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 Web site at:


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 © 1998 - 2012. Trend Micro Incorporated. All rights reserved.

Document Part No. SMEM105374_120409

Release Date: June 2012

Document Version No.: 1.0

Product Name and Version No.: Trend Micro™ ScanMail™ for Microsoft™ Exchange
10.2 SP1

Protected by U.S. Patent No.: 5,951,698
The user documentation for Trend Micro ScanMail for Microsoft Exchange 10.2 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
Contents

Preface

ScanMail Documentation ................................................................. P-ii
Audience ......................................................................................... P-ii
Document Conventions ................................................................. P-iii

Chapter 1: Introducing Trend Micro ScanMail for Microsoft Exchange

What’s New ...................................................................................... 1-2
  What’s New in Version 10.2 SP1 ................................................. 1-2
  What’s New in Version 10.2 ....................................................... 1-2
Features and Benefits ................................................................. 1-4
Version Comparison ................................................................. 1-10
How ScanMail Protects the Microsoft Exchange Environment .... 1-12
  About Uncleanable Files ......................................................... 1-17
About Trend Micro Smart Protection ............................................. 1-18
  Smart Protection Services ..................................................... 1-19
  Smart Protection Sources ..................................................... 1-21
  Smart Protection Pattern Files ............................................. 1-22
ScanMail Technology ................................................................. 1-23
  The Trend Micro Scan Engine .............................................. 1-23
  The Trend Micro Pattern Files ............................................... 1-25
About Scans .................................................................................. 1-26
About ActiveUpdate ................................................................. 1-28
About Trend Micro™ IntelliScan™ ............................................... 1-29
About IntelliTrap .......................................................................... 1-30
Trend Micro™ ActiveAction™ ..................................................... 1-30
About Hot Fixes, Patches, and Service Packs ......................... 1-31
Enterprise Protection Strategy .................................................. 1-31
Outbreak Prevention Services .................................................... 1-32
Understanding the Server Management Console ....................................... 4-3
Activating Server Management .............................................................. 4-3
Granting Access Rights in Exchange Server 2003 Environments .... 4-4
Using the Server Management Console ................................................. 4-5
Viewing Servers from the Product Console ........................................... 4-7
Viewing Virtual Servers on a Cluster ...................................................... 4-8
Using Server Management to Replicate Configurations ...................... 4-8
Manually Creating a ScanMail Resource for Virtual Servers .............. 4-9
Starting and Stopping the Services ....................................................... 4-13
Understanding ScanMail Icons ............................................................. 4-14

Chapter 5: Configuring Scanning

Configuring Scans .................................................................................... 5-2
Local Sources Settings ........................................................................... 5-2
Compressed File Handling ..................................................................... 5-3
About ScanMail Actions ......................................................................... 5-6
Notifications ........................................................................................... 5-8
About Security Risk Scans ...................................................................... 5-12
Scan Methods ......................................................................................... 5-14
Security Risk Scan Actions ................................................................... 5-14
Configuring Macro Scanning ................................................................. 5-17

Configuring Attachment Blocking ........................................................ 5-18

Configuring Content Filtering .............................................................. 5-21
About Content Filtering Policies ......................................................... 5-21
Content Filtering ................................................................................... 5-23

Configuring Data Loss Prevention ........................................................ 5-28
Defining Data Identifiers ...................................................................... 5-28
Adding and Editing Expressions .......................................................... 5-28
Importing Expressions ......................................................................... 5-29
Adding and Editing Keyword Lists ...................................................... 5-30
Importing Keyword Lists ..................................................................... 5-31
Defining Data Loss Prevention Templates .......................................... 5-31
Understanding Data Loss Prevention Policies .................................. 5-35
Configuring Spam Prevention ................................................................. 5-40
  Email Reputation ............................................................................. 5-40
  Content Scanning ........................................................................... 5-42

Configuring Web Reputation ................................................................. 5-43

Chapter 6: Managing the Quarantine Area

About the Quarantine ........................................................................... 6-2
Configuring the Quarantine Folder/Directory ....................................... 6-2
Quarantine Query ............................................................................... 6-3
  Performing a Quarantine Query ...................................................... 6-3
Scheduling Automatic Quarantine Maintenance .................................... 6-3
Manually Performing Quarantine Maintenance .................................... 6-4
Resending Quarantined Messages ....................................................... 6-4

Chapter 7: Monitoring ScanMail

Viewing the Summary Screen ............................................................... 7-2
  Summary: System ............................................................................ 7-2
  Summary: Security Risks ................................................................. 7-3
  Summary: Spam ............................................................................. 7-4
About Alerts ........................................................................................ 7-4
  System Events ................................................................................. 7-4
  Outbreak Alerts ............................................................................. 7-6
  Alert Notification Settings .............................................................. 7-7
About Reports .................................................................................... 7-7
  One-time Reports ........................................................................... 7-8
  Scheduled Reports ......................................................................... 7-9
  Report Maintenance ...................................................................... 7-11
About Logs .......................................................................................... 7-11
  Log Query ....................................................................................... 7-13
  Log Maintenance .......................................................................... 7-15
  Performing Log Maintenance ......................................................... 7-15
Chapter 8: Performing Administrative Tasks

Configuring Proxy Settings ................................................................. 8-2
Configuring Notification Settings ....................................................... 8-2
Spam Maintenance ............................................................................. 8-4
Configuring Real-time Scan Settings ................................................ 8-4
About Access Control ......................................................................... 8-5
Access Control Settings ...................................................................... 8-5
  Access Control Permissions ............................................................... 8-6
  Configuring Access Control ............................................................... 8-6
Special Groups .................................................................................. 8-7
  Configuring Special Groups .............................................................. 8-7
Configuring Internal Domains ............................................................ 8-8
Product License .................................................................................. 8-9
World Virus Tracking Program ........................................................... 8-9
About Trend Micro Control Manager ................................................. 8-11
  Configuring Control Manager Settings .......................................... 8-11
About Trend Micro Management Communication Protocol .......... 8-12
Using ScanMail with Control Manager ............................................. 8-12
Registering to Control Manager ....................................................... 8-13
Trend Support / System Debugger ..................................................... 8-14

Chapter 9: Understanding Security Risks

Understanding the Terms .................................................................... 9-2
About Internet Security Risks ............................................................. 9-2
Viruses/ Malware ............................................................................... 9-3
Virus/ Malware Writers ...................................................................... 9-5
Worms .............................................................................................. 9-6
Trojan Horse Programs ...................................................................... 9-6
Joke Programs ................................................................................... 9-7
About Mass-Mailing Attacks ............................................................. 9-7
About Compressed Files .................................................................... 9-8
Zip of Death ....................................................................................... 9-9
Chapter 10: Getting Support and Contacting Trend Micro

Frequently Asked Questions .................................................................10-2
  Why I Am Unable to Log On to the Product Console on Windows
  Server 2008? ...................................................................................10-2
  What if the Remote SQL Server Database Account Password is
  Changed? ......................................................................................10-2
  What are Phish Attacks? .................................................................10-3
  What is Spyware/Grayware? .............................................................10-4
  How Do I Use Operators with Keywords? ......................................10-5
  Where Can I Find the Latest Patches for Updating ScanMail? ......10-8
  What is the EICAR Test Virus? ........................................................10-8
  How do I Send Trend Micro Suspected Internet Threats? ..............10-9
  How do I Send Trend Micro Detected Viruses? ..............................10-9
  Where Can I Find My Activation Code and Registration Key? ......10-9
  Do I Have the Latest Pattern File or Service Pack? .........................10-10
  How Do I Handle Large Files? .........................................................10-11
  How Do I Calculate the Size of a Decompressed File? ....................10-11
  What is a Compression Ratio? ........................................................10-12
  Are Some Files Dangerous? ..........................................................10-13
  What are False Positives? ..............................................................10-13
  What are Regular Expressions? .......................................................10-14
  How Do I Use Keywords? ..............................................................10-22

Troubleshooting .............................................................................10-25
  Update the Scan Engine Manually ...............................................10-25
  Update the Pattern File Manually .................................................10-26
  Known Issues .................................................................................10-27

Contacting Technical Support .......................................................10-28
Before Contacting Technical Support ................................................. 10-29
Contacting Trend Micro ................................................................. 10-29
  TrendLabs .................................................................................... 10-30
Knowledge Base ................................................................................ 10-30
Security Information Site ............................................................... 10-31
Email Technical Support ................................................................. 10-31

Appendix A: Introducing Trend Micro™ Control Manager™
  Control Manager Standard and Advanced ..................................... A-2
  How to Use Control Manager ......................................................... A-3
  Control Manager Architecture ...................................................... A-5
  Registering ScanMail to Control Manager .................................... A-7
  Control Manager User Access ....................................................... A-8
    Control Manager User Access with ScanMail User Access .......... A-10
  Managed Product MCP Agent Heartbeat ....................................... A-10
    Using the Schedule Bar ............................................................ A-12
    Determining the Right Heartbeat Setting .................................... A-13
  Managing ScanMail From Control Manager ............................... A-14
    Understanding Product Directory ............................................. A-15
  Downloading and Deploying New Components from Control Manager ... A-28
    Manually Downloading Components ....................................... A-29
    Configuring Scheduled Download Exceptions ......................... A-34
    Understanding Scheduled Downloads ..................................... A-35
    Configuring Scheduled Downloads and Enabling Scheduled
      Component Downloads ......................................................... A-36
    Understanding Deployment Plans .......................................... A-43
    Configuring Proxy Settings ..................................................... A-45
    Configuring Update/Deployment Settings ............................... A-45
  Using Logs .................................................................................. A-47
    Understanding Managed Product Logs ................................... A-47
    Querying Log Data ................................................................. A-47
Appendix B: Windows Event Log Codes

Appendix C: Database Schema for 64-bit Operating Systems

Log Database Schema ................................................................. C-2
Example 1: Get event log from table "tblActivityEntries" .......... C-12
Example 2: Query: Get Quarantine Log(storage_reason=1) ....... C-14
Example 3: Get Backup Log(storage_reason=2) ..................... C-15
Example 4: Get Archive Log(storage_reason=3) ...................... C-15
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' ...... C-17
Example 6: Get message information that needs to be resent ...... C-18
Example 7: Get Last Configuration Replication ....................... C-18
Example 8: Get Engine Pattern Information ............................. C-18
Example 9: Get Scanning Summary Count - Blocked attachment. C-18

Log View Database Schema ........................................................ C-20
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' ......................... C-37
Example 2: Get Storage Log ...................................................... C-38

Report Database Schema ......................................................... C-39
Example 1: Get Last Summary Time from table[tblSummary]. ...... C-45
Example 2: Get MOM Report Counter ....................................... C-45
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) . C-46
Example 4: Get Virus Summary ................................................ C-46
Example 5: Get Virus Graph By Week ..................................... C-46
Example 6: Get Virus Graph By Day. ................................. C-47
Example 7: Get Top 3 Viruses.(Note: virusinfo_cate_id =151) .... C-47
Example 8: Get Viruses Actions. (Note: virusinfo_cate_id =153) C-48
Appendix D: Database Schema for 32-bit Operating Systems

Log Database Schema ..........................................................D-2
Example 1: Get event log from table "tblActivityEntries" ..........D-13
Example 2: Query :Get Quarantine Log(storage_reason=1). ......D-15
Example 3: Get Backup Log(storage_reason=2) .........................D-16
Example 4: Get Archive Log(storage_reason=3) ..........................D-16
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'.
And the event type is in ‘1’ and ‘2’. .................................D-18
Example 6: Get message information that needs to be resent ......D-19
Example 7: Get all Administrators ............................................D-19
Example 8: Get Last Configuration Replication ..........................D-19
Example 9: Get Engine Pattern Information ...............................D-19
Example 10: Get Scan Summary Count. .....................................D-19

Log View Database Schema ..................................................D-21
Example 1: Query information about virus log, content filtering log, or
attachment blocking log from table ‘vwAVLogs’, ‘vwCFLogs’,
‘vwABLogs’ between 12/12/2008 09:00:00’ AND
12/18/2008 09:00:00’. ..........................................................D-38
Example 2: Get Storage Log ...................................................D-38

Report Database Schema .....................................................D-39
Example 1: Get Last Summary Time from table[tblSummary] .....D-46
Example 2: Get MOM Report Counter .................................D-46
Example 3: Get All Virus Count during 12/12/2008 09:00:00’ AND
12/19/2008 09:00:00’. (Note : virusinfo_cate_id =151) .D-47
Example 4: Get Virus Summary ...............................................D-47
Example 5: Get Virus Graph By Week ....................................D-47
Example 6: Get Virus Graph By Day. ....................................D-48
Example 7: Get Top 3 Viruses.(Note : virusinfo_cate_id =151) ....D-48
Example 8: Get Viruses Actions. (Note : virusinfo_cate_id =153) D-49
Example 9: Get Viruses Actions. (Note : virusinfo_cate_id =152) ....D-49

Appendix E: Best Practices
Real-time Scan Settings for Server Roles .................................................... E-2
Attachment Blocking Policies ................................................................. E-3
  Exception Rule Replication ............................................................... E-4
Sample Usage Scenarios ..................................................................... E-4
Content Filtering Active Directory Integrated Policies ....................... E-5
  Content Filtering Policy Replication ............................................... E-6
Data Loss Prevention Policies ............................................................... E-6
  Internal Domains ........................................................................ E-8
  Hidden Keys .................................................................................. E-8
Optimizing Web Reputation ................................................................. E-9
  Troubleshooting Web Reputation Performance Issues .................... E-9
Recommended Settings ....................................................................... E-10

Index
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 ii
- Audience on page ii
- Document Conventions on page iii
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 are also posted and a dynamic list of the most frequently asked question is also displayed.

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


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 2010 and 2007 server role configurations
- Various message formats
Document Conventions

To help you locate and interpret information easily, the documentation uses the following conventions.

**TABLE P-1. Conventions used in the documentation**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TOOLS &gt; CLIENT TOOLS</strong></td>
<td>A &quot;bread crumb&quot; found at the start of procedures that helps users navigate to the relevant web console screen. Multiple bread crumbs mean that there are several ways to get to the same screen.</td>
</tr>
<tr>
<td>&lt;Text&gt;</td>
<td>Indicates that the text inside the angle brackets should be replaced by actual data. For example, C:\Program Files&lt;file_name&gt; can be C:\Program Files\sample.jpg.</td>
</tr>
<tr>
<td>Monospace</td>
<td>Examples, sample command lines, program code, web URL, file name, and program output</td>
</tr>
<tr>
<td><strong>Note: text</strong></td>
<td>Provides configuration notes or recommendations</td>
</tr>
<tr>
<td><strong>Tip: text</strong></td>
<td>Provides best practice information and Trend Micro recommendations</td>
</tr>
<tr>
<td><strong>WARNING! text</strong></td>
<td>Provides warnings about activities that may harm your computer or your network</td>
</tr>
</tbody>
</table>
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:

• What’s New on page 1-2
• Features and Benefits on page 1-4
• About Trend Micro Smart Protection on page 1-18
• ScanMail Technology on page 1-23
• About Scans on page 1-26
• About Attachment Blocking on page 1-33
• About Content Filtering on page 1-34
• About Data Loss Prevention on page 1-35
• About Spam Prevention on page 1-42
• About Licenses on page 1-48
What’s New

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

What’s New in Version 10.2 SP1

Enhanced Data Loss Prevention

This version of ScanMail provides enhanced Data Loss Prevention capabilities. Administrators can now create customized data identifiers (expressions and keyword lists) or select from a greatly expanded selection of more than a hundred new predefined templates and data identifiers.

Enhanced Web Reputation

- Administrators can exempt users from web reputation queries by adding trusted users to the new Approved Senders List.
- The additional "Quarantine entire message" action is available for messages containing suspicious URLs. Administrators can evaluate suspicious messages in the quarantine directory before they leave the network.

IPv6 Support

ScanMail provides full support for IPv6 environments.

Policy Management from Control Manager 6.0

Control Manager 6.0 allows administrators to create and deploy Data Loss Prevention policies to the ScanMail for Microsoft Exchange servers that Control Manager manages. For details, see the Control Manager Administrator's Guide.

What’s New in Version 10.2

Data Loss Prevention

Trend Micro Data Loss Prevention helps organizations protect information from accidental disclosure and intentional theft. Through use of fully customizable, company-specific policies, and pre-packaged regulatory templates, Data Loss Prevention helps companies manage, control and monitor their sensitive information.
To protect and maintain the integrity of your digital assets, Data Loss Prevention utilizes the following mechanisms:

- **Regulatory Templates**: Administrators can meet regulatory requirements using the pre-packaged templates. Data Loss Prevention templates include over forty expression definitions and over twenty keyword lists.

- **Policy Creation**: Companies can create policies to fit their specific business rules. Policies can apply to the entire business, groups, or individual endpoints, regulating the flow of sensitive data at all levels. Data Loss Prevention also provides six pre-packaged governmental policies.

- **Data Loss Prevention Logs and Notifications**: Comprehensive logs and notifications allow administrators and endpoints to remain constantly aware of any breaches in company security policies.

For more information, see About Data Loss Prevention on page 1-35.

**Enhanced Web Reputation**

Companies with bandwidth usage or privacy concerns can maintain a local Smart Protection Server. This server provides local Web Reputation services without a query to Trend Micro servers. Clients can update the Web Blocking List manually or on a scheduled update from Trend Micro servers. Additional information about the state of the connection to the servers providing Web Reputation services, notifications, and logs provide quick references for administrators to manage and monitor their Web Reputation services.

For more information, see Smart Protection Sources on page 1-21.

**URL Scanning in Attachments**

This version of ScanMail provides the capability to scan email message attachments for suspicious URLs.

For more information, see Web Reputation Services on page 1-20.

**Enhanced Server Management**

Administrators can now sort the company’s servers by name or priority. The Server Management console in ScanMail also displays the following information:

- Pattern and engine versions
• Scanning results
• Scanning status
• Last replication time
• Smart Protection status

Additional Platform Support
ScanMail provides support for the following:
• Microsoft Exchange Server 2010 Service Pack 2
• Veritas Cluster support for Veritas 5.1 Service Pack 2
• Veritas Cluster support for Microsoft Exchange Server 2010

Features and Benefits
ScanMail features provide the following 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 ensuring that company-wide policies remain consistent across all servers

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
Fast and Simple Installation

- Install to a single or multiple Microsoft Exchange servers using a single installation program.
- Install to cluster environments.

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.

Attachment Blocking

- Block named attachments or block attachments by true file type, file extension, or file name.

Content Filtering

- Use rule-based filters to screen out message content deemed to be offensive or otherwise objectionable.

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.

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.

Quarantine
• Set ScanMail to quarantine suspicious email messages.
• Query logs for quarantine events and resend quarantined messages when you decide they are safe.

Web Based Product Console
• Use SSL to access remote servers through a secure product console.

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
Introducing Trend Micro ScanMail for Microsoft Exchange

- 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 10.2 Installation Package: `tool\admin\trend.mib`.

**Informative and Timely Reports and Logs**

- Keep up-to-date using activity logs that detail system events, viruses/malware, and program update events.
- Send or print graphical reports.

**Updates**

Receive scheduled or on-demand component updates and customize your update source.

**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.

**Content Filter Log**

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.
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.

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 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. ScanMail offers incremental scan options only with Exchange Server 2010 and 2007. There are three options:

• Scan messages delivered during a time period
• Scan messages with attachments
• Scan messages that have not been scanned by ScanMail
Cluster Support

ScanMail supports clusters.

**TABLE 1-1. Supported Cluster Models**

<table>
<thead>
<tr>
<th>EXCHANGE VERSION</th>
<th>CLUSTER MODEL</th>
</tr>
</thead>
</table>
| 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 |
| Exchange 2003     | • Shared disk cluster model  
                    • VERITAS Cluster 5.1SP2 |

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.
**Version Comparison**

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

**TABLE 1-2.  ScanMail version comparison**

<table>
<thead>
<tr>
<th>SUPPORT</th>
<th>SCANMAIL 7.0</th>
<th>SCANMAIL 8.0</th>
<th>SCANMAIL 10.x</th>
</tr>
</thead>
</table>
| Operating system version | • Microsoft™ Windows™ 2000 Server, with Service Pack 2 or above  
• Microsoft™ Windows Server™ 2003 | • Microsoft™ Windows™ 2000 Server with Service Pack 4 or above  
• Microsoft™ Windows™ Server 2003 with Service Pack 1, Service Pack 2, or R2 (32-bit or 64-bit)  
• Microsoft™ Windows Server™ 2008 | • 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) |
### TABLE 1-2. ScanMail version comparison (Continued)

<table>
<thead>
<tr>
<th>SUPPORT</th>
<th>ScanMail 7.0</th>
<th>ScanMail 8.0</th>
<th>ScanMail 10.x</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Exchange Version</td>
<td>• Microsoft™ Exchange 2000 Server Service Pack 3</td>
<td>• Microsoft™ Exchange 2000 Server with Service Pack 3 or above</td>
<td>• Microsoft™ Exchange Server 2003 with Service Pack 2</td>
</tr>
<tr>
<td></td>
<td>• Microsoft™ Exchange Server 2003</td>
<td>• Microsoft™ Exchange Server 2003 with Service Pack 2 or above</td>
<td>• Microsoft™ Exchange Server 2007 with Service Pack 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Microsoft™ Exchange Server 2007</td>
<td>• Microsoft™ Exchange Server 2010</td>
</tr>
<tr>
<td>Scan mechanism</td>
<td>• VSAPI 2.0</td>
<td>• VSAPI 2.0</td>
<td>• VSAPI 2.5</td>
</tr>
<tr>
<td></td>
<td>• VSAPI 2.5</td>
<td>• VSAPI 2.5</td>
<td>• VSAPI 2.6</td>
</tr>
<tr>
<td>Exchange Information Store scanning</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SMTP (Transport) scanning</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Quarantine Manager</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Message Filter</td>
<td>Integrated as delete function for inbound and outbound messages</td>
<td>Integrated as delete function for inbound and outbound messages</td>
<td>Integrated as delete function for inbound and outbound messages</td>
</tr>
</tbody>
</table>
**How ScanMail Protects the Microsoft Exchange Environment**

Trend Micro recognizes the unique dangers posed by viruses/malware 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. When each message arrives at the Exchange server, ScanMail subjects the email message to each filter in the following order:

- Spam prevention
- Data Loss Prevention
- Content filtering
- Attachment blocking
- Security risk scan
- Web reputation

---

**TABLE 1-2. ScanMail version comparison (Continued)**

<table>
<thead>
<tr>
<th>SUPPORT</th>
<th><strong>ScanMail 7.0</strong></th>
<th><strong>ScanMail 8.0</strong></th>
<th><strong>ScanMail 10.x</strong></th>
</tr>
</thead>
</table>
| Notification| Collaborative Data Object | • Collaborative Data Object  
• Collaborative Data Object EX | • 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.
In addition, ScanMail provides notifications and log queries to assist administrators to monitor and react to security risks.

**TABLE 1-3. How ScanMail protects the Microsoft Exchange Environment**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam Prevention</td>
<td><strong>Email Reputation</strong>&lt;br&gt;ScanMail includes Email Reputation, which allows you to block spam messages before they enter the network. <strong>Content Scanning</strong>&lt;br&gt;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. ScanMail performs one of the following actions on detected spam:&lt;br&gt;• Quarantines spam messages to a spam message folder&lt;br&gt;• Deletes the spam message&lt;br&gt;• Tags and delivers messages as spam</td>
</tr>
</tbody>
</table>
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 one of the following actions on email messages that contain undesirable content in the message body or attachments:

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

Data Loss Prevention

ScanMail can filter content for sensitive information in a message header, subject, body, and/or attachment based on policies set by the administrator. ScanMail filters outgoing email messages and can perform one of the following actions on email messages that contain sensitive information in the message body or attachments:

- Replace with text/file
- Quarantine entire message
- Quarantine message part
- Delete entire message
- Backup
- Pass message part
**TABLE 1-3. How ScanMail protects the Microsoft Exchange Environment**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Attachment blocking              | ScanMail can block undesirable attachments according to administrator-defined types or specific names. During manual or scheduled scanning, ScanMail can replace the detected file with a text message and then deliver the message to the intended recipient. During real-time scanning, ScanMail can perform one of four actions against blocked attachments:  
  • Replace attachment with text/file  
  • Quarantine entire message  
  • Quarantine message part  
  • Delete entire message                                                                 |
| Security risk scan               | Security risk scan employs the latest version of the Trend Micro 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. |
| 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.  
  Depending on the configuration, web reputation performs one of actions:  
  • Quarantine message to user's spam folder  
  • Delete entire message  
  • Tag and deliver                                                                                                                   |
Real-time scan

ScanMail guards possible virus/malware entry points with real-time scanning of all incoming 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.

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 virus/malware outbreaks and significant system events. Outbreak alerts notify administrators when the number of detected viruses/malware, uncleanable files, or blocked attachments exceed a set number. This enables administrators to react quickly to security breaches in their Exchange environment.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Real-time scan</td>
<td>ScanMail guards possible virus/malware entry points with real-time scanning of all incoming 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.</td>
</tr>
<tr>
<td>Manual/Scheduled scans</td>
<td>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.</td>
</tr>
<tr>
<td>Alerts and notifications</td>
<td>ScanMail can send alerts about virus/malware outbreaks and significant system events. Outbreak alerts notify administrators when the number of detected viruses/malware, uncleanable files, or blocked attachments exceed a set number. This enables administrators to react quickly to security breaches in their Exchange environment.</td>
</tr>
</tbody>
</table>
Introducing Trend Micro ScanMail for Microsoft Exchange

TABLE 1-3. How ScanMail protects the Microsoft Exchange Environment

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reports and logs</td>
<td>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.</td>
</tr>
</tbody>
</table>

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.
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 clients to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. As more products, services and users access the network, customers’ protection updates and strengthens automatically, creating a real-time neighborhood watch protection service for 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 an endpoint are, for the most part, delivered on a scheduled basis. Trend Micro delivers patterns in batches to endpoints. Upon receiving a new update, the virus/malware prevention software on the endpoint reloads this batch of pattern definitions for new virus/malware risks into memory. If a new virus/malware risk emerges, it is necessary to partially or fully update this pattern once again and reload it on the endpoint 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 affect server and workstation performance, network bandwidth usage, and, in general, the overall time it takes to deliver quality protection - or "time to protect".
Trend Micro has pioneered a new approach to handling the volume of threats that aims to make Trend Micro customers immune to the threat of virus/malware volume. The technology and architecture used in this pioneering effort leverage technology that offloads the storage of virus/malware signatures and patterns to the cloud. By offloading 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 offloads a large number of anti-malware signatures that were previously stored on endpoint computers to smart protection sources. For details, see File Reputation Services on page 1-19.

- **Web Reputation Services**: Web Reputation Services allows local smart protection sources to host URL reputation data that were previously available only on the Trend Micro Smart Protection Network. Both technologies ensure smaller bandwidth consumption when updating patterns or checking a URL’s validity. For details, see Web Reputation Services on page 1-20.

**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-client architecture offers more immediate protection and eliminates the burden of pattern deployment besides significantly reducing the overall client footprint.

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

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 threats encompass a broad array of threats that originate from the Internet. Web threats employ sophisticated methods, using a combination of various files and techniques rather than a single file or approach. For example, web threat creators constantly change the version or variant used. Because the web threat is in a fixed location of a website rather than on an infected computer, the web threat creator constantly modifies its code to avoid detection.

Web reputation blocks web pages based on their reputation ratings. Web reputation queries Trend Micro servers or a local Smart Protection Server 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 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.
Smart Protection Sources

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

Smart protection sources provide File Reputation Services by hosting the virus/malware pattern definitions. A client 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. A client sends web reputation queries to smart protection sources to check the reputation of websites that a user is attempting to access. The client correlates a website's reputation with the specific web reputation policy enforced on the computer to determine whether to allow or block access to the site.

Trend Micro Smart Protection Network

The Smart Protection Network is the Trend Micro network that retains a vast repository of web reputation information. The Smart Protection Network verifies all queries against Trend Micro web reputation data and provides the highest level of security against malicious web pages.

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 1-4.  Comparison between smart protection sources**

<table>
<thead>
<tr>
<th>BASIS OF COMPARISON</th>
<th>SMART PROTECTION SERVER</th>
<th>TREND MICRO SMART PROTECTION NETWORK</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>Designed and intended to localize smart protection services to the corporate network to optimize efficiency</td>
<td>A globally scaled, Internet-based infrastructure that provides smart protection services to clients who do not have immediate access to their corporate network</td>
</tr>
<tr>
<td>Administration</td>
<td>ScanMail administrators manage these smart protection sources</td>
<td>Trend Micro maintains this source</td>
</tr>
<tr>
<td>Pattern update source</td>
<td>Trend Micro ActiveUpdate server</td>
<td>Trend Micro ActiveUpdate server</td>
</tr>
<tr>
<td>Client connection protocols</td>
<td>HTTP and HTTPS</td>
<td>HTTPS</td>
</tr>
</tbody>
</table>

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.

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.

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

The Trend Micro 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 an email message, ScanMail performs an immediate real-time scan on the requested message.

ScanMail supports SMTP real time email message scans.

• Non-redundant scanning
When ScanMail completes a scan of a message, it logs the message as scanned. If you access the message again, ScanMail checks to see if it has already scanned the message and does not scan the message a second time.

International computer security organizations, including the International Computer Security Association (ICSA), annually certify the Trend Micro scan engine.

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 on an Exchange server, 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.

Note: The anti-spam pattern file uses a different numbering system.

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.
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.

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

Note: The scan engine includes an automatic cleanup routine for old pattern files (to help manage disk space).
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 scans on the client and improve scan management efficiency. You can configure and apply Scheduled Scan settings to one or several clients and domains, or to all clients that the server manages.

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

Manual Scans and Scheduled Scans during failover or following 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.

About ActiveUpdate

ActiveUpdate provides the latest downloads of all ScanMail components over the Internet. ScanMail components include pattern files for viruses/malware and spyware/grayware.

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.

**About Trend Micro™ IntelliScan™**

IntelliScan optimizes performance by examining file headers using true file type recognition and scanning only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by using a harmless file extension type. The following are just a couple of the benefits IntelliScan offers to administrators:

- **Performance optimization:** Server system resources allotted to scan will be minimal. Using IntelliScan will not interfere with other crucial applications running on the server.
- **Time saving:** Since IntelliScan uses true file type identification, the scan time for running IntelliScan is significantly less than the time required for all attachment files. This means that only files with a greater risk of being infected are scanned. This time difference is noticeable when you use IntelliScan with Manual scan.
About IntelliTrap

Virus writers often attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering your 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, Trend Micro recommends quarantining (not deleting or cleaning) files when you enable IntelliTrap. If your users regularly exchange real-time compressed executable files, you should 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 ScanMail detects a virus/ malware, it takes the recommended action (clean, quarantine message part, delete entire message) on the virus/ malware type to protect your environment's vulnerable points.

If 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, Trend Micro recommends using ActiveAction.

Using ActiveAction provides the following benefits:
• **Time saving and easy to maintain:** ActiveAction uses scan actions recommended by Trend Micro. You 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.
- **Security Patch**: a single hot fix or group of hot fixes suitable for deployment to all customers.
- **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?
About Attachment Blocking

Attachment blocking prevents email messages containing suspicious attachments from being delivered to the Exchange Information Store. ScanMail can block attachments according to the attachment type, attachment name, attachment extension, or when the attachment contains a suspicious URL and then replace, quarantine, or delete all the messages that have attachments that match your configuration. 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, you can decrease the security risk to your 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. You can temporarily quarantine all high-risk file types or those with a specific name associated with a known virus/malware. Later, when you have more time, you 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 will be 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, you 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.
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 "AD user1", then the policy only applies to AD user2.
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\d\s]*\d{2}\s[A-Za-z0-9]{11,27}|\d{4,6}\d{1,3,4}|\d{4,6}\s\d{1,3,4}[\w\d\s]*
```
Messages that contain the string "IBAN" do not trigger this policy. Strings such as "BE68 5390 0754 7034 " will match the regular expression and trigger this policy.

About Data Loss Prevention

Data Loss Prevention utilizes customizable data identifiers, templates, and policies to define, monitor, and protect your company-specific sensitive data from intentional or accidental loss.

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

- What data needs protection from unauthorized users?
- How does the sensitive information transmit through the network?
- What users have permission to access or transmit the sensitive data?
- What action should occur 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 templates and company policies in the Data Loss Prevention system.

Data Identifier Types

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

- Expressions: Data that has a certain structure. For details, see Expressions on page 1-36.
• Keyword Lists: A list of special words or phrases. For details, see Keyword Lists on page 1-39.

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.

Predefined Expressions

ScanMail comes with a set of predefined expressions. These expressions cannot be modified or deleted.

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

Customized Expressions

Create customized expressions if none of the predefined expressions meet your requirements.

Expressions are a powerful string-matching tool. Ensure that you are 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, if you are creating an expression that includes a date, you can refer to the expressions prefixed with "Date".
• Note that ScanMail 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.
There are several criteria that you can choose from when creating expressions. An expression must satisfy your chosen criteria before ScanMail subjects it to a DLP policy. The following tables lists the criteria options for customized expressions.

**TABLE 1-5. Criteria for Customized Expressions**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>All: Names from US Census Bureau</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expression: `[^\w](^[A-Z][a-z]{1,12}(s,</td>
</tr>
<tr>
<td>Specific characters</td>
<td>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.</td>
<td>US - ABA Routing Number</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Expression: <code>[^\w\\\{\.-=\}]([0123678]\d{8})[^\w-]+</code></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Characters: 0123456789</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minimum characters: 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maximum characters: 9</td>
</tr>
</tbody>
</table>

1-37
### Criteria for Customized Expressions

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>RULE</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Suffix</td>
<td>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.</td>
<td>All - Home Address&lt;br&gt;Expression: `&lt;\D(\d+\s[a-z.]+\s([a-z]+\s){0,2}(lane</td>
</tr>
<tr>
<td>Single-character separator</td>
<td>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.</td>
<td>All - Email Address&lt;br&gt;Expression: <code>[^\w.\{\w\}1,20]@^[a-zA-Z0-9]{2,20}\[.\][a-zA-Z0-9]{2,5}\[a-zA-Z0-9]{0,10}\[^\w.</code>]&lt;br&gt;Separator: @&lt;br&gt;Minimum characters to the left: 3&lt;br&gt;Maximum characters to the left: 15&lt;br&gt;Maximum characters to the right: 30</td>
</tr>
</tbody>
</table>
Keyword Lists

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 ScanMail 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".

Predefined Keyword Lists

ScanMail 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.

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 ScanMail subjects it to a DLP 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**

The following table lists the criteria options for keyword lists:

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>RULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any keyword</td>
<td>A file must contain at least one keyword in the keyword list.</td>
</tr>
<tr>
<td>All keywords</td>
<td>A file must contain all the keywords in the keyword list.</td>
</tr>
</tbody>
</table>

TABLE 1-6. Criteria for a Keyword List
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 ScanMail 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, will usually result in faster scanning time but will only cover 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.

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>RULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>All keywords within &lt;x&gt; characters</td>
<td>A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within &lt;x&gt; characters of each other. For example, your 3 keywords are WEB, DISK, and USB and the number of characters you specified is 20. If ScanMail detects all keywords in the order DISK, WEB, and USB, the number of characters from the &quot;D&quot; (in DISK) to the &quot;W&quot; (in WEB) and from the &quot;W&quot; to the &quot;U&quot; (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 &quot;D&quot; and &quot;W&quot;) When deciding on the number of characters, remember that a small number, such as 10, will usually result in faster scanning time but will only cover 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.</td>
</tr>
</tbody>
</table>
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.

You can use some 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 pre-existing, user-defined templates can import and export templates to maintain policy consistency throughout their organization.

### TABLE 1-6. Criteria for a Keyword List

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>RULE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined score for keywords exceeds threshold</td>
<td>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 &quot;salary increase&quot; 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.</td>
</tr>
</tbody>
</table>

About Data Loss Prevention Templates
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.

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.
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.

**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 following features to screen messages for spam:

**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.
Consider the Following Points After Installing ScanMail

- 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.

ScanMail Takes One of the Following Actions Depending on Your Configuration

- Quarantine message to user's spam folder
  ScanMail moves the message to the Spam Mail folder located on the server-side of the Information Store.

- 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 spam and then delivers it to the intended recipient.

**Note**: This feature is not available on ScanMail Standard versions.
Manage 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.

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.

About Licenses

A license to Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s then-current Maintenance fees.

A Maintenance Agreement is a contract between your organization and Trend Micro, regarding your right to receive technical support and product updates in consideration for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.

Note: The Maintenance Agreement expires. Your License Agreement does not. If the Maintenance Agreement expires, scanning can still occur, but you will not be able to update the virus pattern file, scan engine, or program files (even manually). Nor will you be entitled to receive technical support from Trend Micro.

Typically, sixty days before the Maintenance Agreement expires, ScanMail alerts you of the pending discontinuation on the Summary and Product License screens of the web console. You can update your Maintenance Agreement by purchasing renewal maintenance from your reseller, Trend Micro sales, or on the Trend Micro Online Registration URL:

https://olr.trendmicro.com/registration/
Renewing a Maintenance Agreement

Trend Micro or an authorized reseller provides technical support, virus pattern downloads, and program updates for one (1) year to all registered users, after which you must purchase renewal maintenance.

If your Maintenance Agreement expires, scanning will still be possible, but virus pattern and program updates will stop. To prevent this, renew the Maintenance Agreement as soon as possible.

• To purchase renewal maintenance, contact the same vendor from whom you purchased the product. A Maintenance Agreement, extending your protection for a year, will be sent by post to the primary company contact listed in your company’s Registration Profile.

• To view or modify your company’s Registration Profile, log in to the account at the Trend Micro online registration website:

  https://olr.trendmicro.com/registration/
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
- Using the Product Console on page 2-2
- Registering ScanMail on page 2-8
- Activating ScanMail on page 2-10
- Updating ScanMail on page 2-16
- Rolling Back a Component Update on page 2-21
Getting Started

After installing ScanMail, there are a number of tasks you can perform to ensure that everything is set up and working properly, and that you will be making full use of the many features.

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, such as Server Management and End User Quarantine (if not completed during Setup).
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.
7. Obtain the EICAR test file to confirm that your installation is working.

Using 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 computer on your network. The ScanMail product console is password protected ensuring only authorized administrators can modify ScanMail settings. You can view the product console from any computer on your network that is running a supported browser.
To view the product console for a local server:

1. Click **Start** > **Programs** > **Trend Micro ScanMail for Microsoft Exchange** > **ScanMail Management Console**.
2. Type your user name and password.
3. Click **Log on**.

---

**Note:** Use an account that belongs to the **SMEX Admin Group** to log on to ScanMail installations with Exchange 2003. Use the account that belongs to **Management Group** configured during Setup to log on to ScanMail installations with Exchange 2010 or 2007.

---

To view the web console from a remote server:

1. Use a supported browser to access:
   - `http://<servername>:<portnumber>/smex`
   - `https://<servername>:<portnumber>/smex`

   Where "servername" is the name of the server on which you installed ScanMail and "port number" is the port number you use to access that computer.

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

2. Type your 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 you need to configure and manage ScanMail.

![The product console](image)

**Figure 2-1** The product console

Product Console Elements

Banner

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

![Product console banner](image)

**Figure 2-2** 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 4-3.

• **Log Off**: click to end your session and close the product console. 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**: open the online help table of contents and index
  • **Knowledge base**: access 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.

![Product console side menu image]

**FIGURE 2-3** Product console side menu
Configuration area

The configuration area is the working area where you configure and modify all ScanMail configurations and options.

![Product console configuration area](image)

**Figure 2-4  Product console configuration area**

**Getting Help While Using the ScanMail Product Console**

ScanMail offers the following types of help:

- 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.
Registering ScanMail

When you purchase ScanMail, you receive a Registration Key with your product package or from your Trend Micro reseller. Registering ScanMail entitles you to standard support that 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, but is usually 12 months.

You need to register and activate ScanMail to enable pattern file and scan engine updates (use either an Activation Code, or an annual one). Even if you are already using an evaluation copy of the product, and activated the product using an evaluation-version Activation Code.

Online Purchase

When your online purchase is complete, you will receive licensing and registration information from Trend Micro, including a number that you must use 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 you are 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.

**To register your product:**

Use one of the following methods to register:

- **During installation**
  
  The installation program will prompt you to use your Registration Key to register online. Follow the link to the Trend Micro website, register your product, and then return to the installation program to complete your installation.

- **Online**
  
  Visit the following Trend Micro website to register online. You receive an Activation Code to activate your product.

  [http://olr.trendmicro.com/registration](http://olr.trendmicro.com/registration)

- **Contact Trend Micro directly**
  
  Provide a Trend Micro representative with your Registration Key and he or she will give you an Activation Code. Trend Micro maintains a list of contacts at:


---

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

---

For more information, see [Contacting Technical Support](#) on page 10-28.
Activating ScanMail

The following conditions require activation.

- Installing ScanMail for the first time
  For example, when you purchase the standard or suite version from a Trend Micro reseller and use the registration key to obtain an Activation Code.

- Changing from an evaluation version to a full version, or changing to a Suite version from a Standard version.
  For example, when you obtain a new Activation Code from a Trend Micro representative and want to use the product console to activate your new version.

**Note:** The evaluation version is fully functional for 30 days, after which ScanMail tasks will continue to run, but no security risk scan, message filtering, or component update will occur.

You can activate ScanMail during installation or using the product console.

**To activate ScanMail during installation:**

1. Run the installation program.
2. Type the Activation Code in the Product Activation screen.
3. Complete the installation to activate ScanMail.

**To activate ScanMail after installation using the product console:**

1. Click Administration > Product License.
2. If you have not registered ScanMail, click Upgrade Instruction. This opens the Trend Micro website which allows you to register online. Register online to get an Activation Code.
3. Click New Activation Code from the Product License screen.
4. Type your 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 security risk scan and attachment blocking. You will receive scan engine and pattern file updates and be able to run scans in real time, manually, and according to schedules. ScanMail detects infected attachments and takes actions against them.

**TABLE 2-1. Standard Activation Code features**

<table>
<thead>
<tr>
<th>MAINTENANCE AGREEMENT</th>
<th>STANDARD FEATURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation</td>
<td>Using the evaluation Activation Code allows you to implement all ScanMail functions for a limited duration. During the evaluation period, ScanMail performs security risk scan and attachment blocking as well as scan engine and pattern file updates.</td>
</tr>
<tr>
<td>Fully licensed</td>
<td>A fully licensed Activation Code entitles you to standard maintenance agreement and allows you to implement all ScanMail functions except spam prevention, content filtering, and the End User Quarantine tool. ScanMail warns you when your license agreement is close to expiration.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Maintenance Agreement</th>
<th>Suite Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evaluation</td>
<td>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.</td>
</tr>
<tr>
<td>Fully licensed</td>
<td>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.</td>
</tr>
</tbody>
</table>
Suite Activation Code with Additional Feature

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**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SUITE AC</th>
<th>STANDARD AC</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FULL</td>
<td>TRIAL</td>
</tr>
<tr>
<td>Product console</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Spam prevention, content filtering, and web reputation items on reports, logs, and quarantine manager</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security Risk Scan</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Attachment Blocking</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Spam Prevention: Content Scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Content Filtering</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Reactivating ScanMail

You may need to reactivate ScanMail if you want to change your Standard version to a Suite version. Reactivating involves changing your Activation Code from one number to another. When you click New Activation Code, you can type your new Activation Code and receive all the benefits of the ScanMail version that it matches.

To reactivate a new version of ScanMail

1. Click Administration > Product License to open the Product License screen.
2. Click New Activation Code. The Product License screen displays a field where you can type the Activation Code for your version of ScanMail.
3. Click Activate. This activates the new version of ScanMail and enables all the functions available according to that license.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SUITE AC</th>
<th>SUITE AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual Scan / Scheduled Scan</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart Protection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ActiveUpdate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>End User Quarantine</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Control Manager Support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Updating ScanMail

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

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.

**Complete the following tasks before updating ScanMail:**

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 Your 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

To configure the proxy server:
1. Log on to the ScanMail product console.
2. On the sidebar, click Administration > Proxy. The Proxy screen appears.
3. Select Use a proxy server for Web Reputation, updates and product license notifications.
4. Type the server name or IP address of the proxy server and its port number.
5. Select Use SOCKS 5 proxy protocol to use SOCKS 5 protocol.
6. If your proxy server requires a password, type your user name and password in the fields provided.
7. Click Save to save your settings.
Configuring Manual Updates

Trend Micro recommends manually updating your scan engines and pattern files immediately after installing ScanMail or whenever there is an outbreak. This establishes a security baseline for your Exchange environment.

Manually Updating Your Components

The following lists the procedure required for configuring manual updates.

To manually update your components:

1. Log on to the ScanMail product console.
2. Click Updates > Manual.
3. Select the component that you wish to update.
4. 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.

Setting Scheduled Updates

The following lists the procedure required for configuring scheduled updates.

To configure scheduled updates:

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.

Setting the Download Source

The following lists the procedure required for configuring the download source.

To set the update source, select one of the following locations:

- Trend Micro ActiveUpdate 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**
  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 speed 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**
  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**
  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.

To manually roll back to a previous component:

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\n   <Installation folder>\AU_Data\AU_Temp\n   <Installation folder>\AU_Data\AU_Storage\n   <Installation folder>\web\activeupdate\n
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
   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 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\n
  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)
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 3-5
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.

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 Updating ScanMail 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

<table>
<thead>
<tr>
<th>ACTION</th>
<th>BENEFIT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduled updates</td>
<td>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.</td>
</tr>
<tr>
<td>Scheduled scans</td>
<td>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.</td>
</tr>
<tr>
<td>Enable action on mass-mailing behavior</td>
<td>Select <strong>Enable action on mass-mailing behavior</strong> from the Security Risk Scan Action screen to provide early warning of outbreaks.</td>
</tr>
<tr>
<td>Outbreak Alerts</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.


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/quarantine
- SMEX/storage/Backup
- 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.
     
     
   - If you need more assistance, contact Trend Micro support. See Contacting Technical Support on page 10-28.

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.
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 4-3
- Manually Creating a ScanMail Resource for Virtual Servers on page 4-9
- Starting and Stopping the Services on page 4-13
- Understanding ScanMail Icons on page 4-14
Understanding Real-time Monitor

The Real-time monitor displays information about one Exchange server in real time. It shows ScanMail scanning incoming and outgoing messages as they arrive. It also gives the current count of detected viruses/malware, spyware/grayware, spam, and suspicious URLs on the server.

You can use Real-time monitor to monitor your local server, or any server connected to your network. This is a useful method for managing your ScanMail servers from a centralized location.

**Note:** Details may be different depending on the Exchange version, server role, and license version you use.

---

**Figure 4-1** Real-time monitor

To view real-time monitor for a remote server:

1. Access the remote server using the product console.
2. Click **Real-time monitor**. The Real-time monitor screen opens displaying information about the remote servers.
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 domain when you install ScanMail with Exchange 2003. View all ScanMail servers when you install ScanMail with Exchange 2010 and 2007.

[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. You must log on using an account with local administrator privileges to activate Server management. Then click the Server management link at the top of the product console.

To activate Server Management for ScanMail with Exchange Server 2003:

- Select to Specify an existing account from Active Directory or create a new account. The activation wizard prompts you through the steps required to activate Server Management.

To activate Server Management for ScanMail with Exchange Server 2010 and 2007:

- Specify an existing group in Active Directory and the activation wizard prompts you through the steps required to activate Server Management.
Granting Access Rights in Exchange Server 2003 Environments

In Exchange Server 2003 environments, special permissions are required to view and replicate settings to servers belonging to different domains within the same domain forest.

**Note:** This procedure is not required for Exchange Server 2010 and 2007.

To grant access rights to other domains in the same forest for Exchange Server 2003:

1. Run `regedit`.
2. Navigate to `HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg`.
3. Right click `winreg` from the popup menu.
4. Select **Permissions**.
5. Add the **SMEX Admin Group** of the domain the controlling Server Management console belongs to and allow **Read**.
6. Navigate to `HKEY_LOCAL_MACHINE\SOFTWARE\TRENDMICRO\ScanMail for Exchange`.
7. Right click **ScanMail for Exchange** from the popup menu.
8. Select **Permissions**.
9. Add the **SMEX Admin Group** of the domain the controlling Server Management console belongs to and allow **Full Control**.
# Using the Server Management Console

Use the Server Management console to do the following:

<table>
<thead>
<tr>
<th>TABLE 4-1. Server Management console features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FEATURE</strong></td>
</tr>
<tr>
<td>View pattern and engine version</td>
</tr>
</tbody>
</table>
| 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  
  - Virus/Malware Uncleanable  
  - Blocked attachments  
  - Spam  
  - Data Loss Prevention  
  - Content violations  
  - Suspicious URLs  
  - Unscannable message parts |
| View scan status | Indicates whether the scan type is enabled or disabled.  
  - On Exchange Server 2003, you can view the scan status for security risk scan, attachment blocking, content filtering, spam prevention, and web reputation for remote ScanMail servers.  
  - On Exchange Server 2010 and 2007, you can view the scan status for 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, and web reputation for remote ScanMail servers. |
<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View last replication</td>
<td>View the server name, status, and duration of the last replication.</td>
</tr>
<tr>
<td>Replicate settings to remote servers</td>
<td>Replicate settings to one or multiple remote servers in the list.</td>
</tr>
<tr>
<td></td>
<td>- All Settings</td>
</tr>
<tr>
<td></td>
<td>- Specified Settings</td>
</tr>
<tr>
<td></td>
<td>- Security risk scan</td>
</tr>
<tr>
<td></td>
<td>- Spam prevention</td>
</tr>
<tr>
<td></td>
<td>- Data Loss Prevention</td>
</tr>
<tr>
<td></td>
<td>- Manual scan</td>
</tr>
<tr>
<td></td>
<td>- Smart Protection</td>
</tr>
<tr>
<td></td>
<td>- Updates</td>
</tr>
<tr>
<td></td>
<td>- Alerts</td>
</tr>
<tr>
<td></td>
<td>- Reports</td>
</tr>
<tr>
<td></td>
<td>- Logs</td>
</tr>
<tr>
<td></td>
<td>- Administration (Proxy, Notification settings, Access Control, World Virus Tracking, Control Manager)</td>
</tr>
<tr>
<td></td>
<td>- Special group</td>
</tr>
<tr>
<td></td>
<td>- Internal domain</td>
</tr>
<tr>
<td></td>
<td>- Product license</td>
</tr>
<tr>
<td></td>
<td>- Attachment blocking</td>
</tr>
<tr>
<td></td>
<td>- Web reputation</td>
</tr>
<tr>
<td></td>
<td>- Data Loss Prevention templates</td>
</tr>
<tr>
<td></td>
<td>- Scheduled scan</td>
</tr>
<tr>
<td></td>
<td>- Content filtering</td>
</tr>
<tr>
<td></td>
<td>- Overwrite server - dependent settings (such as quarantine and back up directories)</td>
</tr>
<tr>
<td>View Smart Protection status</td>
<td>View information about your Smart scan servers including the server name, scan service, scan setting, smart protection source, and server status.</td>
</tr>
</tbody>
</table>
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. For ScanMail with Exchange Server 2003, you can use an account that is part of the "SMEX Admin Group". For ScanMail with Exchange Server 2010 and 2007, you 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.

**To view the product console from a local server**

1. Click **Start > Programs > Trend Micro ScanMail for Microsoft Exchange > ScanMail Management Console**.
2. Type your user name and password.
3. Click **Enter**.

**To view the product console 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.

To replicate the settings from a server to one or more target server(s):

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.

**Windows Server 2003**

1. Create a ScanMail resource by selecting the correct resource type:
   - Microsoft Exchange Server 2003 MSC: ScanMail for Exchange Cluster Agent
   - 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 2003: Physical/ Mount-point disk, network name, and Microsoft Exchange Information store
- 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** checkbox.

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>


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
   ```

---


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 checkbox.

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

Exchange 2007 SCR Cluster

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 checkbox.

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

• **ScanMail for Microsoft Exchange System Watcher**: Monitors logs for system events.

• **ScanMail EUQ Migrator Service**: ScanMail adds this service if Integrate with End User Quarantine or Integrate with Outlook Junk E-Mail were switched from one to the other.

• **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>
<thead>
<tr>
<th>ICON</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Help icon" /></td>
<td>Click to view the ScanMail Help.</td>
</tr>
<tr>
<td><img src="image" alt="Enabled" /></td>
<td>Click to disable a rule or policy. When this icon displays, the rule or policy is currently enabled.</td>
</tr>
<tr>
<td><img src="image" alt="Disabled" /></td>
<td>Click to enable a rule or policy. When this icon displays, the rule or policy is currently disabled.</td>
</tr>
<tr>
<td><img src="image" alt="Refresh" /></td>
<td>Click to refresh the information on the screen.</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>This indicates a warning status.</td>
</tr>
<tr>
<td><img src="image" alt="Enabled" /></td>
<td>This indicates an enabled status.</td>
</tr>
<tr>
<td><img src="image" alt="Disabled" /></td>
<td>This indicates a disabled status.</td>
</tr>
<tr>
<td><img src="image" alt="Delete" /></td>
<td>Click to delete a template.</td>
</tr>
</tbody>
</table>
### Table 4-2. ScanMail icons (Continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Tooltip" /></td>
<td>Mouse over this icon to see helpful information about a feature.</td>
</tr>
<tr>
<td><img src="image" alt="Show details" /></td>
<td>Click to expand the drop down.</td>
</tr>
<tr>
<td><img src="image" alt="Hide details" /></td>
<td>Click to collapse the drop down.</td>
</tr>
</tbody>
</table>
Chapter 5

Configuring Scanning

This chapter explains how to configure scans to protect your Exchange environment.

Topics include:

- Configuring Scans on page 5-2
- About Security Risk Scans on page 5-12
- Configuring Attachment Blocking on page 5-18
- Configuring Content Filtering on page 5-21
- Configuring Data Loss Prevention on page 5-28
- Configuring Spam Prevention on page 5-40
- Configuring Web Reputation on page 5-43
Configuring 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.

**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.

For more information on the different scan types, see About Scans on page 1-26.

Local Sources Settings

Configure the local sources settings to use smart scan in Security Risk Scans. For more information about Local Sources, see Smart Protection Sources on page 1-21.

Configuring Local Sources

**To configure local sources:**

1. Log on to the product console.
2. Click Smart Protection > Local Sources from the main menu. The Local Sources screen displays.
3. Click Add. The Add Smart Protection Server screen appears.
4. Type the Server name or address for the server you want to add.
5. 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.

6. For a Smart Protection Server providing file reputation services, optionally select to enable Secure Sockets Layer (SSL) protocol.
7. Click the appropriate test connection button to verify a successful connection to the server.
8. Click Add. The Smart Protection Server displays at the bottom of the Smart Protection Server List.
9. 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.
10. Click Proxy Settings and configure proxy settings if ScanMail requires a proxy for server communication with Smart Protection Server.
11. Click Save.

Compressed File Handling

Manual or Scheduled Scans > Security Risk Scan and Attachment Blocking links

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.

To balance security and performance, Trend Micro recommends that you read the following before choosing compressed file settings:

Attachment Blocking

- **Block all compressed files**: Choose this option to have ScanMail prevent the client from receiving compressed files. Users can be notified through their mail client that ScanMail blocked the attached file (Attachment Blocking > Notification)
  - Click Attachment Blocking > Target.
  - Click Specific attachments, then click Attachment types and expand the category.
• Click **Compressed files**. If needed, expand the category and specify types.
• Click **Action** and select an action. Click **Notification** and select a notification method

**Security Risk Scan > Advanced Options > Scan Restriction Criteria**

Compressed files scanning restrictions:

• Click **Decompressed file count exceeds**: and 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.

• Click **Size of decompressed files exceeds**: and 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.

• Click **Number of layers of compression exceeds**: and 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.

• Click **Size of decompressed file is "x" times the size of compressed file**: and type a number. 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.
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.

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)
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.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean</td>
<td>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).</td>
</tr>
<tr>
<td></td>
<td><strong>Tip:</strong> Trend Micro recommends using the default scan action &quot;clean&quot; for viruses/malware.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>During a manual or scheduled scan, ScanMail updates the Information Store and replaces the file with the cleaned one.</td>
</tr>
<tr>
<td>Replace with text/file</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> 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.</td>
</tr>
</tbody>
</table>
## Table 5-1. ScanMail Actions (Continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quarantine entire message</td>
<td>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.</td>
</tr>
<tr>
<td>Quarantine message part</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Note:</strong> 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.</td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>ScanMail backs up the message, delivers, and records the detection in logs.</td>
</tr>
<tr>
<td><strong>Note:</strong> This action behaves the same as archive in previous versions of ScanMail.</td>
<td></td>
</tr>
<tr>
<td>Delete entire message</td>
<td>During real-time scanning, ScanMail deletes the entire email message. The delete action in ScanMail 10.2, 10.0, and 8.0 differs from that of ScanMail 7.0. ScanMail 7.0 does not have this option for manual scan or scheduled scan.</td>
</tr>
<tr>
<td>Pass</td>
<td>ScanMail records the detection in logs and delivers the message unchanged.</td>
</tr>
<tr>
<td>Pass entire message</td>
<td>ScanMail records the detection in a log and delivers the message unchanged.</td>
</tr>
</tbody>
</table>
Notifications

You can configure ScanMail to send a notification by email message or SNMP when ScanMail takes action against detected security risks and undesirable content during security risk scans, attachment blocking, content filtering, or Data Loss Prevention scanning. You can also automatically record Notifications in the Windows Event Log.

Send notifications to:
- Warn the original recipients that their email message was altered
- Notify an administrator or other network security professional of a security risk
- Display information to the recipient 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.

<table>
<thead>
<tr>
<th>ACTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pass message part</td>
<td>ScanMail records the detection in a log and delivers the message unchanged.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For Data Loss Prevention and content filtering, this does not apply to low priority policies.</td>
</tr>
<tr>
<td>Tag and deliver</td>
<td>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.</td>
</tr>
<tr>
<td>Quarantine to user’s spam folder</td>
<td>ScanMail moves the email message to the Spam Mail folder located on the server-side of the Information Store.</td>
</tr>
<tr>
<td>Forward to sender’s manager</td>
<td>Forward the email message to the sender’s manager.</td>
</tr>
<tr>
<td>Forward to specific email address(es)</td>
<td>Forward the email message to the specific email address(es).</td>
</tr>
</tbody>
</table>
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.

**TABLE 5-2. Notification settings**

<table>
<thead>
<tr>
<th>WHERE TO SEND NOTIFICATIONS</th>
<th>NOTIFICATION DETAILS</th>
</tr>
</thead>
</table>
| 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 virus/malware occurrences by typing a number in the box.  
                              | • **Send individual notifications**: ScanMail sends an email message notification every time ScanMail performs a filtering action. |
### TABLE 5-2. Notification settings (Continued)

<table>
<thead>
<tr>
<th>WHERE TO SEND NOTIFICATIONS</th>
<th>NOTIFICATION DETAILS</th>
</tr>
</thead>
</table>
| 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. 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 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. |
### TABLE 5-2. Notification settings (Continued)

<table>
<thead>
<tr>
<th>WHERE TO SEND NOTIFICATIONS</th>
<th>NOTIFICATION DETAILS</th>
</tr>
</thead>
</table>
| 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. |
• **Advanced notification**: Configure SNMP notifications and Windows notifications.

**TABLE 5-3. Advanced notification settings**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
</table>
| 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. |

• **Save**: Click to save changes.  
• **Reset**: Click to revert to default settings.

**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 5-4. Security risk scan characteristics**

<table>
<thead>
<tr>
<th>Type of Scan</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan method</td>
<td>There are two methods for security risk scans:</td>
</tr>
<tr>
<td></td>
<td>• Conventional Scan</td>
</tr>
<tr>
<td></td>
<td>• Smart Scan</td>
</tr>
<tr>
<td>Real-time scan</td>
<td>ScanMail scans the following in real time:</td>
</tr>
<tr>
<td></td>
<td>• All incoming and outgoing email messages</td>
</tr>
<tr>
<td></td>
<td>• Public-folder postings</td>
</tr>
<tr>
<td></td>
<td>• All server-to-server replications</td>
</tr>
<tr>
<td>Manual scan and scheduled</td>
<td>During manual and scheduled scans, ScanMail scans messages stored in the mailbox</td>
</tr>
<tr>
<td>scheduled scan</td>
<td>and public folder stores.</td>
</tr>
<tr>
<td></td>
<td>Starting another scheduled scan does not interrupt the scheduled scan that is</td>
</tr>
<tr>
<td></td>
<td>already in progress.</td>
</tr>
<tr>
<td></td>
<td>ActiveUpdate does not interrupt a scheduled scan.</td>
</tr>
<tr>
<td></td>
<td>On cluster servers:</td>
</tr>
<tr>
<td></td>
<td>Each virtual server has a scan task list. You can specify the store database</td>
</tr>
<tr>
<td></td>
<td>that belongs to the current virtual server. When there is a running scheduled</td>
</tr>
<tr>
<td></td>
<td>scan task, new tasks are queued. When another task is triggered at the same time,</td>
</tr>
<tr>
<td></td>
<td>then the task will be queued and finished eventually.</td>
</tr>
</tbody>
</table>
Scan Methods

There are two methods for security risk scans:

• **Conventional scan**: the scan method used in previous ScanMail versions. All components used for security risk scans are stored locally on the ScanMail server.

• **Smart scan**: 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.

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.

**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 Settings**

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.

• 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.

Configuring Security Risk Scan Targets

To configure security risk scan target settings:

1. On the Security Risk Scan page for real-time, manual, or scheduled scans, click the Target tab. The Target screen displays.

2. Select one of the following for security risk scan:
   • All attachment files
   • IntelliScan: uses "true file type" identification
   • Specify file types

3. To scan the message body, select Scan message body.

4. To use IntelliTrap technology, select Enable IntelliTrap.

5. To scan for spyware/grayware, select Select All for Spyware/Grayware Scan or select from the following:
   • Spyware
   • Dialers
   • Hacking Tools
   • Password Cracking Applications
   • Adware
   • Joke Programs
   • Remote Access Tools
   • Others

6. Click Scan Restriction Criteria if performance improvement is required.

7. Select from the following options to skip scans for files that fall within this criteria and specify the value:
   • Message body size exceeds:
Attachment size exceeds:
Decompressed file count exceeds:
Size of decompressed file exceeds:
Number of layers of compression exceeds:
Size of decompressed file is "x" times the size of compressed file:

8. Click Save.
9. Click the Notification tab.
10. Select notification options. See Notifications on page 5-8.
11. Click Save.

Configuring Security Risk Scan Actions

To configure security risk scan action settings:

2. Select one of the following:
   • ActiveAction
   • Customized action for detected threats:
3. To back up the infected file, select Backup infected file before performing action.
4. Select Do not clean infected compressed files to optimize performance. if performance improvement is required.
5. Configure Advanced Options as necessary.
   a. Click Macros to configure macro scan.
      i. Select Enable advanced macro scan.
      ii. Select one of the following:
         • Heuristic level
         • Delete all macros detected by advanced macro scan
   b. Click Unscannable Message Parts to specify actions for encrypted and password protected files and files not in the scan restriction criteria.
      • Select Replace with text/ file, Quarantine entire message, Delete entire message, Pass, or Quarantine message part.
• Select **Do not notify** or **Notify** to send notifications when this action is triggered.

c. Click **Backup and Quarantine Setting** to specify the directory paths.
d. Click **Replacement Settings** to configure the text or file name that replaces infected content.
   i. Specify the **Replacement file name**.
   ii. Specify the **Replacement text**.

6. Click **Save**.

### Configuring Security Risk Scan Notifications

**To specify security risk scan notification settings:**

1. Select the check boxes corresponding to the people ScanMail will notify. Refer to **Notifications** on page 5-8 for details.
2. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
3. 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 Virus Scanning 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 Virus Scanning screen. When you select **Delete all macros detected by advanced macro scan**, then ScanMail strips all macro code from the scanned files.
To configure ScanMail to scan unknown macro viruses:

1. Click Security Risk Scan > Action.
2. Click Advanced Options > 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 Attachment Blocking

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.

Enabling Attachment Blocking

To enable attachment blocking:

1. Log on to the product console.
2. Click Attachment Blocking from the main menu. The Attachment Blocking screen displays.
3. Select **Enable transport level attachment blocking**.
4. Select **Enable store level attachment blocking**. (Exchange Server 2010 and 2007)
   Select **Enable real-time attachment blocking**. (Exchange Server 2003)
5. Click **Save** to enable attachment blocking.

**Adding an Exception to the Attachment Blocking Global Policy**

**To add an exception to the attachment blocking global policy:**

1. Log on to the product console.
2. Click **Attachment Blocking** from the main menu. The Attachment Blocking screen displays.
3. Click **Add Exception**. The Select Accounts screen displays.
4. Click **specific recipients**. The Recipients screen displays.
5. Select one of the following:
   - **Anyone**: Apply this exception to all recipients.
   - **Specific accounts**: Select from Active Directory groups or ScanMail special groups.
6. Select accounts to exclude from this exception by clicking **Exclude Accounts** and search from Active Directory groups or ScanMail special groups.
7. Click **Save**. The Select Accounts screen displays.
8. Click **Next >**. The Specify Policy screen displays.
9. Select **Attachment types** and/or **Attachment names**.
10. Click **Show details** to specify specific types or names.
11. Click **Next**. The Name and Priority screen displays.
12. Ensure the **Enable this exception** check box is selected.
13. Type the **Exception name**.
14. Type a number for the **Priority**.
15. Click **Save**.
Configuring Attachment Blocking Targets

To configure attachment blocking target settings:

1. For manual or scheduled scans, click the Attachment Blocking hyperlink. The Attachment Blocking screen displays. For real-time scans, click Attachment Blocking and click Global Policy from the list of policies and exceptions. The Global policy settings screen displays.

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 to exclude and/or Attachment names to exclude. Click Show details to specify specific types or names.

4. Select Block attachment types or names within compressed files.

5. Click Save.

Configuring Attachment Blocking Actions

To configure attachment blocking action settings:

1. For manual or scheduled scans, click the Attachment Blocking hyperlink. The Attachment Blocking screen displays. For real-time scans, click Attachment Blocking and click Global Policy from the list of policies and exceptions. The Global policy settings screen displays.

2. Click the Action tab. The Action screen displays.

3. Select an action. For details on actions, see About ScanMail Actions on page 5-6.

4. Specify whether to send notifications when attachments are blocked by selecting Notify or Do not notify.

5. (Optional) Click Quarantine Settings to specify a different quarantine directory.

6. (Optional) Click Replacement Settings to customize the Replacement file name and Replacement text.

7. Click Save.
Configuring Attachment Blocking Notifications

To configure attachment blocking notification settings:

1. For manual or scheduled scans, click the Attachment Blocking hyperlink. The Attachment Blocking screen displays. For real-time scans, click Attachment Blocking and click Global Policy from the list of policies and exceptions. The Global policy settings screen displays.

2. Click the Notification tab. The Notification screen displays.

3. Select the check boxes corresponding to the people ScanMail will notify. Refer to Notifications on page 5-8 for details.

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

5. Click Save.

Configuring Content Filtering

Content filtering monitors email messages for instances of undesirable keywords and takes action when these keywords exist in the header and/or contents of a message (see About Content Filtering on page 1-34). Before content filtering can actively protect your business, you must configure the content filtering settings.

About 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 5-5. Content filtering policies

<table>
<thead>
<tr>
<th>POLICY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match any or apply to all</td>
<td>This type of policy is capable of filtering content from any message in real-time or during a manual or scheduled scan.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Active Directory integration is available for Exchange Server 2010 and 2007 Hub Transport server roles.</td>
</tr>
<tr>
<td>Match all conditions</td>
<td>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.</td>
</tr>
<tr>
<td>Match any condition</td>
<td>This type of policy scans the message content of particular email account(s). These policies are similar to general content filter policies, except that they only filter content from specified email account(s).</td>
</tr>
<tr>
<td>Exceptions</td>
<td>This type of policy creates an exception for specific email account(s).</td>
</tr>
</tbody>
</table>
Content Filtering

When content filtering is enabled, you can enable and disable individual content filter 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.

Adding a Content Filtering Policy

You can create policies that filter email messages according to:

• **Any of the conditions in your policy**: Select **Match any or apply to all** and click **Next**.
• **All of the conditions in your policy**: Select **Match all conditions** and click **Next**.
• Any matches to the header of messages policy: Select **Match any condition** and click **Next**.
• **Exception policies**: Select **Exceptions** and click **Next**.

The following is an example of how to create a policy that filters email messages for any condition in your policy:

**Select a Type of Policy** on page 5-23

**Step 1: Select Accounts (Senders/ Recipients)** on page 5-24

**Step 2: Specify Policy** on page 5-24

**Step 3: Specify Actions** on page 5-26

**Step 4: Specify Notifications** on page 5-27

**Step 5: Name & Priority** on page 5-27

**Select a Type of Policy**

**To select a type of policy:**

1. From the Content Filtering screen, click **Add**.
2. Select **Match any or apply to all**. The Step 1: Select Accounts screen displays.
Step 1: Select Accounts (Senders/Recipients)

To configure specified accounts (senders/recipients) the policy scans:

1. Select From specific senders to any recipients or From any senders to specific recipients.
2. Click specific senders/ specific recipients.
3. Select Specific accounts on the Select Accounts screen.
4. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list.
5. Search and select AD Users/Groups/Contacts/Special Groups and add them to the Selected Account(s) list on the Exclude Accounts screen.
6. Click Save.
7. Click Next.

Step 2: Specify Policy

To specify the policy:

1. Click the message part to filter for undesirable content. ScanMail can filter email messages by header (From, To, and Cc), subject, body, or attachment.
2. Select whether ScanMail filters content for any specified keywords or for all specified keywords.
   - Any specified keywords tells ScanMail to take action against content that contains any of the keywords in the list.
   - All specified keywords tells ScanMail to take action against content only when the content contains all of the keywords in the list.
3. Type or import keywords.
   - Type a keyword in the space provided.
   - Click Add to add it to the list of keywords that ScanMail checks when filtering content.
   - Click Remove to remove keywords from the list.

Note: By default, ScanMail searches for exact matches of the keywords that you add.
**TABLE 5-6. Imported text file for content filtering**

<table>
<thead>
<tr>
<th>THE IMPORTED TEXT FILE contains</th>
<th>THE KEYWORD LIST DISPLAYS</th>
</tr>
</thead>
<tbody>
<tr>
<td>win cash prize</td>
<td>win cash prize</td>
</tr>
<tr>
<td>win</td>
<td>win</td>
</tr>
<tr>
<td>cash</td>
<td>cash</td>
</tr>
<tr>
<td>prize</td>
<td>prize</td>
</tr>
</tbody>
</table>

**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.

4. (Optional) Click **Match case-sensitive** to have ScanMail disregard words that do not match the keyword's case when filtering content.

5. (Optional) Configure a list of synonyms.
   - Click **Match synonym** to have ScanMail consider all the synonyms of the keyword when filtering content.
   - Click **Show details** next to Match synonym to display the list of synonyms. When you select a keyword, all of the keyword's synonyms display in the Synonyms to exclude list. Use the arrow keys to add and delete synonyms for each corresponding keyword.

6. Click **Next**
Step 3: Specify Actions

To configure the action ScanMail takes against content that matches a keyword:

1. Select an action for ScanMail to take when it detects undesirable content. ScanMail can perform the following actions when it detects content that matches the policy conditions:
   - **Replace with text/file**: ScanMail replaces the filtered content with a text file. You cannot replace text from the From, To, Cc, or Subject fields
     
     **Note:** 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 the quarantine directory.
   - **Quarantine message part**: ScanMail quarantines the message body or the attachment file of the message.
     
     **Note:** ScanMail does not perform this action in transport level scans when the violation is in the header/subject of the email message.
   
   - **Delete entire message**: ScanMail deletes the entire email message.
   - **Backup**: ScanMail delivers backed up email messages to the intended recipient and keeps a copy of the message in the specified backup directory.
   - **Pass message part**: Records the violation event in the content filtering logs, but take no action on the message part. This does not apply to low priority policies.

2. To notify specific individuals:
   a. Select the check box **Forward to sender's manager**.
   b. Select the check box **Forward to specific email address(es)** and type the email address of the recipients.

3. Select **Notify** to configure ScanMail to notify the designated individuals when it takes action against undesirable content. Select **Do not notify** for ScanMail to execute the actions, but not notify the designated individual.

4. Click **Next**.
Step 4: Specify Notifications

To configure the notifications ScanMail sends when it takes an action:

1. Click on the check boxes corresponding to the people ScanMail will notify.
2. Click Show details to customize the notification for that recipient.
3. Select from the notification options. Refer to Notifications on page 5-8 for details.
4. Click Write to Windows event log to have ScanMail write the notification to a Windows event log.
5. Click Next >.

Step 5: Name & Priority

To enable content filtering policies:

1. Select Enable to enable this policy.
2. Type the name of your policy in the Policy name space.
3. Type the priority of your policy in the Priority space.
4. Click Save.

Adding 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.

To add a content filtering exception policy:

1. Log on to the product console.
2. Click Content Filtering from the main menu. The Content Filtering screen displays.
3. Click Add and select Exceptions from the drop down menu.
4. Type an email address under Enter address(es).
5. Click Add. The email address appears in the list.
6. Click Next after adding all addresses. The Name and Priority screen displays.
7. Type a Policy name.
8. Type a number for the Priority.
9. Click Save.

Configuring Data Loss Prevention

Before you can monitor sensitive data for potential loss, you must first define the digital assets and template rules for your company. Data identifiers act as the foundation rules for defining digital assets; templates act as the foundation rules for policy management.

After defining your company's sensitive data, create policies to monitor the email traffic across your network.

For more information on Data Loss Prevention, see About Data Loss Prevention on page 1-35.

Defining Data Identifiers

ScanMail uses data identifiers to identify sensitive information. Data identifiers include expressions and keyword lists.

Adding and Editing Expressions

Create customized expressions if none of the predefined expressions meet your requirements. For details about data identifier expressions, see Expressions on page 1-36.

To add or edit an expression:

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, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will 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

See Customized Expressions on page 1-36 for details about the criteria and additional settings.
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 if you are satisfied with the result.

**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**

Use this option if you have a properly-formatted .dat file containing the expressions. You can generate the file by exporting the expressions from either the ScanMail server you are currently accessing or from another ScanMail server.

To import expressions:
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, informing you if the import was successful.

**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 pre-existing expression and adds the new expression to the list.

## Adding and Editing Keyword Lists

Keywords are special words or phrases. You can 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 your requirements. For details about data identifier keyword lists, see [Keyword Lists](#) on page 1-39.

**To add a keyword list:**

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
   
   See [Customized Keyword Lists](#) on page 1-39 for details about the criteria and additional settings.
7. To manually add keywords to the list:
**Configuring Scanning**

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

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

**Importing Keyword Lists**

Use this option if you have a properly-formatted .dat file containing the keyword lists. You can generate the file by exporting the keyword lists from either the ScanMail server you are currently accessing or from another ScanMail server.

To import keyword lists:

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 **Import** and then locate the .dat file containing the keyword lists.
4. Click **Open**. A message appears, informing you if the import was successful.

---

**Note:** Each keyword list contains a unique ID value. If a keyword list with the same ID already exists, ScanMail overwrites the existing keyword list. If a keyword list with the same display name already exists, ScanMail appends the suffix “Original” to the pre-existing keyword list and adds the new keyword list to the list.

**Defining Data Loss Prevention Templates**

Data Loss Prevention templates define the sensitive data in your organization using keyword lists and expressions. Define templates to use in Data Loss Prevention policies and protect sensitive information that is specific to your business. For more information on Data Loss Prevention Templates, see **About Data Loss Prevention Templates** on page 1-41.
To define a Data Loss Prevention template:

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

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 $\exists$ 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 $\exists$ control. Remove criteria by clicking the $\Box$ 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 (-trash can) 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.
Modifying Data Loss Prevention Templates

Modify existing template structures to suit your business requirements.

To modify a Data Loss Prevention template:

1. On the left navigation bar, click **Data Loss Prevention > DLP Templates**. A list of Data Loss Prevention templates appears.
2. Click the name of the template you want to edit. The Edit Data Loss Prevention Template screen appears.

---

**Note:** You 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.

---

3. Modify the **Name** and **Description** as necessary.
4. From the drop-down box under **Condition Statement**, beside the $ control, select the criteria **Expressions** or **Keyword Lists**.
5. Select an expression or keyword list from the drop-down box beside the selected criteria.
6. 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.

---

7. Add additional criteria by clicking the $ control. Remove criteria by clicking the $ control.
8. Click **Add** to add the condition to the **Template Definition** list or click **Clear** to clear the condition statement.
9. 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.
10. To remove a definition from the **Template Definition** list, click the delete icon (🗑️) to the right of the definition.
11. Click **Save**. The Data Loss Prevention Templates screen appears.

### Deleting a Data Loss Prevention Template

**Note:** You 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.

To delete a Data Loss Prevention template:

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

You can import Data Loss Prevention templates from other ScanMail servers or other Trend Micro products to keep pre-defined rules consistent throughout your organization.

To import a Data Loss Prevention template:

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

**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 pre-existing template and adds the new template to the list.

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 pre-defined rules consistent throughout your organization.

**To export a Data Loss Prevention template:**

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.
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.

---

**Understanding Data Loss Prevention Policies**

When you enable Data Loss Prevention, 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.

**Creating a Data Loss Prevention Policy**

Data Loss Prevention policies govern the actions ScanMail takes when it discovers sensitive information in email messages (see About Data Loss Prevention Policies on page 1-42).

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

1. **Step 1: Select Accounts** on page 5-36
2. **Step 2: Specify Rule** on page 5-37
3. **Step 3: Specify Action** on page 5-37
4. **Step 4: Specify Notification** on page 5-39
5. **Step 5: Name and Priority** on page 5-39

**Step 1: Select Accounts**

To select accounts that the policy applies to:

1. On the left navigation pane, click **Data Loss Prevention > DLP Policies**. The Data Loss Prevention Policies screen appears.
3. Select **Anyone** to apply the policy to everyone in the organization. If you want to apply this policy to specific groups, users, or contacts, select **Specific accounts**:
   a. In the drop-down box under Specific accounts, select **Browse from special groups** to view a list of special user groups (see Configuring Special Groups on page 8-7). To view a list of AD users, groups, or contacts, select **Search for AD users/ groups/ contacts**:
      i. Type the name of the AD users, groups, or contacts you want to search for.
      ii. Select the check box(es) next to **Users, Groups, and/or Contacts**.
   b. Select the desired account from the Available Account(s) and click **Add >>**.
4. Expand the Exclude Accounts screen to select accounts to exclude from the policy.
5. In the drop-down box under Specific accounts, select **Browse from special groups** to view a list of special user groups (see Configuring Special Groups on page 8-7). To view a list of AD users, groups, or contacts, select **Search for AD users/ groups/ contacts**:
   a. Type the name of the AD users, groups, or contacts you want to search for.
   b. Select the check box(es) next to **Users, Groups, and/or Contacts**.
6. Select the desired account from the Available Account(s) and click **Add >>**.
7. Click **Next >** to continue to Step 2: Specify Rule.
Step 2: Specify Rule

To specify a Data Loss Prevention policy rule:

1. 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**, and **Attachment**.

2. Select templates from the list of available templates and click **Add >>** to apply them to your policy.

   **Note:** A Data Loss Prevention policy requires selecting at least one template before activation.

3. In the Available DLP Template(s) toolbar, click **Add** to create a new template (see [Defining Data Loss Prevention Templates](#)) or click **Import** to import a template file (see [Importing a Data Loss Prevention Template](#)).

4. Click **Next >** to continue to Step 3: Specify Action.

Step 3: Specify Action

To configure the actions ScanMail takes when a policy incident occurs:

1. Select an action for ScanMail to take when it detects a policy incident. ScanMail can perform the following actions when it detects content that matches the policy conditions:

   - **Replace with text/file:** ScanMail replaces the filtered content with a text file. You cannot replace text in the From, To, CC, or subject fields.

   **Note:** 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 the quarantine directory.

   - **Quarantine message part:** ScanMail quarantines the message body or the attachment file of the message.
Note: ScanMail does not perform this action in Transport level scans when the violation is in the header/subject of the email message.

- **Delete entire message**: ScanMail deletes the entire email message.
- **Backup**: ScanMail delivers backed up email messages to the intended recipient and keeps a copy of the message in the specified backup directory.
- **Pass message part**: ScanMail records the Data Loss Prevention incident in the Data Loss Prevention logs, but takes no action on the message part.

2. To notify specific individuals:
   a. Select the check box **Forward to sender’s manager**.
   b. Select the check box **Forward to specific email address(es)** and type the email address of the recipients.

3. Select **Notify** to configure ScanMail to notify the designated individuals when it takes action against undesirable content. Select **Do not notify** for ScanMail to execute the actions, but not notify the designated individual.

4. Configure Advanced Options by clicking the setting name.
   - **Quarantine and Backup Settings**: Specify the folder location to store quarantined messages.
   - **Replacement Settings**: Specify the file name and text to replace the text that violated a policy rule. This will inform users of the quarantined status of the message when you select **Quarantine message part** or **Replace with text/file**.
   - **Forward Email Message Settings**: Specify the Subject and Message text that ScanMail forwards to the selected recipients.

5. Click **Next >** to continue to Step 4: Specify Notification.
Step 4: Specify Notification

To configure the notifications ScanMail sends when it takes an action:

1. Select the check box(es) corresponding to the people ScanMail will notify.
2. Click **Show details** to customize the notification for that recipient. Refer to **Notifications** on page 5-8 for details.
3. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.
4. Click **Next >** to continue to Step 5: Name & Priority.

Step 5: Name and Priority

To enable Data Loss Prevention policies:

1. Select **Enable this policy** to enable this policy.
2. Type the name of your policy in the **Policy name** space.
3. Type the priority of your policy in the **Priority** space.
4. Click **Finish** to save the policy.

Modifying a Data Loss Prevention Policy

Modify existing policies to suit your business requirements.

To modify a Data Loss Prevention policy:

1. On the left navigation pane, click **Data Loss Prevention > DLP Policies** and click the policy name that you want to modify. The **Target** tab on the Data Loss Prevention: Edit Policy screen appears.
2. Modify the necessary components in the **Accounts**, **Target**, **Action**, and/or **Notification** tabs. For details about the available settings in these tabs, see **Creating a Data Loss Prevention Policy** on page 5-35.
3. Click **Save** to save your changes.
Deleting a Data Loss Prevention Policy

Delete old policies that no longer apply to your business strategy.

To delete a Data Loss Prevention policy:
1. On the left navigation pane, click Data Loss Prevention > DLP Policies. Select the check box next to the policy you want to delete.
2. On the Policy list toolbar, click the Delete button.

Configuring Spam Prevention

ScanMail provides two powerful spam prevention features to protect your network resources:

- Email Reputation
- Content scanning

In order to use Email Reputation and content scanning, you must first configure each feature’s target settings, actions, and enable the feature. For more information on Spam Prevention, see About Spam Prevention on page 1-42.

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.

For more information on Email Reputation, see About Email Reputation on page 1-43.

Configuring Email Reputation Targets

To configure Email Reputation target settings:
1. Log on to the product console.
2. Click Spam Prevention > Email Reputation. The Email Reputation screen displays.
3. Configure the following settings:
   - Click Smart Protection Network portal to configure advanced settings.
• Type an approved IP address and click Add.
4. Click Save.

Configuring Email Reputation Actions

To configure Email Reputation action settings:
1. Log on to the product console.
2. Click Spam Prevention > Email Reputation. The Email Reputation screen displays.
3. Click the Action tab.
4. Select one of the following for the Standard Reputation Database:
   • 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.
   • Bypass.
5. (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.
   • Bypass.
6. Click Save.

Enabling Email Reputation

To enable Email Reputation:
1. Log on to the product console.
2. Click Spam Prevention > Email Reputation. The Email Reputation screen displays.
3. Select Enable Email Reputation.
4. Click Save.
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.

For more information on Content Scanning, see About Content Scanning on page 1-44.

Configuring Content Scanning Targets

To configure Content Scanning target settings:

1. Log on to the product console.
2. Click Spam Prevention > Content Scanning. The Content Scanning screen displays.
3. Select a detection level. Select Low, Medium, or High from the Spam Detection Rate list. ScanMail uses this rate to screen all messages.
4. Select Detect phishing to scan for phishing email messages.
5. Add addresses to the list of Approved Senders and Blocked Senders.
6. Click Save.
Configuring Content Scanning Actions

To configure Content Scanning action settings:
1. Log on to the product console.
2. Click Spam Prevention from the main menu. A drop down menu displays.
3. Click Content Scanning from the drop down menu. The Content Scanning screen displays.
4. Select one of the following actions for Spam messages:
   • Quarantine message to user’s spam folder
   • Delete entire message
   • Tag and deliver
5. Select one of the following actions for Phishing messages:
   • Delete entire message
   • Tag and deliver
6. Click Save.

Enabling Content Scanning

To enable content scanning:
1. Log on to the product console.
2. Click Spam Prevention > Content Scanning. The Content Scanning screen displays.
3. Select Enable content scanning.
4. Click Save.

Configuring Web Reputation

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.
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 1-21.

To configure Web Reputation scan service settings:

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.
      i. 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 5-2.
4. Click Save.

Configuring Web Reputation Targets

To configure Web Reputation target settings:

1. Log on to the product console.
2. Click **Web Reputation** from the main menu. The Web Reputation screen displays.
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 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

**To configure Web Reputation action settings:**

1. Log on to the product console.
2. Click **Web Reputation** from the main menu. The Web Reputation screen displays.
3. Click the **Action** tab. The Action screen displays.
4. Select an action.
5. Select **Take action on URLs that have not been assessed by Trend Micro** to apply a strict Web Reputation policy.
6. Select **Notify** or **Do not notify**.
7. Click **Save**.

### Configuring Web Reputation Notifications

**To configure Web Reputation notification settings:**

1. Log on to the product console.
2. Click **Web Reputation** from the main menu. The Web Reputation screen displays.
3. Click the **Notification** tab. The Notification screen displays.
4. Select the check boxes corresponding to the people ScanMail will notify. Refer to **Notifications** on page 5-8 for details.
5. Click **Write to Windows event log** to have ScanMail write the notification to a Windows event log.

6. Click **Save**.

**Enabling Web Reputation**

To enable Web Reputation:

1. Log on to the product console.
2. Click **Web Reputation** from the main menu. The Web Reputation screen displays.
3. Select **Enable Web Reputation**.
4. Click **Save**.
Chapter 6

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 6-2
- Configuring the Quarantine Folder/Directory on page 6-2
- Scheduling Automatic Quarantine Maintenance on page 6-3
- Manually Performing Quarantine Maintenance on page 6-4
- Resending Quarantined Messages on page 6-4
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.

To specify a global directory:

1. Click Content Filtering from the main menu.
2. Click Global Settings on the Content Filtering Policy toolbar. The Content Filtering > Global Settings screen opens.
3. Type the directory path under Quarantine Directory that you want ScanMail to use as the global quarantine directory.
4. Click Apply to All.

ScanMail will move all files that violate content filtering rules to the directory you specify.

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

Performing a Quarantine Query

To perform a quarantine query:

1. Log on to the product console.
2. Click **Quarantine** from the main menu and click **Query** from the drop down menu. The Quarantine Query screen displays.
3. Select the date range.
4. Select the reasons.
5. Select the resend status.
6. (Optional) Specify the sender, recipient, and/or subject of the message.
7. Specify the option for **Sort by**.
8. Specify the number of items to display per page.
9. Click **Search**.

Scheduling Automatic Quarantine Maintenance

Configure scheduled deletion of quarantined messages or manually delete quarantined messages from the Quarantine Maintenance screen.

To schedule automatic deletion of quarantined messages:

1. Log on to the product console.
2. Click **Quarantine** from the main menu and click **Maintenance** from the drop down menu. The Quarantine Maintenance screen displays.
3. Click the **Automatic** tab.
4. Select the files to delete.
5. Specify the number of days to keep files before deleting.
6. Click **Save**.
Manually Performing Quarantine Maintenance

To manually delete quarantined messages:

1. Log on to the product console.
2. Click Quarantine from the main menu and click Maintenance from the drop down menu. The Quarantine Maintenance > Manual screen displays.
3. Select the files to delete.
4. Specify the number of days to keep files before deleting.
5. Click Delete Now to delete messages.

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.

To resend quarantined messages:

1. Log on to the product console.
2. Click Quarantine from the main menu and click Query from the drop down menu. The Quarantine Query screen displays.
3. 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.
4. Select the email messages that you want to resend from the results of your query.
5. Click Resend. The Quarantine > Resend screen opens displaying resending options.
6. Click Add original recipients to have ScanMail send the email message to the original recipient.
7. 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 2010 and 2007 Edge Transport server role.

8. 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.

9. Type a message in the **Body** field for ScanMail to use as the body of your resent email message.

10. 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).

11. Click **Resend Now**. ScanMail sends the email message immediately. A progress bar appears to show you the progress of the resend process.

12. When the Resend process is complete, click **OK** to return to the Quarantine Query screen.

---

**WARNING!** Automatically deleting messages after resending deletes the quarantine record in the database.
Monitoring ScanMail

This chapter describes notifications, reports, and logs to help you monitor your network.

Topics include:

• About Alerts on page 7-4
• About Reports on page 7-7
• About Logs on page 7-11
Viewing the Summary Screen

The Summary screen provides a simple and current report on the ScanMail system and functions. Monitor detections, whether components are current, and if updates were successful. To see more detailed information, generate reports from the Reports menu.

Summary: System

A brief description of the options available on this screen is available below.

- **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**: The number of detected viruses/malware that could not be cleaned.

- **Detected spyware/grayware**: The number of detected spyware/grayware.

- **Blocked attachments**: The number of attachments blocked by the attachment blocking policy.

- **Spam messages**: The number of spam messages detected by content scanning.

- **Phishing messages**: The number of phishing messages detected by content scanning.

- **Content filtering violations**: The number of content filtering rule violations detected.

- **Suspicious URLs - Web reputation**: The number of suspicious URLs detected by Web reputation.

- **Data Loss Prevention incidents**: The number of Data Loss Prevention policy incidents detected.

- **Blocked connections - Email reputation**: 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**: The number of message body and attachments not scanned as specified by the Scan Restriction Criteria.

- **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**: Use this information to determine whether your components are current.

• **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**

You can monitor the status of security risk detections from this screen.

A brief description of the options available on this screen is available below.

• **Security Risk Summary for Today**: View the total number of security risks detected and the percentage of those that were uncleanable and spyware/grayware.

• **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.

• **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.
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.

A brief description of the options available on this screen is available below.

- **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).
- **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

You can configure ScanMail to send notifications to designated individuals when significant system events or security outbreaks occur. Notifications can be sent by email and Simple Network Management Protocol (SNMP) and written to a Windows event log.

System Events

A brief description of the options available on this screen is available below (**Alerts > System Events**).

- **ScanMail service did not start successfully**: ScanMail service was not started successfully.
- **ScanMail service is unavailable**: ScanMail for Microsoft Exchange Master Services stopped unexpectedly.
- **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.

• **Update - Each time update was**: the update is successful or unsuccessful.

• **Update - Last update time is older than**: the last update time is older than the time you specify.

• **Manual/ Scheduled scan tasks were**: the scan tasks are successful or unsuccessful.

  This option does not display for Exchange Server 2010 and 2007 Edge/ Hub Transport server roles.

• **Manual/ Scheduled scan time exceeds**: the time to perform scan tasks exceeds the time you specify.

  This option does not display for Exchange Server 2010 and 2007 Edge/ Hub Transport server roles.

• **The disk space on the local drive (volume) of the backup, quarantine, and archive directory is less than**: the available disk space reaches the minimum you specify.

• **The quarantine and log database size exceeds**: 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.

  If ScanMail is not registered to Control Manager this does not display.

• **Outbreak Prevention Mode stopped and restored configuration successfully**: ScanMail is no longer in Outbreak Prevention Mode.

  If ScanMail is not registered to Control Manager this does not display.

• **The SMTP messages queued continuously exceeds the following number within the specified time**: the SMTP messages queued exceeds the number you specify within a time frame.

  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**: the available disk space reaches the minimum you specify.

  This option does not display for Exchange Server 2010 and 2007 Edge/ Hub Transport server roles.
• **The mail store size exceeds**: the mail store size exceeds the size you specify. This option does not display for Exchange Server 2010 and 2007 Edge/Hub Transport server roles.

Note: To use Microsoft™ Operations Manager (MOM) or 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 Microsoft™ Operations Manager (MOM) or System Center Operations Manager (SCOM).

---

**Outbreak Alerts**

A brief description of the options available on this screen is available below (Alerts > Outbreak Alert).

• **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.

• **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 on an Outbreak Alert Condition to display the Outbreak Alert notification screen. A brief description of the options available on this screen is available below.

- **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 on a message element and add it to the notification.
  For example, click [Time] and add it to the message list. The notification message will contain the time when ScanMail took the action.
- **SNMP**: Select to send SNMP notifications.
- **IP address**: Specify the SNMP IP address.
- **Community**: Specify the SNMP Community name.
- **Write to Windows event log (Select this to allow Microsoft™ Operations Manager 2005 and Microsoft™ System Center Operations Manager 2007 to retrieve the Windows event log for alerts.)**: Select to send notifications to Windows event log.

**Note:** To use Microsoft™ Operations Manager (MOM) or 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 Microsoft™ Operations Manager (MOM) or System Center Operations Manager (SCOM).

About Reports

You can generate reports to view ScanMail log events in an organized and graphically appealing format. Reports can be printed or sent by email to a specified address. You configure the number of reports you want ScanMail to save from the Report Maintenance page. When the number of reports exceeds the number you set, the excess reports are deleted beginning with the report that has been retained for the longest time.

Example: If you have 15 reports and you set 10 for the maximum number of reports to save, 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. You can then print or email the one-time report.

ScanMail saves generated reports in a cache so that you can view them at a later time. ScanMail retains reports until you delete them manually or ScanMail deletes them by following the report maintenance settings.

A brief description of the options available on this screen is available below.

- **Generate Report**: Click to generate a new report.
- **Delete**: Click to delete a report.
- **View**: Click to view that report.
- **Page**: Jumps to the page that you specify
- **Rows per page**: Displays 10, 20, or All rows per page.

Generating One-time Reports

The following lists the procedure required to generate a one-time report.

**To generate a one-time report:**

1. Click **Reports > One-time Reports** to open the One-time Reports screen.
2. Click **Generate report**. The screen expands to display report options.
3. Type a name for the **Report**.
4. Set the time range by typing a date or clicking the calendar icon to select a date. ScanMail gathers data to include in your report for the time range you specify.
5. Click the type of information that you want ScanMail to gather for your report. Click next to the report type to view detailed options for that report.
   - **Scan status summary**
   - **Security risk scan report**
   - **Attachment blocking report**
   - **Content filtering report**
   - **Data Loss Prevention report**
   - **Spam report**
• Unscannable message report
• Web Reputation report
• Traffic report

6. Click Generate.

Note: When using Secure Sockets Layer (SSL) protocol, the SQL statement used to generate the report cannot be viewed.

Scheduled Reports

ScanMail generates scheduled reports according to the schedule you set. Schedules are daily, weekly, or monthly. ScanMail generates the report at the time you specify. ScanMail can be set to deliver reports by email to an administrator or other recipient.

Scheduled reports follow a template. To generate individual scheduled reports you first set up the template and then ScanMail generates reports according to that template. You specify the schedule and the content that you want to include in each individual report for the report template. Then, at the time you specified in the template, ScanMail generates a report. Each template can have many individual reports that can be viewed by clicking List Reports from the Scheduled Reports screen. You can view the content of the template by clicking the template name.

A brief description of the options available on this screen is available below.

• Add: Select to specify a new report template.
• Delete: Select to delete a report template.
• Report Template: Select the check box next to Report Template to select that report.
• Page: Jumps to the page that you specify
• Rows per page: Displays 10, 20, or All rows per page.
Generating Scheduled Reports

The following lists the procedure required to generate a scheduled report.

To set up a scheduled report template:

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 your report template.
4. Specify the schedule that the template uses to generate individual reports. It 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: If you specify the schedule to be weekly every Sunday and configure 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 type of report that ScanMail generates according to your schedule.
7. Set a person to receive a report each time the template generates one.
8. Click Send to email:
9. Type the recipient's email address
10. Click Save. The browser returns to the Scheduled Reports screen. The new template is added to the list of Report templates.

Note: When using Secure Sockets Layer (SSL) protocol, the SQL statement used to generate the report cannot be viewed.
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 your specified limit, excess reports are deleted, beginning with the report that has been retained the longest amount of time. For scheduled reports saved in each template, the number that you type limits the amount of saved reports for each template.

For example, you have five saved report templates: Report-virus, Report-spam, Report-blocking, Report-content, and Report-traffic. You set the limit for Scheduled reports saved in templates to 4. This means that each template can generate four individual reports, for a total of 20 reports (5 templates x 4 reports each). If the Report-virus template generated another report, then ScanMail would delete the oldest generated report for that template, keeping the total number of reports at 20.

A brief description of the options available on this 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 of security risk scan, content filtering, attachment blocking, web reputation, updates, scan events, unscannable message parts, back up, and event tracking. These logs provide a valuable source of system information. You can use them when analyzing your system security and configuring ScanMail to provide optimal protection for your Exchange environment.

To view log information, you must perform a log query. You can use the Log Query page to set up and run your queries.
Types of Logs

The following table lists the type of logs:

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk Scan</td>
<td>Information about messages with detected security risks.</td>
</tr>
<tr>
<td>Attachment Blocking</td>
<td>Information about the messages with attachments that ScanMail scanned and blocked.</td>
</tr>
<tr>
<td>Content Filtering</td>
<td>Information about the messages ScanMail filtered for undesirable content.</td>
</tr>
<tr>
<td>Updates</td>
<td>Information about whether components were updated successfully. Components include scan engines and pattern files.</td>
</tr>
<tr>
<td>Scan Events</td>
<td>Information about whether manual and scheduled scans have been successful or unsuccessful.</td>
</tr>
<tr>
<td>Backup for Security Risk</td>
<td>Information about the files that Security Risk Scan moved to the backup folder before taking action against them.</td>
</tr>
<tr>
<td>Backup for Content Filter</td>
<td>Information about the files that Content Filtering moved to the backup folder before taking action against them.</td>
</tr>
<tr>
<td>Unscannable Message Parts</td>
<td>Information about message parts not scanned as defined by the Scan Restriction Criteria.</td>
</tr>
<tr>
<td>Event Tracking</td>
<td>Information about all product console operations.</td>
</tr>
</tbody>
</table>

*Note:* Scan events do not display for Exchange Server 2010 and 2007 edge/hub transport server roles.
TABLE 7-1. Log types (Continued)

<table>
<thead>
<tr>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Loss Prevention</td>
<td>Information about messages that triggered Data Loss Prevention policy incidents.</td>
</tr>
<tr>
<td>Backup for Data Loss Prevention</td>
<td>Information about the files that Data Loss Prevention moved to the backup folder before taking action against them</td>
</tr>
<tr>
<td>Web Reputation</td>
<td>Information about messages that ScanMail detected with malicious URLs.</td>
</tr>
</tbody>
</table>

Log Query

A brief description of the options available on this screen is available below (Logs > Query).

- **Dates**: Select the time period to query.
- **Type**: Select the type of log to query.
  - **Security Risk Scan**
  - **Attachment Blocking**
  - **Content Filtering**
  - **Updates**
  - **Scan Events**
  - **Backup for Security Risk**
  - **Backup for Content Filter**
  - **Unscannable Message Parts**
  - **Event Tracking**
  - **Data Loss Prevention**
  - **Backup for Data Loss Prevention**
  - **Web Reputation**
- **Found in**: Specify the location of the email message.
- **Sender**: Specify the sender of the email message.
• **Recipient**: Specify the recipient of the email message.
• **Subject**: Specify the text to search for in the subject.
• **Attachment**: Specify the attachment file name to search for in email messages.
• **Sort by**: Specify the sorting method.
• **Display**: Specify the number of results to display per page.
• **Display Logs**: Click to display the results of the query.

**Querying Logs**

The following lists the procedure required to query logs.

**To query logs:**

1. Log on to the product console.
2. Click **Logs** from the main menu and click **Query** from the drop down menu. The Log Query screen displays.
3. Select the date range.
4. Select the type of entry.
5. (Optional) Specify the any of the following criteria:
   • Found in
   • Sender
   • Recipient
   • Subject
   • Attachment
6. Specify the option for **Sort by**.
7. Specify the number of items to display per page.
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 Log Maintenance

The following lists the procedure required to perform log maintenance.

To manually delete logs:
1. Log on to the product console.
2. Click Logs from the main menu and click Maintenance from the drop down menu. The Log Maintenance > Manual screen displays.
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.

To schedule automatic deletion logs:
1. Log on to the product console.
2. Click Logs from the main menu and click Maintenance from the drop down menu. The Log Maintenance screen displays.
3. Click the Automatic tab.
4. Select the logs or events to delete.
5. Specify the number of days to keep logs before deleting.
6. Specify the number of days to keep events before deleting.
7. Click Save.
Performing Administrative Tasks

This chapter describes administrative tasks.

Topics include:
• Configuring Proxy Settings on page 8-2
• Configuring Notification Settings on page 8-2
• Spam Maintenance on page 8-4
• Configuring Real-time Scan Settings on page 8-4
• Access Control Settings on page 8-5
• Configuring Special Groups on page 8-7
• Configuring Internal Domains on page 8-8
• Product License on page 8-9
• Configuring World Virus Tracking Program on page 8-10
• About Trend Micro Control Manager on page 8-11
• Configuring Control Manager Settings on page 8-11
Configuring Proxy Settings

Configure proxy settings if your network uses a proxy server.

To configure proxy settings:

1. Log on to the product console.
2. Click Administration from the main menu and click Proxy from the drop down menu.
3. Select the 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.
4. Type the proxy server name or IP address.
5. Type the Port.
6. (Optional) Select Use SOCKS 5 proxy protocol.
7. If your proxy server requires authentication, specify the user ID and password.

Configuring Notification Settings

You can configure ScanMail to send notifications when it takes actions against various security risks. Usually, notifications are sent to the Exchange administrator, using a global default for the administrator’s email address.

Notifications can be set up for the person who is to receive the notification and the person who is listed as the sender for the notification. That is, when ScanMail sends notifications, it lists the address that you set up in this screen as the sender of the message. People receiving the message can contact the sender that you describe about the problem.

Setting a global default address for an administrator and applying the address, changes the address in the following locations:

- Security Risk Scan
- Attachment Blocking
- Content Filtering
- Data Loss Prevention
Performing Administrative Tasks

• Spam Prevention
• Web Reputation
• System Alerts
• Outbreak Alerts

Note: You can customize the notification addresses for each of the above locations after you apply 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 when it does the following:
• 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), 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.
To configure global notification settings:

1. Log on to the product console.
2. Click Administration from the main menu and click Notification Settings from the drop down menu.
3. Type the email address of the administrator that will receive notifications.
4. Type the email address of the sender who will send alerts and notifications.
5. Specify an SNMP IP address and community.
6. 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.
7. Click Save.

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.

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.

To configure Real-time Scan Settings:

1. Log on to the product console.
2. Click Administration from the main menu and click Real-time Scan Settings from the drop down menu.
3. Select the Do not perform on-access scan on email messages older than the following number of days check box.
4. Specify the number of days.
5. Click Save.
About Access Control

Use the role based administration feature to grant and control access to ScanMail product console menu and submenu items. If there are multiple ScanMail administrators in your organization, this feature can help you delegate management tasks to administrators and manage the menu items accessible to each administrator. In addition, you can 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 Settings

A brief description of the options available on this screen is available below.

- **Enable Single Sign-On:** Select 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.
- **Role:** Click a role name to configure settings for that role.
- **Status:** Click the icon under Status to enable or disable the role.
- **Save:** Click to save changes.
- **Reset:** Click to reset to default.
Access Control Permissions

A brief description of the options available on this screen 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>
<thead>
<tr>
<th>Feature</th>
<th>Permission Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update</td>
<td>Operators can configure manual updates.</td>
</tr>
<tr>
<td>Logs</td>
<td>Operators can query logs.</td>
</tr>
<tr>
<td>Report</td>
<td>Operators can generate logs.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Operators can query quarantined messages and files.</td>
</tr>
</tbody>
</table>

- **None**: Select to hide this feature from users in this group.

Configuring Access Control

The following lists the procedure required to configure access control.

**To enable Access Control:**

1. Log on to the product console.
2. Click **Administration** from the main menu and click **Access Control** from the drop down menu. The Access Control > Authentication screen displays.
3. Click the icon under **Status** to display a green check icon (✔) indicates the policy is disabled, which indicates that the access role is enabled.
4. (Optional) Click **Enable Single Sign-on**.
5. Click **Save**.
To configure Access Control:

1. Log on to the product console.
2. Click **Administration** from the main menu and click **Access Control** from the drop down menu. The Access Control > Authentication screen displays.
3. Click **Administrator** or **Operator**.
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**.

### Special Groups

Special groups can be used in attachment blocking and content filtering exception policies. Create groups of Active Directory (AD) users/groups/contacts and email addresses to easily apply policies to segments of your network. Special groups can be imported or exported for ease of management. Special groups cannot contain other special groups.

If an Active Directory user belonging to a special group is deleted, ScanMail displays a notification message in the Special Group Selected Contact list.

### Configuring Special Groups

Configure special groups for ease of management when creating rules and policies.

**To add a Special Group:**

1. Log on to the product console.
2. Click **Administration** from the main menu and click **Special Groups** from the drop down menu. The Special Group screen displays.
3. Click **Add**. The Add Special Group screen displays.
4. Type a name for the special group and specify a description.
5. Search for Active Directory (AD) users/groups/contacts to add to the special group or specify an SMTP address.

6. Click **Add** to add accounts or **Delete** to delete accounts from this special group.

7. Click **Save**.

**To edit a Special Group:**

1. Log on to the product console.

2. Click **Administration** from the main menu and click **Special Groups** from the drop down menu. The Special Group screen displays.

3. Click the special group to edit. The Edit Special Group screen displays.

4. Add or delete accounts from this special group.

5. Click **Save**.

**Configuring 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 (.)

**Valid wildcard examples:**

- *.smex.com
- *yourcompany.com

**Invalid wildcard examples:**

- *smex.com
- smex.*.com
- smex.*
Performing Administrative Tasks

To configure internal domains:

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

A brief description of the options available on this screen is available below.

• Update License: Click to update your 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](http://www.smartprotectionnetwork.com)

### Configuring World Virus Tracking Program

**To join the World Virus Tracking Program:**

1. Log on to the product console.
2. Click **Administration** from the main menu and click **World Virus Tracking** from the drop down menu.
3. Select **Yes**.
4. Click **Save**.
About Trend Micro Control Manager

Trend Micro™ Control Manager™ is a software management solution that gives you the ability 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.

Configuring Control Manager Settings

Control Manager is a software management solution that gives you the ability 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.

• **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

- You can have multiple ScanMail share the same configuration 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.
• You 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 will update its own virus pattern file and other updates.

• For more information, see the Control Manager documentation.

Registering to Control Manager

You can manage ScanMail using the Trend Micro Control Manager management console. However, you must first install a Control Manager agent on the ScanMail server (during Setup) and then register it with the Control Manager server.

To register ScanMail to a Control Manager server:

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 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.
To unregister ScanMail from the Control Manager server:

1. Click **Administration > Control Manager Settings**. The Control Manager Settings screen displays.
2. Under **Connection Status**, click **Unregister**. A progress screen displays.

**Note:** During Outbreak Prevention, you are not able to unregister from Control Manager or disable communication between the ScanMail MCP agent and the Control Manager server.

---

**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.

**To use the Trend Support/System Debugger:**

1. Log on to the product console.
2. Click **Trend Support/ Debugger** from the main menu. The Trend Support/ System Debugger screen displays.
3. Select the modules to download.
4. Click **Apply**.
Understanding Security Risks

This chapter describes security risks to help you understand possible risks to your network.

Topics include:

- Understanding the Terms on page 9-2
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 Exchange servers 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 9-1. Internet Security Risks**

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial-of-Service (DoS) attack</td>
<td>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.</td>
</tr>
<tr>
<td>Phish</td>
<td>Unsolicited email requesting user verification of private information, such as credit card or bank account numbers, with the intent to commit fraud.</td>
</tr>
<tr>
<td>Spyware/Grayware</td>
<td>Technology that aids in gathering information about a person or organization without their knowledge.</td>
</tr>
</tbody>
</table>
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:

- **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.
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.

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, loss 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. Because a Trojan does not infect a file, there is nothing to clean, though the scan engine may report the file as "uncleanable" and delete it, quarantine it, or 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.
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.

About 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.
About 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, MSCO MP, 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.
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 500KB, that, when decompressed, may reach 15GB 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 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 Exchange 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.

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.
Types of spyware/grayware

ScanMail can detect several types of grayware, including the following:

- **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**: changes computer Internet settings and can force a computer to dial pre-configured phone numbers through a modem.
- **Joke Programs**: causes abnormal computer behavior, such as closing and opening the CD-ROM tray and displaying numerous message boxes.
- **Hacking Tools**: helps hackers enter computers.
- **Remote Access Tools**: help hackers remotely access and control computers.
- **Password Cracking Applications**: helps 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:

- **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.
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).

<table>
<thead>
<tr>
<th>PREFIX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>No prefix</td>
<td>Boot sector viruses or file infector</td>
</tr>
<tr>
<td>1OH</td>
<td>File infector</td>
</tr>
<tr>
<td>ADW</td>
<td>Adware</td>
</tr>
<tr>
<td>ALS</td>
<td>Auto-LISP script malware</td>
</tr>
<tr>
<td>ATVX</td>
<td>ActiveX malicious code</td>
</tr>
<tr>
<td>BAT</td>
<td>Batch file virus</td>
</tr>
<tr>
<td>BHO</td>
<td>Browser Helper Object - A non-destructive toolbar application</td>
</tr>
<tr>
<td>BKDR</td>
<td>Backdoor virus</td>
</tr>
<tr>
<td>CHM</td>
<td>Compiled HTML file found on malicious websites</td>
</tr>
<tr>
<td>COOKIE</td>
<td>Cookie used to track a user's web habits for the purpose of data mining</td>
</tr>
<tr>
<td>COPY</td>
<td>Worm that copies itself</td>
</tr>
<tr>
<td>PREFIX</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>DI</td>
<td>File infector</td>
</tr>
<tr>
<td>DIAL</td>
<td>Dialer program</td>
</tr>
<tr>
<td>DOS, DDOS</td>
<td>Virus that prevents a user from accessing security and antivirus company websites</td>
</tr>
<tr>
<td>ELF</td>
<td>Executable and Link format viruses</td>
</tr>
<tr>
<td>EXPL</td>
<td>Exploit that does not fit other categories</td>
</tr>
<tr>
<td>FLOODER</td>
<td>Tool that allows remote malicious hackers to flood data on a specified IP, causing the target system to hang</td>
</tr>
<tr>
<td>FONO</td>
<td>File infector</td>
</tr>
<tr>
<td>GCAE</td>
<td>File infector</td>
</tr>
<tr>
<td>GENERIC</td>
<td>Memory-resident boot virus</td>
</tr>
<tr>
<td>HKTL</td>
<td>Hacking tool</td>
</tr>
<tr>
<td>HTML</td>
<td>HTML virus</td>
</tr>
<tr>
<td>IRC</td>
<td>Internet Relay Chat malware</td>
</tr>
<tr>
<td>JAVA</td>
<td>Java malicious code</td>
</tr>
<tr>
<td>JOKE</td>
<td>Joke program</td>
</tr>
<tr>
<td>JS</td>
<td>JavaScript virus</td>
</tr>
<tr>
<td>NE</td>
<td>File infector</td>
</tr>
<tr>
<td>NET</td>
<td>Network virus</td>
</tr>
<tr>
<td>PALM</td>
<td>Palm PDA-based malware</td>
</tr>
<tr>
<td>PREFIX</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PARITY</td>
<td>Boot virus</td>
</tr>
<tr>
<td>PE</td>
<td>File infector</td>
</tr>
<tr>
<td>PERL</td>
<td>Malware, such as a file infector, created in PERL</td>
</tr>
<tr>
<td>RAP</td>
<td>Remote access program</td>
</tr>
<tr>
<td>REG</td>
<td>Threat that modifies the system registry</td>
</tr>
<tr>
<td>SPYW</td>
<td>Spyware</td>
</tr>
<tr>
<td>SYMBOS</td>
<td>Trojan that affects telephones using the Symbian operating system</td>
</tr>
<tr>
<td>TROJ</td>
<td>Trojan</td>
</tr>
<tr>
<td>UNIX</td>
<td>Linux/UNIX script malware</td>
</tr>
<tr>
<td>VBS</td>
<td>VBScript virus</td>
</tr>
<tr>
<td>WORM</td>
<td>Worm</td>
</tr>
<tr>
<td>W2KM, W97M, X97M, P97M, A97M, O97M, WM, XF, XM, V5M</td>
<td>Macro virus</td>
</tr>
</tbody>
</table>
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 10

Getting Support and Contacting Trend Micro

This chapter discusses how to perform miscellaneous administrator tasks as well as how to get technical support.

Topics include:
• Frequently Asked Questions on page 10-2
• Troubleshooting on page 10-25
• Update the Pattern File Manually on page 10-26
• Contacting Technical Support on page 10-28
• Before Contacting Technical Support on page 10-29
• Contacting Trend Micro on page 10-29
• Knowledge Base on page 10-30
• Security Information Site on page 10-31
• Email Technical Support on page 10-31
Frequently Asked Questions

Why I Am 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:

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:

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.

**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 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.

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 10-1. Using Operators with Keywords

<table>
<thead>
<tr>
<th>SUPPORTED KEYWORD</th>
<th>HOW IT WORKS</th>
<th>HOW TO USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any keyword</td>
<td>ScanMail searches content that matches the word</td>
<td>Type the word and add it to the keyword list</td>
</tr>
</tbody>
</table>
**TABLE 10-1. Using Operators with Keywords (Continued)**

<table>
<thead>
<tr>
<th>SUPPORTED KEYWORD</th>
<th>HOW IT WORKS</th>
<th>HOW TO USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>OR</td>
<td>ScanMail searches for any of the keywords separated by OR</td>
<td>Type &quot;.OR.&quot; between all the words you want to include</td>
</tr>
<tr>
<td></td>
<td>For example: apple OR orange. ScanMail searches for either apple or orange.</td>
<td>For example: apple .OR. orange</td>
</tr>
<tr>
<td>AND</td>
<td>ScanMail searches for all of the keywords separated by AND</td>
<td>Type &quot;.AND.&quot; between all the words you want to include</td>
</tr>
<tr>
<td></td>
<td>For example: apple AND orange. ScanMail searches for both apple and orange.</td>
<td>For example: apple .AND. orange</td>
</tr>
<tr>
<td>NOT</td>
<td>ScanMail excludes keywords following NOT from search.</td>
<td>Type &quot;.NOT.&quot; before a word you want to exclude</td>
</tr>
<tr>
<td></td>
<td>For example: .NOT. juice. ScanMail searches for content that does not contain &quot;juice&quot;. If the message has &quot;orange soda&quot;, there is a match, but if it contains &quot;orange juice&quot;, there is no match.</td>
<td>For example: &quot;.NOT. juice&quot;</td>
</tr>
</tbody>
</table>
### Table 10-1. Using Operators with Keywords (Continued)

<table>
<thead>
<tr>
<th>Supported Keyword</th>
<th>How it Works</th>
<th>How to Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>WILD</td>
<td>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 &quot;valu&quot;, type &quot;.WILD. valu*&quot;. The words Valumart, valucash, and valubucks all match.</td>
<td>Type &quot;.WILD.&quot; before the parts of the word you want to include.</td>
</tr>
<tr>
<td>REG</td>
<td>To specify a regular expression, add a .REG. operator before that pattern (for example, .REG. a.*e).</td>
<td>Type &quot;.REG.&quot; before the word pattern you want to detect. For example: &quot;.REG. a.*e&quot; matches: &quot;ace&quot;, &quot;ate&quot;, and &quot;advance&quot;, but not &quot;all&quot;, &quot;any&quot;, nor &quot;antivirus&quot;</td>
</tr>
</tbody>
</table>
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.

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.

Obtaining the EICAR Test File:

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.
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://subwiz.trendmicro.com/

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://subwiz.trendmicro.com/subwiz

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.

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:
  xxx-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.

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
• Virus scan engine
• Smart Scan Agent pattern
• Anti-spam pattern
• Anti-spam engine
• Spyware pattern
• IntelliTrap pattern
• IntelliTrap exception pattern
• URL filtering engine
To find out which version ScanMail is running:
1. From the main ScanMail menu, click **Summary**.
2. A list of installed components, the current ScanMail version, and update schedules appears.

To find out the latest available patterns:
Open a web browser to the Trend Micro Update Center.

**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.

---

**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 10-2. Decompressed file examples**

<table>
<thead>
<tr>
<th>FILE SIZE (NOT COMPRESSED)</th>
<th>FILE SIZE (COMPRESSED)</th>
<th>RESULT</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 KB</td>
<td>10 KB (ratio is 50:1)</td>
<td>Scanned</td>
</tr>
<tr>
<td>1000 KB</td>
<td>10 KB (ratio is 100:1)</td>
<td>Scanned</td>
</tr>
<tr>
<td>1001 KB</td>
<td>10 KB (ratio is 100.1:1)</td>
<td>Not scanned *</td>
</tr>
<tr>
<td>2000 KB</td>
<td>10 KB (ratio is 200:1)</td>
<td>Not scanned *</td>
</tr>
</tbody>
</table>

* ScanMail takes the action you configure for unscannable files.

**What is a Compression Ratio?**

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

**TABLE 10-3. Compression ratio examples**

<table>
<thead>
<tr>
<th>FILE SIZE (NOT COMPRESSED)</th>
<th>FILE SIZE (COMPRESSED)</th>
</tr>
</thead>
<tbody>
<tr>
<td>500 KB</td>
<td>10 KB (ratio is 50:1)</td>
</tr>
<tr>
<td>1000 KB</td>
<td>10 KB (ratio is 100:1)</td>
</tr>
<tr>
<td>1001 KB</td>
<td>10 KB (ratio exceeds 100:1)</td>
</tr>
<tr>
<td>2000 KB</td>
<td>10 KB (ratio is 200:1)</td>
</tr>
</tbody>
</table>
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 its true file type. In this situation, a user could unintentionally launch even a backup file that has no extension name.

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.
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.
## Counting and Grouping

### TABLE 10-4. Counting and Grouping

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>.</td>
<td>The dot or period character represents any character except new line character.</td>
<td>do. matches doe, dog, don, dos, dot, etc.d.r matches deer, door, etc.</td>
</tr>
<tr>
<td>*</td>
<td>The asterisk character means zero or more instances of the preceding element.</td>
<td>do* matches d, do, doo, dooo, doooo, etc.</td>
</tr>
<tr>
<td>+</td>
<td>The plus sign character means one or more instances of the preceding element.</td>
<td>do+ matches do, doo, dooo, doooo, etc. but not d</td>
</tr>
<tr>
<td>?</td>
<td>The question mark character means zero or one instances of the preceding element.</td>
<td>do?g matches dg or dog but not doog, dooog, etc.</td>
</tr>
<tr>
<td>( )</td>
<td>Parenthesis characters group whatever is between them to be considered as a single entity.</td>
<td>d(eer)+ matches deer or deer-eer or deereeeeer, etc. The + sign is applied to the substring within parentheses, so the regex looks for d followed by one or more of the grouping &quot;eer.&quot;</td>
</tr>
</tbody>
</table>
### TABLE 10-4. Counting and Grouping (Continued)

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>[ ]</code></td>
<td>Square bracket characters indicate a set or a range of characters.</td>
<td>d[aeiouy]+ matches da, de, di, do, du, dy, daa, dae, dai, etc. The + sign is applied to the set within brackets, so the regex looks for d followed by one or more of any of the characters in the set [aei ou y]. 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.</td>
</tr>
<tr>
<td><code>^</code></td>
<td>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.</td>
<td>d[^aeiouy] matches db, dc or dd, d9, d#. d followed by any single character except a vowel.</td>
</tr>
<tr>
<td><code>{ }</code></td>
<td>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.</td>
<td>da{3} matches daaa. d followed by 3 and only 3 occurrences of &quot;r;a&quot;. da{2,4} matches daa, daaa, daaaa, and daaaa (but not daaaaa). d followed by 2, 3, or 4 occurrences of &quot;r;a&quot;. da{4,} matches daaa, daaaaa, daaaaaa, etc. d followed by 4 or more occurrences of &quot;r;a&quot;.</td>
</tr>
</tbody>
</table>
TABLE 10-5.  Character Classes (shorthand)

<table>
<thead>
<tr>
<th><strong>EXAMPLE</strong></th>
<th><strong>WHAT IT MEANS</strong></th>
<th><strong>EXAMPLE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>\d</td>
<td>Any digit character; functionally equivalent to [0-9] or [:digit:]</td>
<td>\d matches 1, 12, 123, etc., but not 1b7. One or more of any digit characters.</td>
</tr>
<tr>
<td>\D</td>
<td>Any non-digit character; functionally equivalent to [^0-9] or [^[:digit:]]</td>
<td>\D matches a, ab, ab&amp;, but not 1. One or more of any character but 0, 1, 2, 3, 4, 5, 6, 7, 8, or 9.</td>
</tr>
<tr>
<td>\w</td>
<td>Any &quot;word&quot; character. That is, any alphanumeric character; functionally equivalent to [_A-Za-z0-9] or [:alnum:]</td>
<td>\w matches a, ab, a1, but not !&amp;. One or more upper- or lower-case letters or digits, but not punctuation or other special characters.</td>
</tr>
<tr>
<td>\W</td>
<td>Any non-alphanumeric character; functionally equivalent to [^A-Za-z0-9] or [^[:alnum:]]</td>
<td>\W matches *, &amp;, but not ace or a1. One or more of any character but upper- or lower-case letters and digits.</td>
</tr>
<tr>
<td>\s</td>
<td>Any white space character; space, new line, tab, non-breaking space, etc.; functionally equivalent to [:space]</td>
<td>vegetable\s matches &quot;vegetable&quot; followed by any non-white space character. So the phrase &quot;I like vegetables in my soup&quot; would trigger the regex, but &quot;I like a vegetable in my soup&quot; would not.</td>
</tr>
<tr>
<td>\S</td>
<td>Any non-white space character; anything other than a space, new line, tab, non-breaking space, etc.; functionally equivalent to [:space]</td>
<td>vegetable\S matches &quot;vegetable&quot; followed by any non-white space character. So the phrase &quot;I like vegetables in my soup&quot; would trigger the regex, but &quot;I like a vegetable in my soup&quot; would not.</td>
</tr>
</tbody>
</table>
Character Classes

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
</table>
| [: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, !@#.
| [: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 |
### Table 10-6. Character classes (Continued)

<table>
<thead>
<tr>
<th>Element</th>
<th>What it means</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>[:lower:]</td>
<td>Any lowercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else it will function as [:alnum:])</td>
<td>.REG. [:lower:] matches abc, Def, sTress, Do, etc., but not ABC, DEF, STRESS, DO, 123, !@#.</td>
</tr>
<tr>
<td>[:upper:]</td>
<td>Any uppercase alphabetic characters (Note: 'Enable case sensitive matching' must be enabled or else it will function as [:alnum:])</td>
<td>.REG. [:upper:] matches ABC, DEF, STRESS, DO, Def, Stress, Do, etc., but not abc, 123, !@#.</td>
</tr>
<tr>
<td>[:xdigit:]</td>
<td>Digits allowed in a hexadecimal number (0-9a-fA-F)</td>
<td>.REG. [:xdigit:] matches 0a, 7E, 0f, etc.</td>
</tr>
</tbody>
</table>
## Pattern Anchor Regular Expressions

### Table 10-7. Pattern anchor regular expressions

<table>
<thead>
<tr>
<th>Element</th>
<th>What it Means</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>^</code></td>
<td>Indicates the beginning of a string.</td>
<td><code>(notwithstanding)</code> matches any block of text that began with &quot;notwithstanding&quot; So the phrase &quot;notwithstanding the fact that I like vegetables in my soup&quot; would trigger the regex, but &quot;The fact that I like vegetables in my soup notwithstanding&quot; would not.</td>
</tr>
<tr>
<td><code>$</code></td>
<td>Indicates the end of a string.</td>
<td><code>(notwithstanding)</code> <code>$</code> matches any block of text that ended with &quot;notwithstanding&quot; So the phrase &quot;notwithstanding the fact that I like vegetables in my soup&quot; would not trigger the regex, but &quot;The fact that I like vegetables in my soup notwithstanding&quot; would.</td>
</tr>
</tbody>
</table>
### Escape Sequences Regular Expressions

**TABLE 10-8. Escape sequences regular expressions**

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>In order to match some characters that have special meaning in regular expression (for example, &quot;+&quot;).</td>
<td>(1) .REG. C\C++ matches 'r;C\C++'.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(2) .REG. * matches *.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3) .REG. ? matches ?.</td>
</tr>
<tr>
<td>\t</td>
<td>Indicates a tab character.</td>
<td>(stress) \t matches any block of text that contained the substring &quot;stress&quot; immediately followed by a tab (ASCII 0x09) character.</td>
</tr>
<tr>
<td>\n</td>
<td>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.</td>
<td>(stress) \n matches any block of text that contained the substring &quot;stress&quot; followed immediately by two new line (ASCII 0x0A) characters.</td>
</tr>
</tbody>
</table>
**TABLE 10-8. Escape sequences regular expressions (Continued)**

<table>
<thead>
<tr>
<th>ELEMENT</th>
<th>WHAT IT MEANS</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>\r</td>
<td>Indicates a carriage return character.</td>
<td>(stress) \r matches any block of text that contained the substring &quot;stress&quot; followed immediately by one carriage return (ASCII 0x0D) character.</td>
</tr>
<tr>
<td>\b</td>
<td>Indicates a backspace character</td>
<td>(stress) \b matches any block of text that contained the substring &quot;r;stress&quot; followed immediately by one backspace (ASCII 0x08) character.</td>
</tr>
<tr>
<td>\xhh</td>
<td>Indicates an ASCII character with given hexadecimal code (where hh represents any two-digit hex value).</td>
<td>\x7E(\w){6} matches any block of text containing a &quot;word&quot; 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.</td>
</tr>
</tbody>
</table>

**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.
Using exact matching and keywords on multiple lines

<table>
<thead>
<tr>
<th>Situation</th>
<th>Example</th>
<th>Match / Non-match</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two words on same line</td>
<td>bare sexy</td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Click here to see bare sexy beauties.&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click here to see bare naked sexy hotties.</td>
</tr>
<tr>
<td>Two words separated by a comma</td>
<td>bare, sexy</td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Click here to see hot, bare, sexy beauties.&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Click here to see hot, bare, and sexy beauties.&quot;</td>
</tr>
<tr>
<td>Multiple words on multiple lines</td>
<td>nude sexy bare naked</td>
<td>When you choose <strong>Any specified keywords</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;This is a nude picture&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Also matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;See young, hot, and sexy beauties&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When you choose <strong>All specified keywords</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;This is a nude picture of sexy buff and bare naked&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;This is a nude picture of sexy buff bare and naked&quot;</td>
</tr>
<tr>
<td>Many keywords on same line</td>
<td>sex bare nude naked buff</td>
<td>Matches:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Click here for sex bare nude naked buff</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does not match:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&quot;Click here to see sex that's bare and buff&quot;</td>
</tr>
</tbody>
</table>
Troubleshooting

Update 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.

To update the scan engine manually:

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

2. Extract the contents of the vsapi-32dll-.###-####.zip file to a temporary directory.

3. Stop the ScanMail services. Click the Windows Start button and navigate to Programs > Administrative Tools > Services.

4. Back up the following scan engine files:
   For 32-bit:
   
   
   \Program Files\Trend Micro\Smex\engine\vsapi\latest\vsapi32.dll
   
   For 64-bit:
   
   \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 ScanMail scan service and select Start in the pop-up menu that appears.

Update the Pattern File Manually

To manually update the pattern file (lpt$vpn.xxx):

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
   Or, a Controlled Pattern Release (CPR) file from this location:

   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/
Contacting Technical Support

There is an abundance of security information and support available through the Trend Micro website. You can find the following:

- Downloadable product upgrades, component updates and hot fix patches
- Security advisories on the latest outbreaks
- Downloadable trial versions of Trend Micro products
- Expert advice on specific viruses/malware in the wild and computer security in general
- An encyclopedia of computer security information, white papers, and virus/malware statistics
- Free downloadable software for security risk scans, web feeds, and security testing

To contact Trend Micro technical support:

1. Visit the following URL:
   http://esupport.trendmicro.com
2. Click the link for the region you want to contact and follow the instructions for contacting support in that region.

You can find Trend Micro contacts in the following regions:

- Asia/Pacific
- Australia and New Zealand
- Latin America
- United States and Canada
Before Contacting Technical Support

While our basic technical support staff is always pleased to handle your inquiries, there are a couple things you can do to quickly find the answer you are seeking.

- Check the documentation: the manual and online help provide comprehensive information about ScanMail. Search both documents to see if they contain your solution.
- To speed up your problem resolution, when you contact our staff please provide as much of the following information as you can:
  - Product serial number
  - ScanMail program, scan engine, pattern file, version number
  - Operating System name and version
  - Internet connection type
  - Exact text of any error message given
  - Steps to reproduce the problem

Contacting Trend Micro

Trend Micro Incorporated has its world headquarters at:

Shinjuku MAYNDS Tower
2-1-1 Yoyogi, Shibuya-ku, Tokyo 151-0053 Japan.

In the United States, Trend Micro is located at:

10101 N. De Anza Blvd.
Cupertino, CA 95014-9985
Tel: +1-408-257-1500
Fax: +1-408-257-2003

Trend Micro has sales and corporate offices located in many cities around the globe. For global contact information, visit the Trend Micro Worldwide site:

http://www.trendmicro.com/en/about/contact/overview.htm

Note: The information on this website is subject to change without notice.
The Trend Micro website has a wealth of sales and corporate information available.

- Corporate information includes our company profile, international business office contacts, and partnering and alliance information.
- Sales information includes product evaluation information and trial downloads, reseller contacts, and virus/malware research information.

**TrendLabs**

TrendLabs℠ is the Trend Micro global infrastructure of antivirus research and product support centers that provide up-to-the minute security information to Trend Micro customers.

The "virus doctors" at TrendLabs monitor potential security risks around the world, to ensure that Trend Micro products remain secure against emerging threats. The daily culmination of these efforts are shared with customers through frequent virus pattern file updates and scan engine refinements.

TrendLabs is staffed by a team of several hundred engineers and certified support personnel that provide a wide range of product and technical support services. Dedicated service centers and rapid-response teams are located in Tokyo, Manila, Taipei, Munich, Paris, and Irvine, CA, to mitigate outbreaks and provide urgent support.

TrendLabs' modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000. It is one of the first antivirus research and support facilities to be so accredited. We believe TrendLabs is the leading service and support team in the antivirus industry.

**Knowledge Base**

The Trend Micro Knowledge Base, maintained at the Trend Micro website, has the most up-to-date answers to product questions. You can also use Knowledge Base to submit a question if you cannot find the answer in the product documentation. Access the Knowledge Base at:

[http://esupport.trendmicro.com](http://esupport.trendmicro.com)
The contents of Knowledge Base are being continuously updated, and new solutions are added daily. If you are unable to find an answer, however, you can describe the problem in email and send it directly to a Trend Micro support engineer who will investigate the issue and respond as soon as possible.

**Security Information Site**

Comprehensive security information is available at the Trend Micro website:

http://www.trendmicro.com/vinfo/

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

**Email Technical Support**

If you are not able to find an answer in the documentation or the knowledge base, you can email your question to Trend Micro technical support.

Email: support@trendmicro.com
Introducing Trend Micro™ Control Manager™

Trend Micro™ Control Manager™ is a central management console that manages Trend Micro products and services, third-party antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products and services throughout the network.

Topics include:

- Control Manager Standard and Advanced on page A-2
- How to Use Control Manager on page A-3
- Registering ScanMail to Control Manager on page A-7
- Control Manager User Access on page A-8
- Managing ScanMail From Control Manager on page A-14
- Downloading and Deploying New Components from Control Manager on page A-28
- Using Logs on page A-47
- Working With Reports on page A-49
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 5.0 Advanced supports the following as child Control Manager servers:

- Control Manager 5.5
- Control Manager 5.0 Advanced
- Control Manager 3.5 Standard or Enterprise Edition
- Control Manager 3.0 SP6 Standard or Enterprise Edition

Control Manager 5.0 Standard servers cannot be child servers.

For a complete list of all features Standard and Advanced Control Manager servers support refer to Trend Micro Control Manager documentation.
How to Use Control Manager

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**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized configuration</td>
<td>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. This helps ensure consistent enforcement of your organization’s virus/malware and content security policies.</td>
</tr>
<tr>
<td>Proactive outbreak prevention</td>
<td>With Outbreak Prevention Services (OPS), take proactive steps to secure your network against an emerging virus/malware outbreak.</td>
</tr>
<tr>
<td>Secure communication infrastructure</td>
<td>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.</td>
</tr>
<tr>
<td>Secure configuration and component download</td>
<td>These features allow you to configure secure management console access and component download.</td>
</tr>
<tr>
<td>Task delegation</td>
<td>System administrators can give personalized accounts with customized privileges to Control Manager management console users. User accounts define what the user can see and do on a Control Manager network. Track account usage through user logs.</td>
</tr>
</tbody>
</table>
## TABLE A-1. Control Manager Features (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Tracking</td>
<td>This feature allows you to monitor all commands executed using the Control Manager management console. Command Tracking is useful for determining whether Control Manager has successfully performed long-duration commands, like virus pattern update and deployment.</td>
</tr>
<tr>
<td>On-demand product control</td>
<td>Control managed products in real-time. Control Manager immediately sends configuration modifications made on the management console to the managed products. System administrators can run manual scans from the management console. This command system is indispensable during a virus/malware outbreak.</td>
</tr>
<tr>
<td>Centralized update control</td>
<td>Update virus patterns, anti-spam rules, scan engines, and other antivirus or content security components to help ensure that all managed products are up-to-date.</td>
</tr>
<tr>
<td>Centralized reporting</td>
<td>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.</td>
</tr>
</tbody>
</table>
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. Refer to Table A-2 on page A-5 for a list of components Control Manager uses.

**Table A-2. Control Manager Components**

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| 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 **management 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. |
### TABLE A-2. Control Manager Components (Continued)

<table>
<thead>
<tr>
<th>COMPONENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Manager server</td>
<td>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 virus/malware and content security events that occur on the Control Manager network.</td>
</tr>
<tr>
<td>Trend Micro Management Communication Protocol (MCP)</td>
<td>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 uses one/two way communication to communicate with Control Manager. MCP agents poll Control Manager for instructions and updates.</td>
</tr>
<tr>
<td>Trend Micro Infrastructure</td>
<td>Handles the Control Manager server interaction with older managed products. The Communicator, or the Message Routing Framework, was the communication backbone of the Control Manager system. The communicator is a component of the Trend Micro Infrastructure (TMI). Communicators handle all communication between the Control Manager server and older managed products. The communicator interacts with Control Manager 2.x agents to communicate to older managed products.</td>
</tr>
</tbody>
</table>
Registering ScanMail to Control Manager

Before registering a 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.

To register a ScanMail server to Control Manager:

1. Log on to the product console.
2. Click Administration > Control Manager Settings. The Control Manager Settings screen displays.
**Note:** Control Manager uses the name specified in the Host name field to identify ScanMail server. The Host name appears in the Product Directory of Control Manager.

3. Under **Connection settings**, type the name of the ScanMail server in the **Entity display name** field.

4. 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.

5. From the Control Manager management console, click **Products**. The Product Directory screen appears.

6. The ScanMail server appears in the Product Directory tree.

**Control Manager User Access**

Access to the Control Manager web console and Control Manager features depends on your user account and account type.

For detailed information about creating new user accounts or account types, see the **Control Manager Administrator's Guide** or the **Control Manager Tutorial**.
Introducing Trend Micro™ Control Manager™

Control Manager 5.0 user access control provides greater flexibility than previous versions of Control Manager. Control Manager administrators can now restrict user access to the following:

- Control Manager menu items and screens
- Managed products and all information relating to the managed products
- Specific Control Manager features

This means that not all Control Manager screens, features, or managed products and their information are available for all users.

User access is split into the following sections:

**TABLE A-3. Control Manager User Account Options**

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>My Account</td>
<td>The My Account screen contains all the account information Control Manager has for a specific user. The information on the My Account screen varies from user to user.</td>
</tr>
<tr>
<td>User Accounts</td>
<td>The User Accounts screen displays all Control Manager users. The screen also provides functions allowing you 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</td>
</tr>
</tbody>
</table>
### 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 ScanMail server while allowing access to Control Manager.

### Managed Product MCP Agent Heartbeat

To monitor the status of ScanMail server, MCP agents poll Control Manager based on a schedule. Polling occurs to indicate the status of the ScanMail server and to check for commands to the ScanMail server from Control Manager. The Control Manager Web console then presents the product status. This means that the ScanMail server status is not a real-time, moment-by-moment reflection of the network's status. Control Manager

---

### TABLE A-3. Control Manager User Account Options (Continued)

<table>
<thead>
<tr>
<th>SECTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Groups</td>
<td>The Group Accounts 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 Control Manager administrators to create a group that shares the same access rights.</td>
</tr>
<tr>
<td>User Types</td>
<td>The Account Types screen displays all Control Manager user roles. The screen also provides functions allowing you to create and maintain Control Manager user roles. User roles define which areas of the Control Manager Web console a user can access.</td>
</tr>
</tbody>
</table>
checks the status of each ScanMail server in a sequential manner in the background. Control Manager changes the status of ScanMail servers to offline, when a fixed period of time elapses without a heartbeat from the ScanMail server.

Active heartbeats are not the only means Control Manager has for determining the status of ScanMail servers. The following also provide Control Manager with the ScanMail server status:

• Control Manager receives logs from the ScanMail server. Once Control Manager receives any type of log from the ScanMail server successfully, this implies that the ScanMail server is working fine.

• In two-way communication mode, Control Manager actively sends out a notification message to trigger the ScanMail server to retrieve the pending command. If server connects to the ScanMail server successfully, it also indicates that the product is working fine and this event will be counted as a heartbeat.

• In one-way communication mode, the managed product’s 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 Control Manager agent heartbeats implement with the following ways:

• **UDP**: If the product can reach the server using UDP, this is the most lightweight, fastest solution available. However, this does not work in NAT or firewall environments. Also the transmitting client cannot make sure 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 ScanMail server 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 ScanMail server activity information to display on the console.
Using the Schedule Bar

Use the schedule bar in the Agent/Communicator Scheduler screen to display and set Communicator schedules. The bar has 24 slots, each representing the hours in a day.

Blue slots 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:

The active periods specified by the bar are from 0:00 A.M. to 7:00 A.M, 8:00 A.M to 3:00 P.M, and from 6:00 P.M. to 12:00 P.M.

Note: The default setting for all managed products registered to Control Manager is 24 hours.

To configure the communication schedule for a ScanMail server:

1. Mouseover Administration > Settings from the Control Manager Web console. A drop-down menu appears.
2. Click Agent Communication Schedule. The Agent Communication Schedule screen appears.
3. Click the link for the ScanMail server to modify. The Set Communicator Schedule screen appears.
4. Specify the time that the ScanMail server communicates with Control Manager.
5. Click Save.
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. Trend Micro's default settings is satisfactory for most situations, however consider the following points when you customize the heartbeat setting:

**TABLE A-4. Heartbeat Recommendations**

<table>
<thead>
<tr>
<th>HEARTBEAT FREQUENCY</th>
<th>RECOMMENDATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Long-interval Heartbeats (above 60 minutes)</td>
<td>The longer the interval between heartbeats, the greater the number of events that may occur before Control Manager reflects the communicator status on the Control Manager management 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).</td>
</tr>
<tr>
<td>Short-interval Heartbeats (below 60 minutes)</td>
<td>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.</td>
</tr>
</tbody>
</table>

**WARNING!** Modification to the heartbeat settings are global and affect all managed products registered to Control Manager.

To configure heartbeat settings:

1. Mouseover **Administration > Settings** from the Control Manager Web console. A drop-down menu appears.
2. Click **Heartbeat Settings**. The Heartbeat Settings 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 management 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**.

### Managing ScanMail From Control Manager

A managed product refers to a ScanMail server, an antivirus, a content security or third party product represented in the Product Directory. The Control Manager management console represents managed products as icons. These icons represent ScanMail servers, other Trend Micro antivirus and content security products, as well as third party products.

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>
<thead>
<tr>
<th><strong>TABLE A-5. Product Directory Options</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Menu Items</strong></td>
</tr>
<tr>
<td>Advanced Search</td>
</tr>
<tr>
<td>Configure</td>
</tr>
</tbody>
</table>
TABLE A-5. Product Directory Options (Continued)

<table>
<thead>
<tr>
<th>Menu Items</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tasks</td>
<td>Click this button, after selecting a managed product/directory, to perform specific function (such as deploying the latest components) to a specific or groups of managed product or child servers. Initiating a task from a directory and Control Manager sends requests to all managed products belonging to that directory.</td>
</tr>
<tr>
<td>Logs</td>
<td>Click this button, after selecting a managed product/directory, to query and view product logs. If you select a managed product, you can only query logs for that specific product. Otherwise, you can query all the products available in the directory.</td>
</tr>
<tr>
<td>Directory Management</td>
<td>Click this button to open the Directory Management screen. From the screen, move entities/directories (by dragging and dropping them) or create new directories.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Buttons</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search</td>
<td>Click this button, after typing a managed product's name, to perform a search for the specified managed product.</td>
</tr>
<tr>
<td>Status</td>
<td>Click this button, after selecting a managed product/directory, to obtain status summaries about the managed product or managed products found in the directory.</td>
</tr>
<tr>
<td>Folder</td>
<td>Click this button, after selecting a directory, to obtain status summaries about the managed products and the managed product clients found in the directory.</td>
</tr>
</tbody>
</table>

Understanding Product Directory

The Product Directory provides a user-specified grouping of managed products which allows you to perform the following for administering managed products:

- Configure managed products
• Request products to perform a Scan Now (if this command is supported)
• View product information, and 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 the structure carefully, because the structure also affects the following:

### TABLE A-6. Product Directory Considerations

<table>
<thead>
<tr>
<th>CONSIDERATION</th>
<th>IMPACT</th>
</tr>
</thead>
<tbody>
<tr>
<td>User access</td>
<td>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.</td>
</tr>
<tr>
<td>Deployment planning</td>
<td>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.</td>
</tr>
<tr>
<td>Outbreak Prevention Policy (OPP) and Damage Control Template (DCT) deployments</td>
<td>OPP and DCT deployments depend on Deployment Plans for efficient distribution of Outbreak Prevention Policy and cleanup tasks.</td>
</tr>
</tbody>
</table>

**Note:** Managed products belonging to child Control Manager servers cannot have tasks applied to them by the parent Control Manager server.
A sample Product Directory appears below:

Managed products identify the registered antivirus or content security product, as well as provide the connection status.

Refer to the Control Manager Understanding Product Directory online help topic for the list of Product Directory icons.

Access the Product Directory

Use the Product Directory to administer ScanMail servers registered with the Control Manager server.

**Note:** Viewing and accessing the folders in the Product Directory depends on the user account folder access rights.

**To access the Product Directory:**

- Click **Products** on the main menu. The Product Directory screen appears.
Deploy Components Using the Product Directory

Manual deployments allow you to update the virus patterns, spam rules, and scan engines of your ScanMail servers and other managed products on demand.

Download new components before deploying updates to specific or groups of ScanMail servers or managed products.

**To manually deploy new components using the Product Directory:**

1. Click **Products** on the main menu.
2. Mouseover **Tasks**. A drop down menu appears.
3. Select **Deploy <component>** from the menu. The **Deploy <component>** screen appears in the Product Directory work area.
4. Click **Deploy Now** to start the manual deployment of new components.
5. Monitor the progress using Command Tracking.
6. Click **Command Details** to view details for the task.

View ScanMail Status Summaries

The Product Status screen displays the Antivirus, Content Security, and Web Security summaries for all ScanMail servers and other managed products present in the Product Directory tree.

There are two ways to view the ScanMail status summary:

- Through Home page
- Through Product Directory

**To access through the Home page**

- Upon opening the Control Manager management console, the Status Summary tab of the Home page shows the summary of the entire Control Manager system. This summary is identical to the summary provided by the Product Status tab in the Product Directory Root folder.

**To access through Product Directory:**

1. Click **Products** on the main menu.
2. Select the desired folder or ScanMail server.
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 available in the Display summary for list.

Configure ScanMail Servers and 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.

To configure a product:

1. Access the Product Directory.
2. Select the desired managed product from the product tree. The product status appears in the right-hand area of the screen.
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 structure.
     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-based console or Control Manager-generated console appears.
     a. Configure the managed product from the Web console.

Issue Tasks to ScanMail Servers and Managed Products

Use the options under the Tasks menu item to start actions on a group or specific ScanMail server or managed product. You can perform the following tasks on ScanMail servers:

- Configuration Replication
- Deploy engines
- Deploy pattern files/ cleanup templates
To issue tasks to ScanMail servers:
1. Click **Products** on the main menu.
2. Mouseover **Tasks**. A drop down menu appears.
3. Select a task from the menu. A screen appears in the Product Directory work area.
4. Initiate the task from the work area.
5. Monitor the task’s progress using Command Tracking.
6. Click **Command Details** to view details for the task.

Querying and Viewing ScanMail and Managed Product Logs
Use the Logs menu item to query and view logs for a group or specific ScanMail server.

For detailed information about querying logs or data views, see the Control Manager Administrator’s Guide or the Control Manager Tutorial.

To query and view ScanMail logs:
1. Click **Products** on the main menu.
2. Select the desired ScanMail server or folder from the Product Directory tree.
3. Click **Logs** from the Product Directory menu. The Ad Hoc Query Step 2: Data View screen appears.
4. Select the data to query by specifying a data view for the log.
5. Click **Next**. The Step 3: Query Criteria screen appears.
6. Specify the data to appear in the log and the order in which the data appears:
   a. Click **Change column display**. The Select Display Sequence screen 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.
   b. Select a query column from the Available Fields list. The selected item highlights.
   c. Select multiple items using the Shift or Ctrl keys.
d. Click > to add items to the Selected Fields list.

e. Specify the order in which the data displays by selecting the item and clicking Move up or Move down.

f. Click Back when the sequence fits your requirements.

7. Specify the filtering criteria for the data:

<table>
<thead>
<tr>
<th>Note:</th>
<th>When querying for summary data, users must specify the items under Required criteria.</th>
</tr>
</thead>
</table>

**Required criteria:**

- Specify a Summary Time for the data or whether you want COOKIES (spyware data only) 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.

<table>
<thead>
<tr>
<th>Tip:</th>
<th>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.</th>
</tr>
</thead>
</table>

8. To save the query:

   Saving queries allows you to reuse them or to share them with others.

   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.
**Tip:** To display 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.

10. To save the settings for the query:
   a. Click **Save query settings**. A confirmation dialog box appears.
   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.

**Recovering ScanMail Servers Removed From the Product Directory**

The following scenarios can cause Control Manager to delete ScanMail servers from the Product Directory:

- Reinstalling the Control Manager server and selecting **Delete existing records and create a new database** option. 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 ScanMail server using the Directory Manager.

If a Control Manager server's managed product records are lost, the agents on the products still "know" where they are registered.

**To recover ScanMail servers removed from the Product Directory:**

- Restart Trend Micro Control Manager service on the managed product server.
- 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, on the server where Control Manager installs, to restart any of the following Control Manager services:

- Trend Micro Management Infrastructure
- Trend Micro CCGI
- Trend Micro Control Manager
Introducing 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, Damage Cleanup Services).

To restart Control Manager services:

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.

Search for ScanMail Servers, Product Directory Folders or Computers

Use the Search button to quickly find and locate a specific managed product in the Product Directory.

To search for a folder or managed product:

2. Type the entity display name of the managed product in the Find Entity field.
3. Click Search.

To perform an advanced search:

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.

Refresh the Product Directory

To refresh the Product Directory:

• In the Product Directory, click the Refresh icon on the upper right corner of the screen.
Understanding the Directory Management Screen

After registering to Control Manager, the ScanMail server appears in the Product Directory under the default folder.

Use the Directory Management screen to customize the Product Directory organization to suit your administration model 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>
<thead>
<tr>
<th>GROUPING TYPE</th>
<th>ADVANTAGES</th>
<th>DISADVANTAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Geographical or Administrative</td>
<td>Clear structure</td>
<td>No group configuration for identical products</td>
</tr>
<tr>
<td>Product type</td>
<td>Group configuration and status is available</td>
<td>Access rights may not match</td>
</tr>
<tr>
<td>Combination of both</td>
<td>Group configuration and access right management</td>
<td>Complex structure, may not be easy to manage</td>
</tr>
</tbody>
</table>
Using the Directory Management Screen Options

Directory Manager provides several options:

• Add directories to the Product Directory
• Rename directories in the Product Directory
• Move managed products/directories in the Product Directory

Note: The Permission Keep check box allows a folder to keep its source permission when moved.

• Remove managed products/directories from the Product Directory

Use these options to manipulate and organize managed products in your Control Manager network.

To use and apply changes in the Directory Management screen:

• Select a managed product/directory and click **Rename** to rename a managed product/directory.
• Click + or the folder to display the managed products belonging to a folder.
• Drag-and-drop managed products/directories to move the managed products/directories in the Product Directory.
• Click **Add Folder** to add a directory to the Product Directory.

Accessing Directory Management

Use Directory Management to group managed products together.

To access the Directory Management:

1. Click **Products** from the main menu. The Product Directory screen appears.

Creating Folders

Group managed products into different folders to suit your organization's Control Manager network administration model.
To create a folder:
2. Select Local Folder. The Local Folder highlights.
3. Click Add Folder. The Add Directory dialog box appears.
4. Type a name for the new directory in the Directory name field.
5. 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 from the Directory Manager.

To rename a folder or managed product:
2. Select the managed product/directory to rename. The item highlights in the Product Directory.
3. Click Rename. The Rename Directory dialog box appears.
4. Type a name for the managed product/directory in the Directory name field.
5. Click Save. A confirmation dialog box appears.
6. Click OK. The managed product/directory displays in the Product Directory with the new name.

Note: Renaming a managed product only changes the name stored in the Control Manager database; there are no effects to the managed product.

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/ folder, the managed product/ folder keeps the
permissions from its source folder. If you clear the Permission Keep check box, and then move a managed product/ folder, the managed product/ folder assumes the access permissions from its new parent folder.

**To transfer or move a folder or managed product to another location:**

2. On the working area, select the folder or managed product to move.
3. Drag-and-drop the folder or managed product to the target new location.
4. Click **Save**.

**Deleting User-Defined Folders**

Take caution when deleting user-defined folders in the Directory Manager, you may accidentally delete a managed product which causes it to unregister from the Control Manager server.

**To delete a user-defined folder:**

Take caution when deleting user-defined folders in the Directory Manager, 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.

**To delete a user-defined folder:**

2. Select the managed product/ directory to delete. The item highlights.
3. Click **Delete**. A confirmation dialog box appears.
4. Click **OK**.
5. Click **Save**.

---

**WARNING!** Take caution when deleting user-defined folders, you may accidentally delete a managed product that you do not want to remove.
Downloading and Deploying New Components from Control Manager

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 virus pattern, damage cleanup template, and Vulnerability Assessment pattern download even if there is no managed product registered on the Control Manager server.

The following are the components to update (listed according to the frequency of recommended update):

- **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.
- **Anti-spam rules**: Anti-spam rules are the Trend Micro-provided files used for anti-spam 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.
- **Product program**: Product specific components (for example, Service Pack releases).

---

**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 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.

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.
Introducing Trend Micro™ Control Manager™

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.

This is the Trend Micro recommend method of configuring 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

To manually download components:

Step 1: Configure a Deployment Plan for your components

1. Mouseover Updates on the main menu. A drop-down menu appears.
2. Click Deployment Plan from the drop-down menu. The Deployment Plan screen appears.
3. Click Add. The Add New Plan screen appears.
4. On the Add New Plan screen, type a deployment plan name in the Name field.
5. Click **Add** to provide deployment plan details. The Add New Schedule screen appears.

6. On the Add New Schedule screen, choose a deployment time schedule by selecting one of the following options:
   - **Delay** - After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify. Use the menus to indicate the duration, in terms of hours and minutes.
   - **Start at** - Performs the deployment at a specific time. Use the menus to designate the time in hours and minutes.

7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

8. Click **OK**.

9. Click **Save** to apply the new deployment plan.

**Step 2: Configure your proxy settings, if you use a proxy server**

1. Mouseover **Administration**. A drop-down menu appears.

2. Mouseover **Settings**. A sub-menu appears.

3. Click **Proxy Settings**. The Connection Settings screen appears.

4. Select **Use a proxy server for pattern, engine, and license updates**.

5. Select the protocol:
   - **HTTP**
   - **SOCKS 4**
   - **SOCKS 5**

6. Type the host name or IP address of the server in the **Server name or IP address** field.

7. Type a port number in the **Port** field.

8. Type a log on name and password if your server requires authentication.

9. Click **Save**.

**Step 3: Select the components to update**

1. Mouseover **Updates** on the main menu. A drop-down menu appears.


3. From the Components 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 Anti-spam rules
   - All Engines
   - Product programs

Step 4: Configure the download settings

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 additional update source. You can configure up to five update sources.

2. Select **Retry frequency** and specify the number or 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, 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

1. Select when to deploy downloaded components from the Schedule 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.

---

2. Select a deployment plan after components download to Control Manager, from the **Deployment plan** list.

3. Click **Save**.

**Step 6: Complete the manual download**

1. Click **Download Now** and then click **OK** to confirm. The download response screen appears. The progress bar displays the download status.

2. Click the **Command Details** to view details from the Command Details screen.

3. Click **OK** to return to the Manual Download screen.

**Accessing Manual Download**

Use the Manual Download screen to immediately obtain new components.

**To access the Manual Download screen:**

1. Mouseover **Updates** on the main menu. A drop down menu appears.


**Configuring Manual Download Settings**

The Download Settings group defines the components Control Manager manually downloads and the download method.
To configure manual download settings:

2. On the working area under Download Settings:
   a. Select components that you want to download.
   b. Select the update source:
      - **Internet**: Trend Micro update server to 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 additional update source. You can configure up to five update sources.
   c. Select **Retry frequency** and specify the number or 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.

d. If you use an HTTP proxy server on the network (that is, the Control Manager server does not have direct Internet access), click **Edit** to configure the proxy settings on the Connection Settings screen.

3. Click **Save**.

Configuring Manual Download and Automatic Deployment Settings

Use the Automatic Deployment Settings group to set how Control Manager deploys updates.

To configure manual download Automatic Deployment Settings:

1. Mouseover **Updates** on the main menu. A drop down menu appears.
3. Select when to deploy downloaded components from the Schedule area:
   • **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

   **Tip:** 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: list.

5. Click **Save**.

   **Note:** The settings in Automatic Deployment Settings only apply to components used by managed products.

   For Damage Cleanup Services and Vulnerability Assessment, Control Manager automatically deploys components (damage cleanup template, damage cleanup engine, vulnerability assessment pattern, and vulnerability assessment engine) whenever newer versions are available.

---

**Configuring 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.
Introducing Trend Micro™ Control Manager™

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**.

**To configure scheduled download exceptions:**

1. Mouseover **Updates** on the main menu. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Scheduled Download Exceptions**. The Scheduled Download Exceptions screen appears.
4. Do the following:
   - To schedule a daily exception, under Daily schedule exceptions, select the check box of the day(s) to prevent downloads, and then select the **Do not download updates on the specified day(s)** check box. Every week, Control Manager blocks all downloads for the selected day(s).
   - To schedule an hourly exception, under Hourly schedule exceptions, select the hour(s) to prevent downloads, and then select the **Do not download updates on the specified hour(s)** check box. Every day, Control Manager blocks all downloads for the selected hours.
5. Click **Save**.

**Understanding 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 downloads 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

### Configuring Scheduled Downloads and Enabling Scheduled Component Downloads

**Step 1: Configure a Deployment Plan for your components**

1. Mouseover **Administration** on the main menu. A drop down menu appears.
2. Click **Deployment Plan** from the drop down menu. The Deployment Plan screen appears.
3. Click **Add**. The **Add New Plan** screen appears.
4. On the Add New Plan screen, type a deployment plan name in the **Name** field.
5. Click **Add** to provide deployment plan details. The Add New Schedule screen appears.
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one of the following options:
   • **Delay** - after Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify. Use the menus to indicate the duration, in terms of hours and minutes.
   • **Start at** - Performs the deployment at a specific time. Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.
8. Click **OK**.
9. Click **Save** to apply the new deployment plan.

**Step 2: Configure your proxy settings, if you use a proxy server**

1. Mouseover **Administration**. A drop down menu appears.
2. Mouseover **Settings**. A sub-menu appears.
3. Click **Proxy Settings**. The Connection Settings screen appears.
4. Select **Use a proxy server for pattern, engine, and license updates**.
5. Select the protocol:
   • **HTTP**
   • **SOCKS 4**
   • **SOCKS 5**
6. Type the host name or IP address of the server in the **Server name** or **IP address** field.
7. Type a port number for the proxy server in the **Port** field.
8. Type a logon name and password if your server requires authentication.
9. Click **Save**.

**Step 3: Select the components to update**

1. Mouseover **Updates** on the main menu. A drop-down menu appears.
2. Click **Scheduled Download**. The Scheduled Download screen appears.
3. From the Components 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 Anti-spam rules
      • All Engines
      • Product programs
      The <Component Name> screen appears. Where <Component Name> represents the name of the selected component.

Step 4: Configure the download schedule
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
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 additional update source. You can configure up to five update sources.
2. Select **Retry frequency** and specify the number or retries and duration between retries for downloading components.
Introducing Trend Micro™ Control Manager™

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, 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

1. Select when to deploy downloaded components from the Schedule 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

Tip: 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 list.

3. Click Save.

Step 7: Enable the schedule and save settings

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.

To configure scheduled download schedule and frequency:

1. Mouseover Updates on the main menu. A drop-down menu appears.
2. Click Scheduled Download. The Scheduled Download screen appears.
3. From the Components 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 Anti-spam rules
      • All Engines
      • Product programs
      The <Component Name> screen appears. Where <Component Name> is the name of the component you selected.
4. 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.
5. Click Save.

Configuring Scheduled Download Settings

The Download Settings group defines the components Control Manager automatically downloads and the download method.

To configure scheduled download settings:

1. Mouseover Updates on the main menu. A drop down menu appears.
2. Click Scheduled Download. The Scheduled Download screen appears.
3. From the Components 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 Anti-spam rules
      • All Engines
      • Product programs

      The <Component Name> screen appears. Where <Component Name> represents the name of the selected component.

4. Under Source, select one of the following update sources:
   • Internet: Trend Micro update server — (default setting) Control Manager downloads latest components from the Trend Micro ActiveUpdate server
   • Other Internet 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.

5. 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.

6. 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.

7. Click **Save**.
Configuring Scheduled Download Automatic Deployment Settings

Use the Auto-deploy Setting group to set how Control Manager deploys updates.

To configure scheduled download auto-deploy settings:

1. Mouseover Updates on the main menu. A drop down menu appears.
2. Click Scheduled Download. The Scheduled Download screen appears.
3. From the Components 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 Anti-spam rules
      • All Engines
      • Product programs
      The <Component Name> screen appears. Where <Component Name> represents the name of the selected component.

Under Automatic deployment settings

4. Select when to deploy downloaded components from the Schedule 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.

5. Select a deployment plan after components download to Control Manager, from the Deployment plan: list.

6. Click Save.

Note: The settings in Automatic Deployment Settings only apply to components used by managed products.

For Damage Cleanup Services and Vulnerability Assessment, Control Manager automatically deploys components (damage cleanup template, damage cleanup engine, vulnerability assessment pattern, and vulnerability assessment engine) whenever newer versions are available.

**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 pages. 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 performs 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 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 are independent of each other.
  For example, if you have three folders that you want to update at five 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.

1. Mouseover Administration on the main menu. A drop down menu appears.
2. Click Deployment Plan from the drop down menu. The Deployment Plan screen appears.
3. Click Add. The Add New Plan screen appears.
4. On the Add New Plan screen, type a deployment plan name in the Name field.
5. Click Add to provide deployment plan details. The Add New Schedule screen appears.
6. On the Add New Schedule screen, choose a deployment time schedule by selecting one the following options:
   - Delay: After Control Manager downloads the update components, Control Manager delays the deployment according to the interval you specify. Use the menus to indicate the duration, in terms of hours and minutes.
   - Start at: Performs the deployment at a specific time. Use the menus to designate the time in hours and minutes.
7. Select the Product Directory folder to which the schedule will apply. Control Manager assigns the schedule to all the products under the selected folder.

8. Click OK.

9. Click Save to apply the new deployment plan.

Configuring Proxy Settings

Configure proxy server connection for component downloads and for license updates.

To configure proxy server settings:

1. Mouseover Administration. A drop down menu appears.


3. Click Proxy Settings. The Connection Settings screen appears.

4. Select Use a proxy server for pattern, engine, and license updates.

5. Select the protocol:
   - HTTP
   - SOCKS 4
   - SOCKS 5

6. Type the host name or IP address of the server in the Server name or IP address field.

7. Type a port number in the Port field.

8. Type a log on name and password if your server requires authentication.

9. Click Save.

Configuring Update/Deployment Settings

Using HTTPS to download components from the Trend Micro ActiveUpdate server or other Internet 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 is any user account from the component source server that has permission to share a folder where Control Manager will download updates.

To enable HTTPS download:

1. Mouseover Updates from the main menu. A drop down menu appears.
3. Click Update/Deployment Settings. The Update/Deployment Settings screen appears.
4. Select Enable HTTPS for the default update download source.
5. Click Save.
7. On the working area under Download settings > Source group, select Internet: Trend Micro update server or specify your organizations component source server in the Other Internet source field.
8. Click Save.

To enable UNC download:

1. Mouseover Updates from the main menu. A drop down menu appears.
3. Click Update/Deployment Settings. The Update/Deployment Settings screen appears.
4. Type the Local Windows Authentication and Remote UNC Authentication user names and passwords.
5. Click Save.
7. On the working area under Download settings > From group, select File path and then specify the shared network folder.
8. 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

To verify the user is on the "Log on as batch job" list:
1. Click **Start > Settings > Control Panel.**
2. Click **Administrative Tools.**
3. Open **Local Security Policy.** The Local Security Settings screen appears.
4. Click **Local Policies > 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 now allows users to query the log data directly from the Control Manager database. The user 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 provide you with information about the performance of your managed products. You can obtain information for specific or groups of products administered by the parent or child server. With Control Manager’s data query on logs and filtering capabilities, administrators can now focus on the information they need.

**Querying Log Data**

Control Manager now supports gathering only the data an administrator needs from Control Manager and managed product logs. Control Manager supports this through the use of Ad Hoc queries. 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). Using Ad Hoc queries to pull data directly from the database provides 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 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 CSV or XML

---

**Note:** Control Manager supports sharing saved Ad Hoc Queries with other users. Saved and shared queries appear on the **Logs/Reports > 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 separates Data Views into two major categories: Product Information and Security Threat Information. See **Appendix B: Understanding Data Views** in the Control Manager Administrator’s Guide for more information about Data Views. The major categories separate further into several sub-categories, with the sub-categories separated into summary information and detailed information.
The Control Manager Web console displays the Data Views and the information available from each Data View.

**TABLE A-8. Control Manager Major Data View Categories**

<table>
<thead>
<tr>
<th><strong>MAJOR DATA VIEW CATEGORY</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
</table>
| Product Information         | Displays information about:  
|                             | • Control Manager  
|                             | • Managed products  
|                             | • Managed product components  
|                             | • Product license information |
| Security Threat Information | Displays information about security threats that managed products detect:  
|                             | • Overall Security Risks  
|                             | • Malware/viruses  
|                             | • Spyware/grayware  
|                             | • Content violations  
|                             | • Spam  
|                             | • Web content violations  
|                             | • Policy/Rule violations  
|                             | • Suspicious threats |

**Working With 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 introduces radical changes over previous Control Manager versions by introducing customized reports for Control Manager administrators. Control Manager 5.0 continues to support report templates from previous Control Manager versions, however Control Manager 5.0 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 5.0 categorizes report templates according to the following types:

- **Control Manager 5.0 templates:** User-defined customized report templates that use direct database queries (database views) and report template elements (charts/graphs/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 5.0 templates, see Understanding Control Manager 5.0 Templates on page A-50.

- **Control Manager 3.0 templates:** Includes all templates provided in Control Manager 3.0 and Control Manager 3.5. For more information on Control Manager 3.0 templates, see Understanding Control Manager 3.0 Templates on page A-51.

Understanding Control Manager 5.0 Templates

Control Manager 5.0 report templates use database views as the information foundation for reports. For more information on data views, see Understanding Data Views on page A-48. The look and feel of generated reports falls to the report elements. Report elements consist of the following:

**TABLE A-9. Control Manager 5.0 Report Template Elements**

<table>
<thead>
<tr>
<th>TEMPLATE ELEMENT</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page break</td>
<td>Inserts a page break for a report. Each report page supports up to three report template elements.</td>
</tr>
<tr>
<td>Static text</td>
<td>Provides a user-defined description or explanation for the report. Static text content can contain up to 4096 characters.</td>
</tr>
<tr>
<td>Bar chart</td>
<td>Inserts a bar chart into a report template.</td>
</tr>
<tr>
<td>Line graph</td>
<td>Inserts a line graph into a report template.</td>
</tr>
<tr>
<td>Pie chart</td>
<td>Inserts a pie chart into a report template.</td>
</tr>
<tr>
<td>Dynamic table</td>
<td>Inserts a dynamic table/pivot table into a report template.</td>
</tr>
</tbody>
</table>
Introducing Trend Micro™ Control Manager™

Each Control Manager 5.0 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.

Adding a Control Manager 5.0 custom template requires the following steps:
1. Access the Add Report Template screen and name the template.
2. Specify the template component to add to the report template.
3. Specify the data view for the template.
4. Specify the query criteria for the template.
5. Specify the data to appear in the report and the order in which the data appears.
6. Complete report template creation.

Understanding Control Manager 3.0 Templates
Trend Micro Control Manager 3.0/3.5 added 65 pre-generated report templates divided into six categories: Desktop, Fileserver, Gateway, Mail Server, Executive Summary, and Network Products.

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.

Adding One-time Reports
Control Manager supports generating one-time reports from Control Manager 3.0 and Control Manager 5.0 report templates. Users need to create Control Manager 5.0 report templates, while Trend Micro created Control Manager 3.0 report templates. The process for creating a one-time report is similar for all report types and involves the following:

<table>
<thead>
<tr>
<th>Template Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grid table</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

**Adding Scheduled Reports**

Control Manager supports generating scheduled reports from Control Manager 3.0 and Control Manager 5.0 report templates. Users need to create Control Manager 5.0 report templates, while Trend Micro created Control Manager 3.0 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.
Windows Event Log Codes

Event Identifications for notifications written into windows event logs have changed a lot from previous versions of ScanMail. This change might impact your monitoring efforts. Consult the following table to understand the Windows event logs.

<table>
<thead>
<tr>
<th>EVENT ID</th>
<th>FACILITY</th>
<th>TYPE/SEVERITY</th>
<th>CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>Alert. ScanMail service did not start successfully.</td>
</tr>
<tr>
<td>4</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>Alert. ScanMail service is unavailable.</td>
</tr>
<tr>
<td>5</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Security risk scan notification.</td>
</tr>
<tr>
<td>6</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Attachment blocking notification.</td>
</tr>
<tr>
<td>7</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Content filtering notification.</td>
</tr>
</tbody>
</table>
### Table B-1. ScanMail Windows Event Log Codes (Continued)

<table>
<thead>
<tr>
<th>EVENT ID</th>
<th>FACILITY</th>
<th>TYPE/ SEVERITY</th>
<th>CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Alert. Manual update successful.</td>
</tr>
<tr>
<td>18</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Alert. Last update time is older than specified time.</td>
</tr>
<tr>
<td>19</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Alert. Manual scan successful.</td>
</tr>
<tr>
<td>20</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>Alert. Manual scan unsuccessful.</td>
</tr>
<tr>
<td>21</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Alert. Scan time exceeds specified time.</td>
</tr>
<tr>
<td>22</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Alert. The disk space on the local drive (volume) of the backup or quarantine directory is less than specified size.</td>
</tr>
<tr>
<td>23</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Alert. The size of database to keep quarantine and logs exceeds specified size.</td>
</tr>
<tr>
<td>24</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Alert. Scheduled scan successful.</td>
</tr>
<tr>
<td>25</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>Alert. Scheduled scan unsuccessful.</td>
</tr>
<tr>
<td>32</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>Alert. Scheduled update unsuccessful.</td>
</tr>
<tr>
<td>EVENT ID</td>
<td>FACILITY</td>
<td>TYPE/SEVERITY</td>
<td>CATEGORY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------</td>
<td>----------</td>
<td>---------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>33</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Alert. Scheduled update successful.</td>
</tr>
<tr>
<td>34</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Web reputation notification.</td>
</tr>
<tr>
<td>35</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Data Loss Prevention notification</td>
</tr>
<tr>
<td>80</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Alert. Outbreak Prevention Mode started.</td>
</tr>
<tr>
<td>82</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Alert. Outbreak Prevention Mode stopped and configuration restored.</td>
</tr>
<tr>
<td>257</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Virus/Malware Outbreak Alert.</td>
</tr>
<tr>
<td>258</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Uncleanable Virus/Malware Outbreak Alert.</td>
</tr>
<tr>
<td>259</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Blocked attachment Outbreak Alert.</td>
</tr>
<tr>
<td>260</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Spyware/Grayware Outbreak Alert.</td>
</tr>
<tr>
<td>513</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>Filter loading exception.</td>
</tr>
<tr>
<td>514</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>Adapter loading exception.</td>
</tr>
<tr>
<td>4097</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Alert. The disk space on the local drive of the MS Exchange transaction log is less than specified size.</td>
</tr>
</tbody>
</table>
TABLE B-1. **ScanMail Windows Event Log Codes (Continued)**

<table>
<thead>
<tr>
<th>EVENT ID</th>
<th>FACILITY</th>
<th>TYPE/SEVERITY</th>
<th>CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>4098</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Alert. The Microsoft Exchange mail store size exceeds specified size.</td>
</tr>
<tr>
<td>4099</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Alert. The Microsoft Exchange SMTP messages queued continuously exceeds the specified number.</td>
</tr>
<tr>
<td>4112</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>ScanMail Master Service stopped due to insufficient disk space. Please free up some disk space and restart ScanMail Master Service.</td>
</tr>
<tr>
<td>8193</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. Processing manual End User Quarantine maintenance task started.</td>
</tr>
<tr>
<td>8194</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. Processing of manual End User Quarantine maintenance task ended.</td>
</tr>
<tr>
<td>8195</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. Processing of schedule End User Quarantine maintenance task started.</td>
</tr>
<tr>
<td>8196</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. End of processing schedule End User Quarantine maintenance task.</td>
</tr>
<tr>
<td>8197</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. Start to process enable End User Quarantine task.</td>
</tr>
<tr>
<td>EVENT ID</td>
<td>FACILITY</td>
<td>TYPE/SEVERITY</td>
<td>CATEGORY</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------</td>
<td>-----------</td>
<td>---------------</td>
<td>----------</td>
<td>-------------</td>
</tr>
<tr>
<td>8198</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. End of processing enable End User Quarantine task.</td>
</tr>
<tr>
<td>8199</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. Start to process disable End User Quarantine task.</td>
</tr>
<tr>
<td>8200</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>EUQ. End of processing disable End User Quarantine task.</td>
</tr>
<tr>
<td>12289</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>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.</td>
</tr>
<tr>
<td>12290</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>The ScanMail transport scan module is unable to send IPC requests to the ScanMail Master service. Check Windows event log for system errors.</td>
</tr>
</tbody>
</table>
### TABLE B-1. ScanMail Windows Event Log Codes (Continued)

<table>
<thead>
<tr>
<th>EVENT ID</th>
<th>FACILITY</th>
<th>TYPE/SEVERITY</th>
<th>CATEGORY</th>
<th>DESCRIPTION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12291</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>12292</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>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.</td>
<td></td>
</tr>
<tr>
<td>12293</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>The ScanMail transport scan module is unable to create a transport agent object. Make sure the ScanMail DLL files are complete.</td>
<td></td>
</tr>
</tbody>
</table>
TABLE B-1.  ScanMail Windows Event Log Codes (Continued)

<table>
<thead>
<tr>
<th>EVENT ID</th>
<th>FACILITY</th>
<th>TYPE/ SEVERITY</th>
<th>CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>12294</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>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.</td>
</tr>
<tr>
<td>12545</td>
<td>Application</td>
<td>Error</td>
<td>None</td>
<td>The MCP agent between ScanMail and Control manager stopped unexpectedly.</td>
</tr>
<tr>
<td>20480</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Log on/off ScanMail product console.</td>
</tr>
<tr>
<td>20481</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>ScanMail configuration change.</td>
</tr>
<tr>
<td>20482</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>ScanMail management operation.</td>
</tr>
<tr>
<td>28672</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Switch security risk scan methods</td>
</tr>
<tr>
<td>28673</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Smart Scan - Each time File Reputation service was Unavailable.</td>
</tr>
</tbody>
</table>
### TABLE B-1. ScanMail Windows Event Log Codes (Continued)

<table>
<thead>
<tr>
<th>EVENT ID</th>
<th>FACILITY</th>
<th>TYPE/SEVERITY</th>
<th>CATEGORY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>28675</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Smart Scan - Each time File Reputation service was Recovered.</td>
</tr>
<tr>
<td>28676</td>
<td>Application</td>
<td>Warning</td>
<td>None</td>
<td>Smart Scan - Each time Web Reputation service was Unavailable.</td>
</tr>
<tr>
<td>28677</td>
<td>Application</td>
<td>Information</td>
<td>None</td>
<td>Smart Scan - Each time Web Reputation service was Recovered.</td>
</tr>
</tbody>
</table>
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-20
- **Report Database Schema** on page C-39
Log Database Schema

Table C-1. Table [tblMsgEntries] stores message information such as the sender, recipient, and message subject.

### Table C-1. Table [tblMsgEntries]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msg_task_id</td>
<td>int</td>
<td>The scan task this message belongs to</td>
</tr>
<tr>
<td>msg_protocol</td>
<td>int</td>
<td>The protocol this message is sent with</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>nvarchar(255)</td>
<td>The place where this message was found</td>
</tr>
<tr>
<td>msg_source</td>
<td>nvarchar(255)</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>nvarchar(255)</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>nvarchar(255)</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>datetime</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_submit_time</td>
<td>datetime</td>
<td>The message submit time</td>
</tr>
</tbody>
</table>
Table C-2. Table [tblFilterEntries] 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]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msg_entry_id</td>
<td>int</td>
<td>The foreign key for tblMsgEntries</td>
</tr>
<tr>
<td>filter_id</td>
<td>smallint</td>
<td>The id of the filter triggered</td>
</tr>
<tr>
<td>filter_rule</td>
<td>nvarchar(64)</td>
<td>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</td>
</tr>
<tr>
<td>filter_rule_supplement</td>
<td>int</td>
<td>The virus/malware type for security risk filter, risk level of a malicious URL for Web Reputation filter</td>
</tr>
<tr>
<td>filter_engine</td>
<td>nvarchar(32)</td>
<td>The engine version used</td>
</tr>
<tr>
<td>filter_pattern</td>
<td>int</td>
<td>The pattern version used</td>
</tr>
<tr>
<td>filter_action</td>
<td>int</td>
<td>The result of the action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
</tbody>
</table>
### TABLE C-2. Table [tblFilterEntries] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_scan_time</td>
<td>datetime</td>
<td>The scan time</td>
</tr>
<tr>
<td>filter_original</td>
<td>nvarchar(255)</td>
<td>The original file name that triggered the rule</td>
</tr>
<tr>
<td>filter_reason</td>
<td>ntext</td>
<td>Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter.</td>
</tr>
<tr>
<td>sent_to_csm</td>
<td>smallint</td>
<td>(internal use)</td>
</tr>
</tbody>
</table>

### Table C-3. Table [tblStorageEntries] stores information about when the quarantine, archive, or backup action was performed.

### TABLE C-3. Table [tblStorageEntries]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msg_entry_id</td>
<td>int</td>
<td>The foreign key for tblMsgEntries</td>
</tr>
<tr>
<td>msg_destination_full</td>
<td>ntext</td>
<td>The full recipient list in XML format</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>datetime</td>
<td>The scan time</td>
</tr>
<tr>
<td>filter_entry_id</td>
<td>int</td>
<td>The foreign key for tblFilterEntries</td>
</tr>
<tr>
<td>filter_id</td>
<td>smallint</td>
<td>Filter ID</td>
</tr>
</tbody>
</table>
### Table [tblStorageEntries] (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_action</td>
<td>int</td>
<td>The result of the action taken. Reference [action_description.xml], which is located in %SMEX_HOME%/web\xml.</td>
</tr>
<tr>
<td>filter_rule</td>
<td>nvarchar(64)</td>
<td>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.</td>
</tr>
<tr>
<td>file_original</td>
<td>nvarchar(255)</td>
<td>The original file name of this storage.</td>
</tr>
<tr>
<td>storage_guid</td>
<td>uniqueidentifier</td>
<td>The GUID of this storage entry. (Used by AMF)</td>
</tr>
<tr>
<td>storage_reason</td>
<td>smallint</td>
<td>The reason (quarantine, archive, or backup) to make this storage entry.</td>
</tr>
<tr>
<td>storage_path</td>
<td>nvarchar(255)</td>
<td>The path the file saved to</td>
</tr>
<tr>
<td>storage_type</td>
<td>smallint</td>
<td>The storage type (message part or entire message)</td>
</tr>
<tr>
<td>storage_resend_count</td>
<td>smallint</td>
<td>The count of this entity has been resent</td>
</tr>
<tr>
<td>sent_to_csm</td>
<td>smallint</td>
<td>(internal use)</td>
</tr>
</tbody>
</table>
Table C-4. Table [tblActivityEntries] stores event log information. For example, information about the start, progress, and completion of manual update.

**TABLE C-4. Table [tblActivityEntries]**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activity_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>activity_severity</td>
<td>int</td>
<td>The severity of this activity entry</td>
</tr>
<tr>
<td>activity_id</td>
<td>int</td>
<td>The id of this activity entry. Ref [dbconf_log.xml]</td>
</tr>
<tr>
<td>activity_time</td>
<td>datetime</td>
<td>The date and time of this activity entry began</td>
</tr>
<tr>
<td>activity_description</td>
<td>ntext</td>
<td>Activity description</td>
</tr>
<tr>
<td>activity_parameter</td>
<td>ntext</td>
<td>To indicate manual/scheduled update component type: pattern/engine/anti-spam rule</td>
</tr>
<tr>
<td>activity_duration_mark</td>
<td>smallint</td>
<td>To indicate this activity duration is either begin, end, or instant.</td>
</tr>
<tr>
<td>sent_to_csm</td>
<td>smallint</td>
<td>(internal use)</td>
</tr>
</tbody>
</table>
Table C-5. Table [tblPatternEngineInfo] stores information about the engine and patterns that are used to scan email messages.

**Table C-5. Table [tblPatternEngineInfo]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>pei_type</td>
<td>int</td>
<td>The type of the pattern/engine.</td>
</tr>
<tr>
<td>pei_current_version</td>
<td>ntext</td>
<td>The current version of pattern/engine.</td>
</tr>
<tr>
<td>pei_latest_version</td>
<td>ntext</td>
<td>The latest version of pattern/engine.</td>
</tr>
<tr>
<td>pei_last_query_time</td>
<td>datetime</td>
<td>The last query time of pattern/engine.</td>
</tr>
<tr>
<td>pei_last_update_time</td>
<td>datetime</td>
<td>The last update time of pattern/engine.</td>
</tr>
<tr>
<td>pei_last_successful_update_time</td>
<td>datetime</td>
<td>The last successful update time of pattern/engine.</td>
</tr>
<tr>
<td>pei_last_update_status</td>
<td>int</td>
<td>The last update status of pattern/engine.</td>
</tr>
<tr>
<td>pei_last_update_status_description</td>
<td>ntext</td>
<td>The last update status description of pattern/engine.</td>
</tr>
</tbody>
</table>
Table C-6. Table [tblScanningSummary] stores the scan summary information of detected security risks for today.

**Table C-6. Table [tblScanningSummary]**

<table>
<thead>
<tr>
<th><strong>FIELD NAME</strong></th>
<th><strong>DATA TYPE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>ss_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>ss_type</td>
<td>int</td>
<td>The type of malicious code (such as virus, spam, blocked attachment). Possible values of the ss_type, reference Note5 of this document.</td>
</tr>
<tr>
<td>ss_time</td>
<td>datetime</td>
<td>The scanning time</td>
</tr>
<tr>
<td>ss_count</td>
<td>int</td>
<td>The count of each type of scanned object</td>
</tr>
</tbody>
</table>

Table C-7. Table [tblCfgReplication] stores the configuration replication server list. Perform configuration replication from the Server Management console or Control Manager..

**Table C-7. Table [tblCfgReplication]**

<table>
<thead>
<tr>
<th><strong>FIELD NAME</strong></th>
<th><strong>DATA TYPE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>cr_session_guid</td>
<td>uniqueidentifier</td>
<td>The session GUID</td>
</tr>
<tr>
<td>cr_time</td>
<td>datetime</td>
<td>The start time</td>
</tr>
<tr>
<td>cr_server_list</td>
<td>ntext</td>
<td>The server list</td>
</tr>
<tr>
<td>cr_selection_list</td>
<td>ntext</td>
<td>The selection list</td>
</tr>
<tr>
<td>cr_id</td>
<td>int</td>
<td>(Not in use)</td>
</tr>
</tbody>
</table>
Table C-8. Table [tblCfgReplicationStatus] stores the configuration replication status.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crs_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>crs_session_guid</td>
<td>uniqueidentifier</td>
<td>The session GUID</td>
</tr>
<tr>
<td>crs_start_time</td>
<td>datetime</td>
<td>The start time of configuration replication</td>
</tr>
<tr>
<td>crs_end_time</td>
<td>datetime</td>
<td>The end time of configuration replication</td>
</tr>
<tr>
<td>crs_server</td>
<td>ntext</td>
<td>The server name which did the configuration replication</td>
</tr>
<tr>
<td>crs_status</td>
<td>int</td>
<td>The status of the configuration replication</td>
</tr>
<tr>
<td>crs_description</td>
<td>ntext</td>
<td>The description of the configuration replication</td>
</tr>
</tbody>
</table>
**Note:** For Event Tracking log query Microsoft Operations Manager (MOM) and System Center Operations Manager (SCOM) will not get the data directly from ScanMail, but the same information can be queried from the ScanMail database.

**Table C-9.** Table [tblAuditLog] stores all event tracking logs.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>ServerName</td>
<td>nvarchar(255)</td>
<td>The virtual server name</td>
</tr>
<tr>
<td>UserName</td>
<td>nvarchar(255)</td>
<td>The user name</td>
</tr>
<tr>
<td>EventTime</td>
<td>datetime</td>
<td>The current time of Audit Event</td>
</tr>
<tr>
<td>IpAddress</td>
<td>nvarchar(255)</td>
<td>The remote host IP address</td>
</tr>
<tr>
<td>EventType</td>
<td>smallint</td>
<td>The event type (Three types: log in/out, configuration, operation)</td>
</tr>
<tr>
<td>SourceType</td>
<td>smallint</td>
<td>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))</td>
</tr>
<tr>
<td>LogDescription</td>
<td>nvarchar(255)</td>
<td>The description of log</td>
</tr>
</tbody>
</table>
Table C-10. Table [tblManagementGroupList] is not used.

**TABLE C-10. Table [tblManagementGroupList]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgl_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>mgl_group_name</td>
<td>ntext</td>
<td>The group name in the management group list</td>
</tr>
</tbody>
</table>

Table C-11. Table [tblManagementServerList] is not used.

**TABLE C-11. Table [tblManagementServerList]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msl_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msl_server_name</td>
<td>ntext</td>
<td>The server name in the management group list</td>
</tr>
<tr>
<td>msl_group_id</td>
<td>int</td>
<td>The group ID to which the server belongs.</td>
</tr>
</tbody>
</table>

Table C-12. Table [tblManagementGroupMemberList] is not used.

**TABLE C-12. Table [tblManagementGroupMemberList]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgml_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>mgml_group_id</td>
<td>int</td>
<td>The group ID from table [tblManagementGroupList]</td>
</tr>
<tr>
<td>mgml_server_id</td>
<td>int</td>
<td>The server ID from table [tblManagementServerList]</td>
</tr>
</tbody>
</table>
Table C-13. Table [tblCfgReplicationHistory] stores the time of the last configuration replication.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>crh_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>crh_session_guid</td>
<td>uniqueidentifier</td>
<td>The session GUID</td>
</tr>
<tr>
<td>crh_time</td>
<td>datetime</td>
<td>The last time of configuration replication</td>
</tr>
</tbody>
</table>

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':

```sql
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
```
Table C-14. Possible values of the activity_id lists the items to note for this example.

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_CMD_ENGINE_PATTERN_UPDATE</td>
<td>1</td>
<td>The engine pattern update command</td>
</tr>
<tr>
<td>ID_CMD_MANUAL_SCAN</td>
<td>3</td>
<td>The manual scan command</td>
</tr>
<tr>
<td>ID_CMD_SCHEDULE_SCAN</td>
<td>4</td>
<td>The schedule scan command</td>
</tr>
<tr>
<td>ID_CMD_CFG_DEPLOYMENT</td>
<td>5</td>
<td>The configuration deployment command</td>
</tr>
<tr>
<td>ID_CMD_CFG_QUERY_PATTERN_ENGINE_VERSION</td>
<td>6</td>
<td>The query the pattern engine version command</td>
</tr>
<tr>
<td>ID_CMD_QM_RESEND</td>
<td>7</td>
<td>The quarantine manager resend message command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_CLEAN_SPAM_MSG</td>
<td>8</td>
<td>The End User Quarantine (EUQ) clean spam message command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_CREATE_SPAM_FOLDER_RULE</td>
<td>9</td>
<td>The End User Quarantine (EUQ) create spam folder rule command</td>
</tr>
<tr>
<td>ID_CMD_LOG_MAINTENANCE</td>
<td>10</td>
<td>The log maintenance command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_HOUSEKEEPING_TASK</td>
<td>11</td>
<td>The EUQ house keeping task command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_ENABLE_EUQ</td>
<td>12</td>
<td>The enable End User Quarantine (EUQ) command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_DISABLE_EUQ</td>
<td>13</td>
<td>The disable End User Quarantine (EUQ) command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_UPDATE_CONFIG</td>
<td>14</td>
<td>The update End User Quarantine (EUQ) configuration command</td>
</tr>
</tbody>
</table>
### TABLE C-14. Possible values of the activity_id (Continued)

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_CMD_UPDATE_COMPONENT</td>
<td>15</td>
<td>The update component command</td>
</tr>
<tr>
<td>ID_CMD_QUERY_LATEST_AU_COMPONENT</td>
<td>16</td>
<td>The query latest AU component command</td>
</tr>
<tr>
<td>ID_CMD_QUERY_LOCAL_LATEST_AU_COMPONENT</td>
<td>17</td>
<td>The query local latest AU component command</td>
</tr>
<tr>
<td>ID_CMD_QM_DELETE</td>
<td>18</td>
<td>The delete quarantine manager message command</td>
</tr>
<tr>
<td>ID_CMD_UPDATE_CLUSTER_COMPONENT</td>
<td>19</td>
<td>The update cluster component command</td>
</tr>
</tbody>
</table>

**Example 2: Query:Get Quarantine Log(storage_reason=1)**

```sql
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;
Table C-15. Possible values of the storage_reason lists the items to note for this example.

**Table C-15. Possible values of the storage_reason**

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR_QUARANTINE</td>
<td>1</td>
<td>The reason for this storage entry is quarantine.</td>
</tr>
<tr>
<td>SR_BACKUP</td>
<td>2</td>
<td>The reason for this storage entry is backup.</td>
</tr>
<tr>
<td>SR_ARCHIVE</td>
<td>3</td>
<td>The reason for this storage entry is archive</td>
</tr>
</tbody>
</table>

Table C-16. Possible values of the filter_id lists the items to note for this example.

**Table C-16. Possible values of the filter_id**

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_FILTERTYPE_VIRUS_SCANNING</td>
<td>1(0x1)</td>
<td>The filter type of security risk scan</td>
</tr>
<tr>
<td>ID_FILTERTYPE_EMANAGER_5X</td>
<td>2(0x2)</td>
<td>The filter type emanager_5X</td>
</tr>
<tr>
<td>ID_FILTERTYPE_FILE_BLOCKING</td>
<td>4(0x4)</td>
<td>The filter type of file blocking</td>
</tr>
<tr>
<td>ID_FILTERTYPE_ANTISPAM</td>
<td>8(0x8)</td>
<td>The filter type of spam prevention</td>
</tr>
<tr>
<td>ID_FILTERTYPE_SIZE_CHECKER</td>
<td>16(0x10)</td>
<td>The filter type of size check</td>
</tr>
<tr>
<td>ID_FILTERTYPE_ACTIVE_MESSAGE_FILTER</td>
<td>32(0x20)</td>
<td>Active message filter</td>
</tr>
</tbody>
</table>
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

Table C-17. Possible values of the EventType lists the items to note for this example.

TABLE C-17. Possible values of the EventType

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE_LOG_IN_OUT</td>
<td>1</td>
<td>Log in/out</td>
</tr>
<tr>
<td>TYPE_CONFIGURATION</td>
<td>2</td>
<td>Configuration</td>
</tr>
<tr>
<td>TYPE_OPERATION_EVENT</td>
<td>3</td>
<td>Operation event</td>
</tr>
</tbody>
</table>
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;
```
Table C-18. Possible values of the `ss_type` lists the items to note for this example.

<table>
<thead>
<tr>
<th>VARIABLE</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST_SCANNED_MESSAGE</td>
<td>100</td>
<td>Scanned message</td>
</tr>
<tr>
<td>ST_DETECTED_VIRUS</td>
<td>110</td>
<td>Detected virus</td>
</tr>
<tr>
<td>ST_BLOCKED_ATTACHMENT</td>
<td>111</td>
<td>Blocked attachment</td>
</tr>
<tr>
<td>ST_DETECTED_SPAM</td>
<td>112</td>
<td>Detected spam.</td>
</tr>
<tr>
<td>ST_CONTENT_VIOLATION</td>
<td>113</td>
<td>Content violation</td>
</tr>
<tr>
<td>ST_DETECTED_ERS</td>
<td>114</td>
<td>Detected ERS</td>
</tr>
<tr>
<td>ST_SUSPICIOUS_URL</td>
<td>115</td>
<td>Malicious URL</td>
</tr>
<tr>
<td>ST_UNCLEANABLE_VIRUS</td>
<td>117</td>
<td>Uncleanable virus</td>
</tr>
<tr>
<td>ST_SCANNED_ATTACHMENT</td>
<td>118</td>
<td>Scanned attachment</td>
</tr>
<tr>
<td>ST_UNKNOWN</td>
<td>119</td>
<td>Unknown type</td>
</tr>
<tr>
<td>ST_DETECTED_PHISH</td>
<td>120</td>
<td>Detected phish</td>
</tr>
<tr>
<td>ST_DETECTEDSpyware</td>
<td>121</td>
<td>Detected spyware</td>
</tr>
<tr>
<td>ST_FALSE_POSITIVE</td>
<td>124</td>
<td>False positive</td>
</tr>
<tr>
<td>ST_UNSCANNABLE_ENTITY</td>
<td>151</td>
<td>Unscannable entity</td>
</tr>
</tbody>
</table>
Log View Database Schema

Table C-19. View [vwMsgFilterEntriesTmp] combines tblMsgEntries and tblFilterEntries.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_entry_id</td>
<td>tblFilterEntries</td>
<td>msg_entry_id</td>
<td>Primary key of the table [tblMsgEntries]</td>
</tr>
<tr>
<td>msg_delivertim</td>
<td>tblMsgEntries</td>
<td>msg_delivertim</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>tblMsgEntries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>tblMsgEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>tblMsgEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>tblMsgEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_id</td>
<td>tblFilterEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>filter_santime</td>
<td>tblFilterEntries</td>
<td>filter_santime</td>
<td>The scan time</td>
</tr>
<tr>
<td>filter_rule</td>
<td>tblFilterEntries</td>
<td>filter_rule</td>
<td>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</td>
</tr>
</tbody>
</table>
Table C-20. View [vwMsgFilterEntries] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>file_original</td>
<td>tblFilterEntries</td>
<td>file_original</td>
<td>The original file name that triggered the rule</td>
</tr>
<tr>
<td>filter_action</td>
<td>tblFilterEntries</td>
<td>filter_action</td>
<td>The result of the action taken</td>
</tr>
<tr>
<td>filter_reason</td>
<td>tblFilterEntries</td>
<td>filter_reason</td>
<td>The detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter</td>
</tr>
<tr>
<td>filter_rule_supplement</td>
<td>tblFilterEntries</td>
<td>filter_rule_supplement</td>
<td>The virus/malware type, used to separate virus and spyware</td>
</tr>
</tbody>
</table>

Table C-20. View [vwMsgFilterEntries] combines table tblStorageEntries and view vwMsgFilterEntriesTmp.

Table C-20. View [vwMsgFilterEntries]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
</tbody>
</table>
### TABLE C-20. View [vwMsgFilterEntries] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>msg_subject</code></td>
<td>vwMsgFilterEntriesTmp</td>
<td><code>msg_subject</code></td>
<td>The subject of this message</td>
</tr>
<tr>
<td><code>filter_rule</code></td>
<td>vwMsgFilterEntriesTmp</td>
<td><code>filter_rule</code></td>
<td>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</td>
</tr>
<tr>
<td><code>filter_reason</code></td>
<td>vwMsgFilterEntriesTmp</td>
<td><code>filter_reason</code></td>
<td>Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter.</td>
</tr>
<tr>
<td><code>file_original</code></td>
<td>vwMsgFilterEntriesTmp</td>
<td><code>file_original</code></td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td><code>msg_entry_id</code></td>
<td>vwMsgFilterEntriesTmp</td>
<td><code>msg_entry_id</code></td>
<td>Primary key of the table [tblMsgEntries]</td>
</tr>
<tr>
<td><code>filter_id</code></td>
<td>vwMsgFilterEntriesTmp</td>
<td><code>filter_id</code></td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td><code>filter_action</code></td>
<td>vwMsgFilterEntriesTmp</td>
<td><code>filter_action</code></td>
<td>The result of the action taken</td>
</tr>
<tr>
<td><code>storage_entry_id</code></td>
<td>tblStorageEntries</td>
<td><code>storage_entry_id</code></td>
<td>Primary key of the table [tblStorageEntries]</td>
</tr>
</tbody>
</table>
### TABLE C-20. View [vwMsgFilterEntries] (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_path</td>
<td>tblStorageEntries</td>
<td>storage_path</td>
<td>The path the file saved to</td>
</tr>
<tr>
<td>storage_reason</td>
<td>tblStorageEntries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) to make this storage entry.</td>
</tr>
<tr>
<td>filter_rule_supplement</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_rule_supplement</td>
<td>The virus/malware type, used to separate virus and spyware.</td>
</tr>
</tbody>
</table>

Table C-21. View [vwMsgStorageEntries] combines table tblMsgEntries and tblStorageEntries

### TABLE C-21. View [vwMsgStorageEntries]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>tblStorageEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table [tblStorageEntries]</td>
</tr>
<tr>
<td>msg_source</td>
<td>tblMsgEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>tblMsgEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>tblMsgEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_id</td>
<td>tblStorageEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>tblStorageEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>FIELD NAME</td>
<td>FROM TABLE</td>
<td>FROM FIELD</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>filter_rule</td>
<td>tblStorageEntries</td>
<td>filter_rule</td>
<td>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</td>
</tr>
<tr>
<td>file_original</td>
<td>tblStorageEntries</td>
<td>file_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td>filter_action</td>
<td>tblStorageEntries</td>
<td>filter_action</td>
<td>The result of the action taken</td>
</tr>
<tr>
<td>storage_reason</td>
<td>tblStorageEntries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) for this storage entry</td>
</tr>
<tr>
<td>storage_resend_count</td>
<td>tblStorageEntries</td>
<td>storage_resend_count</td>
<td>The count of this entry has been resent</td>
</tr>
</tbody>
</table>
Table C-22. View [vwABLogs] select blocked attachments data from view vwMsgFilterEntries.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilterEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEntries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilterEntries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_cf</td>
<td>vwMsgFilterEntries</td>
<td>filter_rule</td>
<td>File type blocked by attachment blocking filter(such as .exe)</td>
</tr>
</tbody>
</table>
### TABLE C-22. View [vwABLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_original</td>
<td>vwMsgFilterEntries</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td>Filter_action</td>
<td>vwMsgFilterEntries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilterEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME%
% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
Database Schema for 64-bit Operating Systems

**Table C-23. View [vwAVLogs]** select security risk scan data from view vwMsgFilterEntries.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilter-Entries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilter-Entries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilter-Entries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilter-Entries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilter-Entries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilter-Entries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilter-Entries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_av</td>
<td>vwMsgFilter-Entries</td>
<td>filter_rule</td>
<td>Virus/malware name</td>
</tr>
<tr>
<td>filter_original</td>
<td>vwMsgFilter-Entries</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
</tbody>
</table>
### TABLE C-23. View [vwAVLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter_action</td>
<td>vwMsgFilter-Entries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
<tr>
<td>filter_rule_supplement</td>
<td>vwMsgFilter-Entries</td>
<td>filter_rule_supplement</td>
<td>The virus/malware type, used to separate virus and spyware.</td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilter-Entries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>storage_reason</td>
<td>vwMsgFilter-Entries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) for this storage entry.</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
Table C-24. **View [vwCFLogs]** select content violation data from view vwMsgFilterEntries.

**TABLE C-24. View [vwCFLogs]**

<table>
<thead>
<tr>
<th><strong>FIELD NAME</strong></th>
<th><strong>FROM TABLE</strong></th>
<th><strong>FROM FIELD</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilterEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEntries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilterEntries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_cf</td>
<td>vwMsgFilterEntries</td>
<td>filter_rule</td>
<td>Rule name for content filter</td>
</tr>
<tr>
<td>filter_original</td>
<td>vwMsgFilterEntries</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
</tbody>
</table>
### TABLE C-24. View [vwCFLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter_action</td>
<td>vwMsgFilter-Entries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\%

<table>
<thead>
<tr>
<th>filter_reason</th>
<th>vwMsgFilter-Entries</th>
<th>filter_reason</th>
<th>Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_id</td>
<td>vwMsgFilter-Entries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
</tbody>
</table>
Table C-25. View [vwDLPLogs] select Data Loss Prevention incident data from view vwMsgFilterEntries.

TABLE C-25. View [vwDLPLogs]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilter-Entries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilter-Entries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilter-Entries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilter-Entries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilter-Entries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilter-Entries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilter-Entries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_dlp</td>
<td>vwMsgFilter-Entries</td>
<td>filter_rule</td>
<td>Rule name for Data Loss Prevention</td>
</tr>
</tbody>
</table>
### TABLE C-25. View [vwDLPLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_action</td>
<td>vwMsgFilter-Entries</td>
<td>filter_action</td>
<td>The result of action taken</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reference [action_description.xml], which is located in %SMEX_HOME%/web/xml.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> %SMEX_HOME% represents the ScanMail installation directory. By default, this is C:\Program Files\Trend Micro\Smex.</td>
</tr>
<tr>
<td>file_original</td>
<td>vwMsgFilter-Entries</td>
<td>file_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td>filter_template</td>
<td>vwMsgFilter-Entries</td>
<td>filter_reason</td>
<td>The triggered Data Loss Prevention template</td>
</tr>
</tbody>
</table>

Table C-26. View [vwUSLogs] select unscannable message data from view vwMsgFilterEntries.

### TABLE C-26. View [vwUSLogs]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilter-Entries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilter-Entries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilter-Entries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
</tbody>
</table>
### TABLE C-26. View [vwUSLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilter-</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilter-</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilter-</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilter-</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_rule_us</td>
<td>vwMsgFilter-</td>
<td>filter_rule</td>
<td>Unscannable reason</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_original</td>
<td>vwMsgFilter-</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
TABLE C-26. View [vwUSLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter_action</td>
<td>vwMsgFilterEntries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%/web/xml.</td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilterEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>storage_reason</td>
<td>vwMsgFilterEntries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) for this storage entry.</td>
</tr>
</tbody>
</table>

Table C-27. View [vwQuarantineLogs] select storage data from view vwMsgFilterEntries.

TABLE C-27. View [vwQuarantineLogs]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilterEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table [tblIStorageEntries]</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>Field Name</td>
<td>From Table</td>
<td>From Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>------------------</td>
<td>--------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule</td>
<td>vwMsgFilterEntries</td>
<td>filter_rule</td>
<td>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</td>
</tr>
<tr>
<td>storage_resend_count</td>
<td>vwMsgFilterEntries</td>
<td>storage_resend_count</td>
<td>The count of this entry has been resent</td>
</tr>
<tr>
<td>storage_reason</td>
<td>vwMsgFilterEntries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) for this storage entry.</td>
</tr>
</tbody>
</table>
Table C-28. View [vwWTPLogs] select data about malicious URL from view vwMsgStorageEntries.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEntries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_uhf</td>
<td>vwMsgFilterEntries</td>
<td>filter_rule_uhf</td>
<td>Risk level of a malicious URL for Web Reputation filter</td>
</tr>
<tr>
<td>Suspicious_url</td>
<td>vwMsgFilterEntries</td>
<td>filter_reason</td>
<td>Suspicious url</td>
</tr>
</tbody>
</table>
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’

```sql
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
```

Note: %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
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 seven tables. These tables are not related to each other.

Table C-29. Table [tblSummary] stores the summary detected security risks per hour.

### TABLE C-29. Table [tblSummary]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>summary_datetime</td>
<td>datetime</td>
<td>This datetime when this record was summarized</td>
</tr>
<tr>
<td>summary_total_message_count</td>
<td>int</td>
<td>The total message scanned count for this period</td>
</tr>
<tr>
<td>summary_total_attachment_count</td>
<td>int</td>
<td>The total attachment scanned count for this period</td>
</tr>
<tr>
<td>Summary_virus_detected_count</td>
<td>int</td>
<td>The virus/malware count for this period</td>
</tr>
<tr>
<td>summary_virus_uncleanable_count</td>
<td>int</td>
<td>The uncleanable virus/malware count for this period</td>
</tr>
<tr>
<td>summary_attachment_blocked_count</td>
<td>int</td>
<td>The blocked attachment count for this period</td>
</tr>
<tr>
<td>summary_content_filtered_count</td>
<td>int</td>
<td>The filtered-count for this period.</td>
</tr>
<tr>
<td>summary_dlp_filtered_count</td>
<td>int</td>
<td>The filtered-count for this period</td>
</tr>
<tr>
<td>Summary_spam_detected_count</td>
<td>int</td>
<td>The spam message count</td>
</tr>
</tbody>
</table>
TABLE C-29. Table [tblSummary] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary_phish_detected_count</td>
<td>int</td>
<td>The phish message count</td>
</tr>
<tr>
<td>summary_false_positive_count</td>
<td>int</td>
<td>The reported false positive count</td>
</tr>
<tr>
<td>Summary_unscannable_entity_count</td>
<td>int</td>
<td>The unscannable count for this period.</td>
</tr>
<tr>
<td>Sent_to_csm</td>
<td>smallint</td>
<td>(internal use)</td>
</tr>
<tr>
<td>summary_ers_count</td>
<td>int</td>
<td>Blocked IP count for this period</td>
</tr>
<tr>
<td>summary_suspicious_url_count</td>
<td>int</td>
<td>The suspicious URL count shown in the report summary</td>
</tr>
<tr>
<td>summary_spyware_detected_count</td>
<td>int</td>
<td>The spyware/grayware count for this period</td>
</tr>
</tbody>
</table>

Table C-30. Table [tblAttachmentInfo] stores blocked attachment information by category.

TABLE C-30. Table [tblAttachmentInfo]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>attachinfo_datetime</td>
<td>datetime</td>
<td>The datetime of summarization</td>
</tr>
<tr>
<td>attachinfo_cate_id</td>
<td>int</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>attachinfo_value</td>
<td>nvarchar(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>attachinfo_count</td>
<td>int</td>
<td>The count of this data category</td>
</tr>
</tbody>
</table>
Table C-31. Table `tblContentInfo` stores content violation information by category.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>contentinfo_datetime</td>
<td>datetime</td>
<td>The datetime of summarization.</td>
</tr>
<tr>
<td>contentinfo_cate_id</td>
<td>int</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>contentinfo_value</td>
<td>nvarchar(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>contentinfo_count</td>
<td>int</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>

Table C-32. Table `tblDLPInfo` stores Data Loss Prevention incident information by category.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>dlpinfo_datetime</td>
<td>datetime</td>
<td>The datetime of summarization.</td>
</tr>
<tr>
<td>dlpinfo_cate_id</td>
<td>int</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>dlpinfo_value</td>
<td>nvarchar(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>dlpinfo_count</td>
<td>int</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>
Table C-33. Table [tblSpamInfo] stores spam information by category.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>spaminfo_datetime</td>
<td>datetime</td>
<td>The date/time of summarization</td>
</tr>
<tr>
<td>spaminfo_cate_id</td>
<td>int</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>spaminfo_value</td>
<td>nvarchar(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>spaminfo_count</td>
<td>int</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>

Table C-34. Table [tblVirusInfo] stores security risk information by category.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>virusinfo_datetime</td>
<td>datetime</td>
<td>The date/time of summarization</td>
</tr>
<tr>
<td>virusinfo_cate_id</td>
<td>int</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>virusinfo_value</td>
<td>nvarchar(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>virusinfo_count</td>
<td>int</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>
**Table C-35.** Table [tblUnscannableInfo] stores unscannable message information by category.

**Table C-35.** Table [tblUnscannableInfo]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>ucanableifo_datatime</td>
<td>datetime</td>
<td>The datetime of summarization.</td>
</tr>
<tr>
<td>ucanableifo_cate_id</td>
<td>int</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>ucanableifo_value</td>
<td>nvarchar(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>ucanableifo_count</td>
<td>int</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>

**Table C-36.** Table [tblReportCollectionSummary] stores the total number of detected security risks. This table is used by MOM/SCOM

**Table C-36.** Table [tblReportCollectionSummary]

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>summary_total_message_count</td>
<td>int</td>
<td>The total message scanned count for this period</td>
</tr>
<tr>
<td>summary_total_attachment_count</td>
<td>int</td>
<td>The total attachment scanned count for this period</td>
</tr>
<tr>
<td>summary_virus_detected_count</td>
<td>int</td>
<td>The virus/malware count for this period</td>
</tr>
<tr>
<td>summary_virus_uncleanable_count</td>
<td>int</td>
<td>The uncleanable virus/malware count for this period</td>
</tr>
<tr>
<td>summary_attachment_blocked_count</td>
<td>int</td>
<td>The blocked attachment count for this period</td>
</tr>
</tbody>
</table>
### TABLE C-36. Table [tblReportCollectionSummary] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary_content_filtered_count</td>
<td>int</td>
<td>The filtered-count for this period.</td>
</tr>
<tr>
<td>summary_dlp_filtered_count</td>
<td>int</td>
<td>The filtered-count for this period.</td>
</tr>
<tr>
<td>summary_spam_detected_count</td>
<td>int</td>
<td>The spam message count</td>
</tr>
<tr>
<td>summary_phish_detected_count</td>
<td>int</td>
<td>The phish message count</td>
</tr>
<tr>
<td>summary_unscannable_entity_count</td>
<td>int</td>
<td>The unscannable count for this period</td>
</tr>
<tr>
<td>summary_worm_trojan_virus_type_count</td>
<td>int</td>
<td>The worm trojan virus type count for this period</td>
</tr>
<tr>
<td>summary_packed_file_virus_type_count</td>
<td>int</td>
<td>The packed file virus type count for this period</td>
</tr>
<tr>
<td>summary_generic_virus_type_count</td>
<td>int</td>
<td>The generic virus/malware type count for this period</td>
</tr>
<tr>
<td>summary_virus_virus_type_count</td>
<td>int</td>
<td>The virus/malware type count for this period</td>
</tr>
<tr>
<td>summary_other_malicious_code_virus_type_count</td>
<td>int</td>
<td>Other malicious code virus type count for this period</td>
</tr>
<tr>
<td>summary_additional_threat_virus_type_count</td>
<td>int</td>
<td>The additional threat virus type count for this period</td>
</tr>
<tr>
<td>summary_ers_count</td>
<td>int</td>
<td>Blocked IP count for this period</td>
</tr>
<tr>
<td>summary_suspicious_url_count</td>
<td>int</td>
<td>The suspicious URL count shown in the report summary</td>
</tr>
</tbody>
</table>
Table C-37. Table [tblURLInfo] (add by WTP) stores malicious URL information by category.

TABLE C-37. Table [tblURLInfo] (add by WTP)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>urlinfo_datetime</td>
<td>Date time</td>
<td>Date &amp; Time</td>
</tr>
<tr>
<td>urlinfo_cate_id</td>
<td>int</td>
<td>Category ID</td>
</tr>
<tr>
<td>urlinfo_value</td>
<td>nvarchar(64)</td>
<td>The name of the report item counter</td>
</tr>
<tr>
<td>urlinfo_count</td>
<td>int</td>
<td>The value of the report item counter</td>
</tr>
</tbody>
</table>

Example 1: Get Last Summary Time from table[tblSummary].

```
SELECT MAX(summary_datetime) AS lastest_datetime
FROM tblSummary;
```

Example 2: Get MOM 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’, ’unsccannable 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;

Table C-38. Possible values of the virusinfo_cate_id lists the items to note for this example.

**TABLE C-38. Possible values of the virusinfo_cate_id**

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPT_CATEID_VS_VIRUS_NAME</td>
<td>151</td>
<td>The count of viruses/malware of a certain virus name.</td>
</tr>
<tr>
<td>RPT_CATEID_VS_VIRUS_TYPE</td>
<td>152</td>
<td>The count of viruses/malware of a certain virus type.</td>
</tr>
<tr>
<td>RPT_CATEID_VS_ACTION</td>
<td>153</td>
<td>The count of viruses/malware which were taken the same action.</td>
</tr>
<tr>
<td>RPT_CATEID_SPYWARE_NAME</td>
<td>154</td>
<td>The count of spyware of a certain spyware name.</td>
</tr>
<tr>
<td>RPT_CATEID_SPYWARE_ACTION</td>
<td>155</td>
<td>The count of spyware which were taken the same action.</td>
</tr>
<tr>
<td>RPT_CATEID_VS_SENDER</td>
<td>156</td>
<td>The count of a single sender who sent virus/malware</td>
</tr>
<tr>
<td>RPT_CATEID_SPYWARE_SENDER</td>
<td>157</td>
<td>The count of a single sender who sent spyware/grayware</td>
</tr>
<tr>
<td>RPT_CATEID_AB_FILETYPE</td>
<td>201</td>
<td>The count of blocked attachment of a certain file type</td>
</tr>
<tr>
<td>RPT_CATEID_AB_EXTENSION</td>
<td>202</td>
<td>The count of blocked attachments of a certain extension</td>
</tr>
<tr>
<td>RPT_CATEID_AB_FILENAME</td>
<td>203</td>
<td>The count of blocked attachments of a certain filename</td>
</tr>
<tr>
<td>RPT_CATEID_CF_SENDER</td>
<td>251</td>
<td>The count for a single sender that triggered the content filtering rules</td>
</tr>
</tbody>
</table>
### TABLE C-38. Possible values of the `virusinfo_cate_id` (Continued)

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPT_CATEID_CF_RECIPIENT</td>
<td>252</td>
<td>The count of content violation of an individual recipient</td>
</tr>
<tr>
<td>RPT_CATEID_CF_RULE</td>
<td>253</td>
<td>The count of content violation of a content filtering rule</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAM_SENDER</td>
<td>301</td>
<td>The count of spam messages from an individual sender</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAM_DOMAIN</td>
<td>302</td>
<td>The count of spam messages from an individual domain</td>
</tr>
<tr>
<td>RPT_CATEID_AS_FALSE_POSITIVE_DOMAIN</td>
<td>303</td>
<td>The count of false positive messages from an individual domain</td>
</tr>
<tr>
<td>RPT_CATEID_AS_FALSE_POSITIVE_SENDER</td>
<td>304</td>
<td>The count of false positive messages from an individual sender</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAM_CATEGORY</td>
<td>305</td>
<td>The count of spam messages of a single spam category</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAM_MAILBOX</td>
<td>306</td>
<td>The count of spam message to an individual recipient</td>
</tr>
<tr>
<td>RPT_CATEID_UNSCANNABLE_ENTITY</td>
<td>351</td>
<td>The count of unscannable messages</td>
</tr>
<tr>
<td>RPT_CATEID_UF_SUSPICIOUS_URL</td>
<td>401</td>
<td>The count of malicious URL</td>
</tr>
<tr>
<td>RPT_CATEID_UF_SENDER</td>
<td>402</td>
<td>The count of a single sender who sent email messages that contained a malicious URL</td>
</tr>
</tbody>
</table>
### Table C-39. Virus Type

<table>
<thead>
<tr>
<th>Virus Type String</th>
<th>Virus Type ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>2</td>
</tr>
<tr>
<td>Trojan</td>
<td>4</td>
</tr>
<tr>
<td>Spyware</td>
<td>16</td>
</tr>
<tr>
<td>Joke</td>
<td>8</td>
</tr>
<tr>
<td>Test_Virus</td>
<td>8</td>
</tr>
<tr>
<td>Other</td>
<td>8</td>
</tr>
<tr>
<td>Packer</td>
<td>16384</td>
</tr>
<tr>
<td>Generic</td>
<td>32768</td>
</tr>
</tbody>
</table>

### Table C-40. Virus Name String

<table>
<thead>
<tr>
<th>Virus Name String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected file</td>
</tr>
<tr>
<td>Over restriction (others)</td>
</tr>
<tr>
<td>Over restriction (mail entity count)</td>
</tr>
<tr>
<td>Over restriction (message body size)</td>
</tr>
<tr>
<td>Over restriction (attachment size)</td>
</tr>
<tr>
<td>Over restriction (decompressed file count)</td>
</tr>
<tr>
<td>VIRUS NAME STRING</td>
</tr>
<tr>
<td>-------------------------------------------</td>
</tr>
<tr>
<td>Over restriction (decompressed file size)</td>
</tr>
<tr>
<td>Over restriction (number of layer of compression)</td>
</tr>
<tr>
<td>Over restriction (compression ratio)</td>
</tr>
</tbody>
</table>
Database Schema for 32-bit Operating Systems

This chapter includes database schema for 32-bit operating systems.

Topics include:
• Log Database Schema on page D-2
• Log View Database Schema on page D-21
Log Database Schema

Table D-1. Table [tblMsgEntries] stores message information such as the sender, recipient, and message subject.

**TABLE D-1. Table [tblMsgEntries]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msg_task_id</td>
<td>Number(Long Integer)</td>
<td>The scan task this message belongs to</td>
</tr>
<tr>
<td>msg_protocol</td>
<td>Number(Long Integer)</td>
<td>The protocol this message is sent with</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>Text(255)</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>Text(255)</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>Text(255)</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>Text(255)</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>Date/Time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_submit_time</td>
<td>Date/Time</td>
<td>The message submit time</td>
</tr>
</tbody>
</table>
Table D-2. Table [tblFilterEntries] 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 D-2. Table [tblFilterEntries]**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msg_entry_id</td>
<td>Number(Long Integer)</td>
<td>The foreign key for tblMsgEntries</td>
</tr>
<tr>
<td>filter_id</td>
<td>Number(Integer)</td>
<td>The id of the filter triggered</td>
</tr>
<tr>
<td>filter_rule</td>
<td>Text(64)</td>
<td>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</td>
</tr>
<tr>
<td>filter_rule_supplement</td>
<td>Number(Long Integer)</td>
<td>The virus/malware type for security risk filter, risk level of a malicious URL for Web Reputation filter</td>
</tr>
<tr>
<td>filter_engine</td>
<td>Text(32)</td>
<td>The engine version used</td>
</tr>
<tr>
<td>filter_pattern</td>
<td>Number(Long Integer)</td>
<td>The pattern version used</td>
</tr>
</tbody>
</table>
### TABLE D-2. Table [tblFilterEntries] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| filter_action | Number(Long Integer) | 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 | Date/Time               | The scan time                                                                                                                                 |
| filter_original | Text(255)               | The original filename that triggered the rule                                                                                             |
| filter_reason  | memo                 | The detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter.       |
| sent_to_csm   | Number(Integer)        | (internal use)                                                                                                                             |
Table D-3. Table [tblStorageEntries] stores information about when the quarantine, archive, or backup action was performed.

**TABLE D-3. Table [tblStorageEntries]**

<table>
<thead>
<tr>
<th><strong>FIELD NAME</strong></th>
<th><strong>DATA TYPE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msg_entry_id</td>
<td>Number(Long Integer)</td>
<td>The foreign key for tblMsgEntries</td>
</tr>
<tr>
<td>msg_destination_full</td>
<td>memo</td>
<td>The full recipient list in XML format</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>Date/Time</td>
<td>The scan time</td>
</tr>
<tr>
<td>filter_entry_id</td>
<td>Number(Long Integer)</td>
<td>The foreign key for tblFilterEntries</td>
</tr>
<tr>
<td>filter_id</td>
<td>Number(Integer)</td>
<td>Filter ID</td>
</tr>
<tr>
<td>filter_action</td>
<td>Number(Long Integer)</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
### Table D-3. Table [tblStorageEntries] (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_rule</td>
<td>Text(64)</td>
<td>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</td>
</tr>
<tr>
<td>file_original</td>
<td>Text(255)</td>
<td>The original file name of this storage.</td>
</tr>
<tr>
<td>storage_guid</td>
<td>Number(Replication ID)</td>
<td>The GUID of this storage entry. (Used by AMF)</td>
</tr>
<tr>
<td>storage_reason</td>
<td>Number(Integer)</td>
<td>The reason (quarantine, archive, or backup) to make this storage entry.</td>
</tr>
<tr>
<td>storage_path</td>
<td>Text(255)</td>
<td>The path the file saved to</td>
</tr>
<tr>
<td>storage_type</td>
<td>Number(Integer)</td>
<td>The storage type (single file or entire message)</td>
</tr>
<tr>
<td>storage_resend_count</td>
<td>Number(Integer)</td>
<td>The count of this entry has been resent</td>
</tr>
<tr>
<td>sent_to_csm</td>
<td>Number(Integer)</td>
<td>(internal use)</td>
</tr>
</tbody>
</table>
Table D-4. Table [tblActivityEntries] stores event log information. For example, information about the start, progress, and completion of manual update.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>activity_entry_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>activity_severity</td>
<td>Number(Long Integer)</td>
<td>The severity of this activity entry</td>
</tr>
<tr>
<td>activity_id</td>
<td>Number(Long Integer)</td>
<td>The id of this activity entry. Ref [dbconf_log.xml]</td>
</tr>
<tr>
<td>activity_time</td>
<td>Date/Time</td>
<td>The date and time of this activity entry began</td>
</tr>
<tr>
<td>activity_description</td>
<td>memo</td>
<td>Activity description</td>
</tr>
<tr>
<td>activity_parameter</td>
<td>memo</td>
<td>To indicate manual/scheduled update component type: pattern/engine/anti-spam rule</td>
</tr>
<tr>
<td>activity_duration_mark</td>
<td>Number(Integer)</td>
<td>To indicate this activity duration is either begin, end, or instant.</td>
</tr>
<tr>
<td>sent_to_csm</td>
<td>Number(Integer)</td>
<td>(internal use)</td>
</tr>
</tbody>
</table>
The `Table [tblPatternEngineInfo]` stores information about the engine and patterns that are used to scan email messages.

### Table D-5. Table [tblPatternEngineInfo]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>pei_type</code></td>
<td>Number(Long Integer)</td>
<td>The type of the pattern/engine.</td>
</tr>
<tr>
<td><code>pei_current_version</code></td>
<td>memo</td>
<td>The current version of pattern/engine.</td>
</tr>
<tr>
<td><code>pei_latest_version</code></td>
<td>memo</td>
<td>The latest version of pattern/engine.</td>
</tr>
<tr>
<td><code>pei_last_query_time</code></td>
<td>Date/Time</td>
<td>The last query time of pattern/engine.</td>
</tr>
<tr>
<td><code>pei_last_update_time</code></td>
<td>Date/Time</td>
<td>The last update time of pattern/engine.</td>
</tr>
<tr>
<td><code>pei_last_successful_update_time</code></td>
<td>Date/Time</td>
<td>The last successful update time of pattern/engine.</td>
</tr>
<tr>
<td><code>pei_last_update_status</code></td>
<td>Number(Long Integer)</td>
<td>The last update status of pattern/engine.</td>
</tr>
<tr>
<td><code>pei_last_update_status_description</code></td>
<td>memo</td>
<td>The last update status description of pattern/engine.</td>
</tr>
</tbody>
</table>
Table D-6. Table [tblScanningSummary] stores the scan summary information of detected security risks for today.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ss_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>ss_type</td>
<td>Number(Long Integer)</td>
<td>The type of scanned object (such as virus/malware, spam, blocked attachment). Refer to Possible values of the ss_type, reference Note5 in this file.</td>
</tr>
<tr>
<td>ss_time</td>
<td>Date/Time</td>
<td>The scanning time</td>
</tr>
<tr>
<td>ss_count</td>
<td>Number(Long Integer)</td>
<td>The count of each type of scanned object.</td>
</tr>
</tbody>
</table>

Table D-7. Table [tblCfgReplication] stores the configuration replication status.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>cr_session_guid</td>
<td>Number(Rplication ID)</td>
<td>The session GUID</td>
</tr>
<tr>
<td>cr_time</td>
<td>Date/Time</td>
<td>The start time</td>
</tr>
<tr>
<td>cr_server_list</td>
<td>memo</td>
<td>The server list</td>
</tr>
<tr>
<td>cr_selection_list</td>
<td>memo</td>
<td>The selection list</td>
</tr>
<tr>
<td>cr_id</td>
<td>Number(Long Integer)</td>
<td>(Not in use)</td>
</tr>
</tbody>
</table>
**Table D-8.** Table [tblCfgReplicationStatus] stores the configuration replication status

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>crs_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>crs_session_guid</td>
<td>Number(Replication ID)</td>
<td>The session GUID</td>
</tr>
<tr>
<td>crs_start_time</td>
<td>Date/Time</td>
<td>The start time of configuration replication</td>
</tr>
<tr>
<td>crs_end_time</td>
<td>Date/Time</td>
<td>The end time of configuration replication</td>
</tr>
<tr>
<td>crs_server</td>
<td>memo</td>
<td>The server name which did the configuration replication</td>
</tr>
<tr>
<td>crs_status</td>
<td>Number(Long Integer)</td>
<td>The status of the configuration replication</td>
</tr>
<tr>
<td>crs_description</td>
<td>memo</td>
<td>The description of the configuration replication</td>
</tr>
</tbody>
</table>
**Table D-9.** Table [tblAuditLog] stores all event tracking logs.

<table>
<thead>
<tr>
<th><strong>FIELD NAME</strong></th>
<th><strong>DATA TYPE</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>ServerName</td>
<td>Text(255)</td>
<td>The virtual server name</td>
</tr>
<tr>
<td>UserName</td>
<td>Text(255)</td>
<td>The user name</td>
</tr>
<tr>
<td>EventTime</td>
<td>Date/Time</td>
<td>The current time of Audit Event</td>
</tr>
<tr>
<td>IpAddress</td>
<td>Text(255)</td>
<td>The remote host IP address</td>
</tr>
<tr>
<td>EventType</td>
<td>Number(Integer)</td>
<td>The event type (Three types: log in/out, configuration, operation)</td>
</tr>
<tr>
<td>SourceType</td>
<td>Number(Integer)</td>
<td>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))</td>
</tr>
<tr>
<td>LogDescription</td>
<td>Text(255)</td>
<td>The description of log</td>
</tr>
</tbody>
</table>
**Table D-10. **Table [tblManagementGroupList] is not used.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgl_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>mgl_group_name</td>
<td>memo</td>
<td>The group name in the management group list</td>
</tr>
</tbody>
</table>

**Table D-11. **Table [tblManagementServerList] is not used.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msl_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>msl_server_name</td>
<td>memo</td>
<td>The server name in the management group list</td>
</tr>
<tr>
<td>msl_group_id</td>
<td>Number(Long Integer)</td>
<td>The group ID to which the server belongs.</td>
</tr>
</tbody>
</table>

**Table D-12. **Table [tblManagementGroupMemberList] is not used.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgml_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>mgml_group_id</td>
<td>Number(Long Integer)</td>
<td>The group ID from table [tblManagementGroupList]</td>
</tr>
<tr>
<td>mgml_server_id</td>
<td>Number(Long Integer)</td>
<td>The server ID from table [tblManagementServerList]</td>
</tr>
</tbody>
</table>
Table D-13. Table [tblCfgReplicationHistory] stores the time of the last configuration replication.

**Table D-13. Table [tblCfgReplicationHistory]**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Data Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crh_id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>crh_session_guid</td>
<td>Number(Replication ID)</td>
<td>The session GUID</td>
</tr>
<tr>
<td>crh_time</td>
<td>Date/Time</td>
<td>The last time of configuration replication</td>
</tr>
</tbody>
</table>

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':

```sql
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
```
**Table D-14. Possible values of the activity_id** lists the items to note for this example.

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_CMD_ENGINE_PATTERN_UPDATE</td>
<td>1</td>
<td>The engine pattern update command</td>
</tr>
<tr>
<td>ID_CMD_MANUAL_SCAN</td>
<td>3</td>
<td>The manual scan command</td>
</tr>
<tr>
<td>ID_CMD_SCHEDULE_SCAN</td>
<td>4</td>
<td>The schedule scan command</td>
</tr>
<tr>
<td>ID_CMD_CFG_DEPLOYMENT</td>
<td>5</td>
<td>The configuration deployment command</td>
</tr>
<tr>
<td>ID_CMD_CFG_QUERY_PATTERNS ENGINE VERSION</td>
<td>6</td>
<td>The query the pattern engine version command</td>
</tr>
<tr>
<td>ID_CMD_QM_RESEND</td>
<td>7</td>
<td>The quarantine manager resend message command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_CLEAN_SPAM_MSG</td>
<td>8</td>
<td>The End User Quarantine (EUQ) clean spam message command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_CREATE_SPAM_FOLDER_RULE</td>
<td>9</td>
<td>The End User Quarantine (EUQ) create spam folder rule command</td>
</tr>
<tr>
<td>ID_CMD_LOG_MAINTENANCE</td>
<td>10</td>
<td>The log maintenance command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_HOUSEKEEPING_TASK</td>
<td>11</td>
<td>The End User Quarantine (EUQ) house keeping task command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_ENABLE_EUQ</td>
<td>12</td>
<td>The enable End User Quarantine (EUQ) command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_DISABLE_EUQ</td>
<td>13</td>
<td>The disable End User Quarantine (EUQ) command</td>
</tr>
<tr>
<td>ID_CMD_EUQ_UPDATE_CONFIG</td>
<td>14</td>
<td>The update End User Quarantine (EUQ) configuration command</td>
</tr>
</tbody>
</table>
### Example 2: Query :Get Quarantine Log(storage_reason=1).

```sql
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;
```
Table D-15. Possible values of the storage_reason lists the items to note for this example.

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>SR_QUARANTINE</td>
<td>1</td>
<td>The reason for this storage entry is quarantine</td>
</tr>
<tr>
<td>SR_BACKUP</td>
<td>2</td>
<td>The reason for this storage entry is backup</td>
</tr>
<tr>
<td>SR_ARCHIVE</td>
<td>3</td>
<td>The reason for this storage entry is archive</td>
</tr>
</tbody>
</table>

Table D-16. Possible values of the filter_id lists the items to note for this example.

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID_FILTERTYPE_VIRUS_SCAN_CANNING</td>
<td>1(0x1)</td>
<td>The filter type of security risk scan</td>
</tr>
<tr>
<td>ID_FILTERTYPE_EMANAGER_5X</td>
<td>2(0x2)</td>
<td>The filter type emanager_5X</td>
</tr>
<tr>
<td>ID_FILTERTYPE_FILE_BLOCKING</td>
<td>4(0x4)</td>
<td>The filter type of file blocking</td>
</tr>
<tr>
<td>ID_FILTERTYPE_ANTISPAM</td>
<td>8(0x8)</td>
<td>The filter type of spam prevention</td>
</tr>
<tr>
<td>ID_FILTERTYPE_SIZE_CHECKER</td>
<td>16(0x10)</td>
<td>The filter type of size check</td>
</tr>
<tr>
<td>ID_FILTERTYPE_ACTIVE_MESSAGE_FILTER</td>
<td>32(0x20)</td>
<td>Active message filter</td>
</tr>
</tbody>
</table>
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'. And the event type is in '1' and '2'.

```sql
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 (EventType in ('1','2'))
AND LogDescription like 'Realtime Scan%'
ORDER BY UserName
```

Table D-17. Possible values of the EventType lists the items to note for this example

```
<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>TYPE_LOG_IN_OUT</td>
<td>1</td>
<td>Log in/out</td>
</tr>
<tr>
<td>TYPE_CONFIGURATION</td>
<td>2</td>
<td>Configuration</td>
</tr>
<tr>
<td>TYPE_OPERATION_EVENT</td>
<td>3</td>
<td>Operation event</td>
</tr>
</tbody>
</table>
```
Example 6: Get message information that needs to be resent

```sql
SELECT msg_subject, msg_source, msg_destination_full, 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 all Administrators

```sql
SELECT distinct(username)
FROM tblAuditLog;
```

Example 8: Get Last Configuration Replication

```sql
SELECT TOP 1 *
FROM tblCfgReplicationHistory
ORDER BY crh_time DESC;
```

Example 9: Get Engine Pattern Information

```sql
SELECT *
FROM tblPatternEngineInfo;
```

Example 10: Get Scan Summary Count.

```sql
SELECT *
FROM tblScanningSummary
WHERE ss_type = 111;
```
Table D-18. Possible values of the ss_type lists the items to note for this example

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST_SCANNED_MESSAGE</td>
<td>100</td>
<td>Scanned message</td>
</tr>
<tr>
<td>ST_DETECTED_VIRUS</td>
<td>110</td>
<td>Detected virus</td>
</tr>
<tr>
<td>ST_BLOCKED_ATTACHMENT</td>
<td>111</td>
<td>Blocked attachment</td>
</tr>
<tr>
<td>ST_DETECTED_SPAM</td>
<td>112</td>
<td>Detected spam.</td>
</tr>
<tr>
<td>ST_CONTENT_VIOLATION</td>
<td>113</td>
<td>Content violation</td>
</tr>
<tr>
<td>ST_DETECTED_ERS</td>
<td>114</td>
<td>Detected ERS</td>
</tr>
<tr>
<td>ST_SUSPICIOUS_URL</td>
<td>115</td>
<td>Malicious URL</td>
</tr>
<tr>
<td>ST_UNCLEANABLE_VIRUS</td>
<td>117</td>
<td>Uncleanable virus</td>
</tr>
<tr>
<td>ST_SCANNED_ATTACHMENT</td>
<td>118</td>
<td>Scanned attachment</td>
</tr>
<tr>
<td>ST_UNKNOWN</td>
<td>119</td>
<td>Unknown type</td>
</tr>
<tr>
<td>ST_DETECTED_PHISH</td>
<td>120</td>
<td>Detected phish</td>
</tr>
<tr>
<td>ST_DETECTED_SPYWARE</td>
<td>121</td>
<td>Detected spyware</td>
</tr>
<tr>
<td>ST_FALSE_POSITIVE</td>
<td>124</td>
<td>False positive</td>
</tr>
<tr>
<td>ST_UNSCANNABLE_ENTITY</td>
<td>151</td>
<td>Unscannable entity</td>
</tr>
</tbody>
</table>
Log View Database Schema


<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_entry_id</td>
<td>tblFilterEntries</td>
<td>msg_entry_id</td>
<td>Primary key of the table [tblMsgEntries]</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>tblMsgEntries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>tblMsgEntries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>tblMsgEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>tblMsgEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>tblMsgEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_id</td>
<td>tblFilterEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>tblFilterEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>filter_rule</td>
<td>tblFilterEntries</td>
<td>filter_rule</td>
<td>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</td>
</tr>
</tbody>
</table>
### Table D-20. View [vwMsgFilterEntries] (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file_original</td>
<td>tblFilterEntries</td>
<td>file_original</td>
<td>The original filename triggered the rule</td>
</tr>
<tr>
<td>filter_action</td>
<td>tblFilterEntries</td>
<td>filter_action</td>
<td>The result of the action taken</td>
</tr>
<tr>
<td>filter_reason</td>
<td>tblFilterEntries</td>
<td>filter_reason</td>
<td>Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter</td>
</tr>
<tr>
<td>filter_rule_supplement</td>
<td>tblFilterEntries</td>
<td>filter_rule_supplement</td>
<td>The virus/malware type, used to separate virus and spyware</td>
</tr>
</tbody>
</table>

Table D-20. View [vwMsgFilterEntries] combines table tblStorageEntries and view vwMsgFilterEntriesTmp.

### Table D-20. View [vwMsgFilterEntries]

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
</tbody>
</table>
### TABLE D-20.  View [vwMsgFilterEntries] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_rule</td>
<td>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</td>
</tr>
<tr>
<td>filter_reason</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_reason</td>
<td>Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter.</td>
</tr>
<tr>
<td>file_original</td>
<td>vwMsgFilterEntriesTmp</td>
<td>file_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td>msg_entry_id</td>
<td>vwMsgFilterEntriesTmp</td>
<td>msg_entry_id</td>
<td>Primary key of the table [tblMsgEntries]</td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
</tbody>
</table>
**TABLE D-20. View [vwMsgFilterEntries] (Continued)**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_action</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_action</td>
<td>The result of the action taken</td>
</tr>
<tr>
<td>storage_entry_id</td>
<td>tblStorageEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table [tblStorageEntries]</td>
</tr>
<tr>
<td>storage_path</td>
<td>tblStorageEntries</td>
<td>storage_path</td>
<td>The path the file saved to</td>
</tr>
<tr>
<td>storage_reason</td>
<td>tblStorageEntries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) to make this storage entry.</td>
</tr>
<tr>
<td>filter_rule_supple</td>
<td>vwMsgFilterEntriesTmp</td>
<td>filter_rule_supplement</td>
<td>The virus/malware type, used to separate virus and spyware.</td>
</tr>
</tbody>
</table>

Table D-21. View [vwMsgStorageEntries] combines table tblMsgEntries and tblStorageEntries

**TABLE D-21. View [vwMsgStorageEntries]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>tblStorageEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table [tblStorageEntries]</td>
</tr>
<tr>
<td>msg_source</td>
<td>tblMsgEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>tblMsgEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_subject</td>
<td>tblMsgEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_id</td>
<td>tblStorageEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>tblStorageEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>filter_rule</td>
<td>tblStorageEntries</td>
<td>filter_rule</td>
<td>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</td>
</tr>
<tr>
<td>file_original</td>
<td>tblStorageEntries</td>
<td>file_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td>filter_action</td>
<td>tblStorageEntries</td>
<td>filter_action</td>
<td>The result of the action taken</td>
</tr>
<tr>
<td>storage_reason</td>
<td>tblStorageEntries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) to make this storage entry.</td>
</tr>
<tr>
<td>storage_resend_count</td>
<td>tblStorageEntries</td>
<td>storage_resend_count</td>
<td>The count of this entry has been resent.</td>
</tr>
</tbody>
</table>
Table D-22. View [vwABLogs] select blocked attachments data from view vwMsgFilterEntries

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilterEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEntries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilterEntries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_cf</td>
<td>vwMsgFilterEntries</td>
<td>filter_rule</td>
<td>File type blocked by attachment blocking filter(such as .exe)</td>
</tr>
</tbody>
</table>
### TABLE D-22. View [vwABLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_original</td>
<td>vwMsgFilterEntries</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td>Filter_action</td>
<td>vwMsgFilterEntries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%/web/xml.</td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilterEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME % represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\
Table D-23. View [vwAVLogs] select security risk scan data from view vwMsgFilterEntries.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilterEnt-</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEnt-</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEnt-</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilterEnt-</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEnt-</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEnt-</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEnt-</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_rule_av</td>
<td>vwMsgFilterEnt-</td>
<td>filter_rule</td>
<td>Virus/malware name</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_original</td>
<td>vwMsgFilterEnt-</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td></td>
<td>ries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**TABLE D-23. View [vwAVLogs] (Continued)**

<table>
<thead>
<tr>
<th>Field name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter_action</td>
<td>vwMsgFilterEntries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
<tr>
<td>filter_rule_supplement</td>
<td>vwMsgFilterEntries</td>
<td>filter_rule_supplement</td>
<td>The virus/malware type, used to separate virus and spyware.</td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilterEntries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>storage_reason</td>
<td>vwMsgFilterEntries</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) for this storage entry.</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex.
Table D-24. View [vwCFLogs] select content violation data from view vwMsgFilterEntries.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilter-</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilter-</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilter-</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilter-</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilter-</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilter-</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilter-</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_rule_cf</td>
<td>vwMsgFilter-</td>
<td>filter_rule</td>
<td>Rule name for content filter</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_original</td>
<td>vwMsgFilter-</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### TABLE D-24. View [vwCFLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter_action</td>
<td>vwMsgFilter-Entries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\  

<table>
<thead>
<tr>
<th>filter_reason</th>
<th>vwMsgFilter-Entries</th>
<th>filter_reason</th>
<th>Detailed information about how the content is being detected for content violation, malicious URL for Web Reputation filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_id</td>
<td>vwMsgFilter-Entries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
</tbody>
</table>
Table D-25. View [vwDLPLogs] select Data Loss Prevention incident data from view vwMsgFilterEntries.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilterEntries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilterEntries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilterEntries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilterEntries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilterEntries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilterEntries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilterEntries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_dlp</td>
<td>vwMsgFilterEntries</td>
<td>filter_rule</td>
<td>Rule name for Data Loss Prevention</td>
</tr>
</tbody>
</table>
Table D-26. View [vwUSLogs] (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_action</td>
<td>vwMsgFilter-Entries</td>
<td>filter_action</td>
<td>The result of action taken</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reference [action_description.xml], which is located in %SMEX_HOME%/web/xml.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> %SMEX_HOME% represents the ScanMail installation directory. By default, this is C:\Program Files\Trend Micro\Smex.</td>
</tr>
<tr>
<td>file_original</td>
<td>vwMsgFilter-Entries</td>
<td>file_original</td>
<td>The original filename that triggered the rule</td>
</tr>
<tr>
<td>filter_template</td>
<td>vwMsgFilter-Entries</td>
<td>filter_reason</td>
<td>The triggered Data Loss Prevention template</td>
</tr>
</tbody>
</table>

Table D-26. View [vwUSLogs] select unscannable message data from view vwMsgFilterEntries

Table D-25. View [vwDLPLogs] (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilter-Entries</td>
<td>storage_entry_id</td>
<td>Primary key of the table &quot;tblStorageEntries&quot;</td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilter-Entries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilter-Entries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
</tbody>
</table>
### TABLE D-26. View [vwUSLogs] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_found_at</td>
<td>vwMsgFilter-Entries</td>
<td>msg_found_at</td>
<td>The place where this message is found at</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilter-Entries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td>msg_destination</td>
<td>vwMsgFilter-Entries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilter-Entries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_us</td>
<td>vwMsgFilter-Entries</td>
<td>filter_rule</td>
<td>Unscannable reason</td>
</tr>
<tr>
<td>filter_original</td>
<td>vwMsgFilter-Entries</td>
<td>filter_original</td>
<td>The original filename that triggered the rule</td>
</tr>
</tbody>
</table>
**TABLE D-27. View [vwQuarantineLogs]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filter_action</td>
<td>vwMsgFilter-</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilter-</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>storage_reason</td>
<td>vwMsgFilter-</td>
<td>storage_reason</td>
<td>The reason (quarantine, archive, or backup) for this storage entry.</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\%

**Table D-27. View [vwUSLogs] (Continued)**

**TABLE D-27. View [vwQuarantineLogs]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilter-</td>
<td>storage_entry_id</td>
<td>Primary key of the table [tblStorageEntries]</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilter-</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilter-</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
<tr>
<td></td>
<td>Entries</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>FROM TABLE</th>
<th>FROM FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter_scan_time</td>
<td>vwMsgFilter-Entries</td>
<td>filter_scan_time</td>
<td>The scan time</td>
</tr>
<tr>
<td>msg_delivery_time</td>
<td>vwMsgFilter-Entries</td>
<td>msg_delivery_time</td>
<td>The message delivery time</td>
</tr>
<tr>
<td>msg_source</td>
<td>vwMsgFilter-Entries</td>
<td>msg_source</td>
<td>The semi-colon delimited sender list</td>
</tr>
</tbody>
</table>
### TABLE D-28. View [vwWTPLogs] (Continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>From Table</th>
<th>From Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msg_destination</td>
<td>vwMsgFilter-Entries</td>
<td>msg_destination</td>
<td>The semi-colon delimited recipient list</td>
</tr>
<tr>
<td>msg_subject</td>
<td>vwMsgFilter-Entries</td>
<td>msg_subject</td>
<td>The subject of this message</td>
</tr>
<tr>
<td>filter_rule_usf</td>
<td>vwMsgFilter-Entries</td>
<td>filter_rule_usf</td>
<td>Risk level of a malicious URL for Web Reputation filter</td>
</tr>
<tr>
<td>Suspicious_url</td>
<td>vwMsgFilter-Entries</td>
<td>filter_reason</td>
<td>Suspicious url</td>
</tr>
<tr>
<td>filter_action</td>
<td>vwMsgFilter-Entries</td>
<td>filter_action</td>
<td>The result of action taken. Reference [action_description.xml], which is located in %SMEX_HOME%\web\xml.</td>
</tr>
<tr>
<td>filter_id</td>
<td>vwMsgFilter-Entries</td>
<td>filter_id</td>
<td>Primary key of the table [tblFilterEntries]</td>
</tr>
<tr>
<td>storage_entry_id</td>
<td>vwMsgFilter-Entries</td>
<td>storage_entry_id</td>
<td>Primary key of the table [tblStorageEntries]</td>
</tr>
</tbody>
</table>

**Note:** %SMEX_HOME% represents the SMEX installation directory. By default, this is C:\Program Files\Trend Micro\Smex\.
Example 1: Query information about virus log, content filtering log, or attachment blocking log from table ‘vwAVLogs’, ‘vwCFLogs’, ‘vwABLogs’ between 12/12/2008 09:00:00’ AND ‘12/18/2008 09:00:00’.

```sql
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

```sql
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 seven tables. These tables are not related to each other.

Table D-29. Table [tblSummary] stores the summary detected security risks per hour.

**TABLE D-29. Table [tblSummary]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>summary_datetime</td>
<td>Date/Time</td>
<td>This datetime when this record was summarized</td>
</tr>
<tr>
<td>summary_total_message_count</td>
<td>Number(Long Integer)</td>
<td>The total message scanned count for this period</td>
</tr>
<tr>
<td>summary_total_attachment_count</td>
<td>Number(Long Integer)</td>
<td>The total attachment scanned count for this period</td>
</tr>
<tr>
<td>Summary_virus_detected_count</td>
<td>Number(Long Integer)</td>
<td>The virus/malware count for this period</td>
</tr>
<tr>
<td>summary_virus_unchangeable_count</td>
<td>Number(Long Integer)</td>
<td>The uncleanable virus/malware count for this period</td>
</tr>
<tr>
<td>summary_attachment_blocked_count</td>
<td>Number(Long Integer)</td>
<td>The blocked attachment count for this period</td>
</tr>
<tr>
<td>summary_content_filtered_count</td>
<td>Number(Long Integer)</td>
<td>The filtered-count for this period</td>
</tr>
<tr>
<td>summary_dlp_filtered_count</td>
<td>int</td>
<td>The filtered-count for this period</td>
</tr>
<tr>
<td>Summary_spam_detected_count</td>
<td>Number(Long Integer)</td>
<td>The spam message count</td>
</tr>
<tr>
<td>summary_phish_detected_count</td>
<td>Number(Long Integer)</td>
<td>The phish message count</td>
</tr>
</tbody>
</table>
**Table D-30. Table [tblAttachmentInfo]** stores blocked attachment information by category

**Table D-30. Table [tblAttachmentInfo]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>attachinfo_datetime</td>
<td>Date/Time</td>
<td>The datetime of summarization.</td>
</tr>
<tr>
<td>attachinfo_cate_id</td>
<td>Number(Long Integer)</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>attachinfo_value</td>
<td>Text(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>attachinfo_count</td>
<td>Number(Long Integer)</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>
Table D-31. Table `tblContentInfo` stores content violation information by category.

### Table D-31. Table `tblContentInfo`

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>contentinfo_datetime</td>
<td>Date/Time</td>
<td>The datetime of summarization</td>
</tr>
<tr>
<td>contentinfo_cate_id</td>
<td>Number(Long Integer)</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>contentinfo_value</td>
<td>Text(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>contentinfo_count</td>
<td>Number(Long Integer)</td>
<td>The count of this data category</td>
</tr>
</tbody>
</table>

Table D-32. Table `tblDLPInfo` stores Data Loss Prevention incident information by category.

### Table D-32. Table `tblDLPInfo`

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>dlpinfo_datetime</td>
<td>datetime</td>
<td>The datetime of summarization</td>
</tr>
<tr>
<td>dlpinfo_cate_id</td>
<td>int</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>dlpinfo_value</td>
<td>nvarchar(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>dlpinfo_count</td>
<td>int</td>
<td>The count of this data category</td>
</tr>
</tbody>
</table>
Table D-33: Table [tblSpamInfo] stores spam information by category.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>spaminfo_datetime</td>
<td>Date/Time</td>
<td>The datetime of summarization.</td>
</tr>
<tr>
<td>spaminfo_cate_id</td>
<td>Number(Long Integer)</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>spaminfo_value</td>
<td>Text(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>spaminfo_count</td>
<td>Number(Long Integer)</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>

Table D-34: Table [tblVirusInfo] stores security risk information by category.

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>virusinfo_datetime</td>
<td>Date/Time</td>
<td>The date/time of summarization.</td>
</tr>
<tr>
<td>virusinfo_cate_id</td>
<td>Number(Long Integer)</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>virusinfo_value</td>
<td>Text(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>virusinfo_count</td>
<td>Number(Long Integer)</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>
Table D-35. Table [tblUnscannableInfo] stores unscannable message information by category

**TABLE D-35. Table [tblUnscannableInfo]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>ucanableifo_datatime</td>
<td>Date/Time</td>
<td>The date/time of summarization</td>
</tr>
<tr>
<td>ucanableifo_cate_id</td>
<td>Number(Long Integer)</td>
<td>The category of this counter</td>
</tr>
<tr>
<td>ucanableifo_value</td>
<td>Text(64)</td>
<td>The value of this counter</td>
</tr>
<tr>
<td>ucanableifo_count</td>
<td>Number(Long Integer)</td>
<td>The count of this data category.</td>
</tr>
</tbody>
</table>

Table D-36. Table [tblReportCollectionSummary] stores the total number of detected security risks. This table is used by MOM/SCOM

**TABLE D-36. Table [tblReportCollectionSummary]**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>summary_total_message_count</td>
<td>Number(Long Integer)</td>
<td>The total message scanned count for this period</td>
</tr>
<tr>
<td>summary_total_attachment_count</td>
<td>Number(Long Integer)</td>
<td>The total attachment scanned count for this period</td>
</tr>
</tbody>
</table>
### TABLE D-36. Table [tblReportCollectionSummary] (Continued)

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary_virus_detected_count</td>
<td>Number(Long Integer)</td>
<td>The virus/malware count for this period</td>
</tr>
<tr>
<td>summary_virus_uncleanable_count</td>
<td>Number(Long Integer)</td>
<td>The uncleanable virus count for this period</td>
</tr>
<tr>
<td>summary_attachment_blocked_count</td>
<td>Number(Long Integer)</td>
<td>The blocked attachment count for this period</td>
</tr>
<tr>
<td>summary_content_filtered_count</td>
<td>Number(Long Integer)</td>
<td>The filtered-count for this period.</td>
</tr>
<tr>
<td>summary_dlp_filtered_count</td>
<td>Number(Long Integer)</td>
<td>The filtered-count for this period.</td>
</tr>
<tr>
<td>summary_spam_detected_count</td>
<td>Number(Long Integer)</td>
<td>The spam message count</td>
</tr>
<tr>
<td>summary_phish_detected_count</td>
<td>Number(Long Integer)</td>
<td>The phish message count</td>
</tr>
<tr>
<td>summary_unscannable_entity_count</td>
<td>Number(Long Integer)</td>
<td>The unscannable count for this period</td>
</tr>
<tr>
<td>summary_worm_trojan_virus_type_count</td>
<td>Number(Long Integer)</td>
<td>The worm trojan virus type count for this period</td>
</tr>
<tr>
<td>FIELD NAME</td>
<td>DATA TYPE</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>summary_packed_file_virus_type_count</td>
<td>Number(Long Integer)</td>
<td>The packed file virus type count for this period</td>
</tr>
<tr>
<td>summary_generic_virus_type_count</td>
<td>Number(Long Integer)</td>
<td>The generic virus type count for this period</td>
</tr>
<tr>
<td>summary_virus_virus_type_count</td>
<td>Number(Long Integer)</td>
<td>The virus/malware type count for this period</td>
</tr>
<tr>
<td>summary_other_malicious_code_virus_type_count</td>
<td>Number(Long Integer)</td>
<td>Other malicious code virus type count for this period</td>
</tr>
<tr>
<td>summary_additional_threat_virus_type_count</td>
<td>Number(Long Integer)</td>
<td>The additional threat virus type count for this period</td>
</tr>
<tr>
<td>summary_ers_count</td>
<td>Number(Long Integer)</td>
<td>Blocked IP count for this period</td>
</tr>
<tr>
<td>summary_suspicious_url_count</td>
<td>Number(Long Integer)</td>
<td>The suspicious url count shown in the reoprt summary</td>
</tr>
</tbody>
</table>
Table D-37. Table [tblURLInfo] (add by WTP) stores malicious URL information by category

**TABLE D-37. Table [tblURLInfo] (add by WTP)**

<table>
<thead>
<tr>
<th>FIELD NAME</th>
<th>DATA TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>Auto increment</td>
<td>Primary key</td>
</tr>
<tr>
<td>urlinfo_datetime</td>
<td>Date time</td>
<td>Date &amp; Time</td>
</tr>
<tr>
<td>urlinfo_cate_id</td>
<td>Number (Long Integer)</td>
<td>Category id</td>
</tr>
<tr>
<td>urlinfo_value</td>
<td>Text(64)</td>
<td>The name of the report item counter</td>
</tr>
<tr>
<td>urlinfo_count</td>
<td>Number (Long Integer)</td>
<td>The value of the report item counter</td>
</tr>
</tbody>
</table>

Example 1: Get Last Summary Time from table[tblSummary]

```sql
SELECT MAX(summary_datetime) AS lastest_datetime
FROM tblSummary;
```

Example 2: Get MOM Report Counter

```sql
SELECT *
FROM tblReportCollectionSummary.
```

//The example below is all about virus. And the query expressions of 'Attachment blocking report', 'Content filter report',' Anti-spam report',' Unscannable Entity report' is the same as virus.
Example 3: Get All Virus Count during 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;
Table D-38. Possible values of the virusinfo_cate_id lists the items to note for this example

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPT_CATEID_VS_VIRUS_NAME</td>
<td>151</td>
<td>The count of viruses/malware of a certain virus/malware name</td>
</tr>
<tr>
<td>RPT_CATEID_VS_VIRUS_TYPE</td>
<td>152</td>
<td>The count of viruses/malware of a certain virus/malware type</td>
</tr>
<tr>
<td>RPT_CATEID_VS_ACTION</td>
<td>153</td>
<td>The count of viruses/malware which had the same action applied</td>
</tr>
<tr>
<td>RPT_CATEID_SPYWARE_NAME</td>
<td>154</td>
<td>The count of spyware/grayware of a certain spyware/grayware name.</td>
</tr>
<tr>
<td>RPT_CATEID_SPYWARE_ACTION</td>
<td>155</td>
<td>The count of spyware/grayware which had the same action applied</td>
</tr>
<tr>
<td>RPT_CATEID_VS_SENDER</td>
<td>156</td>
<td>The count of a single sender who sent virus/malware</td>
</tr>
<tr>
<td>RPT_CATEID_SPYWARE_SENDER</td>
<td>157</td>
<td>The count of a single sender who sent spyware/grayware</td>
</tr>
<tr>
<td>RPT_CATEID_AB_FILETYPE</td>
<td>201</td>
<td>The count of blocked attachment of a certain file type.</td>
</tr>
<tr>
<td>RPT_CATEID_AB_EXTENSION</td>
<td>202</td>
<td>The count of blocked attachments of a certain extension.</td>
</tr>
<tr>
<td>RPT_CATEID_AB_FILENAME</td>
<td>203</td>
<td>The count of blocked attachments of a certain filename.</td>
</tr>
<tr>
<td>RPT_CATEID_CF_SENDER</td>
<td>251</td>
<td>The count for a single sender that triggered the content filtering rules.</td>
</tr>
<tr>
<td>RPT_CATEID_CF_RECIPIENT</td>
<td>252</td>
<td>The count of content violation of an individual recipient.</td>
</tr>
</tbody>
</table>
### TABLE D-38. Possible values of the virusinfo_cate_id (Continued)

<table>
<thead>
<tr>
<th>SYMBOL</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPT_CATEID_CF_RULE</td>
<td>253</td>
<td>The count of content violation of a content filtering rule.</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAM_SENDER</td>
<td>301</td>
<td>The count of spam messages from an individual sender.</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAM_DOMAIN</td>
<td>302</td>
<td>The count of spam messages from an individual domain.</td>
</tr>
<tr>
<td>RPT_CATEID_AS_FALSE_POSITIVE_DOMAIN</td>
<td>303</td>
<td>The count of false positive messages from an individual domain</td>
</tr>
<tr>
<td>RPT_CATEID_AS_FALSE_POSITIVE_SENDER</td>
<td>304</td>
<td>The count of false positive messages from an individual sender.</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAMCATEGORY</td>
<td>305</td>
<td>The count of spam messages of a single spam category.</td>
</tr>
<tr>
<td>RPT_CATEID_AS_SPAM_MAILBOX</td>
<td>306</td>
<td>The count of spam message to an individual recipient</td>
</tr>
<tr>
<td>RPT_CATEID_UNSCANABLEENTITY</td>
<td>351</td>
<td>The count of unscannable messages</td>
</tr>
<tr>
<td>RPT_CATEID_UF_SUSPICIOUS_URL</td>
<td>401</td>
<td>The count of malicious URL</td>
</tr>
<tr>
<td>RPT_CATEID_UF_SENDER</td>
<td>402</td>
<td>The count of a single sender who sent email messages that contained a malicious URL</td>
</tr>
</tbody>
</table>
Table D-39. Virus Type lists the items to note for this example

### TABLE D-39. Virus Type

<table>
<thead>
<tr>
<th>Virus Type String</th>
<th>Virus Type ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus</td>
<td>2</td>
</tr>
<tr>
<td>Trojan</td>
<td>4</td>
</tr>
<tr>
<td>Spyware</td>
<td>16</td>
</tr>
<tr>
<td>Joke</td>
<td>8</td>
</tr>
<tr>
<td>Test_Virus</td>
<td>8</td>
</tr>
<tr>
<td>Other</td>
<td>8</td>
</tr>
<tr>
<td>Packer</td>
<td>16384</td>
</tr>
<tr>
<td>Generic</td>
<td>32768</td>
</tr>
</tbody>
</table>

Table D-40. Virus Name String lists the items to note for this example

### TABLE D-40. Virus Name String

<table>
<thead>
<tr>
<th>String</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected file</td>
</tr>
<tr>
<td>Over restriction (others)</td>
</tr>
<tr>
<td>Over restriction (mail entity count)</td>
</tr>
<tr>
<td>Over restriction (message body size)</td>
</tr>
<tr>
<td>Over restriction (attachment size)</td>
</tr>
<tr>
<td>Over restriction (decompressed file count)</td>
</tr>
<tr>
<td>STRING</td>
</tr>
<tr>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Over restriction (decompressed file size)</td>
</tr>
<tr>
<td>Over restriction (number of layer of compression)</td>
</tr>
<tr>
<td>Over restriction (compression ratio)</td>
</tr>
</tbody>
</table>
Best Practices

This chapter provides best practice information.

Topics include:

• Real-time Scan Settings for Server Roles on page E-2
• Attachment Blocking Policies on page E-3
• Content Filtering Active Directory Integrated Policies on page E-5
• Data Loss Prevention Policies on page E-6
• Optimizing Web Reputation on page E-9
• Recommended Settings on page E-10
Real-time Scan Settings for Server Roles

Table E-1 lists the recommended real-time scan settings for different server roles.

**TABLE E-1. Recommended scan settings for different server roles**

<table>
<thead>
<tr>
<th>EXCHANGE ROLE</th>
<th>TRANSPORT LEVEL REAL-TIME SCAN</th>
<th>STORE LEVEL REAL-TIME SCAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge</td>
<td>• Security Risk Scan&lt;br&gt;• Email Reputation&lt;br&gt;• Content Scanning&lt;br&gt;• Web Reputation&lt;br&gt;• (Optional) Attachment Blocking&lt;br&gt;• (Optional) Content Filtering&lt;br&gt;• (Optional) Data Loss Prevention</td>
<td>N/A</td>
</tr>
<tr>
<td>Hub</td>
<td>• Security Risk Scan&lt;br&gt;• Attachment Blocking&lt;br&gt;• Content Filtering&lt;br&gt;• Data Loss Prevention&lt;br&gt;• (Optional) Email Reputation&lt;br&gt;• (Optional) Content Scanning&lt;br&gt;• (Optional) Web Reputation</td>
<td>N/A</td>
</tr>
<tr>
<td>Mailbox</td>
<td>N/A</td>
<td>• Security Risk Scan&lt;br&gt;• (Optional) Attachment Blocking&lt;br&gt;• (Optional) Content Filtering</td>
</tr>
</tbody>
</table>
**Note:** Exchange 2003 does not have server roles, so these settings only apply to Exchange 2010 and 2007. Customize manual and scheduled scans as per your requirement on Mailbox server roles.

### Attachment Blocking Policies

Table E-2 lists the recommended attachment blocking settings.

**TABLE E-2. Recommended attachment blocking settings**

<table>
<thead>
<tr>
<th>SERVER ROLE</th>
<th>SETTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge server</td>
<td>Disable</td>
</tr>
<tr>
<td>Transport Level Real-time Scan</td>
<td>Enable</td>
</tr>
<tr>
<td>Store Level Real-time Scan</td>
<td>Disable</td>
</tr>
</tbody>
</table>
Exception Rule Replication

Replicate exception rules using the Server Management console.

TABLE E-3. Attachment blocking exception rule limitations

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>LIMITATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Exceptions are only supported for:</td>
</tr>
<tr>
<td></td>
<td>• Exchange 2010 RTM or above.</td>
</tr>
<tr>
<td></td>
<td>• Exchange 2007 with Service Pack 1 or above.</td>
</tr>
<tr>
<td>Server Roles</td>
<td>• In Edge server, ScanMail cannot obtain sufficient information from Windows Active Directory to implement attachment blocking policies.</td>
</tr>
<tr>
<td></td>
<td>• Exception rules will not be applied in Store Level real time scan, manual scan, and scheduled scan.</td>
</tr>
<tr>
<td></td>
<td>• Exception rules only display on the Summary screen for transport level real time scan.</td>
</tr>
<tr>
<td></td>
<td>• On store level scan and edge servers, only the global policy is applied.</td>
</tr>
</tbody>
</table>

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, .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
Table E-4 lists the recommended Content Filtering settings.

<table>
<thead>
<tr>
<th>SERVER ROLE</th>
<th>SETTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edge server</td>
<td>Disable</td>
</tr>
<tr>
<td>Transport Level Realtime Scan</td>
<td>Enable</td>
</tr>
<tr>
<td>Store Level Realtime Scan</td>
<td>Disable</td>
</tr>
</tbody>
</table>
Content Filtering Policy Replication

Use Server Management to replicate settings between different exchange servers. Only replicate the settings between same server roles.

<table>
<thead>
<tr>
<th>RESOURCE</th>
<th>LIMITATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform</td>
<td>Policies are only supported for:</td>
</tr>
<tr>
<td></td>
<td>• Exchange 2010 RTM or above.</td>
</tr>
<tr>
<td></td>
<td>• Exchange 2007 with Service Pack 1 or above.</td>
</tr>
<tr>
<td>Server Roles</td>
<td>• Content filtering policies only apply for Transport level real time scan</td>
</tr>
<tr>
<td></td>
<td>• Store level scan and edge server only apply the global policy.</td>
</tr>
</tbody>
</table>

Data Loss Prevention Policies

Table E-6 lists the recommended Data Loss Prevention settings for real-time scans.

<table>
<thead>
<tr>
<th>SERVER ROLE</th>
<th>SETTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hub server</td>
<td>Apply policies to &quot;Outbound messages&quot;</td>
</tr>
<tr>
<td>Edge server</td>
<td>Disable</td>
</tr>
</tbody>
</table>

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.
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

Hidden Keys

You can configure Data Loss Prevention through use of the following hidden keys.

**TABLE E-7.  Hidden keys used in Data Loss Prevention configuration**

<table>
<thead>
<tr>
<th>NAME</th>
<th>TYPE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmMaxEntitySize</td>
<td>REG_DWORD</td>
<td>Use this key to customize the bypassing attachment size for Data Loss Prevention scans. The hidden key indicates the file scan threshold in megabytes.</td>
</tr>
<tr>
<td>DmcDisableMask</td>
<td>String</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

---

**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.
Symbols
1-36—1-37

A
access control 8-5
  configuring 8-6
permissions 8-6
  full 8-6
  read 8-6
role 8-5
settings 8-5
actions 5-6
  compressed files 9-8
Data Loss Prevention 5-37
mass-mailing attack 9-7
security risk scan 5-14
spam prevention
  content scanning 5-43
activating ScanMail 2-10, 2-15
  Activation Code 2-11
    additional features 2-14
    standard 2-12
    suite 2-13
  reactivating 2-15
  Activation Code 2-11
    locating 10-9
    reactivating 2-15
    standard 2-12
    suite 2-13
  suite with additional features 2-14
ActiveAction 1-30, 5-14
ActiveUpdate 1-28, 2-19, A-28
  incremental updates 1-28
adware 9-10
alerts 7-4—7-5, 7-8
  notifications 7-7
  outbreak 7-6
  scheduled 7-9
  system events 7-4
attachment blocking 1-33, 7-8
  actions 5-6
    configuring 5-20
  compressed file handling 5-3
  configuring 5-18
  enabling 5-18
  exceptions 5-19
  global policy 5-19
  logs 7-11
  notifications 5-8
  target
    configuring 5-20
C
compressed files 5-3, 9-3, 9-8, 10-11
  actions 9-8
  compression ratios 10-12
  compression types 5-5
Denial-of-Service 5-4
zip-of-death 5-3
compression types 9-8
configuring
  access control 8-6
  content filtering 5-23
Control Manager accounts A-8
Control Manager settings 8-11
Data Loss Prevention 5-35
internal domains 8-8
local sources 5-2
macro scans 5-17
notifications 8-2
proxy settings 8-2
quarantine folder/directory 6-2
real-time scan 8-4
security risk scan
  target 5-15
spam prevention
  content scanning 5-42
  email reputation 5-40
special groups 8-7
web reputation 5-44
World Virus Tracking Program 8-10
contacting
  technical support 10-28, 10-31
Trend Micro 10-29
content filtering 1-34
  actions 5-6
  alerts 7-8
configuring 5-23
data leakage prevention 1-35
exceptions 5-27
  Step 1 - Select Type 5-23
  Step 2 - Select Accounts 5-24
  Step 3 - Specify Policy 5-24
  Step 4 - Specify Action 5-26
  Step 5 - Specify Notification 5-27
  Step 6 - Name and Priority 5-27
content scanning 1-44
  actions 5-43
  configuring 5-42
  enabling 5-43
  target 5-42
Control Manager
  see Trend Micro Control Manager 8-11
conventional scan 5-14
D
data identifiers
  expressions
    creating 5-28
    importing 5-29
  keyword lists
    creating 5-30
    importing 5-31
data leakage prevention 1-35
Data Loss Prevention 1-35
  actions 5-6, 5-37
  alerts 7-8
configuring 5-35
data identifiers
  expressions 1-36–1-37, 5-28–5-29
  keyword lists 5-30–5-31
logs 7-13
notifications 5-8
policies 1-42, 5-35–5-37, 5-39–5-40
  creating 5-35
  deleting 5-40
  modifying 5-39
Step 1 - Select Accounts 5-36
Step 2 - Specify Rule 5-37
Step 3 - Specify Action 5-37
Step 4 - Specify Notification 5-39
Step 5 - Name & Priority 5-39

templates 1-41
creating 5-31
deleting 5-34
exporting 5-35
importing 5-34
modifying 5-33

Denial-of-Service 5-4, 9-2
dialers 9-10
disease vector 9-15

E
EICAR 10-8
email reputation
  actions 5-41
  configuring 5-40
  enabling 5-41
  target 5-40
email reputation services 1-43
  advanced 1-43
  standard 1-43
encoding types 9-11
End User Quarantine 1-47, 8-4
Enterprise Protection Strategy 1-31
Exchange Server 2003
  granting access rights 4-4

F
false positive 10-13
FAQ 10-2
file reputation services 1-19
frequently asked questions 10-2
  calculating decompressed file size 10-11
  checking pattern file updates 10-10
  checking service pack updates 10-10
  compression ratios 10-12
dangerous files 10-13
EICAR test virus 10-8
false positives 10-13
handling large files 10-11
latest patches 10-8
locating Activation Code 10-9
locating Registration Key 10-9—10-10
phish attacks 10-3
regular expressions 10-14
remote SQL server password changed 10-2
sending detected viruses to Trend Micro 10-9
sending suspected threats to Trend Micro 10-9
spyware/grayware 10-4
unable to log on to product console 10-2
using keywords 10-22—10-24
using operators with keywords 10-5

G
global policy 5-19
global settings
  quarantine folder/directory 6-2

H
hacking tools 9-10
hot fixes 1-31

I
icons 4-14
in Trend Micro Control Manager A-47
integrated server 1-21
IntelliScan 1-29, 5-15
IntelliTrap 1-30, 5-15
internal domains 8-8
  configuring 8-8

J
joke program 9-7, 9-10

K
keywords 10-22—10-24
Knowledge Base 10-30
known issues 10-27

L
licenses 1-48, 8-9
    Maintenance Agreement 1-48
    registering 2-8
local sources
    configuring 5-2
    settings 5-2
    Smart Protection Server 5-2
log query 7-13
logs 7-11, A-47
    maintenance 7-15
    query 7-13
    querying 7-14
    querying from Control Manager A-20, A-47
types 7-11
    Windows events B-1

M
macro scan 5-17
macro viruses/malware 9-9
maintaining security 3-3
Maintenance Agreement 1-48
    renewal 1-49
    URL 1-48
managing outbreak situations 3-5
    analyzing 3-6
    confirming the outbreak 3-5
    recovering 3-6
    responding 3-6
manual scan 1-27
    alerts 7-5
    characteristics 5-13
    compressed file handling 5-3
    notifications 5-8
manual updates 2-18
mass-mailing attack 9-7
actions 9-7
master services
    ScanMail EUQ Migrator Service 4-13
    ScanMail EUQ Monitor 4-13
    ScanMail for Exchange Remote Configuration
        Server 4-13
    ScanMail for Microsoft Exchange Master
        Services 4-13
    ScanMail for Microsoft Exchange System
        Watcher 4-13
    starting and stopping 4-13
multipart internet mail extensions 9-15

N
notifications 5-8, 8-2
    actions that trigger 8-3
    alerts 7-7
    configuring 8-2
    global settings 8-4

O
one-time reports 7-8—7-9
    generating 7-8
    in Control Manager A-51
online help
    accessing 2-7
operator 8-6
outbreak alerts 7-6
Outbreak Prevention Services 1-32
    alerts 7-5

P
password cracking applications 9-10
patches 1-31
    updating FAQ 10-8
pattern files 1-22, 1-25, 10-10, 10-26
    in Control Manager A-28
incremental updates 1-28
    in Control Manager A-28
Smart Scan Agent pattern 1-22
Smart Scan pattern 1-23
spam pattern files 1-47
updates 2-16
updating manually 10-26
Web Blocking list 1-23
phish 9-2, 9-16, 10-3
policies
  content filtering 5-21
  Data Loss Prevention 1-42, 5-35
product console 2-2
  banner 2-4
  configuration area 2-7
  getting help 2-7
  side menu 2-6
  unable to log on 10-2
  viewing remote servers 4-7
  viewing servers 4-7
  viewing virtual servers 4-8
proxy servers 2-17
  configuring 2-17
proxy settings 2-17, 8-2
  configuring 8-2
  in Control Manager A-45
QR
quarantine
  alerts 7-5
  configuring 6-2
  folder/directory 6-2
  global settings 6-2
  queries 6-3
    maintenance 6-3–6-4
    performing 6-3
    resending messages 6-4
quarantine folder/directory 6-2
  alerts 7-5
quarantine query 6-3
maintenance
  automatic 6-3
  manual 6-4
performing 6-3
resending messages 6-4
R
reactivating ScanMail 2-15
real-time monitor 4-2
  viewing remote servers 4-2
real-time scan 1-26, 8-4
  characteristics 5-13
  configuring 8-4
  notifications 5-8
regions 10-28
registering ScanMail 2-8
  contacts 2-9
  how to 2-9
  online purchase 2-8
  Registration Key 2-8
  reseller purchase 2-8
  to Control Manager 8-13, A-7
URL 2-9
Registration Key
  locating 10-9–10-10
regular expressions 10-14
remote access tools 9-10
remote servers
  viewing with real-time monitor 4-2
replicating configurations 4-8
reports 7-7
  generating scheduled 7-10
  in Control Manager A-49
  maintenance 7-11
  one-time reports 7-8–7-9
resources
  creating for virtual servers 4-9–4-12
  creating for Windows 2003 4-9
  creating for Windows 2008 4-10–4-11
  Exchange 2007 CCR Cluster 4-11
  Exchange 2007 SCC Cluster 4-10
  Exchange 2007 SCR Cluster 4-12
role
    operator 8-6
roll back 2-21

S
scan engine 1-23
    update manually 10-25
    updates 1-24
    URL 1-24
scan method 5-14
ScanMail
    manage from Control Manager A-14
ScanMail EUQ Migrator Service 4-13
ScanMail EUQ Monitor 4-13
ScanMail for Exchange Remote Configuration Server 4-13
ScanMail for Microsoft Exchange Master Services 4-13
ScanMail for Microsoft Exchange System Watcher 4-13
ScanMail technology 1-23
    ActiveAction 1-30
    ActiveUpdate 1-28
    attachment blocking 1-33
    content filtering 1-34
    Data Loss Prevention 1-35
    Enterprise Protection Strategy 1-31
    hot fixes, patches and service packs 1-31
    IntelliScan 1-29
    IntelliTrap 1-30
    Outbreak Prevention Services 1-32
scan engine 1-23
scans 1-26
    about scans 1-26
    actions 5-6
    logs 7-11
    macro scan 5-17
    manual scan 1-27
on cluster servers 1-28
real-time scan 1-26
scheduled scan 1-27
scheduled scan 1-27
    alerts 7-5
    characteristics 5-13
    compressed file handling 5-3
    notifications 5-8
scheduled updates 2-18
security baseline 3-2
    managing real-time monitor 3-2
    performing a manual scan 3-2
    update ScanMail 3-2
security information site 10-31
security risk scan 5-12
    actions 5-14
        settings 5-16
    ActiveAction 5-14
    compressed file handling 5-3
    configuring target settings 5-15
    custom settings 5-14
    IntelliScan 5-15
    IntelliTrap 5-15
    logs 7-11
    report 7-8
    scan methods 5-14
    summary screen 7-3
security risks 9-2
    compressed files 9-3
    Denial-of-Service 9-2
    disease vector 9-15
    encoding types 9-11
    joke program 9-7
    macro viruses/ malware 9-9
    mass-mailing attack 9-7
    multipurpose internet mail extensions 9-15
    other malicious codes 9-3
packed files 9-3
phish 9-2, 9-16
spyware/grayware 9-2, 9-9
Trojan Horse 9-3, 9-6
ture file type 9-15
virus/malware writers 9-5
viruses/malware 9-3
worms 9-3, 9-6
zip-of-death 9-9
server management console 4-3
activating 4-3
replicating configurations 4-8
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
servers
configuring A-19
service packs 1-31, 10-10
services
starting and stopping 4-13
Smart Protection 1-18
file reputation services 1-19
integrated server 1-21
pattern files 1-22
Smart Protection Network 1-21
Smart Protection Server 1-21
source comparison 1-22
sources 1-21
standalone server 1-21
The Need for a New Solution 1-18
virus/malware pattern 1-21
web reputation services 1-19
Smart Protection Network 1-21, 5-44, 8-10
web reputation 5-44
Smart Protection Server 1-21, 5-44
alerts 7-4
integrated server 1-21
security risk scan
alerts 7-4
standalone 1-21
web reputation 5-44, 7-5
Smart Protection sources 1-21
comparison 1-22
integrated server 1-21
local source settings 5-2
protocols 1-22
Smart Protection Network 1-21
Smart Protection Server 1-21
standalone server 1-21
smart scan 5-14
spam engine 1-47
spam maintenance 8-4
End User Quarantine 8-4
spam pattern files 1-47
spam prevention 1-42
alerts 7-8
content scanning 1-44
actions 5-43
configuring 5-42
enabling 5-43
target 5-42
email reputation 5-40
actions 5-41
configuring 5-40
enabling 5-41
target 5-40
email reputation services 1-43
End User Quarantine 1-47
maintenance 8-4
notifications 5-8
spam engine 1-47
spam pattern files 1-47
special groups 8-7
adding 8-7
configuring 8-7
editing 8-8
spyware/grayware 5-15, 9-2, 9-9, 10-4
adware 9-10
dialers 9-10
entering the network 9-11
Growing Hazard 10-5
hacking tools 9-10
joke program 9-10
malware naming 9-12
password cracking applications 9-10
remote access tools 9-10
risks and threats 9-10
SQL server
  manually updating password 10-3
standalone server 1-21
summary 7-2
  security risks 7-3
  spam tab 7-4
  system tab 7-2
support/system debugger 8-14
  modules 8-14
  using 8-14
T
technical support 10-28
  checklist 10-29
templates 1-41
  creating 5-31
  deleting 5-34
  exporting 5-35
  importing 5-34
  modifying 5-33
Trend Micro
  headquarters 10-29
  Knowledge Base 10-30
  TrendLabs 10-30
Trend Micro Control Manager 8-11
  agent 8-11, A-7
  architecture A-5
  communication protocol 8-12
  communicator 8-11
  components A-28
    anti-spam rules A-28
    automatic deployment A-33
    configuring manual download A-32
    configuring scheduled downloads A-36
    download A-28
    engines A-28
    manual download steps A-29–A-32
    pattern files/cleanup templates A-28
    product program A-28
    scheduled download deployment A-42
    scheduled download exceptions A-34
    scheduled download frequency A-40
    scheduled download settings A-40
    scheduled downloads A-35
    configuring accounts A-8–A-9
    configuring ScanMail 8-11
    configuring ScanMail servers A-19
    data views A-48
    deployment plans A-43
    Directory Management A-24
      creating folders A-25
      deleting folders A-27
      moving folders/products A-26
      renaming folders/products A-26
      entity 8-11
    Event Center A-5
    features A-3
    introduction A-1
    issuing tasks to ScanMail A-19
    logs A-47
      querying data A-47
mail server A-5
Management Communication Protocol A-6
heartbeat A-10
heartbeat settings A-13
ScanMail server status A-11
schedule bar A-12
management console A-7
managing ScanMail A-14
Outbreak Prevention Policy A-16
policy
   Log on as batch job A-46
Product Directory A-15
   accessing A-17
   deploying components A-18
proxy settings A-45
querying logs A-20
recovering server lists A-22
registering ScanMail 8-13, A-7
report server A-6
report templates A-50
reports A-49
   one-time reports A-51
   scheduled A-52
ScanMail user access A-10
searching for ScanMail entities A-23
server 8-11, A-5
services A-22
SQL database A-5
Trend Micro Infrastructure A-6
unregistering ScanMail 8-14
update/deployment settings A-45
user accounts A-9
using ScanMail 8-12
versions A-2
viewing ScanMail summaries A-18
web server A-5
TrendLabs 10-30
Trojan Horse 9-3, 9-6
troubleshooting 10-25
true file type 9-15

U
unregistering
   ScanMail from Control Manager 8-14
updates 1-24
   ActiveUpdate 1-28
   alerts 7-5
   components on clusters 2-17
   Control Manager components A-28
download source 2-19
   latest patches FAQ 10-8
   logs 7-11
   manual configurations 2-18
   pattern file, manual 10-26
   pattern files 2-16
   rolling back 2-21
   scan engine, manual 10-25
   scheduled configurations 2-18
   settings in Control Manager A-45
updating ScanMail 2-16
URLs
   email technical support 10-31
   Knowledge Base 10-27, 10-30
   scan engine version 1-24
   security information site 10-31
   technical support 10-28
   Trend Micro Worldwide 10-29
   update center 10-27

V
virtual servers 4-8, 5-13
   creating ScanMail resources 4-9—4-12
   viewing from the product console 4-8
Virus Scan Application Programming Interface (VS API)
   scan engine 1-23
virus/malware pattern 1-21
viruses/malware 9-3, 9-9
  boot 9-4
  file 9-4
  malware naming 9-12
  script 9-4
  writers 9-5

W
web reputation 5-44, 5-46
  actions 5-6
  alerts 7-5, 7-9
  configuring 5-44
  enabling 5-46
  logs 7-13
  notifications 5-8
  Smart Protection Network 5-44
  Smart Protection Server 5-44
web reputation services 1-19–1-20
wildcard 8-8, 10-7
Windows event log codes B-1
World Virus Tracking Program 8-10
  configuring 8-10
worms 9-3, 9-6

Z
zip-of-death 5-3, 9-9