logical operators	Use uppercase logical operators (AND, OR, NOT) to separate multiple keywords.	• administrator AND password Matches mailbox components that contain both the words “administrator” and “password” • administrator OR salary Matches mailbox components that contain either the word “administrator” or “salary” • administrator AND NOT payroll Matches mailbox components that contain the word “administrator” and do not contain the word “payroll”
Parentheses	Use parentheses () to group keywords in specific patterns.	• (administrator OR password) AND NOT salary Matches mailbox components that contain either the word “administrator” or “password” and do not contain the word “salary” • (administrator AND NOT password) OR salary Matches mailbox components that contain the word “administrator” and do not contain the word “password”, or mailbox components that contain the word “salary”

Type of Syntax	Description	Examples
Double quotation marks	Use double quotation marks ("") to search for phrases.	• "administrator salary" Matches mailbox components that contain the phrase "administrator salary" • "administrator salary" AND "year ending" Matches mailbox components that contain both the phrases "administrator salary" and "year ending" • ("administrator salary" OR payroll) AND "year ending") Matches mailbox components that contain the phrase "administrator salary" or the word "payroll", and also contain the phrase "year ending"
Wildcard (asterisk)	Use an asterisk (*) as a wildcard operator to search for a range of keywords starting with a specific string. **Note** ScanMail only supports the use of wildcard symbols at the end of a string.	• admin* Matches mailbox components containing words beginning with "admin" Examples: admin, administrator, administration, administrative

Type of Syntax	Description	Examples
Advanced Query Syntax (AQS)	AQS is a Windows search query language that allows for programmatic searching of the Exchange 2010 environment.	For a detailed explanation and code examples for using AQS, refer to the following website: http://msdn.microsoft.com/en-us/library/bb266512.aspx
Keyword Query Language (KQL)	KQL is a search query language that allows for programmatic searching of the Exchange 2013 environment.	For a detailed explanation and code examples for using KQL, refer to the following website: http://msdn.microsoft.com/en-us/library/ee558911.aspx

Mailbox Search Options

ScanMail provides multiple search options to narrow the scope of mailbox searches. Properly configured mailbox searches reduce the usage of system resources and return only relevant search results.

Tip

Trend Micro recommends performing an estimated search before performing **Search Now** or **Search Later**. Copying large amounts of data to the discovery mailbox requires more system resources and could result in reduced performance.

Configure the following search options to streamline mailbox search matching.

TABLE 13-3. Mailbox Search Options

OPTION	DESCRIPTION
Keywords	ScanMail searches for the keywords or phrases that the administrator specifies. Use logical operators, parentheses, double quotation marks, wildcards, AQS expressions (for Exchange 2010), or KQL expressions (for Exchange 2013) to narrow the search parameters. For details on searching for keywords, see *Syntax Used for Keyword Strings on page 13-6*. **Note** The maximum allowable character length of the **Keywords** field is 8192.

OPTION	DESCRIPTION
Mailboxes	Administrators may choose to search all mailboxes in the Exchange environment or choose specific users or distribution groups. **Note** Trend Micro recommends performing mailbox searches on a limited number of users or distribution groups. Copying large amounts of data to the discovery mailbox requires more system resources and could result in reduced performance. To select **Specific user or distribution group members' mailboxes**: 1. Type a search string in the text box to find the available users, distribution groups, or databases and click **Search**. 2. Select the accounts or databases to search in the available list and click **Add >>**. Alternatively, administrators can import pre-existing lists from properly formatted .txt files. **Note** The maximum allowable number of email addresses to search is 500. When importing a file, ScanMail only adds addresses to the **Selected Mailbox(es)** list until the list contains 500 addresses.

OPTION	DESCRIPTION
Mailbox Components	ScanMail can search all mailbox components in the Exchange environment or administrators may choose to scan only specific components. When choosing specific components, the following options are available: • **Email** • **Meetings** • **Journal** • **Tasks** • **Contacts** • **Notes** • **Instant messaging conversations** **Note** When selecting **All mailbox components (including components not listed below)**, ScanMail includes results found in any component that exists in the Exchange mailbox.
Specific Senders or Recipients	ScanMail searches email messages addressed to the specified recipients or from the specified senders. **Note** ScanMail can search specific senders and recipients using display names, email addresses, or domain names.
Date	Administrators may choose to search all components in the Exchange environment or only those components created within a specified date range.
Discovery Mailbox	Administrators may choose to use a specific discovery mailbox for the search or accept the previously configured default Search & Destroy discovery mailbox.

OPTION	DESCRIPTION
Action	ScanMail provides two search actions: • **Search and compile**: All matched results are compiled for review (recommended) • **Search and delete**: All matched results are automatically deleted (not recommended) **Note** Trend Micro only recommends automatically deleting messages in high security environments.

Configuring a Mailbox Search

Procedure

1. Go to **Search & Destroy** > **Mailbox Search**.

   The **Mailbox Search** screen appears.

2. Click **New**.

   The **New Mailbox Search** screen appears.

3. Type a **Name** for the mailbox search.

4. Specify the **Keywords** for ScanMail to locate.

   For details on searching for keywords, see *Syntax Used for Keyword Strings on page 13-6*.

   Note
   The maximum allowable character length of the **Keywords** field is 8192.

5. Specify the **Mailboxes** to search.

Tip

Trend Micro recommends selecting specific mailboxes for each mailbox search. Selecting to **Search all mailboxes** requires more system resources and could result in reduced performance.

6. Optionally configure the following additional search options:

   - **Mailbox Components**
   - **Specific Senders or Recipients**
   - **Date**
   - **Discovery Mailbox**
   - **Action**

   For details on the search criteria, see *Mailbox Search Options on page 13-9*.

7. Click one of the following buttons:

   - **Estimate Matches**: Starts searching for the specified criteria. ScanMail returns an estimated count and an estimated size of the mailbox components that matched the search criteria.

     Tip

     Trend Micro recommends performing an estimated search before performing **Search Now** or **Search Later**. Copying large amounts of data to the discovery mailbox requires more system resources and could result in reduced performance.

   - **Search Now**: Starts searching for the specified criteria. ScanMail copies the mailbox components that match the search criteria to the specified discovery mailbox.
   - **Search Later**

     The Mailbox Search Schedule screen appears.

     a. Select the **Time zone** for the search to use.

b. Specify the **Date and time** of the search.

c. Click **OK** to schedule the search.

- **Save**: Saves the search criteria options without searching the Exchange environment.
- **Cancel**: Discards all changes.

Note

A mailbox search may take some time to complete. Administrators can continue using ScanMail and navigate away from the Search & Destroy feature without interrupting the search.

After initiating or saving a mailbox search, the search appears in the table on the **Mailbox Search** screen.

Modifying a Mailbox Search

ScanMail allows administrators to modify the search criteria for a mailbox search even after the search completes. If a search returns a large number of results, administrators may want to narrow the scope of the search to obtain more accurate results.

WARNING!

Modifying the search criteria of a search that has already completed automatically deletes any of the original search results stored in the Exchange discovery mailbox and the ScanMail database.

Procedure

1. Click **Search & Destroy** > **Mailbox Search**.
2. Click the **Name** of the search to modify.

   The **View Mailbox Search** screen appears.

3. Select **Allow changes to the search options**.

   ScanMail unlocks all of the search criteria fields for editing.

4. Modify the necessary settings.

   For details on refining keyword strings, see *Syntax Used for Keyword Strings on page 13-6*. For details on search criteria options, see *Mailbox Search Options on page 13-9*.

5. Click one of the following buttons:

   - **Estimate Matches**: Starts searching for the specified criteria. ScanMail returns an estimated count and an estimated size of the mailbox components that matched the search criteria.

     Tip

     Trend Micro recommends performing an estimated search before performing **Search Now** or **Search Later**. Copying large amounts of data to the discovery mailbox requires more system resources and could result in reduced performance.

   - **Search Now**: Starts searching for the specified criteria. ScanMail copies the mailbox components that match the search criteria to the specified discovery mailbox.

   - **Search Later**

     The Mailbox Search Schedule screen appears.

     a. Select the **Time zone** for the search to use.

     b. Specify the **Date and time** of the search.

     c. Click **OK** to schedule the search.

   - **Save**: Saves the search criteria options without searching the Exchange environment.

   - **Cancel**: Discards all changes.

Note

A mailbox search may take some time to complete. Administrators can continue using ScanMail and navigate away from the Search & Destroy feature without interrupting the search.

After initiating or saving a mailbox search, the search appears in the table on the **Mailbox Search** screen.

Deleting a Mailbox Search

Administrators can choose to delete a mailbox search from ScanMail only, or delete both the ScanMail results and the results stored in the discovery mailbox.

Note

Deleting a mailbox search does not delete the mailbox components stored in the users' mailboxes.

Procedure

1. Go to **Search & Destroy** > **Mailbox Search**.

   The **Mailbox Search** screen appears.

2. Select the check box next to the mailbox search to delete.

3. Click the **Delete** button and select from the following:

   - **Delete search only**: Deletes only the mailbox search and the search criteria
   - **Delete search and discovery mailbox results**: Deletes the mailbox search, search criteria, and all related messages stored in the Exchange discovery mailbox

Viewing Mailbox Search Results

After ScanMail completes a mailbox search, administrators can view a detailed list of the messages retrieved.

Procedure

1. Click **Search & Destroy** > **Mailbox Search**.

   The **Mailbox Search** screen appears.

2. Choose to view a summary of the search operation before the complete list of search results or directly view a complete list of the search results.

   - To view a summary of the search operation first:

     a. Click the **Name** of the search.

     b. View the summary information in the **Status** section.

     Consider refining the search criteria if the search produced a large number of matches. For details, see *Modifying a Mailbox Search on page 13-15*.

     c. Click **View Search Results**.

   - To view the search results directly, click the **View** link under the **Search Result** column of the table beside the name of the search.

   The **Mailbox Search Results** screen appears.

3. Administrators have the option to create, copy, and delete PST files containing all search results. The **Search results package (.pst file)** status determines the options available to administrators:

   - **Not generated**: Click the **Generate** button to create the PST package in the <ScanMail installation path>\SmexSDPst folder.

   - **Available on server**

     - Click the **Download** button to copy the PST file to a local location.

- Click the **Delete** button to delete the PST file from the <ScanMail installation path>\SmexSDPst folder.

Note

ScanMail automatically deletes the PST file if the administrator performs the same mailbox search again.

4. Administrators can perform the following tasks on the search results:

- Filter the search results

  a. Select which part of the message to search in by selecting from the **Filter by** drop-down box.

  b. Type the search text in the text box.

  c. Click **Filter**.

  Note

  Click **Show All** to reset the filter criteria.

- **Delete** selected results
- **Delete All** search results

Note

When deleting messages, if a message selected for deletion has been moved to another location or already deleted by the end user, ScanMail cannot locate the message and reports a successful deletion.

- Export results to a CSV file
- View details about individual messages by moving the mouse pointer over the **Subject** of the message

Configuring Search & Destroy Settings

Specify the Active Directory service account and the discovery mailbox that stores the search results.

Note

Ensure that a properly configured Active Directory service account and discovery mailbox exist in the Exchange organization before changing the Search & Destroy settings.

Procedure

1. Click **Search & Destroy** > **Settings**.

   The **Search & Destroy Settings** screen appears.

2. Type the **User name** for the service account that performs the backend searches.

   Note

   The format for the service account is as follows:

   domain\user name

3. Type the **Password** for the service account.

4. Select a discovery mailbox that stores the Search & Destroy search results from the **Available Discovery Mailbox(es)** list.

5. Optionally select the **Allow Search & Destroy users to generate a .pst file containing all search results** option to display the PST generation options on the **Mailbox Search Results** screen.

Note

- ScanMail automatically creates the folder <ScanMail installation path>\SmexSDPst and shares the folder with the Exchange Trusted Subsystem.
- Ensure that the account is a member of the Exchange Mailbox Import Export role
- Create a mailbox for this account (Exchange 2013 only)

6. Click **Save**.

Viewing Search & Destroy Event Logs

ScanMail records detailed event tracking logs for Search & Destroy. Because Search & Destroy allows administrators to view and delete Exchange components from users' mailboxes, a comprehensive audit trail of Search & Destroy operations may be useful in case of user misunderstandings.

Procedure

1. Go to **Logs** > **Query**.

   The **Log Query** screen appears.

2. Specify the dates to search.
3. In the **Type** drop-down, select **Event Tracking**.
4. Select the user account(s) for ScanMail to locate and click **Add**.
5. Select **Search & Destroy logs** beside **Log type**.
6. From the drop-down beside Search & Destroy logs, select from the following events:
   - **All**
   - **Configuration change**

- **Operation**
- **Task status change**

7. Optionally, type a description for the logs.
8. Specify the **Sort by** and **Display** options.
9. Click **Display Logs**.

Troubleshooting Search & Destroy

The following table lists possible reasons why Search & Destroy search tasks may be unsuccessful. Because the Exchange server returns the error results, ScanMail cannot predict all reasons.

TABLE 13-4. Possible Reasons Why Search Actions Are Unsuccessful

ERROR	POSSIBLE REASONS	UNSUCCESSFUL MAILBOX SEARCH ACTION
Search & Destroy service account is invalid	• The service account has expired • The password provided is inaccurate • The service account is not a member of the Exchange discovery management group	• Estimate Matches/Search • Delete (message) • Delete task and mail in discovery mailbox • Stop Search

Error	Possible Reasons	Unsuccessful Mailbox Search Action
Discovery mailbox connection error	• The Exchange system discovery mailbox is unreachable	• Estimate Matches/Search • Stop Search
	• The selected discovery mailbox is unreachable	• Estimate Matches/Search • Delete (message) • Delete task and mail in discovery mailbox
	• The selected discovery mailbox is full	• Estimate Matches/Search
End user mailbox connection error	The end user mailbox is unreachable	• Estimate Matches/Search • Delete (message)
Exchange web service is unavailable	• WinRM error • CAS server error	• Estimate Matches/Search • Delete (message) • Delete task and mail in discovery mailbox • Stop Search
Parse search result was unsuccessful	• The Exchange discovery management group does not have full access permission to the selected discovery mailbox • The Exchange web service is unavailable • The discover mailbox is not accessible	• Search

Error	Possible Reasons	Unsuccessful Mailbox Search Action
The current Exchange settings only allow searches of 1 -%N mailboxes. Select a valid number of mailboxes or change the current Exchange settings and try again.	• No mailboxes exist in the selected database • The number of mailboxes in the selected database exceeds the maximum limit defined in the Exchange throttling policy For details on modifying the Exchange throttling policy, see *Exchange Server 2013 Throttling Policy Settings on page D-17*.	Estimate Matches/Search

Chapter 14

Configuring Virtual Analyzer

This chapter explains how to configure Virtual Analyzer settings to protect your Exchange environment.

Topics include:

- *About Virtual Analyzer on page 14-2*
- *Configuring Virtual Analyzer Settings on page 14-2*

About Virtual Analyzer

Virtual Analyzer is a secure virtual environment used to manage and analyze samples submitted by Trend Micro products. Sandbox images allow observation of file and network behavior in a natural setting without any risk of compromising the network. Virtual Analyzer performs static analysis and behavior simulation to identify potentially malicious characteristics. During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the sample based on the accumulated ratings.

Virtual Analyzer includes the following features:

- Threat execution and evaluation summary
- In-depth tracking of malware actions and system impact
- Network connections initiated
- System file/Registry modification
- System injection behavior detection
- Identification of malicious destinations and command-and-control (C&C) servers
- Exportable forensic reports and PCAP files
- Generation of complete malware intelligence for immediate local protection

ScanMail supports integration with Virtual Analyzer in the following Trend Micro separately-licensed products:

- Deep Discovery Analyzer 5.0
- Deep Discovery Advisor 2.92 or later

Configuring Virtual Analyzer Settings

Before configuring the Virtual Analyzer settings, select the **Enable Advanced Threat Scan Engine** option on the **Security Risk Scan: Target** screen. Advanced Threat Scan Engine performs the aggressive scanning necessary to detect advanced threats.

Important

- Virtual Analyzer settings are not configurable until an administrator enables the Advanced Threat Scan Engine.
- Before enabling Virtual Analyzer integration, administrators must enable the Exchange replay folder.

  For details on enabling the Exchange replay folder, see *Virtual Analyzer - Integration Pre-requisites on page D-19*.

WARNING!

Disabling the Exchange replay folder after enabling the Virtual Analyzer integration may cause unexpected issues. Trend Micro recommends disabling Virtual Analyzer integration before disabling the Exchange replay folder.

Procedure

1. Go to **Virtual Analyzer**.
2. Select **Submit email messages to Virtual Analyzer**.
3. Configure the Virtual Analyzer connection settings:
   - Type the **IP address**.

     Note

     The IP address supports IPv4 format.
   - Type the **Port** number.
   - Type the **API key**.

     Note

     Contact the Virtual Analyzer administrator to obtain the IP address, port number, and a valid API key.
4. Select **Use a proxy server to connect to Virtual Analyzer** if ScanMail requires a proxy for server communication with Virtual Analyzer.

a. Click the expand button ( ) to display the proxy settings.

b. Type the server name or IP address of the proxy server and its port number.

c. If your proxy server requires a password, type your user name and password in the fields provided.

5. Click one of the following buttons:

- **Register**: Establishes the connection to Virtual Analyzer
- **Test Connection**: Verifies the connection settings to Virtual Analyzer but does not register ScanMail to the server

Note

To enable sending messages to Virtual Analyzer, register Virtual Analyzer before saving the connection settings.

6. Select the traffic direction of the messages to analyze.

7. Choose the recipients of the messages to analyze by searching and selecting AD Users/Groups/Contacts/Special Groups and adding them to the Selected Account(s) list.

8. Select the attachment types to analyze.

Tip

As application and executable files pose the greatest threats in respect to advanced threats, Trend Micro recommends only selecting to analyze these file types.

9. Configure the **Security Level** settings for the messages and files that Virtual Analyzer analyzes.

- Security level: The security level determines whether ScanMail performs an action on messages and files analyzed and rated by Virtual Analyzer. The available security level settings are: **High**, **Medium**, or **Low**.

Note

For messages and files with a rating that violates the configured security level, ScanMail performs the action configured for **Advanced threats** on the Security Risk Scan **Actions** tab (**Security Risk Scan** > **Action**). For more information, see *Configuring Security Risk Scan Actions on page 7-8*.

- **Maximum wait time for analysis ratings**: Select the maximum amount of time to temporarily quarantine messages while Virtual Analyzer analyzes the risk of the message.
- **Action on time out**: Select the action that ScanMail performs on messages for which Virtual Analyzer did not return a rating within the configured wait time.

Part III

Managing ScanMail

Chapter 15

Managing the Quarantine Area

This chapter describes how to manage the quarantine area. Quarantine is one of the actions that ScanMail can take when messages matches certain rules.

Topics include:

- *About the Quarantine on page 15-2*
- *Configuring the Quarantine Folder/Directory on page 15-2*
- *Performing a Quarantine Query on page 15-3*
- *Scheduling Automatic Quarantine Maintenance on page 15-4*
- *Manually Performing Quarantine Maintenance on page 15-5*
- *Resending Quarantined Messages on page 15-5*

About the Quarantine

ScanMail uses Quarantine to move infected messages to a quarantine directory, replace the infected files, and deliver the remaining messages to the original recipient.

You can configure ScanMail to quarantine or back up email messages when it detects content filtering violations. You can set the quarantine or backup folder for each content filtering rule individually from the Select an action screen, or you can specify a global directory.

Configuring the Quarantine Folder/Directory

When you specify a global quarantine or backup directory, ScanMail moves all files that it quarantines or performs backup on as a result of content rule violations to the directory that you specify.

Specify the quarantine directory separately for each scan filter.

TABLE 15-1. Quarantine Directory Scan Filter Reference

SCAN FILTER	REFERENCE
Security Risk Scan	*Configuring Security Risk Scan Actions on page 7-8*
Attachment Blocking	*Configuring Attachment Blocking Actions on page 8-5*
Content Filtering	• For policy-specific directories: *Configuring Content Filtering Actions on page 9-10* • For global directories: *Global Settings on page 9-4*
Data Loss Prevention	• For policy-specific directories: *Configuring DLP Actions on page 10-22* • For global directories: *Global Settings on page 10-18*

SCAN FILTER	REFERENCE
Web Reputation	*Configuring Web Reputation Actions on page 12-6*

Performing a Quarantine Query

You can perform a query on quarantined messages before deciding on the action to be taken. After viewing the message details, you can choose to release or delete the quarantined messages.

Procedure

1. Click **Quarantine** > **Query**.

   The **Quarantine Query** screen displays.

2. Select the date range.

3. Select **All reasons** or **Specified reasons**:

   - **Security risk scan**
   - **Attachment blocking**
   - **Content filtering**
   - **Data Loss Prevention**
   - **Unscannable message parts**
   - **Web Reputation**

4. Select the resend status.

   - **Never been resent**
   - **Resent at least once**
   - **Any status**

5. (Optional) Specify the sender, recipient, and/or subject of the message.

6. Specify the option for **Sort by**.
7. Specify the number of items to display per page.
8. Select the **Query targets** for the query.
   - **Local server**
   - **Remote server(s)**
     a. Select the **Server group** from the drop-down.
     b. Click the server name in the **Available Server(s)** list and click **Add >>** to include the server(s) to the **Selected Server(s)** list.
9. Click **Search**.

Scheduling Automatic Quarantine Maintenance

Configure scheduled deletion of quarantined messages or manually delete quarantined messages from the **Quarantine Maintenance** screen.

Procedure

1. Click **Quarantine** > **Maintenance**.

   The **Quarantine Maintenance** screen displays.
2. Click the **Automatic** tab.
3. Select **Enable automatic maintenance** to delete logs automatically.
4. Select the files to delete:
   - **All quarantined files**: Select to delete all quarantined files.
   - **Quarantined files that have never been resent**: Select to delete quarantined files that have never been resent.
   - **Quarantined files that have been resent at least once**: Select to delete quarantined files that have been resent at least once.

5. Specify the number of days to keep files before deleting.
6. Click **Save**.

Manually Performing Quarantine Maintenance

Procedure

1. Click **Quarantine** > **Maintenance**.

   The **Quarantine Maintenance** screen displays.
2. Click the **Manual** tab.
3. Select the files to delete:
   - **All quarantined files**: Select to delete all quarantined files.
   - **Quarantined files that have never been resent**: Select to delete quarantined files that have never been resent.
   - **Quarantined files that have been resent at least once**: Select to delete quarantined files that have been resent at least once.
4. Specify the number of days to keep files before deleting.
5. Click **Delete Now**.

Resending Quarantined Messages

You can resend messages that you consider to be safe to the original recipient. When you resend messages, the entire email message or the message part is resent.

Procedure

1. Click **Quarantine** > **Query**.

The Quarantine Query screen displays.

2. Set up and run a query for the kind of message you want to resend.

   The query runs and displays the results at the bottom of the screen.

3. Select the email messages that you want to resend from the results of your query.

4. Click **Resend**.

   The **Quarantine > Resend** screen opens displaying resending options.

5. Click **Add original recipients** to have ScanMail send the email message to the original recipient.

6. Type an email address in the forward field. ScanMail will send the quarantined email message to the person at this email address in addition to, or instead of, the original recipient.

Note

Type the recipient's email address in the **Fw** field for ScanMail with Exchange Server 2013, 2010, and 2007 Edge Transport server role.

---

7. Append the original email message:

   a. Click **Append the original email subject**.

      This has ScanMail include the message that appears in the subject line when it resends the email message.

   b. Type a new subject for the resent email in the **Subject** field or do nothing to accept the default.

      The default subject line cautions the recipient about opening a resent email message.

8. Type a message in the **Body** field for ScanMail to use as the body of your resent email message.

9. Click **Delete all related quarantined files after resending** to have ScanMail delete the original quarantined message after it is resent.

By default, ScanMail keeps email messages when they are resent (the check box is clear).

10. Click **Resend Now**.

    ScanMail sends the email message immediately. A progress bar appears to show you the progress of the resend process.

11. When the Resend process is complete, click **OK** to return to the **Quarantine Query** screen.

Note

Automatically deleting messages after resending deletes the quarantine record in the database.

Chapter 16

Monitoring ScanMail

This chapter describes notifications, reports, and logs to help you monitor your network.

Topics include:

- *Viewing the Summary Screen on page 16-2*
- *About Alerts on page 16-5*
- *About Reports on page 16-11*
- *About Logs on page 16-15*

Viewing the Summary Screen

The **Summary** screen provides a simple and current report on the ScanMail system and functions. Monitor the current status of the different features and the number of security threats ScanMail has detected. To see more detailed information, generate reports from the **Reports** menu.

Summary: System

TABLE 16-1. The System Summary Screen Information

ITEM	DESCRIPTION
Scan Summary for Today	
Detected viruses/ malware	The number of virus/malware detections is not the number of unique viruses/malware. The number of virus/malware detections is the number of times ScanMail detects a virus/ malware.
Uncleanable viruses/ malware	View the number of detected viruses/malware that could not be cleaned.
Detected spyware/ grayware	View the number of detected spyware/grayware.
Detected advanced threats	View the number of detected advanced threats.
Blocked attachments	View the number of attachments blocked by the attachment blocking policy
Spam messages	View the number of spam messages detected by content scanning.
Phishing messages	View the number of phishing messages detected by content scanning.
Content filtering violations	View the number of content filtering rule violations detected.

ITEM	DESCRIPTION
Suspicious URLs - Web reputation	View the number of suspicious URLs detected by Web reputation.
Data Loss Prevention incidents	View the number of Data Loss Prevention policy incidents detected
Blocked connections - Email reputation	View the number of Email reputation detections of messages from spam sources. Email reputation blocks messages from spam sources from entering the network, so there are no messages to scan.
Unscannable message parts	View the number of message bodies and attachments not scanned as specified by the Scan Restriction Criteria.
Scan Method	
Security risk scan method	View the security risk scan method in this section.
Web reputation source	View the web reputation source in this section.
Smart Protection Service	View the current server address and status for each Smart Protection service running.
Update Status	
Update	Click to update the selected components.
Component	View the component's current version, available version, and update status. Select components to manually update.

Note

ScanMail Standard version does not include spam prevention, content filtering, or Data Loss Prevention capabilities.

Summary: Security Risks

TABLE 16-2. Summary: Security Risk Information

ITEM	DESCRIPTION
Security Risk Summary for Today	View the total number of security risks detected and the percentage of those that were uncleanable, spyware/grayware, and advanced threats.
Viruses/Malware Graph	View the total messages scanned and the number of viruses/malware detected in a graph.
Spyware/Grayware Graph	View the total messages scanned and the number of spyware/grayware detected in a graph.
Advanced Threats Graph	View the total messages scanned and the number of advanced threats detected in a graph.
Top Viruses/Malware	View the viruses/malware that have been detected the most number of times.
Top Spyware/Grayware	View the spyware/grayware that have been detected the most number of times.
Top Advanced Threats	View the advanced threats that have been detected the most number of times.

Summary: Spam

The **Summary** screen provides a simple and current report on the ScanMail system and functions. To see more detailed information, generate reports from the **Reports** menu.

TABLE 16-3. Summary Spam Information

ITEM	DESCRIPTION
Scan Status for Today	Click the current spam detection level to change the setting.
Spam Summary for Today	View the total number of messages, spam, phishing, and reported false positive(s).

ITEM	DESCRIPTION
Spam Detection Graph	View a graph of the total messages scanned, reported false positives, and spam detected.
Top Reported False Positives	View the false positives that have been reported the most number of times.

Note

ScanMail Standard versions do not have spam prevention, Data Loss Prevention, or content filtering capabilities. Spam prevention features are not available for ScanMail with Exchange Server 2010 and 2007 Mailbox server roles.

About Alerts

Administrators can configure ScanMail to send notifications to designated individuals when significant system events or security outbreaks occur. ScanMail can send notifications by email message and Simple Network Management Protocol (SNMP) or write to a Windows event log.

System Events

A brief description of the system events options is available below (**Alerts** > **System Events**).

Click an event link to configure the alert notification. For details on the notification settings, see *Alert Notification Settings on page 16-10*.

TABLE 16-4. System Events

EVENT	DESCRIPTION
ScanMail Services	
ScanMail service did not start successfully	ScanMail service was not started successfully.

EVENT	DESCRIPTION
ScanMail service is unavailable	ScanMail for Microsoft Exchange Master Services stopped unexpectedly.
ScanMail Events	
Smart Protection Server - Each time File Reputation service was	Select to receive an alert each time the Smart Protection Server is available or unavailable.
Smart Protection Server - Each time Web Reputation service was	Select to receive an alert each time the Smart Protection Server is available or unavailable.
Virtual Analyzer - Each time the Virtual Analyzer server was	Select to receive an alert each time the Analyzer server is available or unavailable.
Update - Each time update was	Select to receive an alert each time an update is successful or unsuccessful.
Update - Last update time is older than	Select to receive an alert each time the last update time is older than the time you specify.
Manual/Scheduled scan tasks were	Select to receive an alert each time the scan tasks are successful or unsuccessful. **Note** This option does not display for Exchange Server 2010 and 2007 Edge/Hub Transport server roles.
Manual/Scheduled scan time exceeds	Select to receive an alert each time the time to perform scan tasks exceeds the time you specify. **Note** This option does not display for Exchange Server 2010 and 2007 Edge/Hub Transport server roles.

EVENT	DESCRIPTION
Search & Destroy - Each time a search was **Note** This alert only appears after activating the Search & Destroy feature.	Select to receive an alert each time a Search & Destroy mailbox search is successful or unsuccessful.
The local drive (volume) space for the backup, quarantine, and archive directories is less than	Select to receive an alert each time the available disk space reaches the minimum you specify.
The quarantine and log database size exceeds **Note** This alert only appears before activating the Search & Destroy feature.	Select to receive an alert each time the size of the database grows larger than the size you specify.
The size of the database for quarantine, logs, and mailbox search results exceeds **Note** This alert only appears after activating the Search & Destroy feature.	Select to receive an alert each time the size of the database grows larger than the size you specify.
Outbreak Prevention Mode started successfully	Control Manager puts ScanMail in Outbreak Prevention Mode. **Note** If ScanMail is not registered to Control Manager this does not display

EVENT	DESCRIPTION
Outbreak Prevention Mode stopped and restored configuration successfully	ScanMail is no longer in Outbreak Prevention Mode. **Note** If ScanMail is not registered to Control Manager this does not display
Exchange Events	
The SMTP messages queued continuously exceeds the following number within the specified time	Select to receive an alert each time the SMTP messages queued exceeds the number you specify within a time frame. **Note** This option does not display for Exchange Server 2010 and 2007 mailbox server roles.
The disk space on the local drive of the transaction log is less than	Select to receive an alert each time the available disk space reaches the minimum you specify. **Note** This option does not display for Exchange Server 2010 and 2007 Edge/Hub Transport server roles.
The mail store size exceeds	Select to receive an alert each time the mail store size exceeds the size you specify. **Note** This option does not display for Exchange Server 2010 and 2007 Edge/Hub Transport server roles.

Note

To use System Center Operations Manager (SCOM), install the management pack found in the ScanMail installation package and select **Write to Windows event log** in each individual alert setting. Exchange events do not integrate with System Center Operations Manager (SCOM).

Outbreak Alerts

A brief description of the options available on this screen is available below (**Alerts** > **Outbreak Alert**).

Click an event link to configure the alert notification. For details on the notification settings, see *Alert Notification Settings on page 16-10*.

TABLE 16-5. Outbreak Events

EVENT	DESCRIPTION
Viruses/Malware detected reach the following number within the shown time	Set the conditions for the outbreak by setting the number of detected viruses/ malware and a duration of time. ScanMail sends an alert when the number of detected viruses/malware reaches this limit.
Uncleanable viruses/malware reach the following number within the shown time	Set the conditions for the outbreak by setting the number of uncleanable viruses/ malware detected and a duration of time. ScanMail sends an alert when the number of detected uncleanable viruses/malware reaches this limit.
Spyware/Grayware detected reach the following number within the shown time	Set the conditions for the outbreak by setting the number of spyware/grayware detected and a duration of time. ScanMail sends an alert when the number of detected spyware/grayware reaches this limit.

EVENT	DESCRIPTION
Blocked attachments reach the following number within the shown time	Set the conditions for the outbreak by setting the number of blocked attachments and a duration of time. ScanMail sends an alert when the number of blocked attachments reaches this limit.

Alert Notification Settings

Click an alert condition to display the alert notification screen.

TABLE 16-6. Notification Settings

SETTING	DESCRIPTION
Administrator Notification	
Mail	Select to send email message notifications.
To	Type the email address for the administrator.
Subject	Type the subject of the message to send to the administrator.
Message	Click a message element and add it to the notification. For example, click **[Time]** and add it to the message list. The notification message contains the time when ScanMail took the action.
Advanced Notification	
SNMP	Select to send SNMP notifications.
IP address	Specify the SNMP IP address.
Community	Specify the SNMP Community name.

SETTING	DESCRIPTION
Message	Click a message element and add it to the notification. For example, click **[Time]** and add it to the message list. The notification message contains the time when ScanMail took the action.
Write to Windows event log (Select this to allow Microsoft™ System Center Operations Manager to retrieve the Windows event log for alerts.)	Select to send notifications to Windows event log. **Note** To use System Center Operations Manager (SCOM), install the management pack found in the ScanMail installation package and select Write to Windows event log in each individual alert setting. Exchange events do not integrate with System Center Operations Manager (SCOM).

About Reports

Administrators can generate reports to view ScanMail log events in an organized and graphically appealing format. Reports can be printed or sent by email message to a specified address. Administrators can configure the number of reports ScanMail saves on the **Report Maintenance** screen. When the number of reports exceeds the configured number, ScanMail deletes the excess reports beginning with the oldest report.

Example: If there are 15 reports and the maximum number of reports to save is 10, then ScanMail deletes the five oldest reports, leaving the 10 most recently saved reports.

One-time Reports

Generate a one-time report to get a quick summary of ScanMail information. The web console displays the report as soon as it is generated. Administrators can then print or send an email message of the one-time report.

ScanMail saves generated reports in a cache for quick viewing at a later time. ScanMail retains reports until the administrator manually deletes the report or ScanMail deletes them by following the report maintenance settings.

Generating One-time Reports

Procedure

1. Click **Reports** > **One-time Reports** to open the **One-time Reports** screen.
2. Click **Generate report**.
3. Type a **Report name**.
4. Set the time range by typing a date or clicking the calendar icon to select a date.

   ScanMail gathers data to include in the report for the specified time range.
5. Select the servers to include in the report.
   - **Local server**
   - **Remote server(s)**
     a. Select the **Server group** from the drop-down.
     b. Click the server name in the **Available Server(s)** list and click **Add >>** to include the server(s) to the **Selected Server(s)** list.
6. Click the type of information that ScanMail includes in the report.

   Click the **Show details** icon next to the report type to view detailed options for that report.
7. Click **Generate**.

Scheduled Reports

ScanMail generates scheduled reports according to the specified day and time. Administrators can configure ScanMail to deliver reports by email message to an administrator or other recipient.

Scheduled reports follow a template. To generate individual scheduled reports, define the template and then ScanMail generates reports according to that template. Specify the schedule and content included in each individual report for the report template. ScanMail generates a report at the time specified in the template. Each template can have many individual reports that administrators can view by clicking **List Reports** from the **Scheduled Reports** screen. View the content of the template by clicking the template name.

Generating Scheduled Reports

Procedure

1. Click **Reports** > **Scheduled Reports** to open the **Scheduled Reports** screen.
2. Click **Add**.

   The **Schedule Reports > Add Report** screen opens to let you set up your report.
3. Type a name for the report template.
4. Specify the schedule that the template uses to generate individual reports.

   ScanMail can generate reports on a daily, weekly, and monthly basis.
5. Specify the **Generate report at** time when the template generates the individual report.

   Note

   ScanMail uses a 24-hour clock for all time settings.

   For example: After specifying the schedule to be weekly every Sunday and configuring the time for report generation to be 02:00, then ScanMail uses the template to generate an individual report every Sunday at 02:00.
6. Select the servers to include in the report.
   - **Local server**
   - **Remote server(s)**

a. Select the **Server group** from the drop-down.

b. Click the server name in the **Available Server(s)** list and click **Add >>** to include the server(s) to the **Selected Server(s)** list.

7. Select the type of report that ScanMail generates according to the schedule.

8. Set a person to receive a report each time the template generates one.

9. Click **Send to email address:**.

10. Type the recipient's email address

11. Click **Save**.

    The browser returns to the **Scheduled Reports** screen. The new template is added to the list of report templates.

Report Maintenance

Configure the **Report Maintenance** screen to specify the number of reports that ScanMail saves. For one-time reports and scheduled reports, type a number. When the number of reports exceeds the specified limit, ScanMail deletes excess reports, beginning with the oldest report. For scheduled reports saved in each template, the number specified limits the amount of saved reports for each template.

For example, there are five saved report templates. The limit for Scheduled reports saved in templates is 4. This means that each template can generate four individual reports, for a total of 20 reports (5 templates x 4 reports each). If a template generates another report, then ScanMail deletes the oldest generated report for that template, keeping the total number of reports at 20.

A brief description of the options available on the **Report Maintenance** (**Reports** > **Maintenance**) screen is available below.

- **One-time reports**: Specify the maximum number of reports to save.
- **Scheduled reports saved in each template**: Specify the maximum number of reports to save.

- **Report templates**: Specify the maximum number of report templates to save.

About Logs

ScanMail keeps detailed logs that administrators can use when analyzing system security and configuring ScanMail to provide optimal protection for the Exchange environment. ScanMail provides the following log types:

- Security Risk Scan
- Attachment Blocking
- Content Filtering
- Update
- Scan Events
- Back up
- Unscannable Message Parts
- Event Tracking
- Data Loss Prevention
- Web Reputation

Perform a log query to view log information. Use the **Log Query** page to set up and run your queries.

Types of Logs

The following table lists the type of logs:

TABLE 16-7. Types of Logs

TYPE	DESCRIPTION
Security Risk Scan	Information about messages with detected security risks

TYPE	DESCRIPTION
Attachment Blocking	Information about the messages with attachments that ScanMail scanned and blocked
Content Filtering	Information about the messages ScanMail filtered for undesirable content
Updates	Information about whether components were updated successfully **Note** Components include scan engines and pattern files.
Scan Events	Information about whether manual and scheduled scans have been successful or unsuccessful **Note** Scan events do not display for Exchange Server 2010 and 2007 edge/hub transport server roles.
Backup for Security Risk	Information about the files that Security Risk Scan moved to the backup folder before taking action against them
Backup for Content Filter	Information about the files that Content Filtering moved to the backup folder before taking action against them
Unscannable Message Parts	Information about message parts not scanned as defined by the Scan Restriction Criteria
Event Tracking	Information about all product console operations including: • System and vulnerability logs • Search & Destroy logs
Data Loss Prevention	Information about messages that triggered Data Loss Prevention policy incidents
Backup for Data Loss Prevention	Information about the files that Data Loss Prevention moved to the backup folder before taking action against them

TYPE	DESCRIPTION
Web Reputation	Information about messages that ScanMail detected with malicious URLs

Querying Logs

Procedure

1. Click **Logs** > **Query**.

   The **Log Query** screen displays.

2. Select the date range.

3. Select the type of entry.

4. (Optional) Specify any of the following criteria:

   - For **Security Risk Scan**, **Attachment Blocking**, **Content Filtering**, **Unscannable Message Parts**, **Data Loss Prevention**, and **Web Reputation** queries:
     - **Found in**
     - **Sender**
     - **Recipient**
     - **Subject**
     - **Attachment**
   - For **Update** and **Scan Events** queries:
     - **Keyword**
   - For **Event Tracking** queries:
     - **Name**
     - **IP address**

- **Log type**
- **Description**
- **Source type**

5. Specify the option for **Sort by**.
6. Specify the number of items to display per page.
7. Select the **Query targets** for the query.
   - **Local server**
   - **Remote server(s)**
     a. Select the **Server group** from the drop-down.
     b. Click the server name in the **Available Server(s)** list and click **Add >>** to include the server(s) to the **Selected Server(s)** list.
8. Click **Display Logs**.

Log Maintenance

ScanMail keeps detailed logs of security risk scan, content filtering, attachment blocking, spam prevention, updates, scan events, back up, and event tracking. These logs provide a valuable source of system information. Perform log maintenance to manage disk space usage.

Performing Manual Log Maintenance

Procedure

1. Click **Logs** > **Maintenance**.

   The **Log Maintenance** screen displays.
2. Click the **Manual** tab.

3. Select the log types to delete.
4. Specify the number of days to keep logs before deleting.
5. Specify the number of days to keep event tracking logs before deleting.
6. Click **Delete Now** to delete logs and events.

Performing Scheduled Log Maintenance

Procedure

1. Click **Logs** > **Maintenance**.

   The **Log Maintenance** screen displays.
2. Click the **Automatic** tab.
3. Select **Enable automatic maintenance**.
4. Select the log types to delete.
5. Specify the number of days to keep logs before deleting.
6. Specify the number of days to keep event tracking logs before deleting.
7. Click **Save**.

Chapter 17

Performing Administrative Tasks

This chapter describes administrative tasks.

Topics include:

- *Configuring Proxy Settings on page 17-2*
- *Global Notification Settings on page 17-2*
- *Configuring Spam Maintenance on page 17-4*
- *Configuring Real-time Scan Settings on page 17-5*
- *About Access Control on page 17-6*
- *About Special Groups on page 17-8*
- *About Server Groups on page 17-9*
- *About Internal Domains on page 17-10*
- *Product License on page 17-11*
- *World Virus Tracking Program on page 17-12*
- *About Trend Micro Control Manager on page 17-13*
- *Using Trend Support / System Debugger on page 17-16*

Configuring Proxy Settings

Proxy servers are used for added security and more efficient use of bandwidth. If your network uses a proxy server, configure the proxy settings to connect to the Internet, download the updated components necessary to keep ScanMail updated, and check the license status online.

Procedure

1. Click **Administration** > **Proxy**.
2. Select **Use a proxy server for Web Reputation, updates, and product license notifications**. Select this check box to use a proxy server for web reputation queries to Trend Micro reputation servers, updates, and product license notifications.
3. Type the proxy server name or IP address.
4. Type the **Port**.
5. (Optional) Select **Use SOCKS 5 proxy protocol**.
6. If the proxy server requires authentication, specify the user name and password.

Global Notification Settings

Configure ScanMail to send notifications after taking an action. ScanMail administrators typically send notifications to the Exchange administrator, using a global default for the administrator's email address.

Administrators can configure ScanMail to send notifications to the person who is to receive the notification and the person listed as the sender for the notification. That is, when sending notifications, ScanMail lists the address configured on the **Notification Settings** screen as the sender of the message. People receiving the message can contact the sender about the problem.

Setting and applying a global default address for an administrator changes the address in the following locations:

- Security Risk Scan
- Attachment Blocking
- Content Filtering
- Data Loss Prevention
- Spam Prevention
- Web Reputation
- System Alerts
- Outbreak Alerts

Note

Administrators can customize the notification addresses for each of the above locations after applying a default address.

ScanMail divides email traffic into two network categories: internal and external. ScanMail queries the Exchange server to learn how the internal and external addresses are defined. All internal addresses share a common domain and all external addresses do not belong to that domain.

For example, if the internal domain address is "@host.com", then ScanMail classifies addresses such as "abc@host.com" and "xyz@host.com" as internal addresses. ScanMail classifies all other addresses, such as "abc@host.com" and "jondoe@otherhost.com" as external.

ScanMail can automatically send notifications in the following situations:

- Detects and takes action against a security risk or other threat detected in an email message
- Blocks an infected attachment
- Detects suspicious URLs
- Filters out undesirable content from an email message
- Detects and takes action against a Data Loss Prevention incident
- Detects a significant system event
- Detects virus/malware outbreak conditions

Note

For correct resolution of ScanMail notifications with Simple Network Management Protocol (SNMP), import the Management Information Base (MIB) file to the network management tools from the following path in the ScanMail Package: tool\admin\trend.mib.

Configuring Global Notification Settings

Procedure

1. Click **Administration** > **Notification Settings**.
2. Type the email address of the administrator that receives notifications.
3. Type the email address of the sender who sends alerts and notifications.
4. Specify an SNMP IP address and community.
5. Specify the **Internal Email Definition** by selecting **Default** and **Custom internal mail definition**.

   This allows you to customize how ScanMail categorizes email messages as internal.
6. Click **Save**.

Configuring Spam Maintenance

The **Spam Maintenance** screen displays the name of the Spam Folder and the number of days that the End User Quarantine (EUQ) tool retains spam messages. End users can rename the spam folder using Microsoft Outlook. ScanMail identifies the folder by ID, not by folder name.

Procedure

- Select **Enable End User Quarantine** to enable End User Quarantine for all mailboxes on the Exchange server.

Note

After disabling End Use Quarantine and clicking **Save**, ScanMail displays a confirmation message box. Select **Delete End User Quarantine spam folder** to remove the spam folder (and all contents) from client accounts.

- In the **End User Quarantine Settings** section, click **Create spam folder and delete spam messages** to create a new spam folder for each new user that added to the Exchange server with End User Quarantine. Clicking **Create spam folder and delete spam messages** immediately creates the spam folder for the new user.
- In the **Client Spam Folder Settings** section, configure the spam message deletion schedule.
- For Exchange Server 2013, in the **End User Quarantine Account** section, configure the account that manages EUQ tasks.

Note

The End User Quarantine account must have Exchange Management Group privileges and the Exchange ApplicationImpersonation role over all users in the organization to perform EUQ tasks.

To add the account to the ApplicationImpersonation role, use the following cmdlet:

```
New-ManagementRoleAssignment -Name { rule name } -Role
ApplicationImpersonation -User { EUQ account }
```

- In the **End User Quarantine Exception List** section, add or remove users from the exception list. ScanMail does not enable EUQ for users added to this list.

Configuring Real-time Scan Settings

ScanMail performs real-time scan on messages as they are accessed if the message has not been previously scanned using the latest pattern file and scan engine.

Procedure

1. Click **Administration** > **Real-time Scan Settings**.
2. Select **Do not perform on-access scan on email messages older than the following number of days** to limit the messages that are scanned based on the number of days.
3. Specify the number of days.
4. Click **Save**.

About Access Control

Use the role-based administration feature to grant and control access to the ScanMail product console menu and submenu items. If there are multiple ScanMail administrators in the organization, this feature can help delegate management tasks to administrators and manage the menu items accessible to each administrator. Administrators can also grant non-administrators "view only" access to the product console.

Note

Access control is not available in non-console mode when using remote desktop.

Access Control Permissions

A brief description of the access control permissions (**Administration** > **Access Control** > **Permissions**) is available below.

- **Full**: Select to allow users in this group to enable, disable, and configure this feature.
- **Read**: Select to allow users in this group to view this feature and perform the following:

TABLE 17-1. Read Permissions

PERMISSION	DESCRIPTION
Updates	Operators can configure manual updates.
Logs	Operators can query logs.
Reports	Operators can generate logs.
Quarantine	Operators can query quarantined messages and files.

- **None**: Select to hide this feature from users in this group.

Enabling Access Control

Procedure

1. Click **Administration** > **Access Control**.

   The **Access Control** screen displays.

2. Click the icon under **Status** to display a green check icon ( ) which indicates that the access role is enabled. A red x icon ( ) indicates the policy is disabled.

3. Select **Enable Single Sign-On** to allow log on with Microsoft™ Windows™ authentication.

   This feature is only supported with Microsoft™ Internet Explorer™. If Internet Explorer Enhanced Security is enabled, add the ScanMail product console site to the **Local intranet** zone to use this feature.

4. Click **Save**.

Configuring Access Control

Procedure

1. Click **Administration** > **Access Control**.

   The **Access Control** screen displays.

2. Click one of the following access control roles:

   - **Administrator**
   - **Operator**
   - **Search & Destroy Administrator**
   - **Search & Destroy Operator**

3. Click the **Authentication** tab.
4. Specify the description for the group.
5. Add accounts from Active Directory using **Search**.
6. Click **Save**.
7. Click the **Permissions** tab.
8. Select the permissions for this group.
9. Click **Save**.

About Special Groups

Create special groups to easily apply policies to segments of the network. Administrators can import and export special groups for ease of management. Special groups cannot contain other special groups.

After deleting an Active Directory user belonging to a special group, ScanMail displays a notification message in the Special Group Selected Account(s) list.

Configuring Special Groups

Configure special groups for ease of management when creating rules and policies.

Procedure

1. Click **Administration** > **Special Groups**.

   The **Special Group** screen displays.

2. Choose to add or edit a special group:

   - For new special groups:

     Click **Add**.

   - For preexisting special groups:

     Click the group name.

3. Type a name for the special group and specify a description.

4. Search for Active Directory (AD) users to add to the special group or specify an SMTP address.

5. Click **Add >>** to add accounts or **<< Remove** to remove accounts from this special group.

6. Click **Save**.

About Server Groups

Create server groups to easily manage multiple ScanMail servers using the **Server Management** screen.

You can also use Server Groups to monitor multiple ScanMail servers by querying logs and quarantined messages, and creating reports from any ScanMail server.

Note

You cannot modify or delete the default server groups ("All servers", "Mailbox servers", and "Transport servers").

Configuring Server Groups

Procedure

1. Click **Administration** > **Server Groups**.

   The **Server Groups** screen displays.

2. Choose to add or edit a server group:

   - For new server groups:

     Click **Add**.

   - For preexisting server groups:

     Click the group name.

3. Type a name for the server group and specify a description.
4. Click **Add >>** to add servers or **<< Remove** to remove servers from this server group.
5. Click **Save**.

About Internal Domains

Configure your company's internal domains to distinguish them from outgoing mail traffic. Data Loss Prevention policies will disregard email messages that transmit through your internal domains according to the policy configurations. When Data Loss Prevention policies apply to outgoing mail only, no policy violations trigger for the internal domains.

ScanMail allows the usage of the asterisk (*) wildcard to specify internal domains. In order to use the wildcard operator, the following rules apply:

- The asterisk placement is at the beginning of the domain name.
- The asterisk precedes a period (.).

TABLE 17-2. Wildcard Examples

VALID WILDCARD EXAMPLES:	INVALID WILDCARD EXAMPLES:
• *.smex.com • *.yourcompany.com	• *smex.com • smex.*.com • smex.*

Configuring Internal Domains

Procedure

1. On the left navigation pane, click **Administration** > **Internal Domains**.

   The **Internal Domains** screen appears.

2. Type the name of the internal domain you want to exclude from scans.
3. Click **Add >>** to move the domain into the Internal Domains list.
4. Click **Import** to import an internal domain list. Click **Export** to save the internal domain list in a TXT file.
5. Click **Save**.

Product License

The **Product License** screen (**Administration** > **Product License**) displays information regarding the license expiry date, status, version, and Activation Code.

Administrators can use the following controls to manage the product license:

- **Update License**: Click to update the product license.
- **New Activation Code**: Click to use a new Activation Code.

World Virus Tracking Program

Trend Micro World Virus Tracking Program provides continuous communication between Trend Micro products and the company's 24/7 threat research centers and technologies. Each new threat identified through a single customer's routine reputation check automatically updates all of Trend Micro's threat databases, blocking any subsequent customer encounters of a given threat. By continuously processing the threat intelligence gathered through its extensive global network of customers and partners, Trend Micro delivers automatic, real-time protection against the latest threats and provides "better together" security. This is much like an automated neighborhood watch that involves the community in the protection of others. The privacy of a customer's personal or business information is always protected because the threat information gathered is based on the reputation of the communication source.

Trend Micro World Virus Tracking Program collects and transfers relevant data from Trend Micro products to the Smart Protection Network for further analysis, and consequently, advanced solutions evolve. These advanced solutions further enhance the protection for clients.

Some samples of information sent to Trend Micro:

- File checksums
- Websites accessed
- File information, including sizes and paths
- Names of executable files

You can terminate your participation to the program anytime from the web console.

Tip

You do not need to participate in World Virus Tracking Program to protect your computers. Your participation is optional and you may opt out at any time. Trend Micro recommends that you participate in World Virus Tracking Program to help provide better overall protection for all Trend Micro customers.

For more information on the Smart Protection Network, visit:

http://www.smartprotectionnetwork.com

Joining the World Virus Tracking Program

Procedure

1. Click **Administration** > **World Virus Tracking**.
2. Click the **Virus Map** to view worldwide scanning results and statistics.
3. Select **Yes**.
4. Click **Save**.

About Trend Micro Control Manager

Trend Micro™ Control Manager™ is a software management solution that provides the capability to control antivirus and content security programs from a central location-regardless of the program's physical location or platform. This application can simplify the administration of a corporate virus/malware and content security policy.

- **Control Manager server**: The Control Manager server is the machine upon which the Control Manager application is installed. The web-based Control Manager management console is generated on this server.
- **Agent**: The agent is an application installed on a product-server that allows Control Manager to manage the product. It receives commands from the Control Manager server, and then applies them to the managed product. It also collects logs

from the product, and sends them to Control Manager. The Control Manager agent does not communicate with the Control Manager server directly. Instead, it interfaces with a component called the Communicator.

- **Communicator**: The Communicator is the communications backbone of the Control Manager system; it is part of the Trend Micro Management Infrastructure. Commands from the Control Manager server to the managed products, and status reports from the products to the Control Manager server all pass through this component. Only one Communicator is installed on each product server; the Communicator then handles the needs of all the agents on the aforementioned server.
- **Entity**: An entity is a representation of a managed product on the Product Directory link. You see these icons in the directory tree of the Entity section. The directory tree is a composition of all managed entities, residing on the Control Manager console.

About Trend Micro Management Communication Protocol

Trend Micro™ Management Communication Protocol (MCP) is the next generation agent for Trend Micro managed products. Management Communication Protocol (MCP) replaces Trend Micro Infrastructure (TMI) as the way Control Manager communicates with Trend Micro ScanMail™ *for Microsoft™ Exchange* . MCP has several new features:

- Reduced network loading and package size
- NAT and firewall traversal support
- HTTPS support
- One-way and Two-way communication support
- Single sign-on (SSO) support
- Cluster node support

Using ScanMail with Control Manager

- Multiple ScanMail servers can share the same configurations by using Trend Micro Control Manager (TMCM).
- Control Manager 6.0 permits administrators to configure and deploy Data Loss Prevention policies (rules) directly to ScanMail servers from the Control Manager web console.
- Administrators can also use Control Manager to synchronize virus pattern file and other downloads (Control Manager contacts Trend Micro through the Internet; Control Manager then distributes the updates to the various instances of ScanMail through the Intranet).
- Unless included as part of a Control Manager domain, each instance of ScanMail on the network updates its own virus pattern file and other updates.

For more information, see the Control Manager documentation.

Registering to Control Manager

Administrators can manage ScanMail using the Trend Micro Control Manager management console.

Procedure

1. Click **Administration** > **Control Manager Settings**.

   The **Control Manager Settings** screen displays.

2. Under **Connection Settings**, type the name of the ScanMail server in the **Entity display name** field.

3. Under **Control Manager Server Settings** specify the following:

   a. Type the Control Manager server IP address or host name in the **Server FQDN or IP address** field.

   b. Type the port number that the MCP agent uses to communicate with Control Manager.

c. If you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products), select **Connect through HTTPS**.

d. If the network requires authentication, type the user name and password for the IIS server in the **Username** and **Password** fields.

e. If using a NAT device, select **Enable two-way communication port forwarding** and type the NAT device's IP address and port number in **IP address** and **port number**.

Refer to the *Trend Micro Control Manager Administrator's Guide* for more information about managing products in Control Manager.

Unregistering ScanMail from Control Manager

Note

During Outbreak Prevention, administrators cannot unregister from Control Manager or disable communication between the ScanMail MCP agent and the Control Manager server.

Procedure

1. Click **Administration** > **Control Manager Settings**.

   The **Control Manager Settings** screen displays.

2. Under **Connection Status**, click **Unregister**.

   A progress screen displays.

Using Trend Support / System Debugger

ScanMail Debugger can assist you in debugging or reporting the status of the ScanMail processes. When you are having unexpected difficulties, you can use the debugger to create debugger reports and send them to Trend Micro technical support for analysis.

Procedure

1. Click **Administration** > **Trend Support/Debugger** from the main menu.

   The **Trend Support/System Debugger** screen displays.

2. Select the modules to debug:

   - **ScanMail for Microsoft Exchange Master Service**
   - **ScanMail for Microsoft Exchange Remote Configuration Server**
   - **ScanMail for Microsoft Exchange System Watcher**
   - **Virus Scan API (VSAPI)**
   - **Transport Service**
   - **Common Gateway Interface (CGI)**
   - **End User Quarantine (EUQ)**

3. Click **Apply**.

Note

ScanMail does not require that the services restart after enabling or disabling debugging.

Part IV

Getting Help

Chapter 18

Understanding Security Risks

This chapter describes security risks to help you understand possible risks to your network.

Topics include:

- *Understanding the Terms on page 18-2*
- *About Internet Security Risks on page 18-2*
- *About Spyware/Grayware on page 18-13*

Understanding the Terms

Computer security is a rapidly changing subject. Administrators and information security professionals invent and adopt a variety of terms and phrases to describe potential risks or uninvited incidents to computers and networks. The following is a list of these terms and their meanings as used in this document.

Some of these terms refer to real security risks and some refer to annoying or unsolicited incidents. Trojans, viruses/malware, and worms are examples of terms used to describe real security risks. Joke programs, spyware/grayware are terms used to describe incidents that might be harmful, but are sometimes simply annoying and unsolicited. ScanMail can protect against all of the incidents described in this chapter.

About Internet Security Risks

Thousands of viruses/malware are known to exist, with more being created each day. In addition to viruses/malware, new security risks designed to exploit vulnerabilities in corporate email systems and websites continue to emerge. These include spyware/grayware, phish sites, network viruses/malware, Trojans, and worms.

Collectively, these threats are known as security risks. Here is a summary of the major security risk types:

TABLE 18-1. Internet Security Risks

THREAT TYPE	CHARACTERISTICS
Advanced threats	Advanced threats use less conventional means to attack or infect a system. Heuristic scanning can detect advanced threats to mitigate the damage to company systems. Some types of advanced threats that ATSE detects include: • Advanced Persistent Threats (APT): Advanced persistent threats are attacks against targeted companies and resources. Typically, a social engineering attack on an employee triggers a series of activities that open up the company to serious risks. • Targeted attacks: Targeted attacks refer to computer intrusions staged by threat actors that aggressively pursue and compromise specific targets. These attacks seek to maintain a persistent presence within the target's network so that the attackers can move laterally and extract sensitive information. • Exploits: Exploits are code purposely created by attackers to abuse or target a software vulnerability. This code is typically incorporated into malware. • Zero-day attacks: Zero-day attacks exploit previously unknown vulnerabilities in software.
Denial-of-Service (DoS) attack	A DoS attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing ScanMail from scanning files that decompress into very large files helps prevent this problem from happening.
Phish	Unsolicited email requesting user verification of private information, such as credit card or bank account numbers, with the intent to commit fraud.
Spyware/Grayware	Technology that aids in gathering information about a person or organization without their knowledge.

Threat Type	Characteristics
Trojan Horse program	Malware that performs unexpected or unauthorized, often malicious, actions. Trojans cause damage, unexpected system behavior, and compromise system security, but unlike viruses/malware, they do not replicate.
Virus/Malware	A program that carries a destructive payload, and replicates - spreading quickly to infect other systems. By far, viruses/malware remain the most prevalent threat to computing.
Worm	A self-contained program or set of programs that is able to spread functional copies of itself or its segments to other computer systems, typically through network connections or email attachments.
Other malicious codes	ScanMail detects some malicious code that is difficult to categorize, but pose a significant threat to Exchange. This category is useful when you want ScanMail to perform an action against a previously unknown threat type.
Packed files	Potentially malicious code in real-time compressed executable files that arrive as email attachments. IntelliTrap scans for packing algorithms to detected packed files. Enabling IntelliTrap allows ScanMail to take user-defined actions on infected attachments, and to send notifications to senders, recipients, or administrators.

Viruses/Malware

A computer virus/malware is a segment of code that has the ability to replicate by infecting files. When a virus/malware infects a file, it attaches a copy of itself to the file in such a way that when the former executes, the virus/malware also runs. When this happens, the infected file also becomes capable of infecting other files. Like biological viruses, computer viruses/malware can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses/malware share another commonality: a damage routine that delivers a payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage.

Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

Generally, there are three kinds of viruses/malware:

TABLE 18-2. Types of Virus/Malware

TYPE	DESCRIPTION
File	File viruses/malware may come in different types—there are DOS viruses/malware, Windows viruses/malware, macro viruses/malware, and script viruses/malware. All of these share the same characteristics of viruses/malware except that they infect different types of host files or programs.
Boot	Boot viruses/malware infect the partition table of hard disks and boot sector of hard disks and floppy disks.
Script	Script viruses/malware are viruses/malware written in script programming languages, such as Visual Basic Script and JavaScript and are usually embedded in HTML documents. VBScript (Visual Basic Script) and Jscript (JavaScript) viruses/malware make use of Microsoft's Windows Scripting Host to activate themselves and infect other files. Since Windows Scripting Host is available on Windows 98, Windows 2000 and other Windows operating systems, the viruses/malware can be activated simply by double-clicking a *.vbs or *.js file from Windows Explorer. What is so special about script viruses/malware? Unlike programming binary viruses/malware, which requires assembly-type programming knowledge, virus/malware authors program script viruses/malware as text. A script virus can achieve functionality without low-level programming and with code as compact as possible. It can also use predefined objects in Windows to make accessing many parts of the infected system easier (for example, for file infection, for mass-mailing). Furthermore, since the code is text, it is easy for others to read and imitate the coding paradigm. Because of this, many script viruses/malware have several modified variants. For example, shortly after the "I love you" virus appeared, antivirus vendors found modified copies of the original code, which spread themselves with different subject lines, or message bodies.

Whatever their type is, the basic mechanism remains the same. A virus contains code that explicitly copies itself. In the case of file viruses/malware, this usually entails making modifications to gain control when a user accidentally executes the infected program.

After the virus code has finished execution, in most cases, it passes back the control to the original host program to give the user an impression that nothing is wrong with the infected file.

Take note that there are also cross-platform viruses/malware. These types of viruses/malware can infect files belonging to different platforms (for example, Windows and Linux). However, such viruses/malware are very rare and seldom achieve 100% functionality.

Virus/Malware Writers

In the traditional scenario, it was an individual, highly technical and working alone, who would write a virus/malware program and then introduce it onto a computer, network server, or the Internet. Why? Ego, revenge, sabotage, and basic disgruntlement have all been cited as motivations.

Now, however, it takes no special skill to create a macro virus/malware, a mass mailer, or other virus/malware with highly disruptive potential. In fact, "virus kits" proliferate on the Internet and are free for the taking for anyone who wants to try their hand at disrupting the Internet or corporate communications.

And increasingly, organized crime from remote countries is getting into the act by creating sophisticated spyware/grayware programs and phish sites. Distributed through a million spam messages, these exploits are low effort but with a high potential for yielding personal information such as passwords, social security numbers, and credit card numbers.

Malware Naming

Malware, with the exception of boot sector viruses and some file infectors, is named according to the following format:

PREFIX_THREATNAME.SUFFIX

The suffix used in the naming convention indicates the variant of the threat. The suffix assigned to a new threat (meaning the binary code for the threat is not similar to any existing security risks) is the alpha character "A." Subsequent strains are given subsequent suffixes, for example, "B", "C", "D". Occasionally a threat is assigned a

special suffix, (.GEN, for generic detection or .DAM if the variant is damaged or malformed).

Prefix	Description
No prefix	Boot sector viruses or file infector
1OH	File infector
ADW	Adware
ALS	Auto-LISP script malware
ATVX	ActiveX malicious code
BAT	Batch file virus
BHO	Browser Helper Object - A non-destructive toolbar application
BKDR	Backdoor virus
CHM	Compiled HTML file found on malicious websites
COOKIE	Cookie used to track a user's web habits for the purpose of data mining
COPY	Worm that copies itself
DI	File infector
DIAL	Dialer program
"DOS, DDOS"	Virus that prevents a user from accessing security and antivirus company websites
ELF	Executable and Link format viruses
EXPL	Exploit that does not fit other categories
FLOODER	Tool that allows remote malicious hackers to flood data on a specified IP, causing the target system to hang
FONO	File infector
GCAE	File infector

Prefix	Description
GENERIC	Memory-resident boot virus
HKTL	Hacking tool
HTML	HTML virus
IRC	Internet Relay Chat malware
JAVA	Java malicious code
JOKE	Joke program
JS	JavaScript virus
NE	File infector
NET	Network virus
PALM	Palm PDA-based malware
PARITY	Boot virus
PE	File infector
PERL	Malware, such as a file infector, created in PERL
RAP	Remote access program
REG	Threat that modifies the system registry
SPYW	Spyware
SYMBOS	Trojan that affects telephones using the Symbian operating system
TROJ	Trojan
UNIX	Linux/UNIX script malware
VBS	VBScript virus
WORM	Worm

PREFIX	DESCRIPTION
W2KM, W97M, X97M, P97M, A97M, O97M, WM, XF, XM, V5M	Macro virus

Compressed Files

Compression and archiving are among the most common methods of file storage, especially for file transfers - such as email attachments, FTP, and HTTP. Before any virus/malware detection can occur on a compressed file, however, you must first decompress it. For other compression file types, ScanMail performs scan actions on the whole compressed file, rather than individual files within the compressed file.

ScanMail currently supports the following compression types:

- Extraction: used when multiple files have been compressed or archived into a single file: PKZIP, LHA, LZH, ARJ, MIME, MSCF, TAR, GZIP, BZIP2, RAR, and ACE.
- Expansion: used when only a single file has been compressed or archived into a single file: PKLITE, PKLITE32, LZEXE, DIET, ASPACK, UPX, MSCOMP, LZW, MACBIN, and Petite.
- Decoding: used when a file has been converted from binary to ASCII, a method that is widely employed by email systems: UUENCODE and BINHEX.

Note

When ScanMail does not support the compression type, then it cannot detect viruses/malware in compression layers beyond the first compression layer.

When ScanMail encounters a compressed file it does the following:

1. ScanMail extracts the compressed files and scans them.

   ScanMail begins by extracting the first compression layer. After extracting the first layer, ScanMail proceeds to the second layer and so on until it has scanned all of the compression layers that the user configured it to scan, up to a maximum of 20.

2. ScanMail performs a user-configured action on infected files.

   ScanMail performs the same action against infected files detected in compressed formats as for other infected files. For example, if you select **Quarantine entire message** as the action for infected files, then ScanMail quarantines entire messages in which it detects infected files.

   ScanMail can clean files from two types of compression routines: PKZIP and LHA. However, ScanMail can only clean the first layer of files compressed using these compression routines.

Joke Programs

A joke program is an ordinary executable program with normally no malicious intent. Virus authors create joke programs for making fun of computer users. They do not intend to destroy data but some inexperienced users may inadvertently perform actions that can lead to data loss (such as restoring files from an older backup, formatting the drive, or deleting files).

Since joke programs are ordinary executable programs, they will not infect other programs, nor will they do any damage to the computer system or its data. Sometimes, joke programs may temporarily reconfigure the mouse, keyboard, or other devices. However, after a joke program finishes its execution or the user reboots the machine, the computer returns to its original state. Joke programs, while normally harmless, can be costly to an organization.

Macro Viruses/Malware

Macro viruses/malware are application-specific. They infect macro utilities that accompany such applications as Microsoft Word (.doc) and Microsoft Excel (.xls). Therefore, they can be detected in files with extensions common to macro capable applications, such as .doc, .xls, and .ppt. Macro viruses/malware travel between data files in the application and can eventually infect hundreds of files if undeterred.

As these file types are often attached to email messages, macro viruses/malware spread readily by means of the Internet in email attachments.

ScanMail prevents macro viruses/malware from infecting your server in the following ways:

- Detects malicious macro code using heuristic scanning

  Heuristic scanning is an evaluative method of detecting viruses/malware. This method excels at detecting undiscovered viruses/malware and threats that do not have a known virus signature.

- Strips all macro code from scanned files

Mass-Mailing Attacks

Email-aware viruses/malware, like the infamous Melissa, Loveletter, AnnaKournikova and others, have the ability to spread through email by automating the infected computer's email client. Mass-mailing behavior describes a situation when an infection spreads rapidly between clients and servers in an Exchange environment. Mass-mailing attacks can be expensive to clean up and cause panic among users. Trend Micro designed the scan engine to detect behaviors that mass-mailing attacks usually demonstrate. The behaviors are recorded in the Virus Pattern file that is updated using the Trend Micro™ ActiveUpdate Servers.

You can enable ScanMail to take a special action against mass-mailing attacks whenever it detects a mass-mailing behavior. The action configured for mass-mailing behavior takes precedence over all other actions. The default action against mass-mailing attacks is **Delete entire message**.

For example: You configure ScanMail to quarantine messages when it detects a worm or a Trojan in an email message. You also enable mass-mailing behavior and set ScanMail to delete all messages that demonstrate mass-mailing behavior. ScanMail receives a message containing a worm such as a variant of MyDoom. This worm uses its own SMTP engine to send itself to email addresses that it collects from the infected computer. When ScanMail detects the MyDoom worm and recognizes its mass-mailing behavior, it will delete the email message containing the worm - as opposed to the quarantine action for worms that do not show mass-mailing behavior.

Trojan Horse Programs

A Trojan is a type of threat named after the Trojan Horse of Greek mythology. Like the Greek Trojan Horse, a Trojan network threat has malicious intent, hidden within its

code. While a Trojan may appear innocent, executing a Trojan can cause unwanted system problems in operation, lost data, and loss of privacy.

For example, a Trojan called "happy birthday" might play a song and display an animated dance on your screen, while at the same time opening a port in the background and dropping files that lets malicious hackers take control of the computer for whatever scheme or exploit he or she may have in mind. One common scheme is to hijack the computer for distributing spam. Another is to collect keystrokes and send them, along with all the data they contain, to the malicious hacker.

Trojans are not viruses/malware. Unlike viruses/malware, they do not infect files, and they do not replicate. The scan engine detects and logs these threats and can take whatever action you specify.

With Trojans, however, simply deleting or quarantining is often not enough to rid your system of the Trojan's effects. You must also clean up after it; that is, remove any programs that may have been copied to the machine, close ports, and remove registry entries.

Worms

A computer worm is a self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems. The propagation usually takes place through network connections or email attachments. Unlike viruses/malware, worms do not need to attach themselves to host programs. Worms often use email and applications, such as Microsoft™ Outlook™, to propagate. They may also drop copies of themselves into shared folders or utilize file-sharing systems, such as Kazaa, under the assumption that users will likely download them, thus letting the worm propagate. In some cases, worms use chat applications such as ICQ, AIM, mIRC, or other Peer-to-Peer (P2P) programs to spread copies of themselves.

Zip of Death

"Zip-of-death" describes a subterfuge designed to bring down a network by overwhelming the antivirus software and/or network traffic checking security applications.

Using special techniques, a hacker can compress a file down to as little as 500 KB, that, when decompressed, may reach 15 GB or more in size. Another version of the exploit

involves compressing such a large number of files, that, when decompressed, it can crash the system.

ScanMail allows you to set limits on the size, as well as the number of files it will extract from a compressed archive. When the limit is reached, ScanMail stops decompressing and takes the action specified for files outside of the scan restriction criteria.

About Spyware/Grayware

Your clients are at risk from potential threats other than viruses/malware. Grayware can negatively affect the performance of the computers on your network and introduce significant security, confidentiality, and legal risks to your organization.

TABLE 18-3. Types of Grayware

TYPE	DESCRIPTION
Spyware	Gathers data, such as account user names and passwords, and transmits them to third parties
Adware	Displays advertisements and gathers data, such as user web surfing preferences, to target advertisements at the user through a web browser
Dialers	Change computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem
Joke Programs	Cause abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes
Hacking Tools	Help hackers enter computers
Remote Access Tools	Help hackers remotely access and control computers
Password Cracking Applications	Help hackers decipher account user names and passwords
Other	Other types not covered above

Potential Risks and Threats

The existence of spyware/grayware on your network has the potential to introduce the following:

TABLE 18-4. Types of Risks

TYPE	DESCRIPTION
Reduced computer performance	To perform their tasks, spyware/grayware applications often require significant CPU and system memory resources.
Increased web browser-related crashes	Certain types of grayware, such as adware, are often designed to create pop-up windows or display information in a browser frame or window. Depending on how the code in these applications interacts with system processes, grayware can sometimes cause browsers to crash or freeze and may even require a system reboot.
Reduced user efficiency	By needing to close frequently occurring pop-up advertisements and deal with the negative effects of joke programs, users can be unnecessarily distracted from their main tasks.
Degradation of network bandwidth	Spyware/grayware applications often regularly transmit the data they collect to other applications running on your network or to locations outside of your network.
Loss of personal and corporate information	Not all data that spyware/grayware applications collect is as innocuous as a list of websites users visit. Spyware/grayware can also collect the user names and passwords users type to access their personal accounts, such as a bank account, and corporate accounts that access resources on your network.
Higher risk of legal liability	If hackers gain access to the computer resources on your network, they may be able to utilize your client computers to launch attacks or install spyware/grayware on computers outside your network. Having your network resources unwillingly participate in these types of activities could leave your organization legally liable to damages incurred by other parties.

How Spyware/Grayware Gets into your Network

Spyware/grayware often gets into a corporate network when users download legitimate software that has grayware applications included in the installation package.

Most software programs include an End User License Agreement (EULA), which the user has to accept before downloading. Often the EULA does include information about the application and its intended use to collect personal data; however, users often overlook this information or do not understand the legal jargon.

Encoding Types

The encoding types supported by ScanMail include:

- BINHEX
- UUencode
- Base64
- Quoted-printable

A growing number of malicious security risks seek to embed themselves within a malformed email in an attempt to fool scanning and bypass antivirus products. The ScanMail scan engine's MIME-parsing algorithm can correctly parse and detect malformed versions of MIME-formatted email. The engine also supports 7-bit and 8-bit encoding/decoding.

Multipurpose Internet Mail Extensions (MIME) Types

Top-level media types

Unless a sub-type is specified, ScanMail automatically includes all subtypes.

- application/
- audio/
- image/
- text/
- video/

True File Type

Files can be easily renamed to disguise their actual type. Programs such as Microsoft Word are "extension independent". They will recognize and open "their" documents regardless of the file name. This poses a danger, for example, if a Word document containing a macro virus has been named "benefits form.pdf". Word will open the file, but the file may not have been scanned if ScanMail is not set to check the true file type.

When set to IntelliScan, ScanMail will confirm a file's true type by opening the file header and checking its internally registered data type.

Only files of that type that is actually capable being infected are scanned. For example, .mid files make up a large volume of all web traffic, but they are known not to be able to carry viruses. With true file type selected, once the true type has been determined, these inert file types are not scanned.

Disease Vector

A "disease vector" is a website or URL known to distribute Internet security risks including spyware/grayware, password-cracking applications, key-stroke trackers, and virus/malware kit downloads.

Another category of disease vectors are sites made to look legitimate, but below the surface the hacker directs all the "back-end" functionality such as links and data posts to his or her own locations.

Trend Micro quickly adds confirmed malicious sites to the phish and spyware pattern file so you can prevent LAN clients from downloading the virus/malware, or from being duped by the look-alike sites.

Phish

Phish, or Phishing, is a rapidly growing form of fraud that seeks to fool web users into divulging private information by mimicking a legitimate website.

In a typical scenario, an unsuspecting user gets an urgent sounding (and authentic looking) email telling him or her there is a problem with their account that they must immediately fix, or the account will be closed. The email will include a URL to a website

that looks exactly like the real thing (it is simple to copy a legitimate email and a legitimate website but then change the so-called back-end—where the collected data is actually sent.

The email tells the user to log on to the site and confirm some account information. Any data entered at the site is directed to a malicious hacker who steals the log on name, password, credit card number, social security number, or whatever data s/he requests.

Phish fraud is fast, cheap, and easy to perpetuate. It is also potentially quite lucrative for those criminals who practice it. Phish is hard for even computer-savvy users to detect. And it is hard for law enforcement to track down. Worse, it is almost impossible to prosecute.

Chapter 19

Frequently Asked Questions

This chapter discusses some commonly asked questions regarding the configuration of ScanMail and the steps involved in addressing the situations.

Topics include:

- *Scanning and Updating on page 19-2*
- *Expressions and Keywords on page 19-3*
- *File Handling on page 19-13*
- *Quarantine and Log Management on page 19-15*
- *Logs, Quarantine Records, and Server Groups on page 19-17*
- *Logging On and Registration on page 19-18*
- *Security Threats on page 19-21*

Scanning and Updating

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

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

Locating the ScanMail Version

Procedure

1. From the main ScanMail menu, click **Summary**.
2. A list of installed components, the current ScanMail version, and update schedules appears.

Where can I find the latest patches for updating ScanMail?

From time to time, Trend Micro may release a patch for a reported known issue or an upgrade that applies to your product. To find out whether there are any patches available, visit the following URL:

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

The **Update Center** screen displays. Select your product from the links on this screen. Patches are dated. If you find a patch that you have not applied, open the readme document to determine whether the patch applies to you. If so, follow the installation instructions in the readme.

Is "Public Folder Scan" supported only on Exchange Server 2013?

This option is only supported on Exchange Server 2013. Exchange Server 2010 and 2007 public folders are based in the database system. To enable public folder scanning on Exchange Server 2010 and 2007, select the **Public Folder Database** option in the **Database Selection** section when performing Manual and Scheduled Scans.

Expressions and Keywords

What are regular expressions?

Regular expressions are used to perform string matching. See the following tables for some common examples of regular expressions.

Note

Regular expressions are a powerful string matching tool. For this reason, it is recommended that an administrator who chooses to use regular expressions should be familiar and comfortable with regular expression syntax. Poorly written regular expressions can have a negative performance impact. Trend Micro's recommendation is to start with simple regular expressions that do not use complex syntax. When introducing new rules, use the backup action and observe how ScanMail manages messages using your rule. When you are confident that the rule has no unexpected consequences, you can change your action.

TABLE 19-1. Counting and Grouping

ELEMENT	WHAT IT MEANS	EXAMPLE
.	The dot or period character represents any character except new line character.	`do.` matches doe, dog, don, dos, dot, etc.d.r matches deer, door, etc.
*	The asterisk character means zero or more instances of the preceding element.	`do*` matches d, do, doo, dooo, doooo, etc.
+	The plus sign character means one or more instances of the preceding element.	`do+` matches do, doo, dooo, doooo, etc. but not d
?	The question mark character means zero or one instances of the preceding element.	`do?g` matches dg or dog but not doog, dooog, etc.
( )	Parenthesis characters group whatever is between them to be considered as a single entity.	`d(eer)+` matches deer or deereer or deereereer, etc. The + sign is applied to the substring within parentheses, so the regex looks for d followed by one or more of the grouping "eer."
[ ]	Square bracket characters indicate a set or a range of characters.	`d[aeiouy]+` matches da, de, di, do, du, dy, daa, dae, dai, etc. The + sign is applied to the set within brackets parentheses, so the regex looks for d followed by one or more of any of the characters in the set [aeioy]. `d[A-Z]` matches dA, dB, dC, and so on up to dZ. The set in square brackets represents the range of all upper-case letters between A and Z.
^	Carat characters within square brackets logically negate the set or range specified, meaning the regex will match any character that is not in the set or range.	`d[^aeiouy]` matches db, dc or dd, d9, d#. d followed by any single character except a vowel.

Element	What It Means	Example
{ }	Curly brace characters set a specific number of occurrences of the preceding element. A single value inside the braces means that only that many occurrences will match. A pair of numbers separated by a comma represents a set of valid counts of the preceding character. A single digit followed by a comma means there is no upper bound.	`da{3}` matches daaa. d followed by 3 and only 3 occurrences of "r;a". da{2,4} matches daa, daaa, daaaa, and daaaa (but not daaaaa). d followed by 2, 3, or 4 occurrences of "r;a". da{4,} matches daaaa, daaaaa, daaaaaa, etc. d followed by 4 or more occurrences of "r;a".

Table 19-2. Character Classes (shorthand)

Element	What It Means	Example
\d	Any digit character; functionally equivalent to [0-9] or [[:digit:]]	`\d` matches 1, 12, 123, etc., but not 1b7. One or more of any digit characters.
\D	Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]	`\D` matches a, ab, ab&, but not 1. One or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.
\w	Any "word" character. That is, any alphanumeric character; functionally equivalent to [_A-Za-z0-9] or [_[:alnum:]]	`\w` matches a, ab, a1, but not !&. One or more upper- or lower-case letters or digits, but not punctuation or other special characters.
\W	Any non-alphanumeric character; functionally equivalent to [^_A-Za-z0-9] or [^_[:alnum:]]	`\W` matches *, &, but not ace or a1. One or more of any character but upper- or lower-case letters and digits.
\s	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [[:space]]	`vegetable\s` matches "vegetable" followed by any non-white space character. So the phrase "I like vegetables in my soup" would trigger the regex, but "I like a vegetable in my soup" would not.

Element	What It Means	Example
\S	Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to [^[:space]]	`vegetable\S` matches "vegetable" followed by any non-white space character. So the phrase "I like vegetables in my soup" would trigger the regex, but "I like a vegetable in my soup" would not.

Table 19-3. Character Classes

Element	What It Means	Example
[:alpha:]	Any alphabetic characters	`.REG. [[:alpha:]]` matches abc, def, xxx, but not 123 or @#$.
[:digit:]	Any digit character; functionally equivalent to \d	`.REG. [[:digit:]]` matches 1, 12, 123, etc.
[:alnum:]	Any "word" character. That is, any alphanumeric character; functionally equivalent to \w	`.REG. [[:alnum:]]` matches abc, 123, but not ~!@.
[:space:]	Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to \s	`.REG. (vegetable)[[:space:]]` matches "vegetable" followed by any white space character. So the phrase "I like a vegetable in my soup" would trigger the regex, but "I like vegetables in my soup" would not.
[:graph:]	Any characters except space, control characters or the like	`.REG. [[:graph:]]` matches 123, abc, xxx, ><", but not space or control characters.
[:print:]	Any characters (similar with [:graph:]) but includes the space character	`.REG. [[:print:]]` matches 123, abc, xxx, ><", and space characters.
[:cntrl:]	Any control characters (e.g. CTRL + C, CTRL + X)	`.REG. [[:cntrl:]]` matches 0x03, 0x08, but not abc, 123, !@#.

Element	What It Means	Example
[:blank:]	Space and tab characters	`.REG. [[:blank:]]` matches space and tab characters, but not 123, abc, !@#
[:punct:]	Punctuation characters	`.REG. [[:punct:]]` matches ; : ? ! ~ @ # $ % & * 'r; "r; , etc., but not 123, abc
[:lower:]	Any lowercase alphabetic characters **Note** **Enable case sensitive matching** must be enabled or else it will function as [:alnum:].	`.REG. [[:lower:]]` matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.
[:upper:]	Any uppercase alphabetic characters **Note** **Enable case sensitive matching** must be enabled or else it will function as [:alnum:].	`.REG. [[:upper:]]` matches ABC, DEF, STRESS, DO, Def, Stress, Do, etc., but not abc, 123, !@#.
[:xdigit:]	Digits allowed in a hexadecimal number (0-9a-fA-F)	`.REG. [[:xdigit:]]` matches 0a, 7E, 0f, etc.

TABLE 19-4. Pattern Anchor Regular Expressions

ELEMENT	WHAT IT MEANS	EXAMPLE
^	Indicates the beginning of a string.	`^ (notwithstanding)` matches any block of text that began with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would not.
$	Indicates the end of a string.	`(notwithstanding) $` matches any block of text that ended with "notwithstanding" So the phrase "notwithstanding the fact that I like vegetables in my soup" would not trigger the regex, but "The fact that I like vegetables in my soup notwithstanding" would.
\	In order to match some characters that have special meaning in regular expression (for example, "+").	• `.REG. C\\C\+\+` matches 'r;C \C++'. • `.REG. \*` matches *. • `.REG. \?` matches ?.
\t	Indicates a tab character.	`(stress) \t` matches any block of text that contained the substring "stress" immediately followed by a tab (ASCII 0x09) character.

Element	What It Means	Example
\n	Indicates a new line character. **Note** Different platforms represent a new line character. On Windows, a new line is a pair of characters, a carriage return followed by a line feed. On Unix and Linux, a new line is just a line feed, and on Macintosh a new line is just a carriage return.	`(stress) \n` matches any block of text that contained the substring "stress" followed immediately by two new line (ASCII 0x0A) characters.
\r	Indicates a carriage return character.	`(stress) \r` matches any block of text that contained the substring "stress" followed immediately by one carriage return (ASCII 0x0D) character.
\b	Indicates a backspace character	`(stress) \b` matches any block of text that contained the substring "r;stress" followed immediately by one backspace (ASCII 0x08) character.
\xhh	Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).	`\x7E(\w){6}` matches any block of text containing a "word" of exactly six alphanumeric characters preceded with a ~ (tilde) character. So, the words 'r;~ab12cd', 'r;~Pa3499' would be matched, but 'r;~oops' would not.

How do I use keywords?

Content Filtering > [Policy Name] > Edit Rule

Keywords are not strictly words. They can be any of the following:

- Numbers
- Typographical characters
- Short phrases
- Words or phrases connected by logical operators
- Words or phrases that use regular expressions

Using Keywords Effectively

ScanMail offers simple and powerful features to create highly specific filters. Consider the following, when creating your Content Filtering rules:

- By default, ScanMail searches for exact matches of keywords. Use regular expressions to set ScanMail to search for partial matches of keywords.
- ScanMail analyzes multiple keywords on one line differently than multiple keywords when each word occupies a single line.
- You can also set ScanMail to search for synonyms of the actual keywords.
- Try to use exact matching, regular expressions, operators with keywords, and import keywords to the keyword list from previous configurations.

TABLE 19-5. Using Exact Matching and Keywords on Multiple Lines

SITUATION	EXAMPLE	MATCH / NON-MATCH
Two words on same line	bare sexy	Matches: "Click here to see bare sexy beauties." Does not match: “Click here to see bare naked sexy hotties.”
Two words separated by a comma	bare, sexy	Matches: "Click here to see hot, bare, sexy beauties." Does not match: "Click here to see hot, bare, and sexy beauties."

SITUATION	EXAMPLE	MATCH / NON-MATCH
Multiple words on multiple lines	nude sexy bare naked	When you choose **Any specified keywords** Matches: "This is a nude picture" Also matches: "See young, hot, and sexy beauties" When you choose **All specified keywords** Matches: "This is a nude picture of sexy buff and bare naked" Does not match: "This is a nude picture of sexy buff bare and naked"
Many keywords on same line	sex bare nude naked buff	Matches: “Click here for sex bare nude naked buff” Does not match: "Click here to see sex that's bare and buff"

How do I use operators with keywords?

To format keywords that use operators, refer to the following:

When typing a keyword or phrase that includes an operator, follow the format in the example below:

Example: `.WILD. valu*`

Note

The operator has a dot immediately preceding and following. There is a space between the final dot and the keyword.

TABLE 19-6. Using Operators with Keywords

SUPPORTED KEYWORD	HOW IT WORKS	HOW TO USE
Any keywords	ScanMail searches content that matches the word	Type the word and add it to the keyword list
OR	ScanMail searches for any of the keywords separated by OR For example: apple OR orange. ScanMail searches for either apple or orange. If content contains either, then there is a match.	Type ".OR." between all the words you want to include For example: apple .OR. orange
AND	ScanMail searches for all of the keywords separated by AND For example: apple AND orange. ScanMail searches for both apple and orange. If content does not contain both, then there is no match.	Type ". AND." between all the words you want to include For example: apple .AND. orange
NOT	ScanMail excludes keywords following NOT from search. For example: .NOT. juice. ScanMail searches for content that does not contain "juice". If the message has "orange soda", there is a match, but if it contains "orange juice", there is no match.	Type ".NOT." before a word you want to exclude For example: ".NOT. juice"

Supported Keyword	How It Works	How To Use
WILD	WILD means wildcard. The wildcard symbol replaces a missing part of the word. Any words that are spelled using the remaining part of the wildcard are matched. For example, if you want to match all words containing "valu", type ".WILD. valu*". The words Valumart, valucash, and valubucks all match. **Note** ScanMail does not support using "?" in the wildcard command ".WILD.".	Type ".WILD." before the parts of the word you want to include
REG	To specify a regular expression, add a .REG. operator before that pattern (for example, .REG. a.*e).	Type ".REG." before the word pattern you want to detect. For example: ".REG. a.*e" matches: "ace", "ate", and "advance", but not "all", "any", nor "antivirus"

File Handling

How do I handle large files?

From the **Security Risk Scan** screen, ScanMail provides the following methods to address large-file scan lag under Scan Restriction Criteria:

- **Message body size exceeds**: ScanMail will not scan email messages larger than the size specified.

- **Attachment size exceeds**: ScanMail will not scan attachments larger than the size specified.

WARNING!

These options effectively allow a hole in your web security - large files will not be scanned. Trend Micro recommends that you only choose this option on a temporary basis.

What is a compression ratio?

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

TABLE 19-7. 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)

How do I calculate the size of a decompressed file?

For compressed files, how can I calculate the "x" value and use it effectively for the option **Size of decompressed file is "x" times the size of compressed file**?

This function prevents ScanMail from scanning a compressed file that might cause a Denial-of-Service (DoS) attack. A DoS attack happens when a mail server's resources are overwhelmed by unnecessary tasks. Preventing ScanMail from scanning files that decompress into very large files helps prevent this problem from happening.

Example: For the table below, the "x" value is 100.

TABLE 19-8. Decompressed File Examples

FILE SIZE (NOT COMPRESSED)	FILE SIZE (COMPRESSED)	RESULT
500 KB	10 KB (ratio is 50:1)	Scanned
1000 KB	10 KB (ratio is 100:1)	Scanned
1001 KB	10 KB (ratio is 100.1:1)	Not scanned *
2000 KB	10 KB (ratio is 200:1)	Not scanned *

* ScanMail takes the action you configure for unscannable files.

Quarantine and Log Management

Are UNC paths supported for quarantine and backup folders?

ScanMail supports the usage of Universal Naming Convention (UNC) paths when configuring the quarantine and backup folders (for example, \\fileserver\directory).

To configure a UNC quarantine or backup folder:

1. Create the necessary folder on a remote endpoint that is in the same domain as the Exchange servers.
2. Ensure that the computer accounts for the Exchange servers have read/write permissions for the UNC path.

Important

- 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.

Are mapped network drives supported for quarantine and backup folders?

ScanMail does not support the use of mapped network drives for the quarantine and backup folders. Use UNC paths to use remote storage locations.

How does ScanMail display the "Scan Time" or "Delivery Time" for remote servers?

ScanMail converts time data and displays the data based on the local time settings of the server polling the database.

For example, a remote server in the GMT+9 time zone queries logs from a server located in the GMT+8 time zone. A log time of 2014-12-15 13:10:21 GMT+9 is converted to 2014-12-15 12:10:21 GMT+8 when queried from the server in the GMT +8 time zone.

How does ScanMail generate centralized report data for multiple servers?

ScanMail retrieves data based on the period specified, regardless of time zone settings. If a server is in a location that has not yet reached the period specified, a value of zero records is received.

Note

For example, it is currently 14:00 GMT+8. A remote server in the GMT+8 time zone queries logs for the period of 13:00 to 14:00 from a server located in the GMT+4 time zone. The server located in the GMT+4 time zone returns no records because the current time is only 10:00.

ScanMail then displays all the data for the specified period collected from the specified servers in a single report. If server A displays 4 log items for the specified period and server B displays 5 log items for the same period, ScanMail displays 9 entries for the period.

Does the ScanMail web service port need to be added to the firewall port exception list before generating centralized logs or quarantine queries?

ScanMail requires that you add the ScanMail web service port to your firewall port exception list to perform centralized log and quarantine queries.

Note

By default, the ScanMail web service port is 16372 for HTTP and 16373 for HTTPS.

Can I re-create the End User Quarantine spam folder after deleting it?

After disabling and selecting the **Delete End User Quarantine spam folder** option, you can re-create the spam folder by enabling the **Enable End User Quarantine** option on the **Administration** > **Spam Maintenance** screen.

Logs, Quarantine Records, and Server Groups

How do I increase number of query results for each remote server?

By default, ScanMail sets a maximum value of 3000 results for each remote server. If you want to query more than 3000 records for each remote server when performing centralized log and quarantine queries, add following hidden registry key:

Path: `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange\CurrentVersion`

Key: MaxRemoteQuery

Type: DWORD

Note

Restart the ScanMail Master service after adding the registry value.

How do I update newly installed ScanMail 11.0 Service Pack 1 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.

Logging On and Registration

Where can I find my Activation Code and Registration Key?

Administration > **Product License**

You can activate ScanMail during the installation process or later using the ScanMail console. To activate ScanMail, you need to have an Activation Code.

Obtaining an Activation Code

- You automatically get an evaluation Activation Code if you download ScanMail from the Trend Micro website.
- You can use a Registration Key to obtain an Activation Code online.
- Activation Codes have 37 characters and look like this:

  xx-xxxx-xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

Obtaining a Registration Key

The Registration Key can be found on:

- Trend Micro Enterprise Solution CD
- License Certificate (which you obtained after purchasing the product)

Registering and activating your copy of ScanMail entitles you the following benefits:

- Updates to the ScanMail pattern files and scan engine
- Technical support
- Easy access in viewing the license expiration update, registration and license information, and renewal reminders
- Easy access in renewing your license and updating the customers profile
- Registration Keys have 22 characters and look like this:

  xx-xxxx-xxxx-xxxx-xxxx

When the full version expires, security updates will be disabled; when the evaluation period expires, both the security updates and scanning capabilities will be disabled. In the **Product License** screen, you can obtain an Activation Code online, view renewal instructions, and check the status of your product.

Why am I unable to log on to the product console on Windows Server 2008?

This issue occurs because the CGI and ASP roles in IIS 7.0 that come with Server 2008 are not installed by default.

To resolve this issue:

Procedure

1. Install the CGI and ASP server role.
   a. Navigate to Server Manager.
   b. Select **Roles** and right-click on the Web Server (IIS).
   c. Click **Add Role Services**.

d. Under **Application Development**, select ASP and CGI.

e. Click **Next** > **Install**.

2. Allow SMEX CGIs (if ISAPI and CGI restrictions are implemented).

   a. Navigate to IIS Manager.

   b. Select the server node and then select ISAPI and CGI Restrictions.

   c. Verify that both cgiDispatcher and cgiCmdNotify are allowed.

   d. Re-open the ScanMail product console.

3. Log on to the ScanMail product console to verify that the issue has been resolved.

What if the remote SQL server database account password is changed?

When you install ScanMail with a remote SQL server, an account is required to connect to the remote SQL server. If the password for this account is changed, the password needs to be manually updated in the ScanMail configuration file.

To manually update the remote SQL server account password:

Procedure

1. Open the command line interface and navigate to the ScanMail installation path tool folder.

   The default path is C:\Program Files\Trend Micro\Smex\tools

2. Use toolChangeRemoteDBPWD.exe to encrypt the new password by typing the following:

   ```
   toolChangeRemoteDBPWD.exe -p <output_folder_path> -c
   <password>
   ```

3. Replace dbcfg_SQLPassword.txt with the newly generated file. The encrypted password file can be found:

- For noncluster server installations:

  ScanMail installation path\config\dbcfg_SQLPassword.txt

- For SCC and VERITAS clusters (on share disks)

  ScanMail data path\config\dbcfg_SQLPassword.txt

- For CCR clusters (on both nodes)

  ScanMail installation path\CCRVSDB$\EVSNAME\config\dbcfg_SQLPassword.txt

4. Restart the ScanMail Master service.

Security Threats

What is spyware/grayware?

Spyware includes software programs and technologies (called "bots") that seek to surreptitiously collect data and transmit it back to a host source.

The category of spyware and other grayware security risks includes adware, Internet cookies, Trojans, and surveillance tools. The type of information collected by spyware ranges from the relatively innocuous (a history of visited websites) to the downright alarming (credit card and Social Security numbers, bank accounts, and passwords).

The majority of spyware/grayware comes embedded in a "cool" software package which a user finds on a website and downloads. Some spyware programs are part of a legitimate program. Others are purely illicit. The network administrator needs to determine whether a given class of software is something he or she wants to allow on the network, or something they want to block.

Spyware installs in a variety of ways, for example:

- As a by-product that results from installing software
- As a result of clicking something in a popup window
- As an invisible addition that is installed along with a legitimate download

- Through Trojans, worms and viruses

The result is typically a background Internet connection, that opens a surveillance channel to the user's computer. Multiple connections may also be established, which can lead to sluggish network performance.

When ScanMail detects spyware/grayware, it can take the following actions:

- **Replace with text/file**: ScanMail deletes the infected, malicious, or undesirable content and replaces it with text or a file.
- **Quarantine entire message**: ScanMail moves the email message to a restricted access folder.
- **Delete entire message**: ScanMail deletes the entire email message.
- **Pass**: ScanMail records the detection in logs and delivers the message unchanged.
- **Quarantine message part**: ScanMail moves the email message body or attachment to a restricted access folder.

Growing Hazard

Increasingly, users are installing more and more malicious types of spyware without their knowledge, either as a "drive-by download", or as the result of clicking some option in a deceptive pop-up window. What concerns corporate security departments is that the more sophisticated types of spyware can be used to monitor keystrokes, scan files, install additional spyware, reconfigure web browsers, and snoop email and other applications. In some cases, spyware can even capture screen shots or turn on web cams.

Theft of confidential information, loss of employee productivity, consumption of large amounts of bandwidth, damage to corporate desktops, and a spike in the number of help desk calls related to spyware are forcing corporations of all sizes to take action. Spyware can represent both a security and system management nightmare.

What are phish attacks?

A phish is an email message that falsely claims to be from an established or legitimate enterprise. The message encourages recipients to click on a link that will redirect their browsers to a fraudulent website where the user is asked to update personal information

such as passwords, social security numbers, and credit card numbers in an attempt to trick a recipient into providing private information that will be used for identity theft.

When the content scanning feature in ScanMail detects a phish message, it can take the following actions:

- Delete entire message

  ScanMail deletes the entire message and Exchange does not deliver it.

- Tag and deliver

  ScanMail adds a tag to the header information of the email message that identifies it as phish and then delivers it to the intended recipient.

What is the EICAR test virus?

The European Institute for Computer Antivirus Research (EICAR) has developed a test "virus" you can use to test your product installation and configuration. This file is an inert text file whose binary pattern is included in the virus pattern file from most antivirus vendors. It is not a virus and does not contain any program code.

You can download the EICAR test virus from the following URLs:

www.trendmicro.com/vinfo/testfiles/

www.eicar.org/anti_virus_test_file.htm

Alternatively, you can create your own EICAR test virus by typing the following into a text file, and then naming the file "eicar.com":

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!
$H+H*
```

Note

Flush the cache in the cache server and local browser before testing.

What are false positives?

A false positive occurs when a website, URL, "infected" file, or email message is incorrectly determined by filtering software to be of an unwanted type. For example, a legitimate email between colleagues may be detected as spam if a job-seeking filter does not distinguish between resume (to start again) and résumé (a summary of work experience).

You can reduce the number of future false positives in the following ways:

1. Update to the latest pattern files.
2. Exempt the item from scanning by adding it to an Approved List.
3. Report the false positive to Trend Micro.

Are some files dangerous?

Are files under quarantine/backup folders dangerous?

ScanMail renames all files in quarantine/backup folders with specially formatted filenames that have the extension name removed. This stops Windows from directly launching the file and prevents any executable files from being launched accidentally (by double-clicking on the file or other attempts to open.)

However, there is danger for users with applications such as Microsoft™ Office 2003 that can recognize a file with it's true file type. In this situation, a user could unintentionally launch even a backup file that has no extension name.

How do I send Trend Micro suspected Internet threats?

You can send Trend Micro the URL of any website you suspect of being a phish site, or other so-called "disease vector" (the intentional source of security risks).

You can do one of the following:

- Send an email to: virusresponse@trendmicro.com, and specify "Phish or Disease Vector" as the Subject

- Use the web-based submission form:

  http://esupport.trendmicro.com/en-us/business/pages/virus-and-threat-removal.aspx

How do I send Trend Micro detected viruses?

If you have a file you think is infected but the scan engine does not detect it or cannot clean it, Trend Micro encourages you to send the suspect file to us. For more information, refer to the following site:

http://esupport.trendmicro.com/en-us/business/pages/virus-and-threat-removal.aspx

Please include in the message text a brief description of the symptoms you are experiencing. The team of antivirus engineers will analyze the file to identify and characterize any virus(es) it may contain, usually the same day it is received.

Chapter 20

Troubleshooting

This chapter discusses some common troubleshooting tasks that administrators can perform manually.

Topics include:

- *Updating the Scan Engine Manually on page 20-2*
- *Updating the Pattern File (lpt$vpn.xxx) Manually on page 20-3*
- *Known Issues on page 20-3*

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#prod_8

2. Extract the contents of the vsapi-32dll-#.###-####.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 temp 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)

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

Procedure

1. Download and save to a temporary directory on the ScanMail server:
   - The latest Official Pattern Release (OPR) file:

     http://www.trendmicro.com/download/pattern.asp
   - A Controlled Pattern Release (CPR) file from this location:

     http://www.trendmicro.com/download/pattern-cpr-disclaimer.asp

   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.
2. Click the Windows **Start** button, then **Programs** > **Administrative Tools** > **Services** to stop all ScanMail services.
3. Extract the contents of the compressed file you downloaded to following folder:

   \Program Files\Trend Micro\Smex\engine\vsapi\latest
4. Restart all the ScanMail services, then refresh the ScanMail console.

Known Issues

Known issues document unexpected ScanMail behavior that might require a temporary workaround.

Trend Micro recommends always checking the readme file for information about system requirements and known issues that could affect installation or performance. Readme

files also contain a description of what's new in a particular release, and other helpful information.

Trend Micro product readme files and other documentation can be found at the Trend Micro Update Center:

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

Known issues and possible workarounds can also be found in the Trend Micro Knowledge Base:

http://esupport.trendmicro.com/

Chapter 21

Contacting Trend Micro

This chapter discusses how to contact Trend Micro to receive help, research security threats, and find the latest product solutions.

Topics include:

- *Contacting Technical Support on page 21-2*
- *Speeding Up Your Support Call on page 21-3*
- *Using the Support Portal on page 21-3*
- *Security Information Site on page 21-4*

Contacting Technical Support

Trend Micro provides technical support, pattern downloads, and program updates for one year to all registered users, after which you must purchase renewal maintenance. If you need help or just have a question, please feel free to contact us. We also welcome your comments.

- Get a list of the worldwide support offices at http://esupport.trendmicro.com
- Get the latest Trend Micro product documentation at http://docs.trendmicro.com

In the United States, you can reach the Trend Micro representatives through phone, fax, or email:

```
Trend Micro, Inc.
10101 North De Anza Blvd.,
Cupertino, CA 95014
Toll free: +1 (800) 228-5651 (sales)
Voice: +1 (408) 257-1500 (main)
Fax: +1 (408) 257-2003
Web address: http://www.trendmicro.com
Email: support@trendmicro.com
```

TrendLabs

Trend Micro TrendLabs℠ is a global network of antivirus research and product support centers providing continuous, 24 x 7 coverage to Trend Micro customers worldwide.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers worldwide ensure rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters earned ISO 9002 certification for its quality management procedures in 2000. TrendLabs is one of the first antivirus research and support facilities to be so accredited. Trend Micro believes that TrendLabs is the leading service and support team in the antivirus industry.

For more information about TrendLabs, please visit:

http://us.trendmicro.com/us/about/company/trendlabs/

Speeding Up Your Support Call

When you contact Trend Micro, to speed up your problem resolution, ensure that you have the following details available:

- Operating System and Service Pack version
- Network type
- Computer brand, model, and any additional hardware connected to your computer
- Browser version
- Amount of memory and free hard disk space on your computer
- Detailed description of the install environment
- Exact text of any error message given
- Steps to reproduce the problem

Using the Support Portal

The Trend Micro Support Portal is a 24x7 online resource that contains the most up-to-date information about both common and unusual problems.

Procedure

1. Go to http://esupport.trendmicro.com.
2. Select a product or service from the appropriate drop-down list and specify any other related information.

   The **Technical Support** product page appears.
3. Use the **Search Support** box to search for available solutions.

4. If no solution is found, click **Submit a Support Case** from the left navigation and add any relevant details, or submit a support case here:

   http://esupport.trendmicro.com/srf/SRFMain.aspx

   A Trend Micro support engineer investigates the case and responds in 24 hours or less.

Security Information Site

Comprehensive security information is available at the Trend Micro website:

http://about-threats.trendmicro.com

In the ScanMail banner at the top of any ScanMail screen, click the **Help** drop down, then **Security Info**.

Information available:

- List of viruses and malicious mobile code are currently "in the wild," or active
- Computer virus hoaxes
- Internet threat advisories
- Virus weekly report
- Virus Encyclopedia, which includes a comprehensive list of names and symptoms for known viruses and malicious mobile code
- Glossary of terms

Appendix A

Introducing Trend Micro™ Control Manager™

Trend Micro Control Manager is a central management console that manages Trend Micro products and services at the gateway, mail server, file server, and corporate desktop levels. Administrators can use the policy management feature to configure and deploy product settings to managed products and endpoints. The Control Manager web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Control Manager enables system administrators to monitor and report on activities such as infections, security violations, or virus/malware entry points. System administrators can download and deploy update components throughout the network, helping ensure that protection is consistent and up to date. Example update components include virus pattern files, scan engines, and anti-spam rules. Control Manager allows both manual and pre-scheduled updates. Control Manager allows the configuration and administration of products as groups or as individuals for added flexibility.

This chapter contains the following topics:

- *Control Manager Standard and Advanced on page A-3*
- *Introducing Control Manager Features on page A-3*
- *Control Manager Architecture on page A-5*

- *Registering ScanMail to Control Manager on page A-8*
- *Understanding User Access on page A-9*
- *Understanding the Product Directory on page A-15*
- *Downloading and Deploying New Components on page A-39*
- *Using Logs on page A-65*
- *Understanding Reports on page A-69*

Control Manager Standard and Advanced

Control Manager is available in two versions: Standard and Advanced. Control Manager Advanced includes features that Control Manager Standard does not. For example, Control Manager Advanced supports a cascading management structure. This means the Control Manager network can be managed by a parent Control Manager Advanced server with several child Control Manager Advanced servers reporting to the parent Control Manager Advanced server. The parent server acts as a hub for the entire network.

Note

Control Manager Advanced supports the following as child Control Manager servers:

- Control Manager 6.0 Advanced
- Control Manager 5.5 Advanced
- Control Manager 5.0 Advanced

Control Manager 5.0/5.5/6.0 Standard servers cannot be child servers.

For a complete list of all features Standard and Advanced Control Manager servers support see the *Trend Micro Control Manager* documentation.

Introducing Control Manager Features

Trend Micro designed Control Manager to manage antivirus and content security products and services deployed across an organization's local and wide area networks.

TABLE A-1. Control Manager Features

FEATURE	DESCRIPTION
Policy management	System administrators can use policies to configure and deploy product settings to managed products and endpoints from a single management console.

Feature	Description
Centralized configuration	Using the Product Directory and cascading management structure, these functions allow you to coordinate virus-response and content security efforts from a single management console. These features help ensure consistent enforcement of your organization's virus/malware and content security policies.
Proactive outbreak prevention	With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus/ malware outbreak.
Secure communication infrastructure	Control Manager uses a communications infrastructure built on the Secure Socket Layer (SSL) protocol. Depending on the security settings used, Control Manager can encrypt messages or encrypt them with authentication.
Secure configuration and component download	These features allow you to configure secure web console access and component download.
Task delegation	System administrators can give personalized accounts with customized privileges to Control Manager web console users. User accounts define what the user can see and do on a Control Manager network. Track account usage through user logs.
Command Tracking	This feature allows you to monitor all commands executed using the Control Manager web console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.
On-demand product control	Control managed products in real time. Control Manager immediately sends configuration modifications made on the web console to the managed products. System administrators can run manual scans from the web console. This command system is indispensable during a virus/malware outbreak.

FEATURE	DESCRIPTION
Centralized update control	Update virus patterns, antispam rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up to date.
Centralized reporting	Get an overview of the antivirus and content security product performance using comprehensive logs and reports. Control Manager collects logs from all its managed products; you no longer need to check the logs of each individual product.

Control Manager Architecture

Trend Micro Control Manager provides a means to control Trend Micro products and services from a central location. This application simplifies the administration of a corporate virus/malware and content security policy. The following table provides a list of components Control Manager uses.

TABLE A-2. Control Manager Components

COMPONENT	DESCRIPTION
Control Manager server	Acts as a repository for all data collected from the agents. It can be a Standard or Advanced Edition server. A Control Manager server includes the following features: • An SQL database that stores managed product configurations and logs Control Manager uses the Microsoft SQL Server database (db_ControlManager.mdf) to store data included in logs, Communicator schedule, managed product and child server information, user account, network environment, and notification settings. • A web server that hosts the Control Manager web console • A mail server that delivers event notifications through email messages Control Manager can send notifications to individuals or groups of recipients about events that occur on the Control Manager network. Configure Event Center to send notifications through email messages, Windows event log, MSN Messenger, SNMP, Syslog, pager, or any in-house/industry standard application used by your organization to send notification. • A report server, present only in the Advanced Edition, that generates antivirus and content security product reports A Control Manager report is an online collection of figures about security threat and content security events that occur on the Control Manager network.

Component	Description
Trend Micro Management Communication Protocol	MCP handles the Control Manager server interaction with managed products that support the next generation agent. MCP is the new backbone for the Control Manager system. MCP agents install with managed products and use one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.
Trend Micro Management Infrastructure	Handles the Control Manager server interaction with older managed products. The Communicator, or the Message Routing Framework, is the communication backbone of the older Control Manager system. It is a component of the Trend Micro Management Infrastructure (TMI). Communicators handle all communication between the Control Manager server and older managed products. They interact with Control Manager 2.x agents to communicate with older managed products.
Control Manager 2.x Agents	Receives commands from the Control Manager server and sends status information and logs to the Control Manager server The Control Manager agent is an application installed on a managed product server that allows Control Manager to manage the product. Agents interact with the managed product and Communicator. An agent serves as the bridge between managed product and communicator. Therefore, install agents on the same computer as managed products.
Web-based management console	Allows an administrator to manage Control Manager from virtually any computer with an Internet connection and Windows™ Internet Explorer™ The Control Manager management console is a web-based console published on the Internet through the Microsoft Internet Information Server (IIS) and hosted by the Control Manager server. It lets you administer the Control Manager network from any computer using a compatible web browser.

COMPONENT	DESCRIPTION
Widget Framework	Allows an administrator to create a customized dashboard to monitor the Control Manager network.

Registering ScanMail to Control Manager

Before registering the ScanMail server to a Control Manager server, you must ensure that both the server and the Control Manager server belong to the same network segment.

Procedure

1. Click **Administration** > **Control Manager Settings**.

   Note

   Control Manager uses the name specified in the Host name field to identify the ScanMail server. The Host name appears in the Product Directory of Control Manager.

   The **Control Manager Settings** screen displays.

2. Under **Connection settings**, type the name of the ScanMail server in the **Entity display name** field.

3. Under **Control Manager Server Settings** specify the following:

   a. Type the Control Manager server IP address or host name in the Server FQDN or IP address field.

   b. Type the port number that the MCP agent uses to communicate with Control Manager.

   c. If you have Control Manager security set to medium (HTTPS and HTTP communication is allowed between Control Manager and the MCP agent of managed products), select **Connect through HTTPS**.

d. If your network requires authentication, type the user name and password for your IIS server in the **Username** and **Password** fields.

e. If you use a NAT device, select **Enable two-way communication port forwarding** and type the NAT device's IP address and port number in **IP address** and **port number**.

Refer to the *Trend Micro Control Manager Administrator's Guide* for more information about managing products in Control Manager.

4. From the Control Manager management console, click **Products**.

The **Product Directory** screen appears.

5. The ScanMail server appears in the Product Directory tree.

Understanding User Access

Control Manager access control consists of the following four sections.

TABLE A-3. Control Manager User Access Options

SECTION	DESCRIPTION
My Account	The **My Account** screen contains all the account information that Control Manager has for a specific user. The information on the **My Account** screen varies from user to user.

SECTION	DESCRIPTION
User Accounts	The **User Accounts** screen displays all Control Manager users. The screen also provides the options for users to create and maintain Control Manager user accounts. Use these functions to define clear areas of responsibility for users by restricting access rights to certain managed products and limiting what actions users can perform on the managed products. The functions are: • Execute • Configure • Edit Directory
User Roles	The **User Roles** screen displays all Control Manager user roles. The screen also provides the options for users to create and maintain Control Manager user roles. User roles define which areas of the Control Manager web console a user can access.
User Groups	The **User Groups** screen contains Control Manager groups and provides options for creating groups. Control Manager uses groups as an easy method to send notifications to a number of users without having to select the users individually. Control Manager groups do not allow administrators to create a group that shares the same access rights.

Note

Assign users with different access rights and privileges to permit the delegation of certain management tasks without compromising security.

Control Manager User Access with ScanMail User Access

ScanMail user access is similar to Control Manager user access. Administrators can control which parts of the ScanMail web console users can access (Power User, Operator, or Administrator).

All user accounts created in Control Manager have administrator access to any managed product to which the user has access. This creates a problem if an administrator wants to restrict a user's access to Power User on the ScanMail server while allowing access to Control Manager.

MCP Heartbeat

To monitor the status of managed products, MCP agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the managed product and to check for commands to the managed product from Control Manager. The Control Manager web console then presents the product status. This means that the managed product's status is not a real-time, moment-by-moment reflection of the network's status. Control Manager checks the status of each managed product in a sequential manner in the background. Control Manager changes the status of managed products to offline when a fixed period of time elapses without a heartbeat from the managed product.

Active heartbeats are not the only means Control Manager determines the status of managed products. The following also provide Control Manager with the managed product's status:

- Control Manager receives logs from the managed product. Once Control Manager receives any type of log from the managed product successfully, this implies that the managed product is working fine.
- In two-way communication mode, Control Manager actively sends out a notification message to trigger the managed product to retrieve the pending command. If server connects to the managed product successfully, it also indicates that the product is working fine and this event counts as a heartbeat.
- In one-way communication mode, the MCP agent periodically sends out query commands to Control Manager. This periodical query behavior works like a heartbeat and is treated as such by Control Manager.

The MCP heartbeats implement in the following ways:

- **UDP**: If the product can reach the server using UDP, this is the lightest weight, fastest solution available. However, this does not work in NAT or firewall environments. In addition, the transmitting client cannot verify that the server does indeed receive the request.
- **HTTP/HTTPS**: To work under a NAT or firewall environment, a heavyweight HTTP connection can be used to transport the heartbeat

Control Manager supports both UDP and HTTP/HTTPS mechanisms to report heartbeats. Control Manager server finds out which mode the managed product applies during the registration process. A separate protocol handshake occurs between both parties to determine the mode.

Aside from simply sending the heartbeat to indicate the product status, additional data can upload to Control Manager along with the heartbeat. The data usually contains managed product activity information to display on the console.

Using the Schedule Bar

Use the schedule bar on the **Agent Communication Schedule** screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

The slots with clock icons denote working status or the hours that the Agent/Communicator sends information to the Control Manager server. White slots indicate idle time. Define working or idle hours by toggling specific slots.

You can specify at most three consecutive periods of inactivity. The sample schedule bar below shows only two inactive hours:

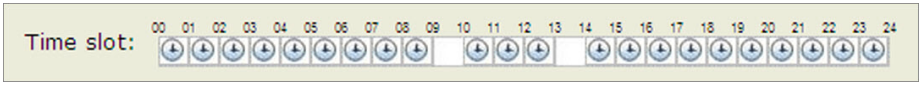


FIGURE A-1. Schedule bar

The active periods specified by the bar are from 0:00 to 7:00, 8:00 to 4:00 PM, and from 6:00 P.M. to midnight.

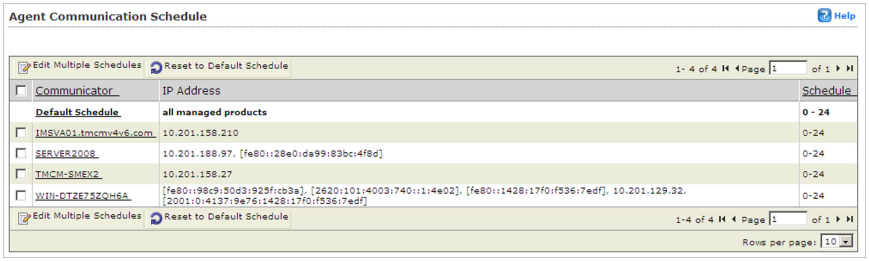
Setting an Agent Communication Schedule for a Managed Product

Procedure

1. Open the Control Manager console.

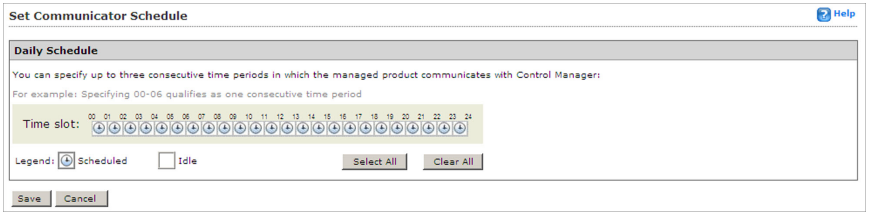
2. Navigate to **Administration** > **Settings** > **Agent Communication Schedule**.

   The **Agent Communication Schedule** screen appears.



3. Select the managed product schedule to modify.

   The **Set Communicator Schedule** screen appears.



4. Define the schedule. Specify a new time or use the default setting:

   - To specify a new setting, change the appropriate time slots in the schedule bar and then click **Save**

   - To use the default setting, return to the **Agent Communication Schedule** screen. Select the schedule to apply and click **Reset to Default Schedule**

Determining the Right Heartbeat Setting

When choosing a heartbeat setting, balance between the need to display the latest managed product status information and the need to manage system resources. The default setting is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

TABLE A-4. Heartbeat Recommendations

HEARTBEAT FREQUENCY	RECOMMENDATION
Long-interval Heartbeats (above 60 minutes)	The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status in the Control Manager web console. For example, if a connection problem with a Communicator is resolved between heartbeats, it then becomes possible to communicate with a Communicator even if the status appears as (inactive) or (abnormal).
Short-interval Heartbeats (below 60 minutes)	Short intervals between heartbeats present a more up-to-date picture of your network status at the Control Manager server. However, this is a bandwidth-intensive option.

Configuring the Agent Communicator Heartbeat

Use the **Communication Time-out** screen to define the frequency and maximum delay times (in minutes) for the Control Manager server and agent communication.

Note

The agent/communicator heartbeat setting only applies to Communicators for managed products directly controlled by the Control Manager server. Child Control Manager server agent/communicators use pre-defined values:

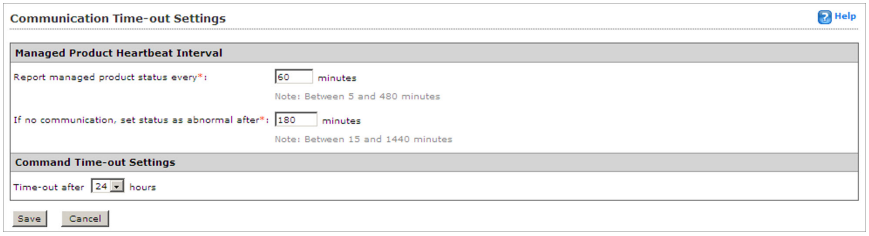
Frequency: 3 minutes

Maximum delay: 5 minutes

Procedure

1. Open the Control Manager console.
2. Navigate to **Administration** > **Settings** > **Communication Time-out Settings**.

   The **Communication Time-out** screen appears.



3. On the working area, leave the default values or specify new settings for the following:
   - **Report managed product status every**: Defines how often the managed product responds to Control Manager server messages. Valid values are between 5 to 480 minutes
   - **If no communication, set status as abnormal after**: Specifies how long Control Manager waits for a response from the managed product before changing its web console status to (inactive). Valid values are between 15 and 1440 minutes.

   Note

   The **If no communication, set status as abnormal after** value must be at least triple the **Report managed product status every** value.

4. Click **Save**.

Understanding the Product Directory

A managed product is a representation of an antivirus, content security, or web protection product in the Product Directory. Managed products display as icons (for

example, ( ) or ( )) in the Control Manager web console Product Directory section. These icons represent Trend Micro antivirus, content security, and web protection products. Control Manager supports dynamic icons, which change with the status of the managed product. See your managed product's documentation for more information on the icons and associated statuses for your managed product.

Indirectly administer the managed products either individually or by groups through the Product Directory. The following table lists the menu items and buttons on the Product Directory screen.

TABLE A-5. Product Directory Options

MENU ITEM	DESCRIPTION
Advanced Search	Click this menu item to specify search criteria to perform a search for one or more managed products.
Configure	After selecting a managed product/ directory, move the cursor over this menu item and select a task, to log on to a web-based console using SSO or to configure a managed product.
Tasks	After selecting a managed product/ directory, move the cursor over this menu item and select a task, to perform a specific function (such as deploying the latest components) to a specific managed product or child server or groups of managed products or child servers. Initiate a task from a directory and Control Manager sends requests to all managed products belonging to that directory.
Directory Management	Click this button to open the **Directory Management** screen. From the screen, move entities/directories (by dragging and dropping them) or create new directories.
Buttons	

MENU ITEM	DESCRIPTION
Search	Click this button, after typing a managed product's name, to perform a search for the specified managed product.
Status	Click this button, after selecting a managed product/directory, to obtain status summaries about the managed product or managed products found in the directory.
Folder	Click this button, after selecting a directory, to obtain status summaries about the managed products and the managed product endpoints found in the directory.

Note

Managed products belonging to child Control Manager servers cannot have tasks issued to them by the parent Control Manager server.

Product Directory Structure Recommendations

Trend Micro recommends the following when planning your Product Directory structure for managed products and child servers:

TABLE A-6. Considerations when Grouping Managed Products or Child Servers

STRUCTURE	DESCRIPTION
Company network and security policies	If different access and sharing rights apply to the company network, group managed products and child servers according to company network and security policies.
Organization and function	Group managed products and child servers according to the company's organizational and functional division. For example, have two Control Manager servers that manage the production and testing groups.

STRUCTURE	DESCRIPTION
Geographical location	Use geographical location as a grouping criterion if the location of the managed products and child servers affects the communication between the Control Manager server and its managed products or child servers.
Administrative responsibility	Group managed products and child servers according to system or security personnel assigned to them. This allows group configuration.

The Product Directory provides a user-specified grouping of managed products which allows you to perform the following for administering managed products:

- Configuring managed products
- Request products to perform a Scan Now (if this command is supported)
- View product information, as well as details about its operating environment (for example, product version, pattern file and scan engine versions, operating system information, and so on)
- View product-level logs
- Deploy virus pattern, scan engine, anti-spam rule, and program updates

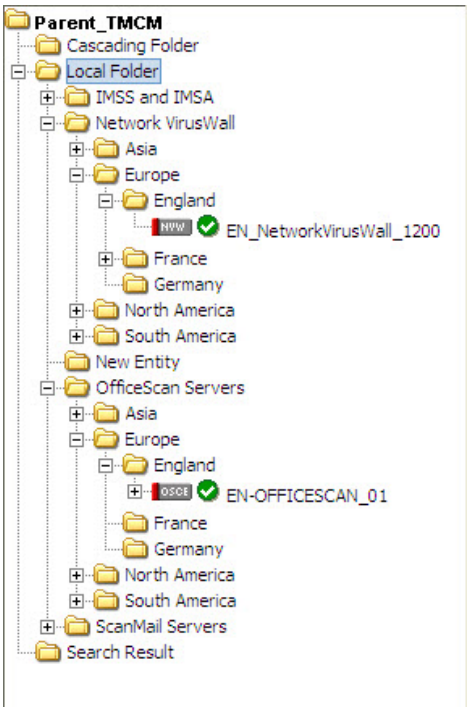
Plan this structure carefully, because the structure also affects the following:

TABLE A-7. Considerations for the Structure

CONSIDER	EFFECT
User access	When creating user accounts, Control Manager prompts for the segment of the Product Directory that the user can access. For example, granting access to the root segment grants access to the entire directory. Granting access to a specific managed product only grants access to that specific product.

CONSIDER	EFFECT
Deployment planning	Control Manager deploys update components (for example, virus pattern files, scan engines, anti-spam rules, program updates) to products based on Deployment Plans. These plans deploy to Product Directory folders, rather than individual products. A well-structured directory therefore simplifies the designation of recipients.
Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments	OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.

A sample Product Directory appears below:



Managed products identify the registered antivirus or content security product, as well as provide the connection status.

Note

All newly registered managed products usually appear in the New Entity folder regardless of the agent type.

TABLE A-8. Managed Product Icons

ICON	DESCRIPTION
EMAN	InterScan eManager
OSCE	OfficeScan Corporate Edition
SPNT	ServerProtect Information Server
	ServerProtect Domain
NT	ServerProtect for Windows (Normal Server)

Icon	Description
	ServerProtect for NetWare (Normal Server)
	InterScan Messaging Security Suite
	InterScan Web Security Suite
	InterScan VirusWall for Windows
	InterScan VirusWall for UNIX
	ScanMail for Microsoft Exchange
	ScanMail for Lotus Notes
	Network VirusWall
	NetScreen Global PRO Firewall
	Managed Product connection status icon

Arrange the Product Directory using the Directory Manager. Use descriptive folder names to group your managed products according to their protection type or the Control Manager network administration model.

Accessing the Product Directory

Use the Product Directory to administer managed products registered to the Control Manager server.

Note

Viewing and accessing the folders in the Product Directory depends on the Account Type and user account access rights.

Procedure

- Click **Products** from the main menu.

  The **Product Directory** screen appears.

Manually Deploying Components Using the Product Directory

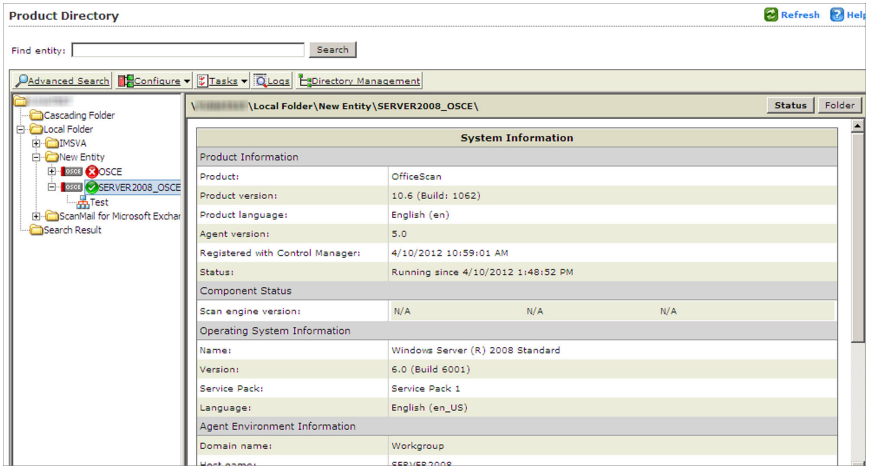
Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your managed products on demand. Use this method of updating components during virus outbreaks.

Download new components before deploying updates to a specific managed product or groups of managed products.

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.



2. Select a managed product or directory from the Product Directory.

   The managed product or directory highlights.

3. Move the cursor over **Tasks** from the Product Directory menu.

4. Select **Deploy <component>** from the drop-down menu.

5. Click **Deploy Now** to start the manual deployment of new components.

6. Monitor the progress through the **Command Tracking** screen.

7. Click the Command Details link on the **Command Tracking** screen to view details for the Deploy Now task.

Viewing Status Summaries for Managed Products

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all managed products present in the Product Directory tree.

There are two ways to view the managed products status summary:

- Through the dashboard using the Threat Detection Results widget (found on the Summary tab)
- Through the Product Directory

Accessing Through the Dashboard

Procedure

- Upon opening the Control Manager web console, the **Summary** tab on the Dashboard displays the summary of the entire Control Manager network. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

Accessing Through the Product Directory

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. From the Product Directory tree, select the desired folder or managed product.

   - If you click a managed product, the Product Status tab displays the managed product's summary.
   - If you click the Root folder, New entity, or other user-defined folder, the Product Status tab displays Antivirus, Content Security, and Web Security summaries.

Note

By default, the Status Summary displays a week's worth of information ending with the day of your query. You can change the scope to **Today**, **Last Week**, **Last Two Weeks**, or **Last Month** in the Display summary for list.

Configuring Managed Products

Depending on the product and agent version you can configure the managed product from the managed product's web console or through a Control Manager-generated console.

Procedure

1. Click **Products** on the main menu.

   The **Product Directory** screen appears.

2. Select the desired managed product from the Product Directory tree.

   The product status appears in the right-hand area of the screen.

3. Move the cursor over **Configure** in the Product Directory menu.
4. Select one of the following:
   - **Configuration Replication**: The **Configuration Settings** screen appears.

     a. Select the folder to which the selected managed product's settings replicate from the Product Directory tree.

     b. Click **Replicate**.

     The selected managed product's settings replicate to the target managed products.
   - **<Managed Product Name> Single Sign On**: The managed product's web console or Control Manager-generated console appears.

     a. Configure the managed product from the web console.

> **Note**
> For additional information about configuring managed products, refer to the managed product's documentation.

Issuing Tasks to Managed Products

Use the Tasks menu item to invoke available actions to a specific managed product. Depending on the managed product, all or some of the following tasks are available:

- Deploy engines
- Deploy pattern files/cleanup templates
- Deploy program files
- Enable or disable Real-time Scan
- Start Scan Now

Deploy the latest spam rule, pattern, or scan engine to managed products with outdated components. To successfully do so, the Control Manager server must have the latest

components from the Trend Micro ActiveUpdate server. Perform a manual download to ensure that current components are already present in the Control Manager server.

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select the managed product or directory to issue a task.
3. Move the cursor over **Tasks**.
4. Click a task from the list. Monitor the progress through Command Tracking. Click the **Command Details** link at the response screen to view command information.

Querying and Viewing Managed Product Logs

Use the Logs tab to query and view logs for a group or a specific managed product.

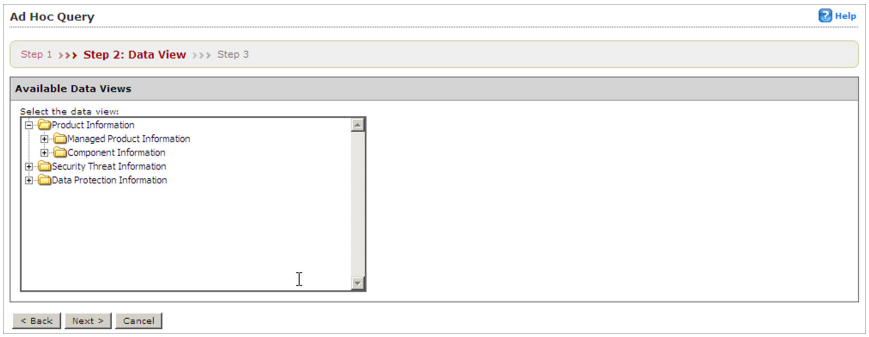
Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. Select the desired managed product or folder from the Product Directory.
3. Move the cursor over **Logs** in the Product Directory menu.
4. Click **Logs** from the drop-down menu.

   The **Ad Hoc Query > Step 2: Select Data View** screen appears.

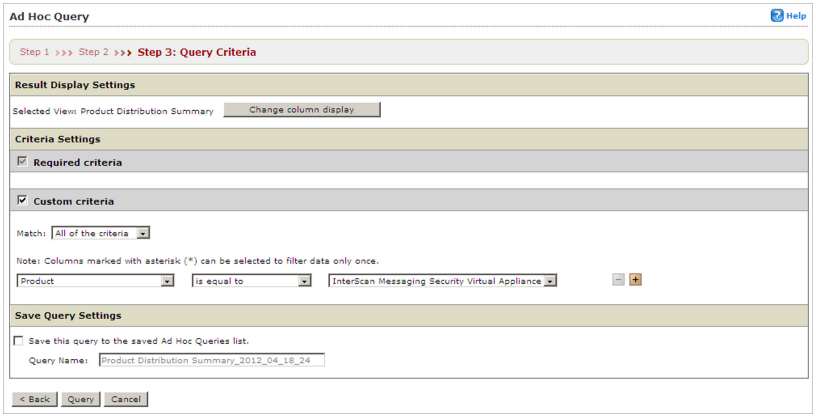


5. Specify the data view for the log:

   a. Select the data to query from the Available Data Views area.

   b. Click **Next**.

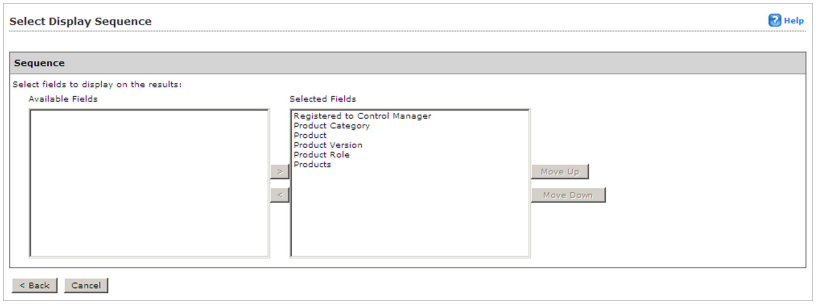
   The **Ad Hoc Query > Step 3: Query Criteria** screen appears.



6. Specify the data to appear in the log and the order in which the data appears. Items appearing at the top of the Selected Fields list appear as the left most column of the table. Removing a field from Selected Fields list removes the corresponding column from the Ad Hoc Query returned table.

   a. Click **Change column display**.

The **Select Display Sequence** screen appears.



b. Select a query column from the Available Fields list. Select multiple items using the **Shift** or **Ctrl** keys.

c. Click **>** to add items to the Selected Fields list.

d. Specify the order in which the data displays by selecting the item and clicking **Move up** or **Move down**.

e. Click **Back** when the sequence fits your requirements.

7. Specify the filtering criteria for the data:

Note

When querying for summary data, users must specify the items under Required criteria.

- Required criteria:
  - Specify a Summary Time for the data or whether you want COOKIES to appear in your reports.
- Custom criteria:

  a. Specify the criteria filtering rules for the data categories:

    - **All of the criteria**: This selection acts as a logical AND function. Data appearing in the report must meet all the filtering criteria.

- **Any of the criteria**: This selection acts as a logical OR function. Data appearing in the report must meet any of the filtering criteria.

b. Specify the filtering criteria for the data. Control Manager supports specifying up to 20 criteria for filtering data.

Tip

If you do not specify any filtering criteria, the Ad Hoc Query returns all results for the applicable columns. Trend Micro recommends specifying filtering criteria to simplify data analysis after the information for the query returns.

8. Save the query:

a. Click **Save this query to the saved Ad Hoc Queries list**.

b. Type a name for the saved query in the **Query Name** field.

9. Click **Query**.

The **Results** screen appears.

10. Save the report as a CSV file:

a. Click **Export to CSV**.

b. Click **Download**.

c. Specify the location to save the file.

d. Click **Save**.

11. Save the report as an XML file:

a. Click **Export to XML**.

b. Click **Download**.

c. Specify the location to save the file.

d. Click **Save**.

Tip

To query more results on a single screen, select a different value in Rows per page. A single screen can display 10, 15, 30, or 50 query results per page.

12. Save the settings for the query:

    a. Click **Save query settings**.

    b. Type a name for the saved query in the **Query Name** field.

    c. Click **OK**.

    The saved query appears on the **Saved Ad Hoc Queries** screen.

About Recovering Managed Products Removed From the Product Directory

The following scenarios can cause Control Manager to delete managed products from the Product Directory:

- Reinstalling the Control Manager server and selecting **Delete existing records and create a new database**

  This option creates a new database using the name of the existing one.

- Replacing the corrupted Control Manager database with another database of the same name

- Accidentally deleting the managed product from Directory Management

If the records for a Control Manager server's managed products are lost, TMI agents on the products still "know" where they are registered. The Control Manager agent automatically re-registers itself after 8 hours or when the service restarts.

MCP agents do not re-register automatically. Administrators must manually re-register managed products using MCP agents.

Recovering Managed Products Removed From the Product Directory

Procedure

- Restart the Trend Micro Control Manager service on the managed product server. For more information, see *Stopping and Restarting Control Manager Services on page A-31*.
- Wait for the Agent to re-register itself: By default, the older Control Manager agents verify their connection to the server every eight (8) hours. If the agent detects that its record has been deleted, it will re-register itself automatically.
- Manually re-register to Control Manager: MCP agents do not re-register automatically and need to be manually re-registered to the Control Manager server.

Stopping and Restarting Control Manager Services

Use the **Windows Services** screen to restart any of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro Common CGI
- Trend Micro Control Manager

Note

These are the services that run in the background on the Windows operating system, not the Trend Micro services that require Activation Codes (for example, Outbreak Prevention Services).

Procedure

1. Click **Start** > **Programs** > **Administrative Tools** > **Services** to open the **Services** screen.

2. Right-click **<Control Manager service>**, and then click **Stop**.
3. Right-click **<Control Manager service>**, and then click **Start**.

Searching for Managed Products, Product Directory Folders, or Computers

Use the **Search** button to quickly locate a specific managed product in the Product Directory.

Searching for a Folder or Managed Product

Procedure

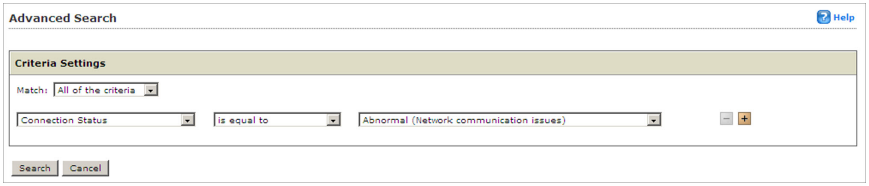
1. Access the Product Directory.
2. Type the display name of the managed product in the **Find entity** field.
3. Click **Search**.

Performing an Advanced Search

Procedure

1. Access the Product Directory.
2. Click **Advanced Search**.

   The **Advanced Search** screen appears.



3. Specify your filtering criteria for the product. Control Manager supports up to 20 filtering criteria for searches.
4. Click **Search** to start searching.

   Search results appear in the **Search Result** folder of the Product Directory.

Refreshing the Product Directory

Procedure

- On the **Product Directory** screen, click the **Refresh** icon on the upper right corner of the screen.

Understanding the Directory Management Screen

After registering to Control Manager, the managed product appears in the Product Directory under the default folder.

Use the Directory Management screen to customize the Product Directory organization to suit your administration needs. For example, you can group products by location or product type (messaging security, web security, file storage protection).

The directory allows you to create, modify, or delete folders, and move managed products between folders. You cannot, however, delete nor rename the New entity folder.

Carefully organize the managed products belonging to each folder. Consider the following factors when planning and implementing your folder and managed product structure:

- Product Directory
- User Accounts
- Deployment Plans
- Ad Hoc Query

- Control Manager reports

Group managed products according to geographical, administrative, or product-specific reasons. In combination with different access rights used to access managed products or folders in the directory, the following table presents the recommended grouping types as well as their advantages and disadvantages.

TABLE A-9. Product Grouping Comparison

GROUPING TYPE	ADVANTAGES	DISADVANTAGES
Geographical or Administrative	Clear structure	No group configuration for identical products
Product type	Group configuration and status is available	Access rights may not match
Combination of both	Group configuration and access right management	Complex structure, may not be easy to manage

Using the Directory Management Screen Options

Use these options to manipulate and organize managed products in your Control Manager network.

The **Directory Management** screen provides several options:

- Add directories to the Product Directory
- Rename directories in the Product Directory
- Move managed products or directories in the Product Directory
- Remove managed products or directories from the Product Directory

Note

The keep permissions check box allows a folder to keep its source permission when moved.

Using the Directory Management Screen

Procedure

- Select a managed product or directory and click **Rename** to rename a managed product or directory
- Click **+** or the folder to display the managed products belonging to a folder
- Drag managed products or directories to move the managed products or directories in the Product Directory
- Click **Add Folder** to add a directory to the Product Directory

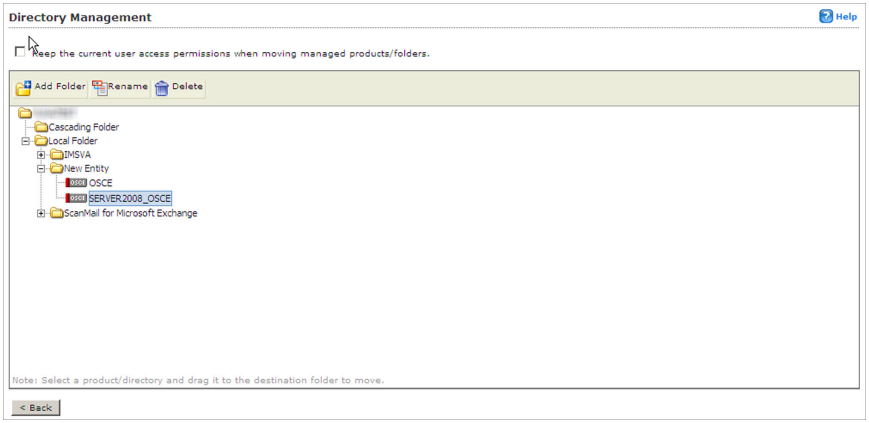
Accessing the Directory Management Screen

Use the **Directory Management** screen to group managed products together.

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.



2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

Creating Folders

Group managed products into different folders to suit your organization's Control Manager network administration model.

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select **Local Folder**.

4. Click **Add Folder**.

   The **Add Directory** screen appears.

5. Type a name for the new directory in the **Directory name** field.

6. Click **Save**.

Note

Except for the **New Entity** folder, Control Manager lists all other folders in ascending order, starting from special characters (!, #, $, %, (,), *, +, -, comma, period, +, ?, @, [,], ^, _, {, |, }, and ~), numbers (0 to 9), or alphabetic characters (a/A to z/Z).

Renaming Folders or Managed Products

Rename directories and managed products on the **Directory Management** screen.

Note

Renaming a managed product only changes the name stored in the Control Manager database; there are no effects to the managed product.

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select the managed product or directory to rename.

4. Click **Rename**.

   The **Rename Directory** screen appears.

5. Type a name for the managed product or directory in the **Directory name** field.

6. Click **Save**.

7. Click **OK**.

   The managed product or directory displays in the Product Directory with the new name.

Moving Folders or Managed Products

When moving folders pay special attention to the **Keep the current user access permissions when moving managed products/folders** check box. If you select this check box and move a managed product or folder, the managed product or folder keeps the permissions from its source folder. If you clear the keep permissions check box, and then move a managed product or folder, the managed product or folder assumes the access permissions from its new parent folder.

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. On the working area, select the folder or managed product to move.

4. Drag the folder or managed product to the target new location.

5. Click **Save**.

Deleting User-Defined Folders

Take caution when deleting user-defined folders on the **Directory Management** screen. You may accidentally delete a managed product which causes it to unregister from the Control Manager server.

Note

You cannot delete the **New Entity** folder.

Procedure

1. Click **Products** from the main menu.

   The **Product Directory** screen appears.

2. Click **Directory Management** from the Product Directory menu.

   The **Directory Management** screen appears.

3. Select the managed product or directory to delete.

4. Click **Delete**.

   A confirmation dialog box appears.

5. Click **OK**.
6. Click **Save**.

Downloading and Deploying New Components

Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats.

By default, Control Manager enables download only on components belonging to managed products registered to the Control Manager server. Control Manager enables virus pattern download even if no managed products are registered to the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update).

TABLE A-10. Available Components

COMPONENT	DESCRIPTION
Pattern files/Cleanup templates	Pattern files/Cleanup templates contain hundreds of malware signatures (for example, viruses or Trojans) and determine the managed product's ability to detect and clean malicious file infections
Antispam rules	Antispam rules are the Trend Micro-provided files used for antispam and content filtering
Engines	Engines refer to virus/malware scan engines, Damage Cleanup engine, VirusWall engines, the Spyware/Grayware engine and so on. These components perform the actual scanning and cleaning functions.

COMPONENT	DESCRIPTION
OfficeScan Plug-in Programs	OfficeScan Plug-in Programs (for example, Trend Micro Security for Mac). **Note** The OfficeScan web console displays all available Plug-in Programs. You can specify to download any of them from Control Manager. However, Control Manager may not have the downloaded the Plug-in Program. Which means that OfficeScan cannot download the specified Plug-in Program from Control Manager. Before specifying a Plug-in Program for download, from Control Manager to OfficeScan, verify that Control Manager has already downloaded the Plug-in Program.
Product programs and widget pool	Product-specific components (for example, Service Pack releases) and the Control Manager widget pool

Note

Only registered users are eligible for components update.

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed product.

The **Component List** screen presents a full list of all components that Control Manager has available for managed products. The list also matches components with managed

products that use the component. Click **Updates** > **Component List** to open the **Component List** screen.

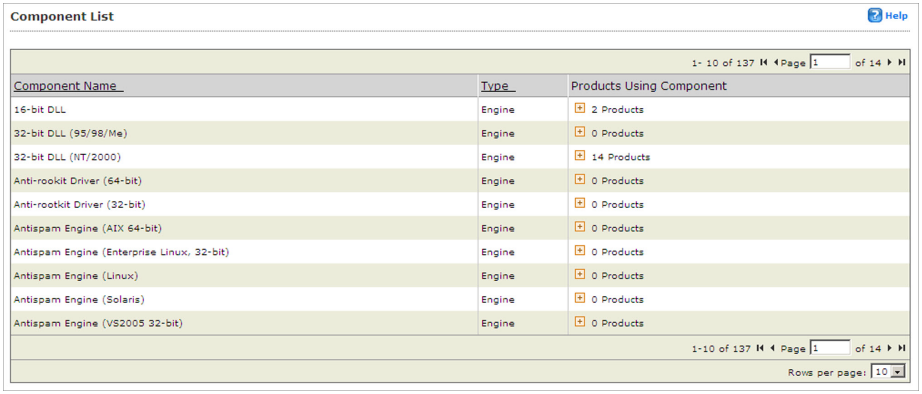


FIGURE A-2. The Component List screen

The Control Manager server only retains the latest component version. You can trace a component's version history by viewing root>:\Program Files\Trend Micro\Control Manager\AU_log\TmuDump.txt entries. TmuDump.txt generates when ActiveUpdate debugging is enabled.

Tip

To minimize Control Manager network traffic, disable the download of components that have no corresponding managed products or services. When you register managed products or activate services at a later time, be sure to configure the manual or scheduled download of applicable components.

Manually Downloading Components

Manually download component updates when you initially install Control Manager, when your network is under attack, or when you want to test new components before deploying the components to your network.

Trend Micro recommends the following method to configure manual downloads. Manually downloading components requires multiple steps:

Tip

Ignore steps 1 and 2 if you have already configured your deployment plan and configured your proxy settings.

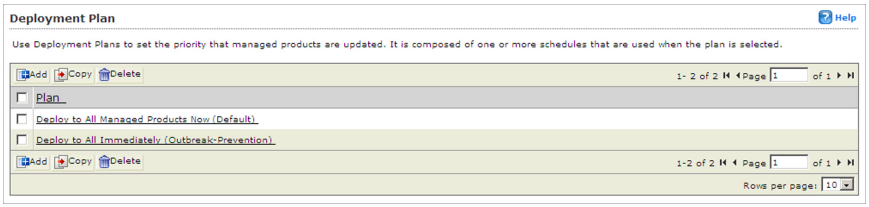
- Step 1: Configure a deployment plan for your components
- Step 2: Configure your proxy settings, if you use a proxy server
- Step 3: Select the components to update
- Step 4: Configure the download settings
- Step 5: Configure the automatic deployment settings
- Step 6: Complete the manual download

Step 1: Configure a Deployment Plan for Your Components

Procedure

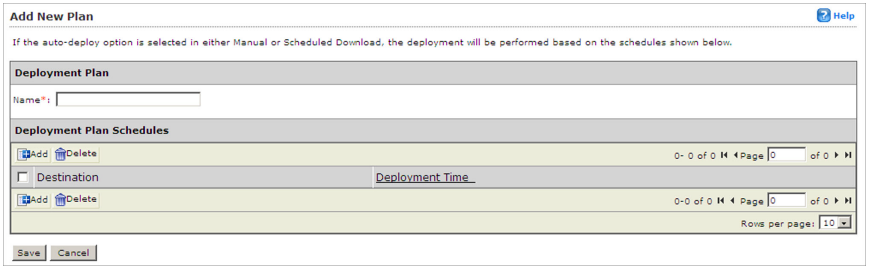
1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.



2. Click **Add**.

   The **Add New Plan** screen appears.



3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

   The **Add New Schedule** screen appears.

5. On the **Add New Schedule** screen, choose a deployment time schedule by selecting one the following options:

   - **Start at**: Performs the deployment at a specific time.

     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.

   The **Add New Plan** screen appears.

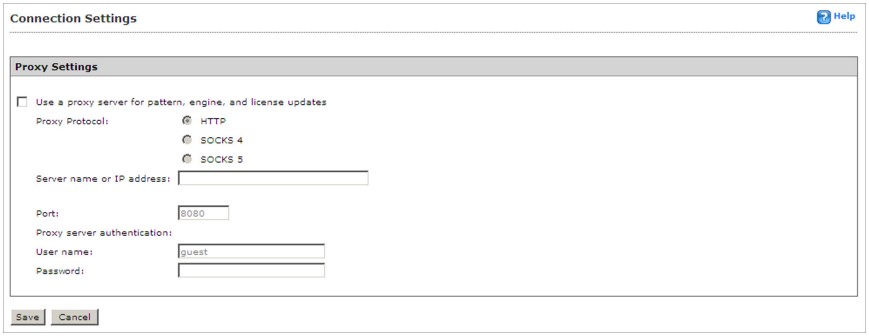
8. Click **Save** to apply the new deployment plan.

Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.



2. Select **Use a proxy server for pattern, engine, and license updates**.

3. Select the protocol:

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Type the host name or IP address of the server in the **Server name or IP address** field.

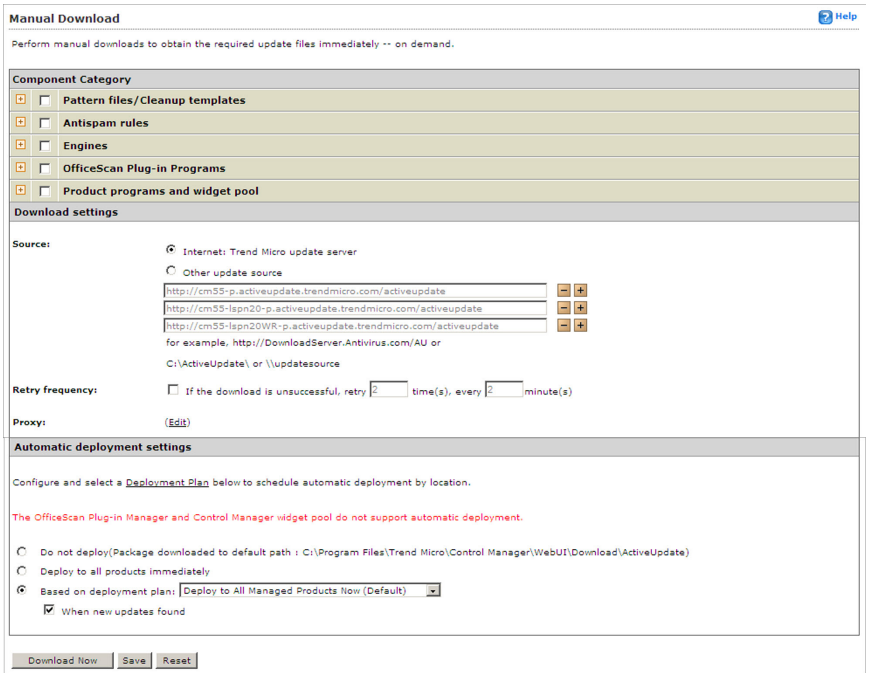
5. Type a port number in the **Port** field.
6. Type a log on name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the Components to Update

Procedure

1. Navigate to **Updates** > **Manual Download**.

   The **Manual Download** screen appears.



2. From the Component Category area select the components to download.

a. Click the + icon to expand the component list for each component group.

b. Select the components to download. To select all components for a group, select:

- **Pattern files/Cleanup templates**
- **Antispam rules**
- **Engines**
- **OfficeScan Plug-in Programs**
- **Product programs and widget pool**

Step 4: Configure the Download Settings

Procedure

1. Select the update source:

   - **Internet: Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server.
   - **Other update source**: Type the URL of the update source in the accompanying field.

     After selecting **Other update source**, you can specify multiple update sources. Click the + icon to add an update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

Tip

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, if the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the **Connection Settings** screen.

Step 5: Configure the Automatic Deployment Settings

Procedure

1. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:
   - **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment
   - **Deploy to all products immediately**: Components download to Control Manager, and then deploy to managed products
   - **Based on deployment plan**: Components download to Control Manager, but deploy to managed products based on the schedule you select
   - **When new updates found**: Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Tip

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

Step 6: Complete the Manual Download

Procedure

1. Click **Download Now** and then click **OK** to confirm.

   The download response screen appears. The progress bar displays the download status.

2. Click **Command Details** to view details from the **Command Details** screen.

3. Click **OK** to return to the **Manual Download** screen.

Understanding Scheduled Download Exceptions

Download exceptions allow administrators to prevent Control Manager from downloading Trend Micro update components for entire day(s) or for a certain time every day.

This feature is particularly useful for administrators who prefer not to allow Control Manager to download components on a non-work day or during non-work hours.

Note

Daily scheduled exceptions apply to the selected days, while hourly scheduled exceptions apply to every day of the week.

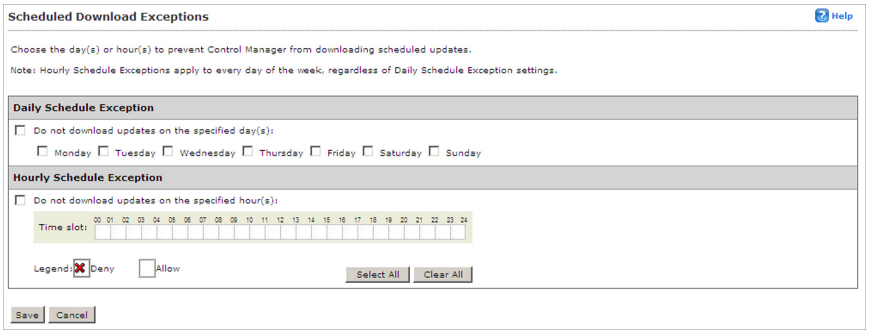
Example: The administrator decides that they do not want Control Manager to download components on weekends or after working hours throughout the week. The administrator enables **Daily Schedule Exception** and selects **Saturday** and **Sunday**. The administrator then enables **Hourly Schedule Exception** and specifies the hours of **00:00 to 9:00** and **18:00 to 24:00**.

Configuring Scheduled Download Exceptions

Procedure

1. Navigate to **Updates** > **Scheduled Download Exceptions**.

   The **Scheduled Download Exceptions** screen appears.



2. Do one or more of the following:

   - To schedule a daily exception, under Daily Schedule Exception, select the day(s) to prevent downloads, and then select **Do not download updates on the specified day(s)**. Every week, Control Manager blocks all downloads during the selected day(s).

   - To schedule an hourly exception, under Hourly Schedule Exception, select the hour(s) to prevent downloads, and then select **Do not download updates on the specified hour(s)**. Every day, Control Manager blocks all downloads during the selected hours.

3. Click **Save**.

Configuring Scheduled Downloads

Configure scheduled downloading of components to keep your components up to date and your network secure. Control Manager supports granular component downloading. You can specify the component group and individual component download schedules.

All schedules are autonomous of each other. Scheduling a download for a component group downloads all components in the group.

Use the **Scheduled Download** screen to obtain the following information for components currently in your Control Manager system:

- **Frequency**: Shows how often the component updates
- **Enabled**: Indicates if the schedule for the component is enabled or disabled
- **Update Source**: Displays the URL or path of the update source

Configuring scheduled component downloads requires multiple steps:

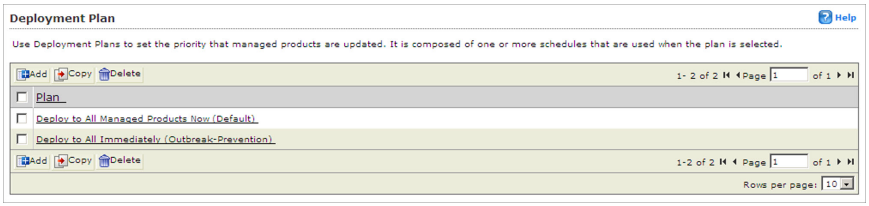
- Step 1: Configure a Deployment Plan for your components
- Step 2: Configure your proxy settings, if you use a proxy server
- Step 3: Select the components to update
- Step 4: Configure the download schedule
- Step 5: Configure the download settings
- Step 6: Configure the automatic deployment settings
- Step 7: Enable the schedule and save settings

Step 1: Configure a Deployment Plan for Your Components

Procedure

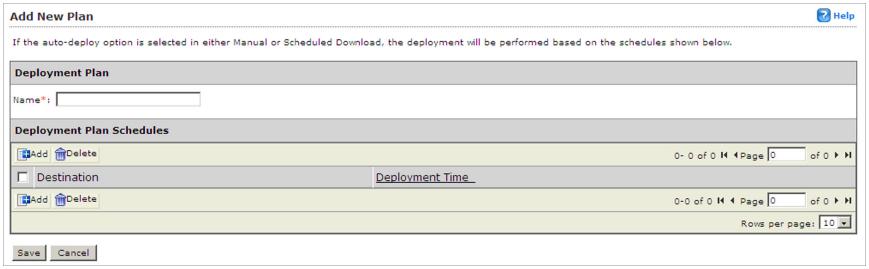
1. Navigate to **Updates** > **Deployment Plan**.

   The **Deployment Plan** screen appears.



2. Click **Add**.

   The **Add New Plan** screen appears.



3. Type a deployment plan name in the **Name** field.

4. Click **Add** to provide deployment plan details.

   The **Add New Schedule** screen appears.

5. Choose a deployment time schedule by selecting one the following options:

   - **Start at**: Performs the deployment at a specific time.

     Use the menus to designate the time in hours and minutes.

   - **Delay**: after Control Manager downloads the update components, Control Manager delays the deployment according to the interval that you specify.

     Use the menus to indicate the duration, in terms of hours and minutes.

6. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

7. Click **Save**.

   The **Add New Plan** screen appears.

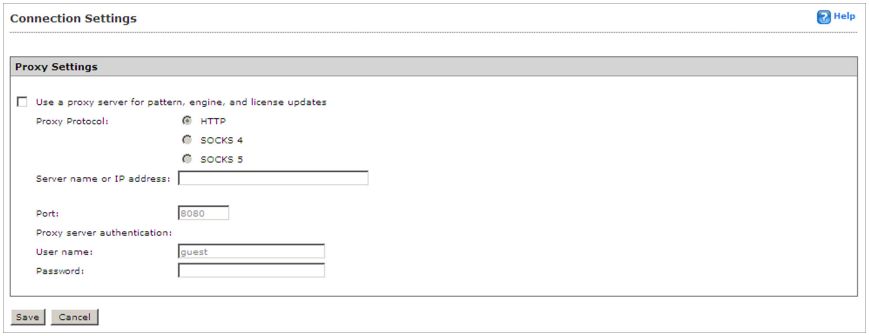
8. Click **Save** to apply the new deployment plan.

Step 2: Configure Your Proxy Settings (If You Use a Proxy Server)

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.



2. Select **Use a proxy server for pattern, engine, and license updates**.

3. Select the protocol:

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Type the host name or IP address of the server in the **Server name or IP** address field.

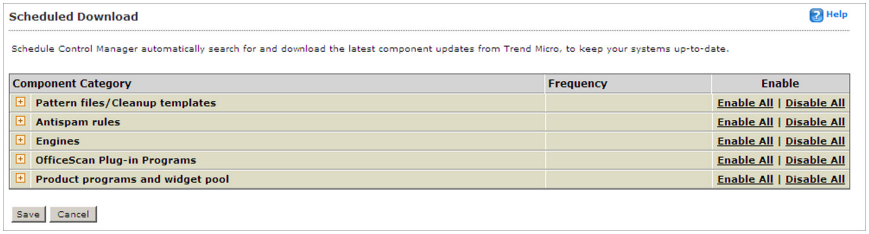
5. Type a port number for the proxy server in the **Port** field.
6. Type a logon name and password if your server requires authentication.
7. Click **Save**.

Step 3: Select the Components to Update

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.



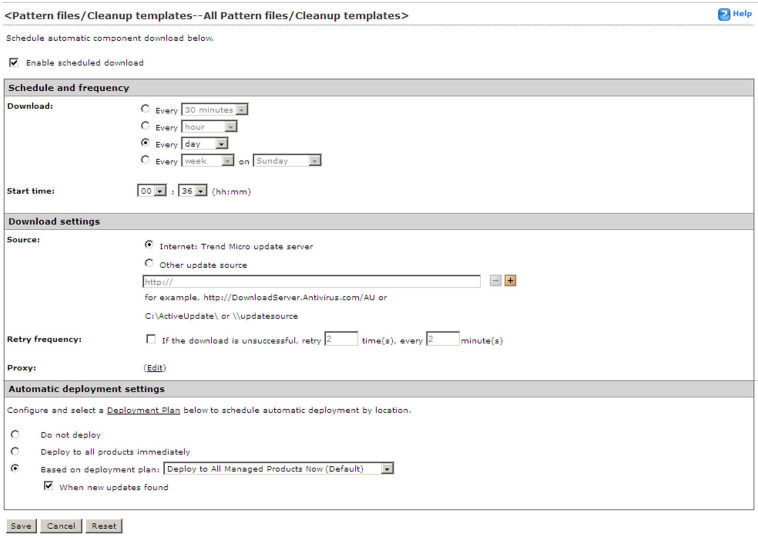
2. From the Component Category area select the components to download.

   a. Click the **+** icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

      The <Component Name> screen appears. Where <Component Name> represents the name of the selected component.



Step 4: Configure the Download Schedule

Procedure

1. Select the **Enable scheduled download** check box to enable scheduled download for the component.
2. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download by minutes, hours, days, or weeks.
3. Use the **Start time** menus to specify the date and time the schedule starts to take effect.

Step 5: Configure the Download Settings

Procedure

1. Select the update source:

   - **Internet**: **Trend Micro update server**: Download components from the official Trend Micro ActiveUpdate server.

   - **Other update source**: Type the URL of the update source in the accompanying field.

     After selecting **Other update source**, you can specify multiple update sources. Click the **+** icon to add an update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number of retries and duration between retries for downloading components.

   Note

   Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

3. If you use an HTTP proxy server on the network (that is, if the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the **Connection Settings** screen.

Step 6: Configure the Automatic Deployment Settings

Procedure

1. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:

   - **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:

  - Deploying to the managed products individually
  - Testing the updated components before deployment
- **Deploy immediately**: Components download to Control Manager, then deploy to managed products
- **Based on deployment plan**: Components download to Control Manager, but deploy to managed products based on the schedule you select
- **When new updates found**: Components download to Control Manager, and deploy to managed products when new components are available from the update source

Note

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

2. Select a deployment plan after components download to Control Manager, from the **Deployment Plan** screen.
3. Click **Save**.

Step 7: Enable the Schedule and Save Settings

Procedure

1. Click the status button in the **Enable** column.
2. Click **Save**.

Configuring Scheduled Download Schedule and Frequency

Specify how often Control Manager obtains component updates at the Schedule and Frequency group.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.

   a. Click the **+** icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        The Component Name> screen appears. Where Component Name> is the name of the component you selected.

3. Under Schedule and frequency:

   a. Define the download schedule. Select a frequency, and use the appropriate drop down menu to specify the desired schedule. You may schedule a download every minutes, hours, days, or weeks.

   b. Use the **Start time** drop-down menus to specify the date and time the schedule starts to take effect.

4. Click **Save**.

Configuring Scheduled Download Settings

The Download Settings group defines the components Control Manager automatically downloads and the download method.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.

   a. Click the **+** icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

        The Component Name> screen appears. Where Component Name> represents the name of the selected component.

3. Under Download settings, select one of the following update sources:

   - **Internet: Trend Micro update server**: (default setting) Control Manager downloads the latest components from the Trend Micro ActiveUpdate server
   - **Other update source**: specify the URL of the latest component source, for example, your company's Intranet server

     After selecting **Other update source**, you can specify multiple update sources. Click the + icon to add an additional update source. You can configure up to five update sources.

4. Select **Retry frequency** to instruct Control Manager to retry downloading latest components. Specify the number of attempts and the frequency of each set of attempts in the appropriate fields.

Note

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

5. If you are using a proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings from the **Connection Settings** screen.

6. Click **Save**.

Configuring Scheduled Download Automatic Deployment Settings

Use the Automatic deployment settings group to set how Control Manager deploys updates.

Procedure

1. Navigate to **Updates** > **Scheduled Download**.

   The **Scheduled Download** screen appears.

2. From the Component Category area select the components to download.

   a. Click the **+** icon to expand the component list for each component group.

   b. Select the components to download. To select all components for a group, select:

      - **All Pattern files/Cleanup templates**
      - **All Antispam rules**
      - **All Engines**
      - **OfficeScan Plug-in Programs**
      - **Product programs and widget pool**

The Component Name> screen appears. Where Component Name> represents the name of the selected component.

3. Select when to deploy downloaded components from the Automatic deployment settings area. The options are:

   - **Do not deploy**: Components download to Control Manager, but do not deploy to managed products. Use this option under the following conditions:
     - Deploying to the managed products individually
     - Testing the updated components before deployment
   - **Deploy immediately**: Components download to Control Manager, then deploy to managed products
   - **Based on deployment plan**: Components download to Control Manager, but deploy to managed products based on the schedule you select
   - **When new updates found**: Components download to Control Manager when new components are available from the update source, but deploy to managed products based on the schedule you select

Note

Click **Save** before clicking **Edit** or **Deployment Plan** on this screen. If you do not click **Save** your settings will be lost.

4. Select a deployment plan after components download to Control Manager, from the **Deployment Plan** screen.

5. Click **Save**.

Note

The settings in Automatic deployment settings only apply to components used by managed products.

Understanding Deployment Plans

A deployment plan allows you to set the order in which Control Manager updates your groups of managed products. With Control Manager, you can implement multiple deployment plans to different managed products at different schedules. For example, during an outbreak involving an email-borne virus, you can prioritize the update of your email message scanning software components such as the latest virus pattern file for Trend Micro ScanMail for Microsoft Exchange.

The Control Manager installation creates two deployment plans:

- Deploy to All Managed Products Now (Default): default plan used during component updates
- Deploy to All Immediately (Outbreak-Prevention): default plan for the Outbreak Prevention Services Prevention Stage

By default, these plans deploy updates to all products in the Product Directory immediately.

Select or create plans from the Manual and Scheduled download screens. Customize these plans, or create new ones, as required by your network. For example, create deployment plans according to the nature of the outbreak:

- Email-borne virus
- File-sharing virus

Deploying updates to the Product Directory is separate from the download process.

Control Manager downloads the components and follows the deployment plan according to manual or scheduled download settings.

When creating or implementing a deployment plan, consider the following points:

- Assign deployment schedules to folders, not to specific products.

  Planning the contents of the Product Directory folders, therefore, becomes very important.

- You can only include one folder for each deployment plan schedule.

  However, you can specify more than one schedule per deployment plan.

- Control Manager bases the deployment plan delays on the completion time of the download, and these delays are independent of each other.

  For example, if you have three folders to update at 5 minute intervals, you can assign the first folder a delay of 5 minutes, and then set delays of 10 and 15 minutes for the two remaining folders.

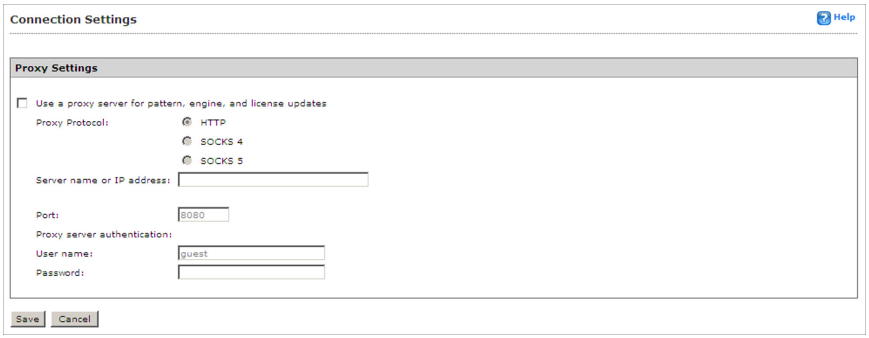
Configuring Proxy Settings

Configure the proxy server connection for component downloads and for license updates.

Procedure

1. Navigate to **Administration** > **Settings** > **Proxy Settings**.

   The **Connection Settings** screen appears.



2. Select **Use a proxy server for pattern, engine, and license updates**.

3. Select the protocol:

   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

4. Type the host name or IP address of the server in the **Server name or IP address** field.
5. Type a port number in the **Port** field.
6. Type a log on name and password if your server requires authentication.
7. Click **Save**.

Configuring Update/Deployment Settings

Using HTTPS to download components from the Trend Micro ActiveUpdate server (the default download source) or other update source provides a more secure method for retrieving components.

Downloading components from a shared folder in a network requires setting the local Windows and Remote UNC authentications.

The local Windows authentication refers to the Active Directory user account in the Control Manager server. The account should have:

- Administrator privilege
- *Log on as a batch job* policy set

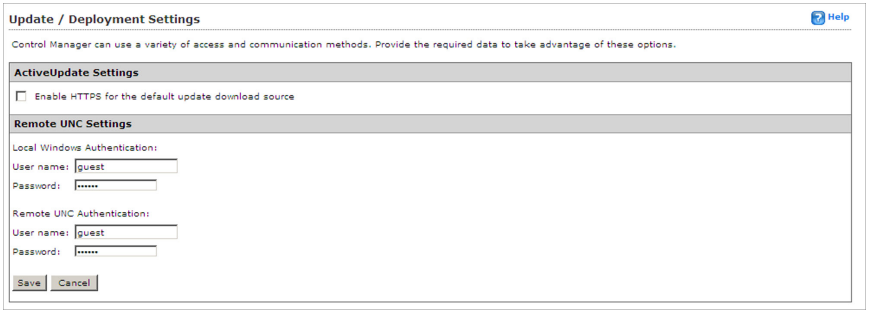
The **remote UNC authentication** feature uses a user account from the component source server that has permission to share a folder to which Control Manager will download updates.

Enabling HTTPS Download

Procedure

1. Navigate to **Updates** > **Update/Deployment Settings**.

   The **Update/Deployment Settings** screen appears.



2. Select **Enable HTTPS for the default update download source**.
3. Click **Save**.
4. Navigate to the **Manual Download** or **Scheduled Download** screen.
5. On the working area under **Download settings**, select **Internet: Trend Micro update server** or specify your organization's component source server in the **Other update source** field.
6. Click **Save**.

Enabling UNC Download

Procedure

1. Navigate to **Updates** > **Update/Deployment Settings**.

   The **Update/Deployment Settings** screen appears.
2. Type the **Local Windows Authentication** and **Remote UNC Authentication** user names and passwords.
3. Click **Save**.
4. Navigate to the **Manual Download** or **Scheduled Download** screen.
5. On the working area under **Download settings**, select **Other update source** and then specify the shared network folder.

6. Click **Save**.

Setting "Log on as batch job" Policy

The local Windows authentication refers to the Active Directory user account in the Control Manager server. The account should have:

- Administrator privilege
- "Log on as a batch job" policy set

Procedure

1. Click **Start** > **Settings** > **Control Panel**.
2. Click **Administrative Tools**.
3. Open **Local Security Policy**. The Local Security Settings screen appears.
4. Click **Local Polices** > **User Rights Assignment**.
5. Double-click **Log on as a batch job**.

   The **Log on as a batch job Properties** dialog box appears.
6. Add the user if they do not appear on the list.

Using Logs

Although Control Manager receives data from various log types, Control Manager allows users to query the log data directly from the Control Manager database. Users can then specify filtering criteria to gather only the data they need.

Control Manager also introduces log aggregation. Log aggregation can improve query performance and reduce the network bandwidth managed products require when sending logs to Control Manager. However, this comes at a cost of lost data through

aggregation. Control Manager cannot query data that does not exist in the Control Manager database.

Understanding Managed Product Logs

Managed product logs contain information about the performance of your managed products. You can obtain information for specific products or groups of products administered by the parent or child server. With Control Manager's data query on logs and data filtering capabilities, administrators can focus on the information they need.

Note

More logs mean abundant information about the Control Manager network. However, these logs occupy disk space. You must balance the need for information with your available system resources.

Managed products generate different kinds of logs depending on their function.

TABLE A-11. Managed Product Logs

LOG CATEGORY	DESCRIPTION
Product Information	Product information logs provide information on subjects ranging from user access and events on managed products to component deployment and update status. • Managed Product Information • Component Information

LOG CATEGORY	DESCRIPTION
Security Threat Information	Security threat logs provide information on known and potential security threats detected on your network. • Virus/Malware Information • Spyware/Grayware Information • Content Violation Information • Spam Violation Information • Policy/Rule Violation Information • Web Violation/Reputation Information • Suspicious Threat Information • Overall Threat Information
Data Protection Information	Data Protection logs provide information on DLP incidents, template matches, and incident sources. • Data Loss Prevention Information

Querying Log Data

Ad Hoc Queries provide administrators with a quick method to pull information directly from the Control Manager database. The database contains all information collected from all products registered to the Control Manager server (log aggregation can affect the data available to query). Ad Hoc Queries provide a very powerful tool for administrators.

While querying data, administrators can filter the query criteria so only the data they need returns. Administrators can then export the data to CSV or XML format for further analysis or save the query for future use. Control Manager also supports sharing saved queries with other users so others can benefit from useful queries.

Completing an Ad Hoc query consists of the following process:

- Step 1: Select the managed product or current Control Manager server for the query

- Step 2: Select the data view to query
- Step 3: Specify filtering criteria and the specific information that displays
- Step 4: Save and complete the query
- Step 5: Export the data to a CSV or XML file

Note

Control Manager supports sharing saved Ad Hoc Queries with other users. Saved and shared queries appear on the **Saved Ad Hoc Queries** screen.

Understanding Data Views

A data view is a table consisting of clusters of related data cells. Data views provide the foundation on which users perform Ad Hoc Queries to the Control Manager database.

Control Manager allows direct queries to the Control Manager database. Data views are available to Control Manager 5 report templates and to Ad Hoc Query requests.

Data views are tables filled with information. Each heading in a data view acts as a column in a table. For example, the Virus/Malware Action/Result Summary data view has the following headings:

- Action Result
- Action Taken
- Unique Endpoints
- Unique Sources
- Detections

As a table, a data view takes the following form with potential subheadings under each heading:

TABLE A-12. Sample Data View

ACTION RESULT	ACTION TAKEN	UNIQUE ENDPOINTS	UNIQUE SOURCES	DETECTIONS

This information is important to remember when specifying how data displays in a report template.

Control Manager separates data views into two major categories: Product Information and Security Threat Information. See the appendix for more information about data views. The major categories separate further into several subcategories, with the subcategories separated into summary information and detailed information.

Understanding Reports

Control Manager reports consist of two parts: report templates and report profiles. Where a report template determines the look and feel of the report, the report profile specifies the origin of the report data, the schedule/time period, and the recipients of the report.

Control Manager 5.0 introduced radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control Manager 6.0 continues to support report templates from previous Control Manager versions, however Control Manager 6.0 allows administrators to design their own custom report templates.

Understanding Control Manager Report Templates

A report template outlines the look and feel of Control Manager reports. Control Manager categorizes report templates according to the following types:

- Control Manager 5 templates: User-defined customized report templates that use direct database queries (database views) and report template elements (charts and tables). Users have greater flexibility specifying the data that appears in their reports compared to report templates from previous Control Manager versions. For more information on Control Manager 5 templates, see *Understanding Control Manager 5 Templates on page A-70*.

- Control Manager 3 templates: Includes pre-defined templates. For more information on Control Manager 3 templates, see *Understanding Control Manager 3 Templates on page A-76*.

Understanding Control Manager 5 Templates

Control Manager 5 report templates use database views as the information foundation for reports. For more information on data views, see *Understanding Data Views on page A-68*. The look and feel of generated reports falls to the report elements. Report elements consist of the following.

TABLE A-13. Control Manager 5 Report Template Elements

TEMPLATE ELEMENT	DESCRIPTION
Page break	Inserts a page break for a report. Each report page supports up to three report template elements.
Static text	Provides a user-defined description or explanation for the report. Static text content can contain up to 4096 characters.
Bar chart	Inserts a bar chart into a report template.
Line chart	Inserts a line graph into a report template.
Pie chart	Inserts a pie chart into a report template.
Dynamic table	Inserts a dynamic table/pivot table into a report template.
Grid table	Inserts a table into a report template. The information in a grid table will be the same as the information that displays in an Ad Hoc Query.

Each Control Manager 5 template can contain up to 100 report template elements. Each page in the report template can contain up to three report template elements. Use page breaks to create report template pages.

To better understand Control Manager 5 report templates, Trend Micro provides the following pre-defined report templates.

Note

Access the **Report Templates** screen to view the Trend Micro pre-defined templates.

TABLE A-14. Control Manager 5 Pre-defined Templates

TEMPLATE	DESCRIPTION
TM-Content Violation Detection Summary	Provides the following information: • Content Violation Detection Grouped by Day (Line chart) • Policy in Violation Count Grouped by Day (Line chart) • Sender/Users in Violation Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Top 25 Policies in Violation (Bar chart) • Content Violation Policy Summary (Grid table) • Top 25 Senders/Users in Violation (Bar chart) • Content Violation Senders/Users in Violation Summary (Grid table) • Action Result Summary (Pie chart)

Template	Description
TM-Managed Product Connection/Component Status	Provides the following information: • Server/Appliance Connection Status (Pie chart) • Client Connection Status (Pie chart) • Server/Appliance Pattern File/Rule Update Status (Pie chart) • Client Pattern File/Rule Update Status (Pie chart) • Server/Appliance Scan Engine Update Status (Pie chart) • Client Scan Engine Update Status (Pie chart) • Pattern File/Rule Summary for Servers/Appliances (Grid table) • Pattern File/Rule Summary for Clients (Grid table) • Scan Engine Summary for Servers/Appliances (Grid table) • Scan Engine Summary for Clients (Grid table)
TM-Overall Threat Summary	Provides the following information: • Complete Network Security Risk Analysis Summary (Grid table) • Network Protection Boundary Summary (Grid table) • Security Risk Entry Point Analysis Information (Grid table) • Security Risk Destination Analysis Information (Grid table) • Security Risk Source Analysis Information (Grid table)

Template	Description
TM-Spam Detection Summary	Provides the following information: • Spam Detection Grouped by Day (Line chart) • Recipient Domain Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Top 25 Recipient Domains (Bar chart) • Overall Spam Violation Summary (Grid table) • Top 25 Spam Recipients (Bar chart) • Spam Recipient Summary (Grid table)
TM-Spyware/Grayware Detection Summary	Provides the following information: • Spyware/Grayware Detection Grouped by Day (Line chart) • Unique Spyware/Grayware Count Grouped by Day (Line chart) • Spyware/Grayware Source Count Grouped by Day (Line chart) • Spyware/Grayware Destination Count Grouped by Day (Line chart) • Top 25 Spyware/Grayware (Bar chart) • Overall Spyware/Grayware Summary (Grid table) • Top 25 Spyware/Grayware Sources (Bar chart) • Spyware/Grayware Source Summary (Grid table) • Top 25 Spyware/Grayware Destinations (Bar chart) • Spyware/Grayware Destination Summary (Grid table) • Action Result Summary (Pie Chart) • Spyware/Grayware Action/Result Summary (Grid table)

Template	Description
TM-Suspicious Threat Detection Summary	Provides the following information: • Suspicious Threat Detection Grouped by Day (Line chart) • Rule in Violation Count Grouped by Day (Line chart) • Sender Count Grouped by Day (Line chart) • Recipient Count Grouped by Day (Line chart) • Source IP Address Count Grouped by Day (Line chart) • Destination IP Address Count Grouped by Day (Line chart) • Top 25 Senders (Bar chart) • Top 25 Recipients (Bar chart) • Suspicious Threat Sender Summary (Grid table) • Suspicious Threat Riskiest Recipient Summary (Grid table) • Top 25 Source IP Addresses (Bar chart) • Top 25 Destination IP Addresses (Bar chart) • Suspicious Threat Source Summary (Grid table) • Suspicious Threat Riskiest Destination Summary (Grid table) • Top 25 Protocol Names (Bar chart) • Suspicious Threat Protocol Detection Summary (Grid table) • Overall Suspicious Threat Summary (Grid table)

Template	Description
TM-Virus/Malware Detection Summary	Provides the following information: • Virus/Malware Detection Grouped by Day (Line chart) • Unique Virus/Malware Count Grouped by Day (Line chart) • Infection Destination Count Grouped by Day (Line chart) • Top 25 Virus/Malware (Bar chart) • Overall Virus/Malware Summary (Grid table) • Top 25 Infection Sources (Bar chart) • Virus/Malware Infection Source Summary (Grid table) • Top 25 Infection Destinations (Bar chart) • Virus/Malware Infection Destination Summary (Grid table) • Action Result Summary (Pie chart) • Virus/Malware Action/Result Summary (Grid table)
TM-Web Violation Detection Summary	Provides the following information: • Web Violation Detection Grouped by Day (Line chart) • Policy in Violation Count Grouped by Day (Line chart) • Client in Violation Count Grouped by Day (Line chart) • URL in Violation Count Grouped by Day (Line chart) • Top 25 Policies in Violation (Bar chart) • Overall Web Violation Summary (Grid table) • Top 25 Clients in Violation (Bar chart) • Web Violation Client IP Address Summary (Grid table) • Top 25 URLs in Violation (Bar chart) • Web Violation URL Summary (Grid table) • Filter/Blocking Type Summary (Pie chart)

Understanding Control Manager 3 Templates

Control Manager added 87 pre-generated report templates divided into six categories: Executive Summary, Gateway, Mail Server, Server, Desktop, Network Products, and Data Loss Prevention.

Note

In Control Manager 3.5, spyware/grayware were no longer considered viruses. This change affects the virus count in all original virus-related reports.

It may take a few seconds to generate a report, depending on its contents. As soon as Control Manager finishes generating a report, the screen refreshes and the **View** link adjacent to the report becomes available.

Use the Report Category list on the Control Manager screen to peruse the six categories of reports listed below:

TABLE A-15. Executive Summary Reports and Report Types

EXECUTIVE SUMMARY REPORTS	REPORT TYPES
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/Grayware (10, 25, 50, 100) • Detected Spyware/Grayware list for all entities
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100) • Virus infection list for all entities

Executive Summary Reports	Report Types
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month) • Damage cleanups, grouped by (Day, Week, Month) • Spam, grouped by (Day, Week, Month)
Vulnerability Reports	• Machine risk level assessment • Vulnerability assessment • Most commonly cleaned infections (10, 25, 50, 100) • Worst damage potential vulnerabilities (10, 25, 50, 100) • Vulnerabilities ranked by risk level

Table A-16. Gateway Product Reports and Report Types

Gateway Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Spam, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)

Gateway Product Reports	Report Types
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary • OPS deployment rate for IMSS

Table A-17. Mail Server Product Reports and Report Types

Mail Server Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10, 25, 50, 100)
Virus Detection Reports	• Viruses detected • Top senders of infected email (10, 25, 50, 100) • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary

Table A-18. Server Based Product Reports and Report Types

Server Based Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10, 25, 50, 100)

Server Based Product Reports	Report Types
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10, 25, 50, 100)
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)
Deployment Rate Reports	• Detailed summary • Basic summary • Detailed failure rate summary

Table A-19. Desktop Product Reports and Report Types

Desktop Product Reports	Report Types
Spyware/Grayware Detection Reports	• Spyware/Grayware detected • Most commonly detected Spyware/ Grayware (10,25,50,100)
Virus Detection Reports	• Viruses detected • Most commonly detected viruses (10,25,50,100)
OfficeScan Client Information Reports	• Detailed summary • Basic summary
OfficeScan Product Registration Report	Registration status
Comparative Reports	• Spyware/Grayware, grouped by (Day, Week, Month) • Viruses, grouped by (Day, Week, Month)

Desktop Product Reports	Report Types
OfficeScan Server Deployment Reports	• Detailed summary • Basic summary • Detailed failure rates summary
OfficeScan Damage Cleanup Services Reports	• Detailed summary • Most commonly cleaned infections (10, 25, 50, 100)

Table A-20. Network Product Reports and Report Types

Network Product Reports	Report Types
Network VirusWall Reports	• Policy violation report, grouped by (Day, Week, Month) • Most commonly detected violative clients (10, 25, 50, 100) • Service violation report, grouped by (Day, Week, Month)
Trend Micro Total Discovery Appliance Reports	• Incident summary report, grouped by (Day, Week, Month) • High risk clients (10, 25, 50, 100) • Summary of known and unknown risks report

TABLE A-21. Data Loss Prevention Reports and Report Types

DATA LOSS PREVENTION REPORTS	REPORT TYPES
Top DLP Incident Sources	• Incidents by sender (10, 20, 30, 40, 50) • Incidents by host name (10, 20, 30, 40, 50) • Incidents by recipient (10, 20, 30, 40, 50) • Incidents by source IP address (10, 20, 30, 40, 50) • Incidents by URL (10, 20, 30, 40, 50) • Incidents by User (10, 20, 30, 40, 50) • Top template matches (10, 20, 30, 40, 50) • Incident distribution by channel • Incident trend, grouped by (Day, Week, Month) • Incidents by channel, grouped by (Day, Week, Month)

Data Loss Prevention Reports	Report Types
Significant Incident Increase	• Significant incident increase (%) by channel (10, 20, 30, 40, 50) • Significant incident increase by channel (10, 20, 30, 40, 50) • Significant incident increase (%) by sender (10, 20, 30, 40, 50) • Significant incident increase by sender (10, 20, 30, 40, 50) • Significant incident increase (%) by hostname (10, 20, 30, 40, 50) • Significant incident increase by hostname (10, 20, 30, 40, 50) • Significant incident increase (%) by user (10, 20, 30, 40, 50) • Significant incident increase by user (10, 20, 30, 40, 50) • Significant incident increase (%) by source IP address (10, 20, 30, 40, 50) • Significant incident increase by source IP address (10, 20, 30, 40, 50) • Significant incident increase (%) by template (10, 20, 30, 40, 50) • Significant incident increase by template (10, 20, 30, 40, 50)

Adding One-time Reports

Control Manager supports generating one-time reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a one-time report is similar for all report types and involves the following:

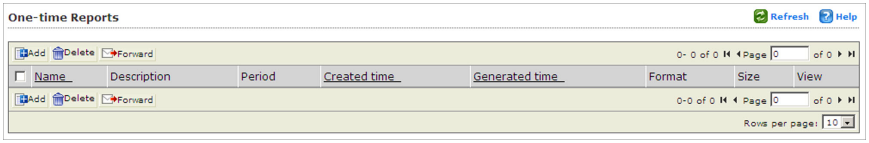
1. Access the **Add One-time Report** screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

Step 1: Access the Add One-time Report Screen and Select the Report Type

Procedure

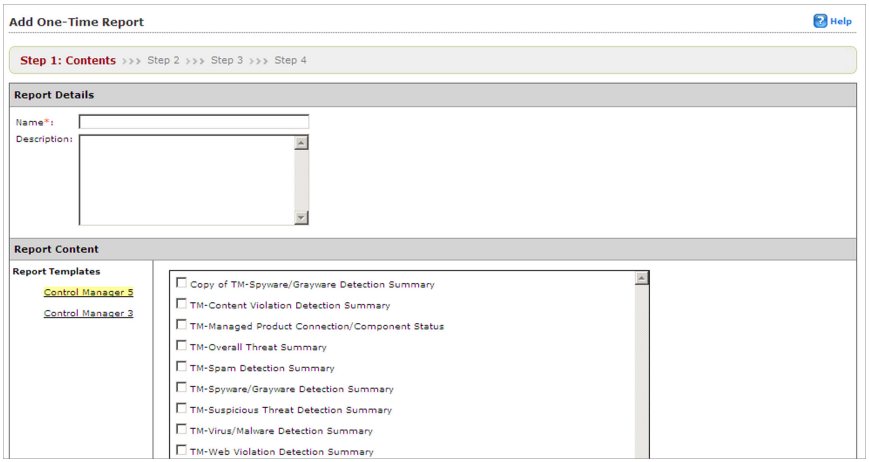
1. Navigate to **Reports** > **One-time Reports**.

The **One-time Reports** screen appears.



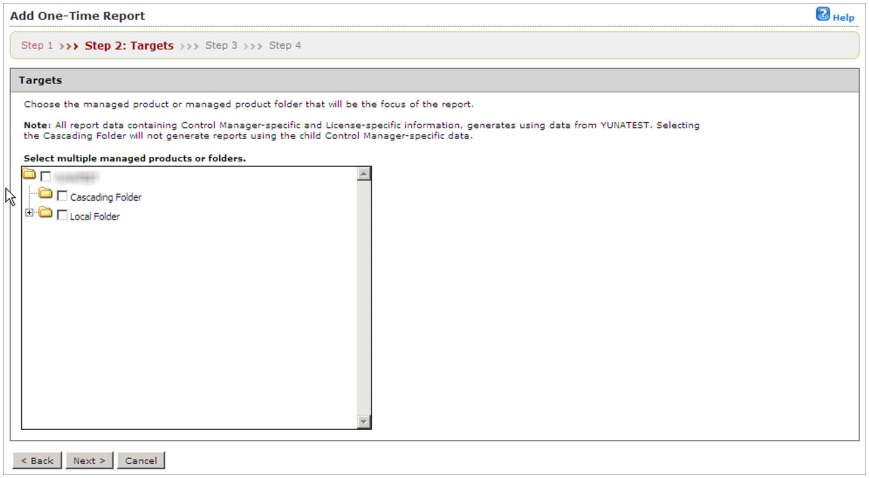
2. Click **Add**.

The **Add One-time Report > Step 1: Contents** screen appears.



3. Type a name for the report in the **Name** field, under Report Details.
4. Type a description for the report in the **Description** field, under Report Details.
5. Select the Control Manager template to generate the report:
   - **Control Manager 5 report template**:
     a. Select the Control Manager 5 template to generate the report. If the existing reports do not fulfill your requirements, create one from the **Report Templates** screen.
   - **Control Manager 3 report template**:
     a. Click **Control Manager 3** under Report Content. The Control Manager 3 templates appear in the work area to the right, under Report Content.
     b. Select the report category on which to base the report.
     c. Select the Control Manager 3 template data on which to base the template.
6. Select the report generation format:
   - **Control Manager 5 report formats**:
     - Adobe PDF Format (*.pdf)
     - HTML Format (*.html)
     - XML Format (*.xml)
     - CSV Format (*.csv)
   - **Control Manager 3 report formats**:
     - Rich Text Format (*.rtf)
     - Adobe PDF Format (*.pdf)
     - ActiveX
     - Crystal Report Format (*.rpt)
7. Click **Next**.

The **Add One-Time Report > Step 2: Targets** screen appears.

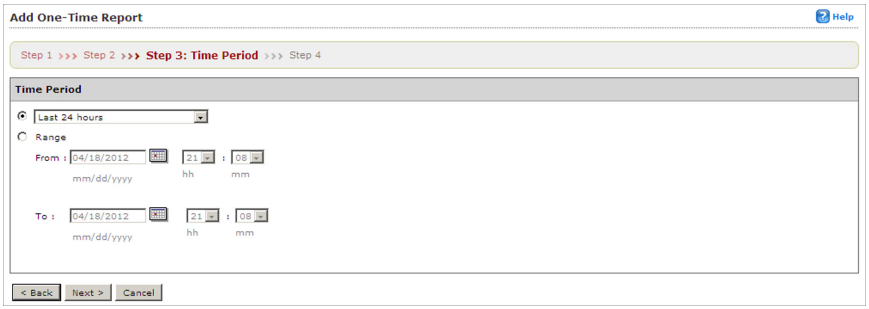


Step 2: Specify the Product/Products From Which the Report Data Generates:

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.
2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   - **All clients**: Reports generate from all Network VirusWall Enforcer devices
   - **IP range**: Reports generate from a specific IP address range
   - **Segment**: Reports generate from a specific network segment
3. Click **Next**.

   The **Add One-Time Report > Step 3: Time Period** screen appears.



Step 3: Specify the Date That the Product/Products Produced the Data:

Procedure

1. Specify the data generation date:
   - From the drop down list select one of the following:
     - All dates
     - Last 24 hours
     - Today
     - Last 7 days
     - Last 14 days
     - Last 30 days
   - Specify a date range:
     - Type a date in the **From** field.
     - Specify a time in the accompanying **hh** and **mm** fields.
     - Type a date in the **To** field.

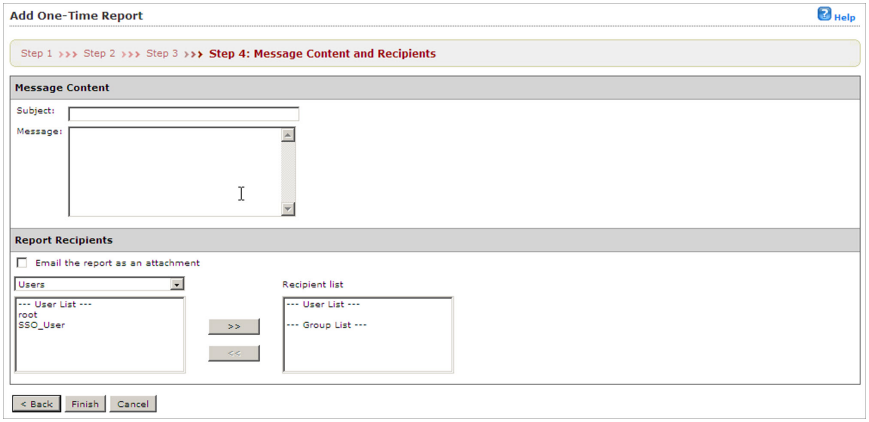
- Specify a time in the accompanying **hh** and **mm** fields.

Note

Click the calendar icon next to the **From** and **To** fields to use a dynamic calendar to specify the date range.

2. Click **Next**.

   The **Add Onetime Report > Step 4: Message Content and Recipients screen** appears.



Step 4: Specify the Recipient of the Report:

Procedure

1. Type a title for the email message that contains the report in the **Subject** field.
2. Type a description about the report in the **Message** field.
3. Select **Email the report as an attachment** to enable sending the report to a specified recipient.
4. Specify to select users or groups from the **Report Recipients** list.

5. Select the users/groups to receive the report and click the **>>** button.

6. Click **Finish** after selecting all users/groups to receive the report.

Adding Scheduled Reports

Control Manager supports generating scheduled reports from Control Manager 3 and Control Manager 5 report templates. Users need to create Control Manager 5 report templates, while Trend Micro created Control Manager 3 report templates. The process for creating a scheduled report is similar for all report types:

1. Access the **Add Scheduled Report** screen and select the report type.
2. Specify the product/products from which the report data generates.
3. Specify the date when the product/products produced the data.
4. Specify the recipient of the report.

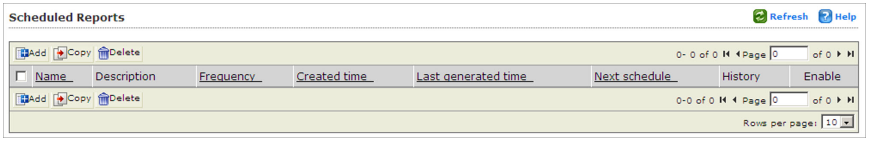
Step 1: Access the Add Scheduled Report Screen and Select the Report Type

---

Procedure

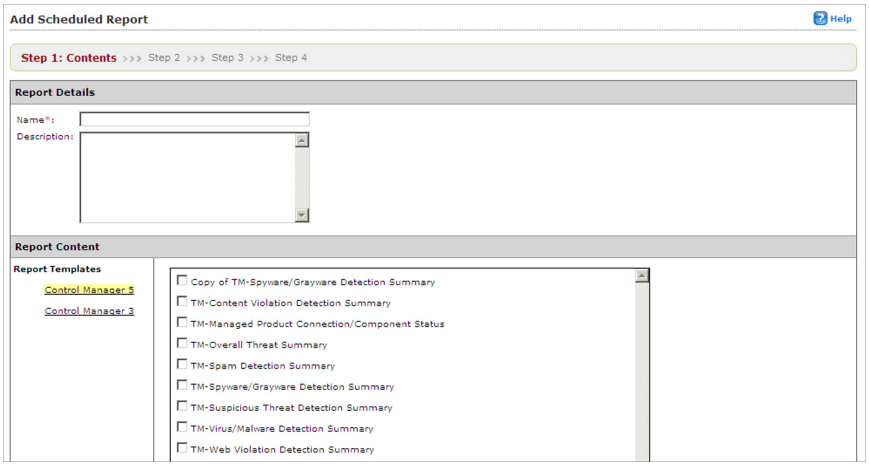
1. Navigate to **Reports** > **Scheduled Reports**.

   The **Scheduled Reports** screen appears.



2. Click **Add**.

   The **Add Scheduled Report > Step 1: Contents** screen appears.



3. Type a name for the report in the **Name** field.

4. Type a meaningful description for the report in the **Description** field.

5. Select the Control Manager template to generate the report:

   - Control Manager 5 report template:

     a. Select the Control Manager 5 template to generate the report. If the existing reports do not fulfill your requirements, create one from the Report Templates screen.

   - Control Manager 3 report template:

     a. Click **Control Manager 3** under Report Content. The Control Manager 3 templates appear in the work area to the right, under Report Content.

     b. Select the report category on which to base the report.

     c. Select the Control Manager 3 template data on which to base the template.

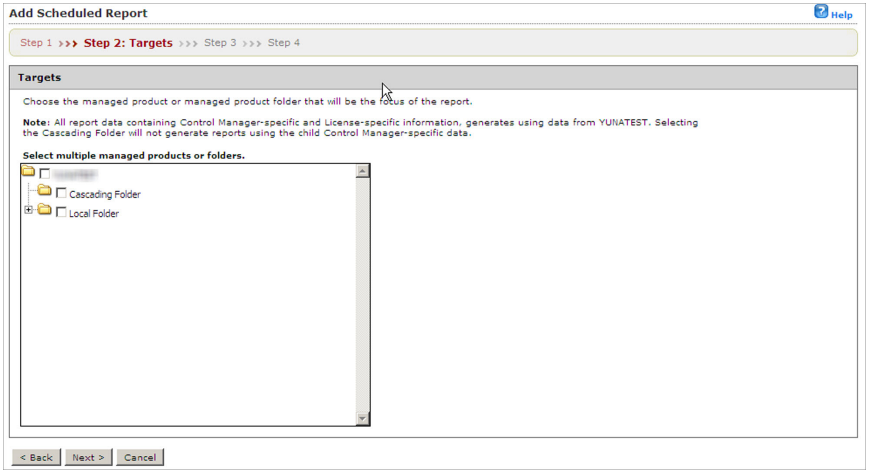
6. Select the report generation format:

   - Control Manager 5 report formats:

    - Adobe PDF Format (*.pdf)
    - HTML Format (*.html)
    - XML Format (*.xml)
    - CSV Format (*.csv)
- Control Manager 3 report formats:
    - Rich Text Format (*.rtf)
    - Adobe PDF Format (*.pdf)
    - ActiveX
    - Crystal Report Format (*.rpt)

7. Click **Next**.

   The **Add Scheduled Report > Step 2: Targets** screen appears.

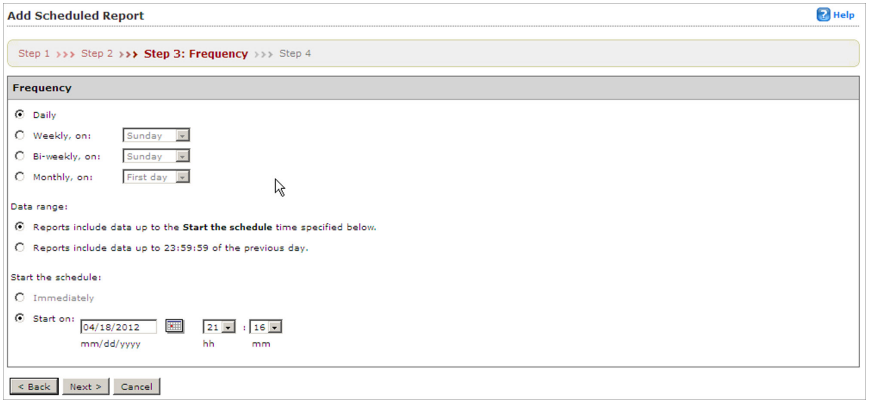


Step 2: Specify the Product/Products from Which the Report Data Generates

Procedure

1. Select the managed product or directory from which Control Manager gathers the report information.
2. If the report contains data from a Network VirusWall Enforcer device, specify the clients from which the reports generate:
   - **All clients**: Reports generate from all Network VirusWall Enforcer devices
   - **IP range**: Reports generate from a specific IP address range
   - **Segment**: Reports generate from a specific network segment
3. Click **Next**.

   The **Add One-Time Report > Step 3: Frequency** screen appears.



Step 3: Specify the Date that the Product/Products Produced the Data

Procedure

1. Specify how often reports generate:
   - **Daily**: Reports generate daily.
   - **Weekly**: Reports generate weekly on the specified day.
   - **Bi-weekly**: Reports generate every two weeks on the specified day.
   - **Monthly**: Reports generate monthly on the first day of the month, the 15th of the month, or the last day of the month.
2. Specify the data range:
   - **Reports include data up to the Start the schedule time specified below**: This means that a report could have up to 23 hours more data contained in the report. While this has a small affect on weekly or monthly reports, this can make a "daily" report with almost two days worth of data depending on the Start schedule time.
   - **Reports include data up to 23:59:59 of the previous day**: This means that data collection for the report stops just before midnight. Reports will be an exact time period (example: Daily reports will be 24 hours) but will not contain the absolute latest data.
3. Specify when the report schedule starts:
   - **Immediately**: The report schedule starts immediately after enabling the report.
   - **Start on**: The report schedule starts on the date and time specified in the accompanying fields.

   a. Type a date in the **mm/dd/yyyy** field.

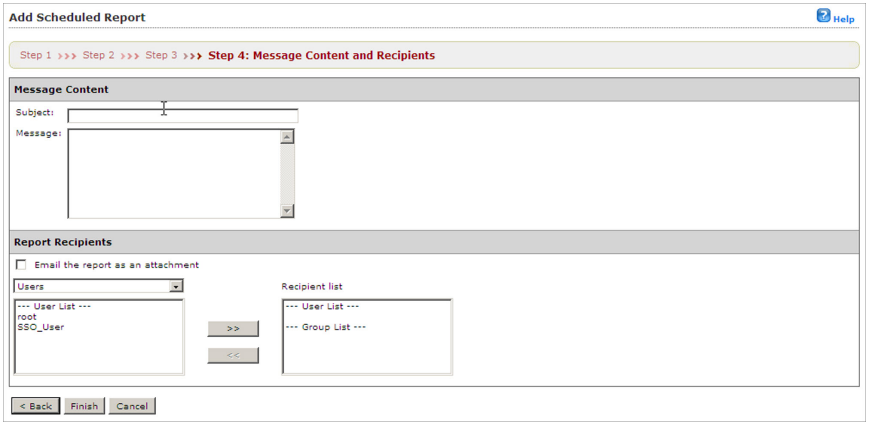
   b. Specify a time in the accompanying **hh** and **mm** fields.

Note

Click the calendar icon next to the **mm/dd/yyyy** field to use a dynamic calendar to specify the date range.

4. Click **Next**.

   The **Add Scheduled Report > Step 4: Message Content and Recipients** screen appears.



Step 4: Specify the Recipient of the Report

Procedure

1. Type a title for the email message that contains the report in the **Subject** field.
2. Type a description about the report in the **Message** field.
3. Select **Email the report as an attachment** to enable sending the report to a specified recipient.
4. Specify to select users or groups from the **Report Recipients** list.
5. Select the users/groups to receive the report and click the **>>** button.

6. Click **Finish** after selecting all users/groups to receive the report.

Appendix B

ScanMail Windows Event Log Codes

Event Identifications for notifications written into Windows event logs may impact the monitoring of ScanMail. Consult the following table to understand the Windows event logs.

TABLE B-1. ScanMail Windows Event Log Codes

EVENT ID	FACILITY	TYPE / SEVERITY	CATEGORY	DESCRIPTION
3	Application	Error	None	Alert. ScanMail service did not start successfully.
4	Application	Error	None	Alert. ScanMail service is unavailable.
5	Application	Warning	None	Security risk scan notification.
6	Application	Warning	None	Attachment blocking notification.
7	Application	Warning	None	Content filtering notification.
16	Application	Warning	None	Alert. Manual update unsuccessful.
17	Application	Information	None	Alert. Manual update successful.
18	Application	Warning	None	Alert. Last update time is older than specified time.

Event ID	Facility	Type / Severity	Category	Description
19	Application	Information	None	Alert. Manual scan successful.
20	Application	Error	None	Alert. Manual scan unsuccessful.
21	Application	Warning	None	Alert. Scan time exceeds specified time.
22	Application	Warning	None	Alert. The disk space on the local drive (volume) of the backup or quarantine directory is less than specified size.
23	Application	Warning	None	Alert. The size of database to keep quarantine and logs exceeds specified size.
24	Application	Information	None	Alert. Scheduled scan successful.
25	Application	Error	None	Alert. Scheduled scan unsuccessful.
32	Application	Error	None	Alert. Scheduled update unsuccessful.
33	Application	Information	None	Alert. Scheduled update successful.
34	Application	Warning	None	Web reputation notification.
35	Application	Warning	None	Data Loss Prevention notification
80	Application	Information	None	Alert. Outbreak Prevention Mode started.
82	Application	Information	None	Alert. Outbreak Prevention Mode stopped and configuration restored.
257	Application	Warning	None	Virus/Malware Outbreak Alert.
258	Application	Warning	None	Uncleanable Virus/Malware Outbreak Alert.
259	Application	Warning	None	Blocked attachment Outbreak Alert.
260	Application	Warning	None	Spyware/Grayware Outbreak Alert.

Event ID	Facility	Type / Severity	Category	Description
513	Application	Error	None	Filter loading exception.
514	Application	Error	None	Adapter loading exception.
4097	Application	Warning	None	Alert. The disk space on the local drive of the MS Exchange transaction log is less than specified size.
4098	Application	Warning	None	Alert. The Microsoft Exchange mail store size exceeds specified size.
4099	Application	Warning	None	Alert. The Microsoft Exchange SMTP messages queued continuously exceeds the specified number.
4112	Application	Error	None	ScanMail Master Service stopped due to insufficient disk space. Please free up some disk space and restart ScanMail Master Service.
8193	Application	Information	None	EUQ. Processing manual End User Quarantine maintenance task started.
8194	Application	Information	None	EUQ. Processing of manual End User Quarantine maintenance task ended.
8195	Application	Information	None	EUQ. Processing of schedule End User Quarantine maintenance task started.
8196	Application	Information	None	EUQ. End of processing schedule End User Quarantine maintenance task.
8197	Application	Information	None	EUQ. Start to process enable End User Quarantine task.
8198	Application	Information	None	EUQ. End of processing enable End User Quarantine task.

Event ID	Facility	Type / Severity	Category	Description
8199	Application	Information	None	EUQ. Start to process disable End User Quarantine task.
8200	Application	Information	None	EUQ. End of processing disable End User Quarantine task.
12289	Application	Error	None	"The transport scan module was unable to load the ScanMail transport hook. This could be caused by improper COM registration, missing DLL files, or privilege issues with the hookSMTP.dll. Check if the required files are complete, manually register hookSMTP.dll, and restart ScanMail Master Service."
12290	Application	Error	None	The ScanMail transport scan module is unable to send IPC requests to the ScanMail Master service. Check Windows event log for system errors.
12291	Application	Error	None	The transport scan module is unable to detect ScanMail or it does not have proper permission to access ScanMail related files or registries. ScanMail Master Service has not started. Please restart ScanMail Master Service.
12292	Application	Error	None	Another transport scan module may be active. Please check if a transport scan module has already been loaded by the Exchange transport service. Another transport scan module is running.
12293	Application	Error	None	The ScanMail transport scan module is unable to create a transport agent object. Make sure the ScanMail DLL files are complete.

Event ID	Facility	Type / Severity	Category	Description
12294	Application	Warning	None	"Transport scan has been disabled and messages have been passed through without being scanned by ScanMail. To enable transport scanning, log on to the ScanMail Management Console and enable any of the following transport level real-time security risk scan, transport level attachment blocking, transport level content filtering, or spam prevention."
12545	Application	Error	None	The MCP agent between ScanMail and Control manager stopped unexpectedly.
20480	Application	Information	None	Log on/off ScanMail product console.
20481	Application	Information	None	ScanMail configuration change.
20482	Application	Information	None	ScanMail management operation.
28672	Application	Information	None	Switch security risk scan methods
28673	Application	Warning	None	Smart Scan - Each time File Reputation service was Unavailable.
28675	Application	Information	None	Smart Scan - Each time File Reputation service was Recovered.
28676	Application	Warning	None	Smart Scan - Each time Web Reputation service was Unavailable.
28677	Application	Information	None	Smart Scan - Each time Web Reputation service was Recovered.
28678	Application	Information	None	Search & Destroy - Each time a search was successful
28679	Application	Error	None	Search & Destroy - Each time a search was unsuccessful

Event ID	Facility	Type / Severity	Category	Description
28681	Application	Warning	None	Virtual Analyzer - Each time the Virtual Analyzer was unavailable
28682	Application	Information	None	Virtual Analyzer - Each time the Virtual Analyzer was recovered

Appendix C

Database Schema for 64-bit Operating Systems

This chapter includes database schema for 64-bit operating systems.

Topics include:

- *Log Database Schema on page C-2*
- *Log View Database Schema on page C-17*
- *Report Database Schema on page C-30*

Log Database Schema

The following table stores message information such as the sender, recipient, and message subject.

TABLE C-1. Table [tblMsgEntries]

FIELD NAME	DATA TYPE	DESCRIPTION
msg_entry_id	Auto increment	Primary key
msg_task_id	int	The scan task this message belongs to
msg_protocol	int	The protocol this message is sent with
msg_found_at	nvarchar(255)	The place where this message was found
msg_source	nvarchar(255)	The semi-colon delimited sender list
msg_destination	nvarchar(255)	The semi-colon delimited recipient list
msg_subject	nvarchar(255)	The subject of this message
msg_delivery_time	datetime	The message delivery time
msg_submit_time	datetime	The message submit time

The following table stores scan logs that include two types of information. The first type includes information about detected security risks such as the security risk name and the name of the file that was infected. The second type includes information about the filter that detected the security risk.

TABLE C-2. Table [tblFilterEntries]

FIELD NAME	DATA TYPE	DESCRIPTION
filter_entry_id	Auto increment	Primary key
msg_entry_id	int	The foreign key for tblMsgEntries
filter_id	smallint	The id of the filter triggered

FIELD NAME	DATA TYPE	DESCRIPTION
filter_rule	nvarchar(64)	The filter rule triggered. Virus/malware name for security risk filter, rule name for content filter, file type blocked by attachment blocking filter (such as.exe), risk level of a malicious URL detected by Web Reputation filter
filter_rule_supplement	int	The virus/malware type for security risk filter, risk level of a malicious URL for Web Reputation filter
filter_engine	nvarchar(32)	The engine version used
filter_pattern	int	The pattern version used
filter_action	int	The result of the action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\ web\xml. **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
filter_scan_time	datetime	The scan time
filter_original	nvarchar(255)	The original file name that triggered the rule
filter_reason	ntext	Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter.
sent_to_csm	smallint	(internal use)

Field Name	Data Type	Description
detected_by	int	The scan mechanism that detected the security risk Possible values: • 1 - Virus Scan Engine • 2 - ATSE • 3 - Virtual Analyzer
risk_level	int	The determined risk level for an advanced threat Possible values: • 0 - Suspicious (ATSE) • 1 - Low • 2 - Medium • 3 - High • 4 - Suspicious (Virtual Analyzer)
url_category	text	The category of the detected URL
atse_aggressive_level	int	ATSE scan level
detected_rule_category	int	ATSE detected rule category
DataContent	longtext	Matched content

The following table stores information about when the quarantine, archive, or backup action was performed.

Table C-3. Table [tblStorageEntries]

Field Name	Data Type	Description
storage_entry_id	Auto increment	Primary key
msg_entry_id	int	The foreign key for tblMsgEntries

FIELD NAME	DATA TYPE	DESCRIPTION
msg_destination_full	ntext	The full recipient list in XML format
filter_scan_time	datetime	The scan time
filter_entry_id	int	The foreign key for tblFilterEntries
filter_id	smallint	Filter ID
filter_action	int	The result of the action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\ web\xml. **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
filter_rule	nvarchar(64)	The filter rule triggered. Virus/malware name for security risk filter, rule name for content filter, file type blocked by attachment blocking filter(such as .exe), risk level of a malicious URL for Web Reputation filter.
file_original	nvarchar(255)	The original file name of this storage
storage_guid	uniqueidentifier	The GUID of this storage entry. (Used by AMF)
storage_reason	smallint	The reason (quarantine, archive, or backup) to make this storage entry.
storage_path	nvarchar(255)	The path the file saved to
storage_type	smallint	The storage type (message part or entire message)
storage_resend_count	smallint	The count of this entity has been resent
sent_to_csm	smallint	(internal use)

The following table stores event log information. For example, information about the start, progress, and completion of manual update.

TABLE C-4. Table [tblActivityEntries]

FIELD NAME	DATA TYPE	DESCRIPTION
activity_entry_id	Auto increment	Primary key
activity_severity	int	The severity of this activity entry
activity_id	int	The id of this activity entry. Ref [dbconf_log.xml]
activity_time	datetime	The date and time of this activity entry began
activity_description	ntext	Activity description
activity_parameter	ntext	To indicate manual/scheduled update component type: pattern/engine/anti-spam rule
activity_duration_mark	smallint	To indicate this activity duration is either begin, end, or instant.
sent_to_csm	smallint	(internal use)

The following table stores information about the engine and patterns that are used to scan email messages.

TABLE C-5. Table [tblPatternEngineInfo]

FIELD NAME	DATA TYPE	DESCRIPTION
pei_type	int	The type of the pattern/engine.
pei_current_version	ntext	The current version of pattern/engine.
pei_latest_version	ntext	The latest version of pattern/engine.
pei_last_query_time	datetime	The last query time of pattern/engine.
pei_last_update_time	datetime	The last update time of pattern/engine.
pei_last_successful_update_time	datetime	The last successful update time of pattern/engine.

Field Name	Data Type	Description
pei_last_update_status	int	The last update status of pattern/engine.
pei_last_update_status_description	ntext	The last update status description of pattern/engine.

The following table stores the scan summary information of detected security risks for today.

Table C-6. Table [tblScanningSummary]

Field Name	Data Type	Description
ss_id	Auto increment	Primary key
ss_type	int	The type of malicious code (such as virus, spam, blocked attachment) Possible values of the ss_type, reference Note5 of this document.
ss_time	datetime	The scanning time
ss_count	int	The count of each type of scanned object

The following table stores the summary information of Search & Destroy mailbox searches.

Table C-7. Table [tblSearchResultMessages]

Field Name	Data Type	Description
srm_id	Auto increment	Primary key
srm_task_name	text	Task name
srm_msg_id	longtext	Message id
srm_msg_pr_search_key	text	Message primary search key
srm_orig_mbx	longtext	Original mailbox
srm_orig_folder	longtext	Original folder

Field Name	Data Type	Description
srm_msg_subject	text	Message subject
srm_msg_recipient	text	Message recipient
srm_msg_sender	text	Message sender
srm_msg_date	datetime	Message date
srm_msg_body	longtext	Message body

The following table stores the configuration replication server list. Perform configuration replication from the Server Management console or Control Manager.

Table C-8. Table [tblCfgReplication]

Field Name	Data Type	Description
cr_session_guid	uniqueidentifier	The session GUID
cr_time	datetime	The start time
cr_server_list	ntext	The server list
cr_selection_list	ntext	The selection list
cr_id	int	(Not in use)

The following table stores the configuration replication status.

Table C-9. Table [tblCfgReplicationStatus]

Field Name	Data Type	Description
crs_id	Auto increment	Primary key
crs_session_guid	uniqueidentifier	The session GUID
crs_start_time	datetime	The start time of configuration replication
crs_end_time	datetime	The end time of configuration replication
crs_server	ntext	The server name which did the configuration replication

FIELD NAME	DATA TYPE	DESCRIPTION
crs_status	int	The status of the configuration replication
crs_description	ntext	The description of the configuration replication

Note

For Event Tracking log query System Center Operations Manager (SCOM) will not get the data directly from ScanMail, but the same information can be queried from the ScanMail database.

The following table stores all event tracking logs.

TABLE C-10. Table [tblAuditLog]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
ServerName	nvarchar(255)	The virtual server name
UserName	nvarchar(255)	The user name
EventTime	datetime	The current time of Audit Event
IpAddress	nvarchar(255)	The remote host IP address
EventType	smallint	The event type (Three types: log in/out, configuration, operation)
SourceType	smallint	The source type (Three types: Configuration change through the UI(Value:1), Configuration change through Control Manager(Value: 2), Configuration change through Server Management(Value:3))
LogDescription	nvarchar(255)	The description of log

The following table is not used.

TABLE C-11. Table [tblManagementGroupList]

FIELD NAME	DATA TYPE	DESCRIPTION
mgl_id	Auto increment	Primary key
mgl_group_name	ntext	The group name in the management group list

The following table is not used.

TABLE C-12. Table [tblManagementServerList]

FIELD NAME	DATA TYPE	DESCRIPTION
msl_id	Auto increment	Primary key
msl_server_name	ntext	The server name in the management group list
msl_group_id	int	The group ID to which the server belongs.

The following table is not used.

TABLE C-13. Table [tblManagementGroupMemberList]

FIELD NAME	DATA TYPE	DESCRIPTION
mgml_id	Auto increment	Primary key
mgml_group_id	int	The group ID from table [tblManagementGroupList]
mgml_server_id	int	The server ID from table [tblManagementServerList]

The following table stores the time of the last configuration replication.

TABLE C-14. Table [tblCfgReplicationHistrory]

FIELD NAME	DATA TYPE	DESCRIPTION
crh_id	Auto increment	Primary key
crh_session_guid	uniqueidentifier	The session GUID

Field Name	Data Type	Description
crh_time	datetime	The last time of configuration replication

Example 1: Get event log from table "tblActivityEntries"

To query Manual update event between '2008-12-12 09:00:00' AND '2008-12-19 09:00:00':

```
SELECT activity_time, activity_description
FROM tblActivityEntries
WHERE activity_id = 15
AND (activity_time
BETWEEN '2008-12-12 09:00:00' AND '2008-12-19 09:00:00')
AND (activity_description LIKE 'Manual update%' )
ORDER BY activity_time
```

The following table lists the items to note for this example.

Table C-15. Possible Values of the activity_id

Variable	Value	Description
ID_CMD_ENGINE_PATTERN_UPDATE	1	The engine pattern update command
ID_CMD_MANUAL_SCAN	3	The manual scan command
ID_CMD_SCHEDULE_SCAN	4	The schedule scan command
ID_CMD_CFG_DEPLOYMENT	5	The configuration deployment command
ID_CMD_CFG_QUERY_PATTERN_ENGINE_VERSION	6	The query the pattern engine version command
ID_CMD_QM_RESEND	7	The quarantine manager resend message command
ID_CMD_EUQ_CLEAN_SPAM_MSG	8	The End User Quarantine (EUQ) clean spam message command

Variable	Value	Description
ID_CMD_EUQ_CREATE_SPAM_FOLDER_RULE	9	The End User Quarantine (EUQ) create spam folder rule command
ID_CMD_LOG_MAINTENANCE	10	The log maintenance command
ID_CMD_EUQ_HOUSE_KEEPING_TASK	11	The EUQ house keeping task command
ID_CMD_EUQ_ENABLE_EUQ	12	The enable End User Quarantine (EUQ) command
ID_CMD_EUQ_DISABLE_EUQ	13	The disable End User Quarantine (EUQ) command
ID_CMD_EUQ_UPDATE_CONFIG	14	The update End User Quarantine (EUQ) configuration command
ID_CMD_UPDATE_COMPONENT	15	The update component command
ID_CMD_QUERY_LATEST_AU_COMPONENT	16	The query latest AU component command
ID_CMD_QUERY_LOCAL_LATEST_AU_COMPONENT	17	The query local latest AU component command
ID_CMD_QM_DELETE	18	The delete quarantine manager message command
ID_CMD_UPDATE_CLUSTER_COMPONENT	19	The update cluster component command

Example 2: Query:Get Quarantine Log(storage_reason=1)

```
SELECT storage_entry_id, filter_scan_time, msg_source,
msg_destination,     msg_subject, filter_id, filter_rule,
file_original,     storage_path as storage_path_quarantine,
storage_resend_count
FROM tblMsgEntries inner join tblStorageEntries
ON tblMsgEntries.msg_entry_id = tblStorageEntries.msg_entry_id
WHERE (storage_reason = 1 )
AND (storage_resend_count
```

```
BETWEEN 0 AND 2)
AND (filter_id IN ('1','4'))
AND (filter_scan_time
BETWEEN '2008-12-12 09:00:00'
AND '2008-12-19 09:00:00')
ORDER BY filter_scan_time
```

Example 3: Get Backup Log(storage_reason=2)

```
SELECT filter_scan_time, msg_source, msg_destination,
msg_subject, filter_rule as filter_rule_av, file_original,
storage_path as storage_path_backup
FROM tblMsgEntries inner join tblStorageEntries
ON tblMsgEntries.msg_entry_id = tblStorageEntries.msg_entry_id
WHERE (storage_reason = 2)
AND (filter_scan_time BETWEEN '2008-12-12 09:00:00'
AND '2008-12-19 09:00:00')
ORDER BY filter_scan_time;
```

Example 4: Get Archive Log(storage_reason=3)

```
SELECT filter_scan_time, msg_source, msg_destination,
msg_subject, filter_rule as filter_rule_cf, file_original,
storage_path as storage_path_archive
FROM tblMsgEntries inner join tblStorageEntries
ON tblMsgEntries.msg_entry_id = tblStorageEntries.msg_entry_id
WHERE (storage_reason = 3)
AND (filter_scan_time BETWEEN '2008-12-12 09:00:00'
AND '2008-12-19 09:00:00')
ORDER BY filter_scan_time;
```

The following table lists the items to note for this example.

TABLE C-16. Possible Values of the storage_reason

VARIABLE	VALUE	DESCRIPTION
SR_QUARANTINE	1	The reason for why this storage entry is quarantine.

Variable	Value	Description
SR_BACKUP	2	The reason for why this storage entry is backup.
SR_ARCHIVE	3	The reason for why this storage entry is archive.

The following table lists the items to note for this example.

Table C-17. Possible Values of the filter_id

Variable	Value	Description
ID_FILTERTYPE_VIRUS_SCANNING	1(0x1)	The filter type of security risk scan
ID_FILTERTYPE_EMANAGER_5X	2(0x2)	The filter type emanager_5X
ID_FILTERTYPE_FILE_BLOCKING	4(0x4)	The filter type of file blocking
ID_FILTERTYPE_ANTISPAM	8(0x8)	The filter type of spam prevention
ID_FILTERTYPE_SIZE_CHECKER	16(0x10)	The filter type of size check
ID_FILTERTYPE_ACTIVE_MESSAGE_FILTER	32(0x20)	Active message filter
ID_FILTERTYPE_UNSCANNABLE_FILTER	64(0x40)	Unscannable filter
ID_FILTERTYPE_URL_FILTER	128(0x80)	URL filter
ID_FILTERTYPE_ANTISPAM_ERS	256(0x100)	Email Reputation spam prevention

Example 5: Get System Event Log about 'Realtime Scan' that occurred between '2008-12-12 09:00:00' AND '2008-12-19 09:00:00'

```
SELECT UserName, IpAddress, EventType, LogDescription,
```

```
SourceType, EventTime
FROM tblAuditLog
WHERE ( EventTime BETWEEN '2008-12-12 09:00:00'
AND '2008-12-19 09:00:00')
AND LogDescription like '%Realtime Scan%'
ORDER BY UserName
```

The following table lists the items to note for this example.

TABLE C-18. Possible Values of the EventType

VARIABLE	VALUE	DESCRIPTION
TYPE_LOG_IN_OUT	1	Log in/out
TYPE_CONFIGURATION	2	Configuration
TYPE_OPERATION_EVENT	3	Operation event

Example 6: Get message information that needs to be resent

```
SELECT msg_subject, msg_source, msg_destination_full,
storage_path, storage_path, file_original, storage_type
FROM tblMsgEntries inner join tblStorageEntries
ON tblMsgEntries.msg_entry_id = tblStorageEntries.msg_entry_id
WHERE storage_entry_id =1;
```

Example 7: Get Last Configuration Replication

```
SELECT TOP 1 *
FROM tblCfgReplicationHistory
ORDER BY crh_time DESC;
```

Example 8: Get Engine Pattern Information

```
SELECT *
FROM tblPatternEngineInfo;
```

Example 9: Get Scanning Summary Count - Blocked attachment

```
SELECT *
FROM tblScanningSummary
WHERE ss_type = 111;
```

The following table lists the items to note for this example.

TABLE C-19. Possible Values of the ss_type

VARIABLE	VALUE	DESCRIPTION
ST_SCANNED_MESSAGE	100	Scanned message
ST_DETECTED_VIRUS	110	Detected virus
ST_BLOCKED_ATTACHMENT	111	Blocked attachment
ST_DETECTED_SPAM	112	Detected spam.
ST_CONTENT_VIOLATION	113	Content violation
ST_DETECTED_ERS	114	Detected ERS
ST_SUSPICIOUS_URL	115	Malicious URL
ST_UNCLEANABLE_VIRUS	117	Uncleanable virus
ST_SCANNED_ATTACHMENT	118	Scanned attachment
ST_UNKNOWN	119	Unknown type
ST_DETECTED_PHISH	120	Detected phish
ST_DETECTED_SPYWARE	121	Detected spyware
ST_FALSE_POSITIVE	124	False positive
ST_UNSCANNABLE_ENTITY	151	Unscannable entity

Log View Database Schema

The following table combines tblMsgEntries and tblFilterEntries.

TABLE C-20. View [vwMsgFilterEntriesTmp]

FIELD NAME	FROM TABLE	FROM FIELD	DESCRIPTION
msg_entry_id	tblFilterEntries	msg_entry_id	Primary key of the table [tblMsgEntries]
msg_delivery_time	tblMsgEntries	msg_delivery_time	The message delivery time
msg_found_at	tblMsgEntries	msg_found_at	The place where this message is found at
msg_source	tblMsgEntries	msg_source	The semi-colon delimited sender list
msg_destination	tblMsgEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	tblMsgEntries	msg_subject	The subject of this message
filter_id	tblFilterEntries	filter_id	Primary key of the table [tblFilterEntries]
filter_scan_time	tblFilterEntries	filter_scan_time	The scan time
filter_rule	tblFilterEntries	filter_rule	The filter rule triggered. Virus/malware name for security risk filter, rule name for content filter, and file type blocked by attachment blocking filter (such as .exe), risk level of a malicious URL for Web Reputation filter
file_original	tblFilterEntries	file_original	The original file name that triggered the rule
filter_action	tblFilterEntries	filter_action	The result of the action taken

Field Name	From Table	From Field	Description
filter_reason	tblFilterEntries	filter_reason	The detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter
filter_rule_supplement	tblFilterEntries	filter_rule_supplement	The virus/malware type, used to separate virus and spyware
url_category	tblFilterEntries	url_category	The category of the detected URL
DataContent	tblFilterEntries	DataContent	Matched content

The following table combines table tblStorageEntries and view vwMsgFilterEntriesTmp.

Table C-21. View [vwMsgFilterEntries]

Field Name	From Table	From Field	Description
filter_scan_time	vwMsgFilterEntriesTmp	filter_scan_time	The scan time
msg_delivery_time	vwMsgFilterEntriesTmp	msg_delivery_time	The message delivery time
msg_found_at	vwMsgFilterEntriesTmp	msg_found_at	The place where this message is found at
msg_source	vwMsgFilterEntriesTmp	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntriesTmp	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntriesTmp	msg_subject	The subject of this message

Field Name	From Table	From Field	Description
filter_rule	vwMsgFilterEntriesTmp	filter_rule	The filter rule triggered. Virus/malware name for security risk filter, rule name for content filter, and file type blocked by attachment blocking filter (such as .exe), risk level of a malicious URL for Web Reputation filter
filter_reason	vwMsgFilterEntriesTmp	filter_reason	Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter
file_original	vwMsgFilterEntriesTmp	file_original	The original filename that triggered the rule
msg_entry_id	vwMsgFilterEntriesTmp	msg_entry_id	Primary key of the table [tblMsgEntries]
filter_id	vwMsgFilterEntriesTmp	filter_id	Primary key of the table [tblFilterEntries]
filter_action	vwMsgFilterEntriesTmp	filter_action	The result of the action taken
storage_entry_id	tblStorageEntries	storage_entry_id	Primary key of the table [tblStorageEntries]
storage_path	tblStorageEntries	storage_path	The path the file saved to
storage_reason	tblStorageEntries	storage_reason	The reason (quarantine, archive, or backup) to make this storage entry
filter_rule_supplement	vwMsgFilterEntriesTmp	filter_rule_supplement	The virus/malware type, used to separate virus and spyware
url_category	tblFilterEntries	url_category	url_category
DataContent	tblFilterEntries	DataContent	Matched content

The following table combines table tblMsgEntries and tblStorageEntries.

TABLE C-22. View [vwMsgStorageEntries]

FIELD NAME	FROM TABLE	FROM FIELD	DESCRIPTION
storage_entry_id	tblStorageEntries	storage_entry_id	Primary key of the table [tblStorageEntries]
msg_source	tblMsgEntries	msg_source	The semi-colon delimited sender list
msg_destination	tblMsgEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	tblMsgEntries	msg_subject	The subject of this message
filter_id	tblStorageEntries	filter_id	Primary key of the table [tblFilterEntries]
filter_scan_time	tblStorageEntries	filter_scan_time	The scan time
filter_rule	tblStorageEntries	filter_rule	The filter rule triggered. Virus/malware name for security risk filter, rule name for content filter, and file type blocked by attachment blocking filter (such as .exe), risk level of a malicious URL for Web Reputation filter
file_original	tblStorageEntries	file_original	The original filename that triggered the rule
filter_action	tblStorageEntries	filter_action	The result of the action taken
storage_reason	tblStorageEntries	storage_reason	The reason (quarantine, archive, or backup) for this storage entry
storage_resend_count	tblStorageEntries	storage_resend_count	The count of this entry has been resent

The following table selects blocked attachments data from view vwMsgFilterEntries.

TABLE C-23. View [vwABLogs]

FIELD NAME	FROM TABLE	FROM FIELD	DESCRIPTION
storage_entry_id	vwMsgFilterEntries	storage_entry_id	Primary key of the table [tblStorageEntries]
filter_scan_time	vwMsgFilterEntries	filter_scan_time	The scan time
msg_delivery_time	vwMsgFilterEntries	msg_delivery_time	The message delivery time
msg_found_at	vwMsgFilterEntries	msg_found_at	The place where this message is found at
msg_source	vwMsgFilterEntries	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntries	msg_subject	The subject of this message
filter_rule_cf	vwMsgFilterEntries	filter_rule	File type blocked by attachment blocking filter (such as .exe)
filter_original	vwMsgFilterEntries	filter_original	The original filename that triggered the rule
filter_action	vwMsgFilterEntries	filter_action	The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\

Field Name	From Table	From Field	Description
filter_id	vwMsgFilterEntries	filter_id	Primary key of the table [tblFilterEntries]

The following table selects security risk scan data from view vwMsgFilterEntries.

Table C-24. View [vwAVLogs]

Field Name	From Table	From Field	Description
storage_entry_id	vwMsgFilterEntries	storage_entry_id	Primary key of the table tblStorageEntries
filter_scan_time	vwMsgFilterEntries	filter_scan_time	The scan time
msg_delivery_time	vwMsgFilterEntries	msg_delivery_time	The message delivery time
msg_found_at	vwMsgFilterEntries	msg_found_at	The place where this message is found at
msg_source	vwMsgFilterEntries	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntries	msg_subject	The subject of this message
filter_rule_av	vwMsgFilterEntries	filter_rule	Virus/malware name
filter_original	vwMsgFilterEntries	filter_original	The original filename that triggered the rule

Field Name	From Table	From Field	Description
filter_action	vwMsgFilterEntries	filter_action	The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml. **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
filter_rule_supplement	vwMsgFilterEntries	filter_rule_supplement	The virus/malware type, used to separate virus and spyware.
filter_id	vwMsgFilterEntries	filter_id	Primary key of the table [tblFilterEntries]
storage_reason	vwMsgFilterEntries	storage_reason	The reason (quarantine, archive, or backup) for this storage entry.

The following table selects content violation data from view vwMsgFilterEntries.

Table C-25. View [vwCFLogs]

Field Name	From Table	From Field	Description
storage_entry_id	vwMsgFilterEntries	storage_entry_id	Primary key of the table tblStorageEntries
filter_scan_time	vwMsgFilterEntries	filter_scan_time	The scan time
msg_delivery_time	vwMsgFilterEntries	msg_delivery_time	The message delivery time
msg_found_at	vwMsgFilterEntries	msg_found_at	The place where this message is found at

Field Name	From Table	From Field	Description
msg_source	vwMsgFilterEntries	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntries	msg_subject	The subject of this message
filter_rule_cf	vwMsgFilterEntries	filter_rule	Rule name for content filter
filter_original	vwMsgFilterEntries	filter_original	The original filename that triggered the rule
filter_action	vwMsgFilterEntries	filter_action	The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml. **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
filter_reason	vwMsgFilterEntries	filter_reason	Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter
filter_id	vwMsgFilterEntries	filter_id	Primary key of the table [tblFilterEntries]

The following table selects Data Loss Prevention incident data from view vwMsgFilterEntries.

TABLE C-26. View [vwDLPLogs]

FIELD NAME	FROM TABLE	FROM FIELD	DESCRIPTION
storage_entry_id	vwMsgFilterEntries	storage_entry_id	Primary key of the table [tblStorageEntries]
filter_scan_time	vwMsgFilterEntries	filter_scan_time	The scan time
msg_delivery_time	vwMsgFilterEntries	msg_delivery_time	The message delivery time
msg_found_at	vwMsgFilterEntries	msg_found_at	The place where this message is found at
msg_source	vwMsgFilterEntries	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntries	msg_subject	The subject of this message
filter_rule_dlp	vwMsgFilterEntries	filter_rule	Rule name for Data Loss Prevention
filter_action	vwMsgFilterEntries	filter_action	The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
file_original	vwMsgFilterEntries	file_original	The original filename that triggered the rule

Field Name	From Table	From Field	Description
filter_template	vwMsgFilterEntries	filter_reason	The triggered Data Loss Prevention template
DataContent	tblFilterEntries	DataContent	Matched content

The following table selects unscannable message data from view vwMsgFilterEntries.

Table C-27. View [vwUSLogs]

Field Name	From Table	From Field	Description
storage_entry_id	vwMsgFilterEntries	storage_entry_id	Primary key of the table tblStorageEntries
filter_scan_time	vwMsgFilterEntries	filter_scan_time	The scan time
msg_delivery_time	vwMsgFilterEntries	msg_delivery_time	The message delivery time
msg_found_at	vwMsgFilterEntries	msg_found_at	The place where this message is found at
msg_source	vwMsgFilterEntries	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntries	msg_subject	The subject of this message
filter_rule_us	vwMsgFilterEntries	filter_rule	Unscannable reason
filter_original	vwMsgFilterEntries	filter_original	The original filename that triggered the rule

Field Name	From Table	From Field	Description
filter_action	vwMsgFilterEntries	filter_action	The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml. **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
filter_id	vwMsgFilterEntries	filter_id	Primary key of the table [tblFilterEntries]
storage_reason	vwMsgFilterEntries	storage_reason	The reason (quarantine, archive, or backup) for this storage entry.

The following table selects storage data from view vwMsgFilterEntries.

Table C-28. View [vwQuarantineLogs]

Field Name	From Table	From Field	Description
storage_entry_id	vwMsgFilterEntries	storage_entry_id	Primary key of the table [tblStorageEntries]
filter_scan_time	vwMsgFilterEntries	filter_scan_time	The scan time
msg_source	vwMsgFilterEntries	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntries	msg_subject	The subject of this message

Field Name	From Table	From Field	Description
filter_rule	vwMsgFilterEntries	filter_rule	The filter rule triggered. Virus/malware name for security risk filter, rule name for content filter, and file type blocked by attachment blocking filter(such as .exe), risk level of a malicious URL for Web Reputation filter
storage_resend_count	vwMsgFilterEntries	storage_resend_count	The count of this entry has been resent
storage_reason	vwMsgFilterEntries	storage_reason	The reason (quarantine, archive, or backup) for this storage entry.

The following table selects data about malicious URL from view vwMsgStorageEntries.

Table C-29. View [vwWTPLogs]

Field Name	From Table	From Field	Description
filter_scan_time	vwMsgFilterEntries	filter_scan_time	The scan time
msg_delivery_time	vwMsgFilterEntries	msg_delivery_time	The message delivery time
msg_source	vwMsgFilterEntries	msg_source	The semi-colon delimited sender list
msg_destination	vwMsgFilterEntries	msg_destination	The semi-colon delimited recipient list
msg_subject	vwMsgFilterEntries	msg_subject	The subject of this message
filter_rule_uf	vwMsgFilterEntries	filter_rule_uf	Risk level of a malicious URL for Web Reputation filter
Suspicious_url	vwMsgFilterEntries	filter_reason	Suspicious URL

Field Name	From Table	From Field	Description
filter_action		filter_action	The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml. **Note** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
filter_id	vwMsgFilterEntries	filter_id	Primary key of the table [tblFilterEntries]
storage_entry_id	vwMsgFilterEntries	storage_entry_id	Primary key of the table [tblStorageEntries]
url_category	tblFilterEntries	url_category	The category of the detected URL

Example 1: Query information about the virus log, content filtering log, or attachment blocking log from tables ‘vwAVLogs’,‘vwCFLogs’, ‘vwABLogs’ between 12/12/2008 09:00:00’ AND ‘12/18/2008 09:00:00’

```
SELECT msg_source,msg_destination,filter_rule_av
FROM vwAVLogs
WHERE filter_scan_time
BETWEEN ‘2008-12-12 09:00:00’ AND ‘2008-12-19 09:00:00’
ORDER BY filter_scan_time;
```

```
SELECT *
FROM vwCFLogs
WHERE filter_scan_time
BETWEEN ‘2008-12-12 09:00:00’ AND ‘2008-12-19 09:00:00’
ORDER BY filter_scan_time;
```

```
SELECT *
FROM vwABLogs
WHERE filter_scan_time
BETWEEN '2008-12-12 09:00:00' AND '2008-12-19 09:00:00'
ORDER BY filter_scan_time;
```

Example 2: Get Storage Log

```
SELECT *
FROM vwMsgStorageEntries
WHERE filter_scan_time
BETWEEN  '2008-12-12 09:00:00' AND '2008-12-19 09:00:00'
ORDER BY filter_scan_time;
```

Report Database Schema

The report database contains nine tables. These tables are not related to each other.

The following table stores the summary detected security risks per hour.

TABLE C-30. Table [tblSummary]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
summary_datetime	datetime	This datetime when this record was summarized
summary_total_message_count	int	The total message scanned count for this period
summary_total_attachment_count	int	The total attachment scanned count for this period.
Summary_virus_detected_count	int	The virus/malware count for this period

Field Name	Data Type	Description
summary_virus_uncleanable_count	int	The uncleanable virus/malware count for this period
summary_attachment_blocked_count	int	The blocked attachment count for this period
summary_content_filtered_count	int	The filtered-count for this period.
summary_dlp_filtered_count	int	The filtered-count for this period
Summary_spam_detected_count	int	The spam message count
summary_phish_detected_count	int	The phish message count
summary_false_positive_count	int	The reported false positive count
Summary_unscannable_entity_count	int	The unscannable count for this period.
Sent_to_csm	smallint	(internal use)
summary_ers_count	int	Blocked IP count for this period
summary_suspicious_url_count	int	The suspicious URL count shown in the report summary
summary_spyware_detected_count	int	The spyware/grayware count for this period
summary_apt_detected_count	int	The ATSE detections for this period

The following table stores blocked attachment information by category.

TABLE C-31. Table [tblAttachmentInfo]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
attachinfo_datetime	datetime	The datetime of summarization
attachinfo_cate_id	int	The category of this counter
attachinfo_value	nvarchar(64)	The value of this counter
attachinfo_count	int	The count of this data category

The following table stores content violation information by category.

TABLE C-32. Table [tblContentInfo]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
contentinfo_datetime	datetime	The datetime of summarization.
contentinfo_cate_id	int	The category of this counter
contentinfo_value	nvarchar(64)	The value of this counter
contentinfo _count	int	The count of this data category.

The following table stores Data Loss Prevention incident information by category.

TABLE C-33. Table [tblDLPInfo]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
dlpinfo_datetime	datetime	The datetime of summarization.
dlpinfo_cate_id	int	The category of this counter
dlpinfo_value	nvarchar(64)	The value of this counter
dlpinfo _count	int	The count of this data category.

The following table stores spam information by category.

TABLE C-34. Table [tblSpamInfo]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
spaminfo_datetime	datetime	The date/time of summarization
spaminfo _cate_id	int	The category of this counter
spaminfo _value	nvarchar(64)	The value of this counter
spaminfo _count	int	The count of this data category.

The following table stores security risk information by category.

TABLE C-35. Table [tblVirusInfo]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
virusinfo_datetime	datetime	The date/time of summarization
virusinfo_cate_id	int	The category of this counter
virusinfo_value	nvarchar(64)	The value of this counter
virusinfo_count	int	The count of this data category.

The following table stores unscannable message information by category.

TABLE C-36. Table [tblUnscannableInfo]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
ucannableifo_datati me	datetime	The datetime of summarization.
ucannableifo_cate_id	int	The category of this counter
ucannableifo_value	nvarchar(64)	The value of this counter
ucannableifo_count	int	The count of this data category.

The following table stores the total number of detected security risks. This table is used by SCOM

TABLE C-37. Table [tblReportCollectionSummary]

FIELD NAME	DATA TYPE	DESCRIPTION
id	Auto increment	Primary key
summary_total_message_count	int	The total message scanned count for this period
summary_total_attachment_count	int	The total attachment scanned count for this period
summary_virus_detected_count	int	The virus/malware count for this period
summary_virus_uncleanable_count	int	The uncleanable virus/malware count for this period
summary_attachment_blocked_count	int	The blocked attachment count for this period
summary_content_filtered_count	int	The filtered-count for this period.
summary_dlp_filtered_count	int	The filtered-count for this period.
summary_spam_detected_count	int	The spam message count
summary_phish_detected_count	int	The phish message count
summary_unscannable_entity_count	int	The unscannable count for this period
summary_worm_trojan_virus_type_count	int	The worm trojan virus type count for this period
summary_packed_file_virus_type_count	int	The packed file virus type count for this period

Field Name	Data Type	Description
summary_generic_virus_type_count	int	The generic virus/malware type count for this period
summary_virus_virus_type_count	int	The virus/malware type count for this period
summary_other_malicious_code_virus_type_count	int	Other malicious code virus type count for this period
summary_additional_threat_virus_type_count	int	The additional threat virus type count for this period
summary_ers_count	int	Blocked IP count for this period
summary_suspicious_url_count	int	The suspicious URL count shown in the report summary
summary_apt_detected_count	int	The ATSE detections for this period

The following table stores malicious URL information by category.

Table C-38. Table [tblURLInfo] (add by WTP)

Field Name	Data Type	Description
id	Auto increment	Primary key
urlinfo_datetime	Date time	Date & Time
urlinfo_cate_id	int	Category ID
urlinfo_value	nvarchar(64)	The name of the report item counter
urlinfo_count	int	The value of the report item counter

Example 1: Get Last Summary Time from table[tblSummary].

```
SELECT MAX(summary_datetime) AS lastest_datetime
FROM tblSummary;
```

Example 2: Get SCOM Report Counter

```
SELECT *
FROM tblReportCollectionSummary.
```

Note

Examples that follow example 2 all query virus information. Query expressions for 'attachment blocking reports', 'content filter reports', 'spam prevention reports', and 'unscannable entity reports' are the same as this example.

Example 3: Get All Virus Count between 12/12/2008 09:00:00' AND '12/19/2008 09:00:00'. (Note: virusinfo_cate_id =151)

```
SELECT virusinfo_value AS virus_name,
Sum(virusinfo_count) AS virus_count
FROM tblVirusInfo
WHERE virusinfo_cate_id = 151
AND virusinfo_datetime >= '2008-12-12 09:00:00'
AND virusinfo_datetime <'2008-12-19 09:00:00'
GROUP BY virusinfo_value;
```

Example 4: Get Virus Summary

```
SELECT Sum(summary_total_message_count) as total_message_count,
Sum(summary_virus_detected_count) as virus_detected_count,
Sum(summary_virus_uncleanable_count)as virus_uncleanable_count
FROM tblSummary
WHERE summary_datetime >= '2008-12-12 09:00:00'
AND summary_datetime < '2008-12-19 09:00:00';
```

Example 5: Get Virus Graph By Week

```
SELECT Min(summary_datetime)as datetime_first,
Sum(summary_total_message_count) as total_message_count,
Sum(summary_virus_detected_count) as virus_detected_count,
Sum(summary_virus_uncleanable_count) as
virus_uncleanable_count, Max(summary_datetime) as
datetime_last, Year(summary_datetime) as datetime_year,
DatePart("ww",summary_datetime) as datetime_week
FROM tblSummary
WHERE summary_datetime  >= '2008-12-12 09:00:00'
AND summary_datetime < '2008-12-19 09:00:00'
GROUP BY Year(summary_datetime), DatePart("ww",
summary_datetime);
```

Example 6: Get Virus Graph By Day

```
SELECT Min(summary_datetime) as datetime_first,
Sum(summary_total_message_count) as total_message_count,
Sum(summary_virus_detected_count) as virus_detected_count,
Sum(summary_virus_uncleanable_count) as
virus_uncleanable_count,     Max(summary_datetime) as
datetime_last,     Year(summary_datetime) as datetime_year,
Month(summary_datetime) as datetime_month,
Day(summary_datetime) as datetime_day
FROM tblSummary
WHERE summary_datetime >='2008-12-12 09:00:00'
AND summary_datetime < '2008-12-19 09:00:00'
GROUP BY Year(summary_datetime), Month(summary_datetime),
Day(summary_datetime);
```

Example 7: Get Top 3 Viruses (Note: virusinfo_cate_id =151)

```
SELECT TOP 3 virusinfo_value AS virus_name,
Sum(virusinfo_count) AS virus_count
FROM tblVirusInfo
WHERE virusinfo_cate_id =151
AND virusinfo_datetime  >='2008-12-12 09:00:00'
AND virusinfo_datetime < '2008-12-19 09:00:00'
```

```
GROUP BY virusinfo_value
ORDER BY Sum(virusinfo_count) DESC;
```

Example 8: Get Viruses Actions (Note: virusinfo_cate_id =153)

```
SELECT virusinfo_value AS virus_action,
Sum(virusinfo_count) AS virus_count
FROM tblVirusInfo
WHERE virusinfo_cate_id =153
AND virusinfo_datetime  >= '2008-12-12 09:00:00'
AND virusinfo_datetime < '2008-12-19 09:00:00'
GROUP BY virusinfo_value
ORDER BY Sum(virusinfo_count) DESC;
```

Example 9: Get Virus Types (Note: virusinfo_cate_id =152)

```
SELECT virusinfo_value AS virus_type,
Sum(virusinfo_count) AS virus_count
FROM tblVirusInfo
WHERE virusinfo_cate_id =152
AND virusinfo_datetime  >= '2008-12-12 09:00:00'
AND virusinfo_datetime < '2008-12-19 09:00:00'
GROUP BY virusinfo_value
ORDER BY Sum(virusinfo_count) DESC;
```

The following table lists the items to note for this example.

TABLE C-39. Possible Values of the virusinfo_cate_id

VARIABLE	VALUE	DESCRIPTION
RPT_CATEID_VS_VIRUS_NAME	151	The count of viruses/malware of a certain virus name.
RPT_CATEID_VS_VIRUS_TYPE	152	The count of viruses/malware of a certain virus type.
RPT_CATEID_VS_ACTION	153	The count of viruses/malware which were taken the same action.

Variable	Value	Description
RPT_CATEID_SPYWARE_NAME	154	The count of spyware of a certain spyware name.
RPT_CATEID_SPYWARE_ACTION	155	The count of spyware which were taken the same action.
RPT_CATEID_VS_SENDER	156	The count of a single sender who sent virus/malware
RPT_CATEID_SPYWARE_SENDER	157	The count of a single sender who sent spyware/grayware
RPT_CATEID_AB_FILETYPE	201	The count of blocked attachment of a certain file type
RPT_CATEID_AB_EXTENSION	202	The count of blocked attachments of a certain extension
RPT_CATEID_AB_FILENAME	203	The count of blocked attachments of a certain filename
RPT_CATEID_CF_SENDER	251	The count for a single sender that triggered the content filtering rules
RPT_CATEID_CF_RECIPIENT	252	The count of content violation of an individual recipient
RPT_CATEID_CF_RULE	253	The count of content violation of a content filtering rule
RPT_CATEID_AS_SPAM_SENDER	301	The count of spam messages from an individual sender
RPT_CATEID_AS_SPAM_DOMAIN	302	The count of spam messages from an individual domain
RPT_CATEID_AS_FALSE_POSITIVE_DOMAIN	303	The count of false positive messages from an individual domain
RPT_CATEID_AS_FALSE_POSITIVE_SENDER	304	The count of false positive messages from an individual sender

Variable	Value	Description
RPT_CATEID_AS_SPAM_CATEGORY	305	The count of spam messages of a single spam category
RPT_CATEID_AS_SPAM_MAILBOX	306	The count of spam message to an individual recipient
RPT_CATEID_UNSCANNABLE_ENTITY	351	The count of unscannable messages
RPT_CATEID_UF_SUSPICIOUS_URL	401	The count of malicious URL
RPT_CATEID_UF_SENDER	402	The count of a single sender who sent email messages that contained a malicious URL

Table C-40. Virus Type

Virus Type String	Virus Type ID
Virus	2
Trojan	4
Spyware	16
Joke	8
Test_Virus	8
Other	8
Packer	16384
Generic	32768

Table C-41. Virus Name String

Virus Name String
Protected file
Over restriction (others)

Virus Name String
Over restriction (mail entity count)
Over restriction (message body size)
Over restriction (attachment size)
Over restriction (decompressed file count)
Over restriction (decompressed file size)
Over restriction (number of layer of compression)
Over restriction (compression ratio)

Appendix D

Best Practices

This chapter provides best practice information.

Topics include:

- *Real-time Scan Settings for Server Roles on page D-2*
- *Attachment Blocking Policies on page D-3*
- *Content Filtering Active Directory Integrated Policies on page D-5*
- *Data Loss Prevention Policies on page D-6*
- *Optimizing Web Reputation on page D-8*
- *Search & Destroy Best Practices on page D-10*
- *Virtual Analyzer - Integration Pre-requisites on page D-19*
- *Internal Domains on page D-20*
- *Recommended Settings on page D-20*

Real-time Scan Settings for Server Roles

The following table lists the recommended real-time scan settings for different server roles.

TABLE D-1. Recommended Scan Settings for Different Server Roles

EXCHANGE ROLE	TRANSPORT LEVEL REAL-TIME SCAN	STORE LEVEL REAL-TIME SCAN
Edge	• Security Risk Scan • Email Reputation • Content Scanning • Web Reputation • (Optional) Attachment Blocking • (Optional) Content Filtering • (Optional) Data Loss Prevention	N/A
Hub	• Security Risk Scan • Attachment Blocking • Content Filtering • Data Loss Prevention • (Optional) Email Reputation • (Optional) Content Scanning • (Optional) Web Reputation	N/A
Mailbox	N/A	• Security Risk Scan • (Optional) Attachment Blocking • (Optional) Content Filtering

Attachment Blocking Policies

The following table lists the recommended attachment blocking settings.

TABLE D-2. 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

Replicate exception rules using the Server Management console.

TABLE D-3. Attachment Blocking Exception Rule Limitations

RESOURCE	LIMITATIONS
Platform	Exceptions are only supported for: • Exchange 2013 • Exchange 2010 RTM or above. • Exchange 2007 with Service Pack 1 or above.
Server roles	• In Edge server, ScanMail cannot obtain sufficient information from Windows Active Directory to implement attachment blocking policies. • Exception rules will not be applied in Store Level real time scan, manual scan, and scheduled scan. • Exception rules only display on the **Summary** screen for transport level real time scan. • On store level scan and edge servers, only the global policy is applied.

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, and .exe files, the user will receive the .doc and .exe files.

Content Filtering Active Directory Integrated Policies

The following table lists the recommended Content Filtering settings.

TABLE D-4. Recommended Content Filtering Settings

SERVER ROLE	SETTING
Edge server	Disable
Transport Level Realtime Scan	Enable
Store Level Realtime Scan	Disable

Content Filtering Policy Replication

Use Server Management to replicate settings between different exchange servers. Only replicate the settings between same server roles.

TABLE D-5. Content Filtering Policy Limitations

RESOURCE	LIMITATIONS
Platform	Policies are only supported for: • Exchange 2013 • Exchange 2010 RTM or above. • Exchange 2007 with Service Pack 1 or above.
Server roles	• Content filtering policies only apply for Transport level real time scan • Store level scan and edge server only apply the global policy.

Data Loss Prevention Policies

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

TABLE D-6. Recommended Data Loss Prevention Settings

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.

Data Identifiers and Template Creation

Data Loss Prevention includes over 100 predefined templates and data identifiers that administrators can use to create Data Loss Prevention policies. These predefined templates and data identifiers should cover the majority of a company's Data Protection needs. Trend Micro recommends using the built-in items when creating policies.

If the predefined items do not meet a company's specific needs, administrators can copy the existing items and modify them accordingly. Select the desired template or data identifier and click **Copy**. Click the newly created item (<DLP Item>_Copy) to edit the content.

Note

Predefined Data Loss Prevention templates and data identifiers cannot be modified or deleted.

Administrators that require completely new expressions can create unique expressions using the web console. ScanMail Data Loss Prevention expressions follow the Perl

Compatible Regular Expression (PCRE) format. Trend Micro recommends testing the user-defined expressions before implementing the new expression in a Data Loss Prevention policy.

Tip

Save the expression only if the testing was successful. An expression that cannot detect any data wastes system resources and may impact performance.

ScanMail allows administrators to import and export Data Loss Prevention templates and data identifiers in DAT files. To edit the contents of a DAT file, import the items back into the ScanMail environment first. Modifying the contents of an exported DAT file can cause data corruption and unusable data.

Data Loss Prevention Policy Replication

When replicating settings between servers using the Server management console, Trend recommends replicating the Data Loss Prevention policy settings between the same server roles.

To maintain the integrity of your Data Loss Prevention policies, ensure that each Exchange server has an identical copy of the current Data Loss Prevention Templates.

Data Loss Prevention: Hidden Keys

You can configure Data Loss Prevention through use of the following hidden keys.

TABLE D-7. Hidden Keys Used in Data Loss Prevention Configuration

NAME	TYPE	DESCRIPTION
EmMaxEntitySize	REG_DWORD	Use this key to customize the bypassing attachment size for Data Loss Prevention scans. The hidden key indicates the file scan threshold in megabytes.

NAME	TYPE	DESCRIPTION
DmcDisableMask	String	Use this key to bypass the scanning of specified file types. By default, Data Loss Prevention scans all files types. The hidden key allows you to choose file types not to scan. This applies to all scan types.

Note

Hidden keys will take effect after you restart the ScanMail main service. See *Starting and Stopping the Services on page 4-14*.

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.

Troubleshooting Web Reputation Performance Issues

If web reputation services is experiencing poor performance, try the following to test your web reputation settings:

- Verify that the network connection is stable.

  ScanMail monitors its connection status to the Smart Protection Network and the Smart Protection Server providing web reputation services. Enable the alert **"Smart Protection Server - Each time Web Reputation service was unavailable/recovered"** to receive notifications whenever ScanMail is unable to connect to the web reputation source. If you frequently receive this alert, it is an indication that your network connection is not very stable.

- Test the speed of one web reputation query

  You can check the web reputation performance log to monitor the speed of the web reputation queries. Add the line `wtp_performance`:1 to the registry key `DebugModule`. The registry key path is as follows:

  HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Exchange \CurrentVersion

  ScanMail will then generate the file wtp_performance.log in the ScanMail debug folder located in <ScanMail install path>\Debug. The default debug folder path is as follows:

  C:\Program Files\Trend Micro\Smex\Debug

  This log will list the time it took to query each URL (in milliseconds).

Note

You do not need to enable the ScanMail debug log to perform this check.

Search & Destroy Best Practices

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

- *Search & Destroy Prerequisites on page D-10*
- *Configuring Search & Destroy in a Multiple Data Center Environment on page D-13*
- *Using Search & Destroy in Mixed Exchange Environments on page D-12*
- *Optimizing Search Criteria on page D-14*
- *Optimizing Mailbox Searches on page D-15*
- *Deleting Mailbox Searches on page D-15*
- *Exchange Management Shell Commands on page D-16*
- *Exchange Server 2013 Throttling Policy Settings on page D-17*

Search & Destroy Prerequisites

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

TABLE D-8. Features

FEATURE	DESCRIPTION
Service account	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: • Ensure that the account is a member of the Exchange discovery management group • Ensure that the account never expires • Ensure that the account is a member of the Exchange Mailbox Import Export role to export search results to a .pst file • Create a mailbox for this account (Exchange 2013 only) For details on Exchange Management Shell Commands related to the service account, see *Service Account Settings on page D-16*.
Discovery mailbox	This mailbox stores the search result messages. ScanMail copies messages from the end users' mailboxes into the discovery mailbox. Configure the discovery mailbox(es) as follows: • Ensure that the discovery management group has full access permission to each discovery mailbox • Assign at least one discovery mailbox to each data center in the organization **Note** Trend Micro recommends that administrators do not place the discovery mailbox in Data Availability Groups (DAG) solutions. The discovery mailbox consumes more database space when used in a DAG solution. For details on Exchange Management Shell Commands related to the discovery mailbox, see *Discovery Mailbox Settings on page D-17*.

FEATURE	DESCRIPTION
Exchange Server 2013 Throttling Policy	Exchange 2013 utilizes a throttling policy to limit the number of concurrent mailbox searches and the number of specified mailboxes each search can search. Administrators must reconfigure the throttling policy to optimize Search & Destroy mailbox searches. For details, see *Exchange Server 2013 Throttling Policy Settings on page D-17*.

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.

Preparing Exchange Server 2013 for Mixed Exchange Environments

Exchange Server 2013 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, configure the mailbox using Exchange Management Shell Commands.

Procedure

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 DB Name"`

   Moves the SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} mailbox to the Exchange Server 2013 mailbox database

3. Execute the command: `Get-MoveRequest`

   Checks the status of the move operation

Note

The move operation may take few minutes to complete.

Configuring Search & Destroy in a Multiple Data Center Environment

Procedure

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 console.

   For details, see *Configuring Search & Destroy Access Accounts on page 13-2*.

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.

For details, see *Activating Search & Destroy on page 13-4*.

6. For each data center, create a search task and only search mailboxes that reside in a single data center.

   For details, see *Mailbox Search Options on page 13-9*.

7. For each search task, select a discovery mailbox that resides at the same level as the target mailboxes.

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 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.xslx", type `attachment:test.xslx`.

    For details on AQS, see http://msdn.microsoft.com/en-us/library/bb266512.aspx.
  - For Exchange 2013, 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.xslx", type `attachment:'test.xslx'`.

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.

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.

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.

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 D-16*
- *Discovery Mailbox Settings on page D-17*
- *Exchange Server 2013 Throttling Policy Settings on page D-17*
- *Backend Search Tasks on page D-18*

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:

TABLE D-9. Service Account Commands

COMMAND	DESCRIPTION
`Add-RoleGroupMember -Identity “Discovery Management” -Member “SERVICE_ACCOUNT_NAME”`	Adds the "SERVICE_ACCOUNT_NAME" account to the Exchange Discovery Management group
`New-ManagementRoleAssignment -Role "mailbox import export" -User “SERVICE_ACCOUNT_NAME”`	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:

TABLE D-10. Discovery Mailbox Commands

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

Exchange Server 2013 Throttling Policy Settings

Exchange 2013 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 2013 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 2013 settings:

TABLE D-11. Throttling Policy Commands

COMMAND	DESCRIPTION
`Get-ThrottlingPolicy |fl *discovery*`	Returns the current policy settings
`New-ThrottlingPolicy -Name [policy_name] -DiscoveryMaxConcurrency 10 -DiscoveryMaxMailboxes 500 -ThrottlingPolicyScope organization`	This command creates the new policy "[policy_name]" and sets the following: • Maximum number of concurrent searches: 10 • Maximum number of specified mailboxes per search: 500

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:

TABLE D-12. Backend Search Commands

EXCHANGE VERSION	COMMAND	DESCRIPTION
Exchange 2010	`Get-mailboxSearch-identity [task_name][server_name]*`	Returns the full search task name and the task status

Exchange Version	Command	Description
Exchange 2013	`get-mailboxsearch |fl name`	Returns the full search task name
	`get-mailboxsearch -identity [task name] |fl`	Returns the task status
Exchange 2010/2013	`remove-mailboxSearch-identity [task_name]`	Removes the mailbox search from the Exchange server and all associated search results from the discovery mailbox

Virtual Analyzer - Integration Pre-requisites

Before enabling Virtual Analyzer integration, administrators must enable the Exchange replay folder.

WARNING!

Disabling the Exchange replay folder after enabling the Virtual Analyzer integration may cause unexpected issues. Trend Micro recommends disabling Virtual Analyzer integration before disabling the Exchange replay folder.

Use the following cmdlet commands to enable the Exchange replay folder using the Exchange Management Shell.

Table D-13. Exchange Management Shell Cmdlet Commands

Cmdlet	Description
`Get-TransportServer | fl replay*`	This cmdlet returns the current replay folder attributes. If the ReplayDirectoryPath attribute is NULL, the Exchange administrator has disabled the replay folder. The Exchange administrator must enable the replay folder using the `Set-TransportServer` command.

CMDLET	DESCRIPTION
`Set-TransportServer -Identity {server name} -ReplayDirectoryPath "E:\Program Files\Microsoft\Exchange Server\TransportRoles\Replay"`	This cmdlet enables the replay folder in the directory specified.

Internal Domains

- The Internal Domain settings synchronize with the accepted domains in Exchange server during ScanMail installation. This information will not update after installation completes. Trend Micro recommends synchronizing the corresponding settings when the Exchange server updates its accepted domain settings.
- ScanMail allows the usage of the asterisk (*) wildcard to specify internal domains. If you want to bypass a domain and its child domains, use the wildcard as a prefix to the parent domain. For example, if you want to bypass smex.com, child1.smex.com, and child2.smex.com, type the following:

  `*.smex.com`

  However, if you want to bypass a domain but still scan its child domains, type the following:

  `smex.com`

Recommended Settings

Although ScanMail is fully configurable, Trend Micro recommends the following settings:

- **Content Scanning**: Set to Quarantine message to user's spam folder.
- **Content Filtering**: Set to Quarantine entire message:

  - Match any or apply to all
  - Match all conditions
  - Match any condition

  Set to Pass for creating an exception for a particular email account.

- **Attachment Blocking**: Set to Pass for suspicious attachments.
- **Security Risk Scan**: Clean
- **Data Loss Prevention**: Set to Quarantine entire message.
- **Other**:
  - Set to Pass for password protected or encrypted message or file.
  - Set to Pass for compressed file over scanning restrictions.

Index

Symbols

"Log on as batch job" policy, A-65

A

access control
    configuring, 13-2, 17-7, 17-8
    enabling, 17-7
    permissions, 17-6
        full, 17-6
        read, 17-6
    role, 17-6
    Search & Destroy administrator, 13-2
actions, 6-10, 6-13–6-21
    attachment blocking, 8-5
    compressed files, 18-9
    Data Loss Prevention, 10-22
    security risk scan, 7-5
    spam prevention
        content scanning, 11-11
    web reputation, 12-6
activating ScanMail
    Activation Code, 2-12
        additional features, 2-14
        suite, 2-13
activating Trend Micro products, 2-11, 2-16
    Activation Code
        standard, 2-13
    reactivating, 2-16
Activation Code, 2-12
    locating, 19-18
    reactivating, 2-16
    standard, 2-13
    suite, 2-13
    suite with additional features, 2-14
ActiveAction, 1-30, 7-5
ActiveUpdate, 1-28, 2-20
    incremental updates, 1-28
advanced threats, 18-3
    actions, 6-10, 6-16
    APT, 18-3
    exploits, 18-3
    targeted attacks, 18-3
    zero-day attacks, 18-3
Advanced Threat Scan Engine, 7-4
    about, 7-4
    actions, 6-10, 6-16
Advanced Threat Scan Engine (ATSE)
    scan engine, 1-25, 7-4
adware, 18-13
alerts, 16-5, 16-6
    notifications, 16-10
    outbreak, 16-9
    system events, 16-5
ATSE, 7-4
    about, 7-4
    actions, 6-10, 6-16
attachment blocking, 8-2
    actions, 6-10, 6-18, 8-5
        configuring, 8-5
    compressed file handling, 6-8
    enabling, 8-3
    exceptions
        add, 8-7
        edit, 8-8
    global policy, 8-7
    logs, 16-15
    notifications
        settings, 8-6

target
configuring, 8-4
automatic deployment settings
Scheduled Download, A-59

C

Command & Control Contact Alert Services, 12-2
categories, 12-3
Global Intelligence list, 12-2
Smart Protection Server, 12-3
Virtual Analyzer, 12-3
Virtual Analyzer list, 12-3
components
downloading, A-39
compressed files, 6-7–6-9, 18-4, 18-9, 19-14
actions, 18-9
compression ratios, 19-14
compression types, 6-8
Denial-of-Service, 6-10
compression types, 18-9
configuring, A-56
access control, 17-7, 17-8
internal domains, 17-11
local sources, 5-7
macro scans, 7-10
managed products, A-24
notifications, 17-2
proxy settings, 2-18, 17-2
quarantine folder/directory, 15-2
real-time scan, 17-5
Scheduled Download
automatic deployment settings, A-59
Scheduled Download Exceptions, A-48
Scheduled Download Settings, A-57
security risk scan
target, 7-6
server groups, 17-9
special groups, 17-8, 17-9
user accounts, A-9
web reputation, 12-3
World Virus Tracking Program, 17-13
contacting
technical support, 21-4
content filtering, 9-2
actions, 6-10, 6-19, 6-20
data leakage prevention, 9-3
enabling, 9-3, 9-14
exceptions, 9-13
global settings, 9-4
keywords, 19-9–19-11
logs, 16-15
policies, 9-4
edit, 9-14
enabling, 9-12
exceptions, 9-13
name and priority, 9-12
selecting accounts, 9-5
specify action, 9-10
specify notification, 9-11
specify target, 9-7
content scanning, 11-6
actions, 11-11
enabling, 11-9
target, 11-9
Control Manager, A-1, A-6
about, A-1
accounts, A-9
agent, A-7
antivirus and content security components, A-39, A-40
basic features, A-3

configuring accounts, A-9
features, A-3
mail server, A-6
managed product, A-15
MCP, A-7
report server, A-6
see Trend Micro Control Manager, 17-13
SQL database, A-6
Trend Micro Management Infrastructure, A-7
web-based management console, A-7
web server, A-6
widget framework, A-8
Control Manager antivirus and content security components
Anti-spam rules, A-39
Engines, A-39
Pattern files/Cleanup templates, A-39
creating
folders, A-36
criteria
customized expressions, 10-4, 10-5
keywords, 10-9, 10-10
customized expressions, 10-3–10-5
criteria, 10-4, 10-5
customized keywords, 10-8
criteria, 10-9, 10-10

D

data identifiers, 10-2
expressions, 10-2
creating, 10-6
importing, 10-7, 10-12
keyword lists
creating, 10-11
keywords, 10-3
data leakage prevention, 9-3
Data Loss Prevention, 10-2
actions, 6-10, 6-20, 10-22
data identifiers, 10-2
best practices, D-6
expressions, 10-6, 10-7, 10-12
keyword lists, 10-11
enabling, 10-18
expressions, 10-3–10-5
global settings, 10-19
hidden keys, D-7
keywords, 10-8–10-10
logs, 16-15
policies, 10-17, 10-19–10-22, 10-24, 10-25
actions, 10-22
creating, 10-19
enabling, 10-25
name and priority, 10-25
notifications, 10-24
selecting accounts, 10-20
targets, 10-21
templates, 10-12, 10-13
best practices, D-6
creating, 10-13
deleting, 10-15
exporting, 10-16
importing, 10-15
data views
understand, A-68
Denial-of-Service, 6-10, 7-8, 18-2
Denial-of-Service attack, 18-3
deployment plans, A-61
dialers, 18-13
Directory Management options, A-34
Directory Manager, A-33
disease vector, 18-16

download components
manually, A-41
downloading and deploying components, A-39

E

EICAR, 19-23
email reputation
actions, 11-5
enabling, 11-4
target, 11-5
email reputation services, 11-3
advanced, 11-4
standard, 11-3
encoding types, 18-15
End User Quarantine, 11-7, 17-4
Enterprise Protection Strategy, 1-31
expressions, 10-2, 10-3
customized, 10-3
criteria, 10-4, 10-5
predefined, 10-3

F

false positive, 19-24
features, A-3
file reputation, 5-3
File Reputation Services, 5-3
files
uncleanable, 1-23
folders
creating, A-36
renaming, A-36
frequently asked questions
backup folders, 19-15, 19-16
calculating decompressed file size, 19-14
central reports, 19-16
checking pattern file updates, 19-2
checking service pack updates, 19-2
compression ratios, 19-14
dangerous files, 19-24
EICAR test virus, 19-23
End User Quarantine spam folder, 19-17
false positives, 19-24
firewall port exceptions, 19-17
handling large files, 19-13
latest patches, 19-2
locating Activation Code, 19-18
locating Registration Key, 19-18
mapped network drives, 19-16
phish attacks, 19-22
public folder scan, 19-3
quarantine folders, 19-15, 19-16
regular expressions, 19-3
remote SQL server password changed, 19-20
sending detected viruses to Trend Micro, 19-25
sending suspected threats to Trend Micro, 19-24
spyware/grayware, 19-21
time settings, 19-16
unable to log on to product console, 19-19
UNC paths, 19-15
using keywords, 19-9–19-11
using operators with keywords, 19-11

G

global policy, 8-7
global settings
quarantine folder/directory, 15-2
grayware, 18-3

H

hacking tools, 18-13
hot fixes, 1-31

I

icons, 4-14
integrated server, 5-5
IntelliScan, 7-6, 7-7
IntelliTrap, 7-6
internal domains, 17-10
    configuring, 17-11

J

joke program, 18-10, 18-13

K

keywords, 10-3, 10-8, 19-9–19-11
    customized, 10-8–10-10
    predefined, 10-8
known issues, 20-3

L

licenses, 17-11
    registering, 2-9
local sources
    configuring, 5-7
    settings, 5-7
    Smart Protection Server, 5-7
logs, 16-15, A-65
    maintenance, 16-18
    querying, 16-17, A-67
    Search & Destroy, 13-21
    types, 16-15
    Windows events, B-1

M

macro scan, 7-10
macro viruses/malware, 18-10
mailbox search
    configuring, 13-13
    criteria
        date, 13-12
        discovery mailbox, 13-12
        keywords, 13-10
        mailbox components, 13-12
        mailboxes, 13-11
        specific senders or recipients, 13-12
    deleting, 13-17
    keywords, 13-6
    modifying, 13-15
    options, 13-9
    results, 13-18
    syntax, 13-6
    types, 13-6
    viewing, 13-18
maintaining security, 3-3
managed products
    configuring, A-24
    issue tasks, A-25
    recovering, A-30
    renaming, A-36
    searching for, A-32
    viewing logs, A-26
managing outbreak situations, 3-4
    analyzing, 3-5
    confirming the outbreak, 3-5
    recovering, 3-6
    responding, 3-5
manually download components, A-41
manual scan, 6-3
    alerts, 16-6
    characteristics, 7-3
    compressed file handling, 6-7–6-9
    settings, 6-5

manual updates, 2-19
mass-mailing attack, 18-11
master services
    ScanMail EUQ Monitor, 4-14
    ScanMail for Exchange Remote Configuration Server, 4-14
    ScanMail for Microsoft Exchange Master Services, 4-14
    ScanMail for Microsoft Exchange System Watcher, 4-14
    starting and stopping, 4-14
MCP, A-7
multipurpose internet mail extensions, 18-15

N

notifications, 6-23–6-26, 17-2
    about, 6-23
    actions that trigger, 17-3
    alerts, 16-10
    configuring, 17-2
    global settings, 17-4
    web reputation, 12-7

O

one-time reports, 16-11, 16-12
    generating, 16-11
online help
    accessing, 2-8
operator, 17-7
outbreak alerts, 16-9
Outbreak Prevention Services, 1-32
    alerts, 16-6

P

password cracking applications, 18-13
patches, 1-31
    updating FAQ, 19-2
pattern files, 1-27, 5-6, 19-2, 20-3
    incremental updates, 1-28
    Smart Scan Agent pattern, 5-7
    Smart Scan pattern, 5-7
    spam pattern files, 11-7
    updates, 2-16
    updating manually, 20-3
    Web Blocking list, 5-7
PCRE, 10-4
Perle Compatible Regular Expressions, 10-4
phish, 18-2, 18-3, 18-16, 19-22
policies
    content filtering, 9-4
    Data Loss Prevention, 10-17
post-installation
    spam folder, 11-2
predefined expressions, 10-3
predefined templates, 10-13
product console, 2-2
    banner, 2-5
    configuration area, 2-8
    getting help, 2-8
    side menu, 2-7
    unable to log on, 19-19
    viewing remote servers, 4-8
    viewing servers, 4-7
    viewing virtual servers, 4-8
Product Directory
    deploying components, A-22
proxy settings, 2-18, 17-2
    configuring, 2-18, 17-2

Q

quarantine
    alerts, 16-6
    configuring, 15-2
    folder/directory, 15-2

global settings, 15-2
queries
maintenance, 15-4, 15-5
performing, 15-3
resending messages, 15-5
quarantine folder/directory, 15-2
alerts, 16-6
quarantine query
maintenance
automatic, 15-4
manual, 15-5
performing, 15-3
resending messages, 15-5
query logs, A-67

R

reactivating Trend Micro products, 2-16
real-time monitor, 4-2
viewing remote servers, 4-4
real-time scan, 6-2, 17-5
characteristics, 7-2
configuring, 17-5
recovering
managed products, A-30
registering
to Control Manager, 17-15, A-8
registering ScanMail
reseller purchase, 2-10
registering Trend Micro products, 2-9
how to, 2-10
online purchase, 2-9
Registration Key, 2-9
Registration Key
locating, 19-18
regular expressions, 19-3
remote access tools, 18-13
remote servers
viewing with real-time monitor, 4-4
renaming
folders, A-36
managed products, A-36
replicating configurations, 4-9
reports, 16-11
generating scheduled, 16-13
maintenance, 16-14
one-time reports, 16-11, 16-12, A-82
scheduled, 16-12
scheduled reports, A-88
templates, A-69
report templates, A-69
resources
creating for virtual servers, 4-10–4-13
creating for Windows 2003, 4-10
creating for Windows 2008, 4-11, 4-12
Exchange 2007 CCR Cluster, 4-12
Exchange 2007 SCC Cluster, 4-11
Exchange 2007 SCR Cluster, 4-13
role
operator, 17-7
roll back, 2-22

S

scan engine, 1-25
ATSE, 1-25, 7-4
hierarchy, 7-3
update manually, 20-2
updates, 2-16
Virtual Analyzer, 1-25, 7-4
VSAPI, 1-24, 7-3
ScanMail EUQ Monitor, 4-14
ScanMail for Exchange Remote Configuration Server, 4-14
ScanMail for Microsoft Exchange Master Services, 4-14

ScanMail for Microsoft Exchange System Watcher, 4-14
ScanMail technology, 1-24
scans, 6-2
about scans, 6-2
actions, 6-10, 6-13–6-21
logs, 16-15
macro scan, 7-10
manual scan, 6-3
manual scan settings, 6-5
on cluster servers, 6-4
real-time scan, 6-2
scheduled scan, 6-4
scheduled scan settings, 6-5
schedule bar, A-12
Scheduled Download
configuring
automatic deployment settings, A-59
Scheduled Download Exceptions
configuring, A-48
Scheduled Download Frequency
configuring, A-56
Scheduled Downloads, A-49
Scheduled Download Schedule
configuring, A-56
Scheduled Download Schedule and Frequency, A-56
Scheduled Download Settings
configuring settings, A-57
scheduled scan, 6-4
alerts, 16-6
characteristics, 7-3
compressed file handling, 6-7–6-9
settings, 6-5
scheduled updates, 2-19
Search & Destroy
about, 13-2
access account, 13-2
configuring, 13-2
activating, 13-4
discovery mailbox, 13-4, 13-20
event logs, 13-21
mailbox search, 13-6
configuring, 13-13
deleting, 13-17
keywords, 13-6
modifying, 13-15
options, 13-9
syntax, 13-6
types, 13-6
viewing, 13-18
service account, 13-4, 13-20
settings, 13-20
troubleshooting, 13-22
Search & Destroy administrator, 13-2
searching
managed products, A-32
security baseline, 3-2
managing real-time monitor, 3-2
performing a manual scan, 3-2
update ScanMail, 3-2
security information site, 21-4
security risks, 18-2
advanced threats, 18-3
compressed files, 18-4
Denial-of-Service, 18-2
Denial-of-Service attack, 18-3
disease vector, 18-16
encoding types, 18-15
grayware, 18-3
joke program, 18-10

macro viruses/malware, 18-10
mass-mailing attack, 18-11
multipurpose internet mail extensions, 18-15
other malicious codes, 18-4
packed files, 18-4
phish, 18-2, 18-3, 18-16
spyware, 18-3
spyware/grayware, 18-2, 18-13
Trojan Horse, 18-4, 18-11
true file type, 18-16
virus/malware writers, 18-6
viruses/malware, 18-4
worms, 18-4, 18-12
zip-of-death, 18-12
security risk scan
about, 7-2
actions, 6-13, 7-5
settings, 7-8
ActiveAction, 7-5
compressed file handling, 6-7, 6-9
configuring target settings, 7-6
custom settings, 7-5
enabling real-time scan, 7-6
IntelliScan, 7-6, 7-7
IntelliTrap, 7-6
logs, 16-15
notifications
settings, 7-12
summary screen, 16-4
server groups, 17-9
configuring, 17-9
server management console, 4-4
activating, 4-4
replicating configurations, 4-9
replicating servers, 4-6
view last replication, 4-6
view pattern and engine version, 4-5
view scan results, 4-5
view scan status, 4-5
view smart scan status, 4-6
Server Management Console
about, 4-4
service packs, 1-31, 19-2
services
starting and stopping, 4-14
smart protection, 5-2, 5-3, 5-5, 5-6
File Reputation Services, 5-3
Smart Protection Network, 5-5
source, 5-5, 5-6
sources
comparison, 5-5
protocols, 5-6
volume of threats, 5-2
Smart Protection, 5-3
File Reputation Services, 5-3
integrated server, 5-5
pattern files, 5-6
Smart Protection Server, 5-5
standalone server, 5-5
Web Reputation Services, 5-3
Smart Protection Network, 5-5, 12-4
web reputation, 12-4
Smart Protection Server, 5-5, 5-8, 5-9, 12-4
alerts, 16-5
integrated server, 5-5
security risk scan
alerts, 16-5
standalone, 5-5
web reputation, 5-8, 5-9, 12-4, 16-6
Smart Protection sources
integrated server, 5-5

local source settings, 5-7
Smart Protection Server, 5-5
standalone server, 5-5
spam engine, 11-7
spam maintenance, 17-4
End User Quarantine, 17-4
spam pattern files, 11-7
spam prevention, 11-2
content scanning, 11-6
actions, 11-11
enabling, 11-9
target, 11-9
email reputation
actions, 11-5
enabling, 11-4
target, 11-5
email reputation services, 11-3
End User Quarantine, 11-7
maintenance, 17-4
spam engine, 11-7
spam pattern files, 11-7
special groups, 17-8, 17-9
configuring, 17-8, 17-9
spyware, 18-3
spyware/grayware, 7-6, 18-2, 18-13, 19-21
adware, 18-13
dialers, 18-13
entering the network, 18-14
hacking tools, 18-13
joke program, 18-13
malware naming, 18-6
password cracking applications, 18-13
remote access tools, 18-13
risks and threats, 18-14
SQL server
manually updating password, 19-20
standalone server, 5-5
summary, 16-2
security risks, 16-4
spam tab, 16-4
system tab, 16-2
support
knowledge base, 21-3
support/system debugger, 17-16
modules, 17-16
using, 17-16

T

targets
web reputation, 12-5
technology
scan engine, 1-25
templates, 10-12, 10-13
creating, 10-13
deleting, 10-15
exporting, 10-16
importing, 10-15
predefined, 10-13
TrendLabs, 21-2
Trend Micro Control Manager, 17-13, 17-15
agent, 17-13
communication protocol, 17-14
communicator, 17-14
entity, 17-14
managed product user access, A-11
registering, 17-15
registering to, A-8
server, 17-13
unregistering, 17-16
Trojan Horse, 18-4, 18-11
true file type, 18-16

U

uncleanable files, 1-23
understand
    data views, A-68
    deployment plans, A-61
    log queries, A-67
    logs, A-65
unregistering
    from Control Manager, 17-16
updates
    ActiveUpdate, 1-28
    alerts, 16-6
    components on clusters, 2-17
    download source, 2-20
    latest patches FAQ, 19-2
    logs, 16-15
    manual updates, 2-19
    pattern file, manual, 20-3
    pattern files, 2-16
    rolling back, 2-22
    scan engine, manual, 20-2
    scheduled updates, 2-19
updating, about, 2-16
URLs
    email technical support, 21-4
    Knowledge Base, 20-3
    security information site, 21-4
    update center, 20-3

V

version comparison, 1-19
viewing
    managed products logs, A-26
Virtual Analyzer, 7-4
    about, 14-2
    configuring, 14-2
    scan engine technology, 1-25
    settings, 14-2
virtual servers, 4-8, 7-3
    creating ScanMail resources, 4-10–4-13
    viewing from the product console, 4-8
viruses/malware, 18-4, 18-10
    boot, 18-5
    file, 18-5
    malware naming, 18-6
    script, 18-5
    writers, 18-6
Virus Scan Application Programming Interface (VSAPI), 1-26
Virus Scan Engine, 1-24
    scan engine, 7-3

W

web reputation, 12-2–12-7
    about, 12-2
    actions, 6-10, 6-21, 12-6
    alerts, 16-6
    configuring, 12-3
    enabling, 12-4
    logs, 16-15
    notifications, 12-7
    Smart Protection Network, 12-4
    Smart Protection Server, 5-8, 5-9, 12-4
    targets, 12-5
Web Reputation Services, 5-3
wildcard, 19-13
wildcards, 17-11
Windows event log codes, B-1
World Virus Tracking Program, 17-12, 17-13
    configuring, 17-13
worms, 18-4, 18-12

Z

zip-of-death, 18-12

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

Item Code: SMEM116853/150119