TREND MICRO™
ScanMail™
Administrator’s Guide
Proactive Antivirus and Content Security for the Domino Environment
for IBM Domino
Trend Micro Incorporated reserves the right to make changes to this document and to the product described herein without notice. Before installing and using the product, review the readme files, release notes, and/or the latest version of the applicable documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com/

© 2019 Trend Micro Incorporated. All Rights Reserved.

Trend Micro, the Trend Micro t-ball logo, 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.

Document Part No. SNEM58574/190117

Release Date: January 2019

Protected by U.S. Patent Nos. 5,951,698 and 5,889,943
The Administrator's Guide for ScanMail for IBM Domino introduces the main features of the software and provides installation instructions for your production environment. Read through it before installing or using the software.

Please refer to Getting Support for technical support information and contact details. Detailed information about how to use specific features within the software is also available in the Help Database and online Knowledge Base at Trend Micro's Web site.

Trend Micro is always seeking to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro documents, please contact us at docs@trendmicro.com. Your feedback is always welcome. Please evaluate this documentation on the following site:

www.trendmicro.com/download/documentation/rating.asp
Privacy and Personal Data Collection Disclosure

Certain features available in Trend Micro products collect and send feedback regarding product usage and detection information to Trend Micro. Some of this data is considered personal in certain jurisdictions and under certain regulations. If you do not want Trend Micro to collect personal data, you must ensure that you disable the related features.

The following link outlines the types of data that ScanMail for IBM Domino collects and provides detailed instructions on how to disable the specific features that feedback the information.


Data collected by Trend Micro is subject to the conditions stated in the Trend Micro Privacy Policy:

Contents

Preface

What’s New in Version 5.8 ................................................................. 1-clxxvii
Audience ......................................................................................... 1-clxxix
Document Conventions ............................................................... 1-clxxx

Chapter 1: Introducing ScanMail for IBM Domino 5.8

Product Overview ............................................................................. 1-2
ScanMail for IBM Domino Standard Features ............................... 1-3
ScanMail for IBM Domino Suite Features ..................................... 1-4
ScanMail for IBM Domino Suite with DLP Features ..................... 1-4
ScanMail for IBM Domino Versions Comparison ........................... 1-4
How ScanMail Works ...................................................................... 1-5
ScanMail Components ................................................................... 1-6

Types of Scans .................................................................................. 1-7
Real-time Mail Scanning ................................................................. 1-7
Real-time Database Scanning ......................................................... 1-8
Manual and Scheduled Database Scanning ..................................... 1-8

Understanding Policies, Rules, and Filters ................................. 1-9
ScanMail Rules .............................................................................. 1-11
ScanMail Filters ............................................................................ 1-11

ScanMail Protection Strategy ......................................................... 1-12
Planning for a Policy-Based Antivirus and Content Security Protection 1-12
Planning to Implement Rules and Filters in a Policy-Based Environment 1-13

Chapter 2: Installing ScanMail for IBM Domino

Planning SMID Deployment ............................................................. 2-2
Upgrading Domino Server ............................................................ 2-3
Chapter 3: Getting Started with SMID

Understanding the SMID Interface ................................................................. 3-2
Getting Help While Using ScanMail .............................................................. 3-3
Running a Manual Scan After Installation .................................................... 3-3
Adding ScanMail Database Icons to the Notes Workspace ....................... 3-3
Signing ScanMail Databases with a Different ID ......................................... 3-4
Defining Access and Roles to ScanMail Databases ...................................... 3-4
Accessing ScanMail Databases ..................................................................... 3-6
Accessing ScanMail Databases Using a Notes Client ................................. 3-7
Accessing ScanMail Databases Using a Web Browser ............................... 3-8
  Limitations when Accessing ScanMail Databases Using a Web Browser .... 3-9
  Set the Internet Password for ScanMail Database Access through a Web Browser ................................................................. 3-9
Accessing other ScanMail Databases through the Configuration Database .................................................................................... 3-10

Chapter 4: Configuring Scan Tasks

Planning for a Policy-based Antivirus and Content Security Protection 4-2
  How Policy-based Protection Works ........................................................... 4-3
Managing Policies .......................................................................................... 4-3
  Creating Policies .......................................................................................... 4-3
  Modifying Policies ...................................................................................... 4-5
  Deleting Policies ......................................................................................... 4-6
  Prioritize Policies ....................................................................................... 4-6
  Managing the Trusted Cluster Servers for a Policy ................................. 4-7
Creating Rules .............................................................................................. 4-9
  Creating Real-time Mail Scan Rules ......................................................... 4-9
    Apply the Strictest Rule .......................................................................... 4-12
    Configure General Mail Scan Rule Settings ........................................... 4-13
  Creating Real-time Database Scan Rules ............................................... 4-14
  Creating Scheduled Database Scan Rules ................................................. 4-16
Organizing Rules ...........................................................................................4-19
Changing a Rule’s Priority ........................................................................4-19
Rule Operators ..........................................................................................4-20
Introducing ScanMail Filters .................................................................4-20
Filter Execution Order ........................................................................4-20
Spam Filtering (Suite Edition or Suite Edition with Data Loss Prevention
only) ...........................................................................................4-22
Content Filtering (Suite Edition, or Suite Edition with Data Loss
Prevention only) ...............................................................................4-24
Expressions ..........................................................................................4-24
Configuring the Scan and Filter Settings ...................................................4-25
Configure Anti-Spam Filtering .................................................................4-26
End User Quarantine .................................................................................4-30
Configure Web Reputation ........................................................................4-36
Local and Global Smart Protection ........................................................4-36
Optimizing Web Reputation ....................................................................4-40
Troubleshooting Web Reputation Performance Issues ................4-40
Configuring Security Risk Scan ...............................................................4-41
Configuring APT Prevention Filter ..........................................................4-45
Starting Deep Discovery Advisor Agent .................................................4-47
Configuring Scan Restrictions .................................................................4-47
Configuring the Message Filter ..............................................................4-48
Configuring the Graymail Filter ..............................................................4-50
Configuring Inbound Gateway IP Address List .......................................4-50
Configuring Graymail Filter Scan Options ...........................................4-50
Configuring the Attachment Filter ..........................................................4-52
Configuring Content Filter .......................................................................4-55
Add New Content Filters Based on Existing Filters .........................4-58
Create New Expressions ........................................................................4-59
Add New Expressions Based on Existing Expressions .......................4-60
Configuring Data Loss Prevention Filter ................................................4-60
Data Loss Prevention Rule Management ...............................................4-61
Data Loss Prevention Template Management .......................................4-61
Data Identifiers ....................................................................................4-62
Configuring Data Loss Prevention Filter Options ................................4-64
Configuring Script Filter .........................................................................4-66
Configuring Redirect Options .................................................................4-67
Chapter 5: Performing Administrative Tasks

Viewing the Summary of All Servers ........................................................... 5-2
Configuring the Server Settings Menu Options ........................................ 5-3
   Creating a Server Setting Rule .............................................................. 5-3
   Modifying a Server Settings Rule .......................................................... 5-4
Configuring a Server Settings Rule .......................................................... 5-5
   Set a Scanning Directory ...................................................................... 5-5
   Set the Memory Size for Scanning ..................................................... 5-5
   Configure the Proxy Server Settings .................................................... 5-6
   Configuring Inbound Gateway IP Addresses ....................................... 5-7
   Configure Local Smart Scan Sources ................................................. 5-8
   Monitor Server Events ....................................................................... 5-11
   Enable Server Task Monitoring .......................................................... 5-11
   Specify the Default Character Set ..................................................... 5-12
   Configure Miscellaneous Settings ..................................................... 5-12
Configuring CM Agent Settings ................................................................. 5-14
Configuring Deep Discovery Advisor Settings ....................................... 5-15
Managing the Filter Lists ........................................................................... 5-17
Configuring the Administration Menu Options ....................................... 5-18
   Applying the Notes Database Properties to ScanMail Databases .... 5-18
   Creating and Applying a New Access Control (ACL) Entry .......... 5-19
   Allowing Tasks to be Viewed through the Domino Administrator 5-20
   Creating a License Profile ................................................................. 5-20
   Deleting a License Profile ................................................................. 5-20
Chapter 6: Updating Components

Understanding the Antivirus and Content Security Components ..........6-2
Updating Components ........................................................................6-3
  Updating Components Manually ......................................................6-3
  Updating Components Automatically Using Scheduled Update Rules ...6-5
  Deploy Specific Components Automatically ..................................6-7
Configuring Update Settings ...............................................................6-8
  Selecting Components to Update ....................................................6-8
  Setting the Update Source ..............................................................6-9
  Defining the Proxy Server Settings for Component Download ..........6-11
Loading Components Manually ..........................................................6-12

Chapter 7: Sending ScanMail for IBM Domino Notifications

Understanding ScanMail Notifications .............................................7-2
  Customizing Notifications .............................................................7-3
Using Email Stamps (Safe Stamps) .....................................................7-6
Setting ScanMail Notifications ..........................................................7-7
  Defining How ScanMail Delivers Notifications .............................7-7
  Configuring ScanMail for Windows Event Logs .............................7-8
Setting the Scan Notifications ............................................................7-9
Setting the Update Notifications .......................................................7-9

Chapter 8: Using the Log and Quarantine Databases

Using the Log Database .................................................................8-2
  Accessing Trend Micro Threat Connect Portal ..................................8-3
  Managing ScanMail Logs ...............................................................8-4
  Searching for Logs ........................................................................8-5
Enabling/Disabling Log Deletion .......................................................8-7
  Deleting Virus Logs Automatically ................................................8-8
  Deleting Virus Logs Manually .......................................................8-9
Viewing Statistics and Charting .......................................................8-9
  Generating, Viewing, and Exporting Statistics ...............................8-10
Generating and Viewing Charts ................................................... 8-11
Using the Quarantine Database ................................................... 8-13
Viewing Quarantined Messages, Documents and Attachments .......... 8-13
Resending Quarantined Messages ................................................ 8-14
Restoring Quarantined Documents .............................................. 8-15
Enabling/Disabling Quarantined Item Deletion ................................ 8-15
Deleting Quarantined Items Automatically ................................... 8-16
Deleting Quarantined Items Manually .......................................... 8-18
Understanding Deep Discovery Advisor Quarantine Database ............ 8-19
Viewing Quarantined Messages ................................................... 8-19

Chapter 9: Using ScanMail for IBM Domino with Trend Micro Control Manager

Introducing Control Manager .......................................................... 9-2
Key Features ....................................................................................... 9-2
Using ScanMail with Control Manager ............................................ 9-3
Introducing the Control Manager Management Communication Protocol 9-3
Introducing Outbreak Prevention Services ......................................... 9-4
Using Control Manager to Administer ScanMail ................................. 9-5
Accessing the Control Manager Management Console .................... 9-5
Managing ScanMail from the Control Manager Management Console .. 9-5
Viewing an Active Outbreak Prevention Policy .................................. 9-7

Chapter 10: Removing SMID

Removing ScanMail ............................................................................ 10-2
Removing ScanMail Automatically .................................................. 10-2
Running a Wizard-based Uninstallation ............................................ 10-2
Removing a Single or Shared ScanMail Installation Manually .......... 10-9
Removing a Single or Shared ScanMail Installation on Windows ....... 10-9
Removing a Single or Shared ScanMail Installation on Linux .......... 10-13
Chapter 11: Troubleshooting
Locating Installation and Uninstallation Logs ...........................................11-2
Held Mail Issues .......................................................................................11-2
  General Held Message Issues ..............................................................11-2
  Scanning for and Releasing Held Mail in the System Mailbox ..........11-2
Update Issues ...........................................................................................11-3
Scheduled Scan/Update Issue .................................................................11-4
Recovering a Corrupt ScanMail Database ..............................................11-5
Using the Database Templates to Recreate ScanMail Databases ..........11-6
Deep Discovery Advisor Agent Issue .........................................................11-7
Debugging ScanMail Tasks ....................................................................11-7
  Debug Levels ..................................................................................11-8
  Debug Results ................................................................................11-8
Understanding ScanMail Error Messages ..............................................11-9
Configuring Exceptions for Directories ..................................................11-12

Chapter 12: Getting Support
Before Contacting Technical Support .......................................................12-2
Contacting Technical Support .................................................................12-2
Reporting Spam and False Positives to Trend Micro .............................12-3
Introducing TrendLabs ...........................................................................12-3
Other Useful Resources .........................................................................12-4

Appendix A: Understanding Threats in a Domino Environment
Understanding Malware ..........................................................................A-2
Contents

Viruses ........................................................................................................ A-2
Worms ........................................................................................................ A-4
Trojan Horses .......................................................................................... A-4
Joke Programs .......................................................................................... A-4
Web Reputation ......................................................................................... A-5
How Malware Spreads in a Notes Environment .................................... A-5

Appendix B: ScanMail for IBM Domino Best Practices
    Tuning the Domino Server ................................................................. B-2
    Performance Recommendations ...................................................... B-2

Appendix C: Program File and Folder Lists
    ScanMail for Windows ....................................................................... C-2
    ScanMail for Linux ........................................................................... C-3

Appendix D: SMID 5.6 SP1 and SMID 5.8 Feature Comparison
This Administrator’s Guide describes ScanMail for IBM Domino (SMID) and provides installation and uninstallation instructions to help you configure SMID functions for your specific needs.

The ScanMail Administrator’s Guide discusses the following topics:

- Introducing ScanMail for IBM Domino 5.8 provides an overview of the product and description of all new features in this release.
- Installing ScanMail for IBM Domino provides step-by-step instructions on installing ScanMail for IBM Domino.
- Getting Started with SMID provides recommended procedures to configure SMID after you have installed it.
- Configuring Scan Tasks provides procedures to create policies, rules, or expressions that SMID will use to protect a Domino environment.
- Performing Administrative Tasks provides procedures to monitor server status and create rules for individual or groups of Domino servers.
- Updating Components provides procedures to update antivirus and content security components.
- Sending ScanMail for IBM Domino Notifications provides procedures to send ScanMail notifications.
- Using the Log and Quarantine Databases provides procedures to maximize the use of the ScanMail Log and Quarantine databases.
- Using ScanMail for IBM Domino with Trend Micro Control Manager provides details on how to use Trend Micro Control Manager™ to manage ScanMail.
• **Removing SMID** provides procedures for removing ScanMail for IBM Domino.
• **Troubleshooting** provides troubleshooting tips.
• **Getting Support** provides guidelines to get more information.

Additionally, the ScanMail Administrator’s Guide contains the following appendices:

• **Understanding Threats in a Domino Environment** provides information on the types of threats found in a Domino environment.
• **ScanMail for IBM Domino Best Practices** provides installation instructions to improve operation and obtain maximum performance for SMID.
• **Program File and Folder Lists** provides a list of the SMID and Control Manager files and folder structures that are available upon a successful application installation.
• **SMID 5.6 SP1 and SMID 5.8 Feature Comparison** provides a comparison of ScanMail for IBM Domino 5.8 and ScanMail for IBM Domino 5.6 SP1 features.
What’s New in Version 5.8

ScanMail for IBM Domino represents a significant advancement in anti-malware, Advanced Persistent Threat (APT) prevention, content security, and data loss prevention for IBM Domino environments. ScanMail for IBM Domino provides state-of-the-art detection based on heuristic rule-based scanning, recognition of Approved/Blocked Senders lists and signature databases. It also includes anti-spam, content filtering, and data loss prevention that may be applied according to the needs of your organization.

Configuration improvements make SMID more flexible and scalable than ever before.

- Latest Platform Support
- Visual C++ 2015 Redistributable Runtime Library (For Windows Platform Only)
- Comply with General Data Protection Regulation (GDPR)
- Masking for Protected Content
- Advanced File Information (AFI) in Advanced Threat Scan Engine
- Enhanced Deep Discovery Advisor Settings
- Enhanced Advanced Threat Scan Engine (ATSE)
- Enhanced Web Reputation Service (WRS)
- Latest Deep Discovery Advisor Support
- New Malware Naming Convention
- Web Reputation Service (WRS) Category Information to Trend Micro Control Manager (TMCM)
- Updated Data Loss Prevention (DLP) Template
- Enhanced Anti-spam Settings

Latest Platform Support

This version of ScanMail supports the latest IBM™ Domino™ 10 and 10.0.1.

Visual C++ 2015 Redistributable Runtime Library (For Windows Platform Only)

This version of Trend Micro ScanMail runs with Microsoft Visual C++ 2015 Redistributable Package.
Comply with General Data Protection Regulation (GDPR)
This version of ScanMail complies with the European regulation, General Data Protection Regulation (GDPR).

Masking for Protected Content
This version enables ScanMail for IBM Domino to mask the protected contents in the subject or mail body of an email message that triggers the Data Loss Prevention (DLP) filter when the "Mask content and pass" action is enabled.

Advanced File Information (AFI) in Advanced Threat Scan Engine
This version allows users to enable ScanMail for IBM Domino to use ATSE Advanced File Information (AFI) to retrieve the file information of executable files, macro files, and script files (VBE, VBS, JS, JSE, WSF, PS1) that were not virus scanned by the engine, and then send these files to Trend Micro Deep Discovery Advisor.

Enhanced Deep Discovery Advisor Settings
This version adds the following settings in the Deep Discovery Advisor Settings for communicating with the Deep Discovery Advisor:

• Maximum wait time for analysis ratings
• Action on unanalyzed risks

This version allows users to enable the following two options under the Default Mail Scan > Scan Options > APT Prevention Filter > Scan Settings > Select attachments to scan setting, simultaneously:

• Suspicious files detected by Advanced Threat Scan Engine
• Files with specified type

Enhanced Advanced Threat Scan Engine (ATSE)
This version of ScanMail supports the following new feature of the Advanced Threat Scan Engine (ATSE):

• aggressive rules level (ATSE 9.750.1016 and higher builds)
Enhanced Web Reputation Service (WRS)

This version of ScanMail enables the Web Reputation Service (WRS) to support the "Ransomware" category. This ensures ScanMail for IBM Domino can detect hyperlinks that contain ransomware and record these information in the log database.

Latest Deep Discovery Advisor Support

This version of ScanMail supports Deep Discovery Advisor 6.0 servers.

New Malware Naming Convention

This version supports the new malware naming convention to help with the proper identification of ransomware components.

Web Reputation Service (WRS) Category Information to Trend Micro Control Manager (TMCM)

This version adds the WRS category information in security logs that ScanMail for IBM Domino sends to Trend Micro Control Manager™.

Updated Data Loss Prevention (DLP) Template

This version updates the Data Loss Prevention (DLP) template to version 3.1.1005 to add the "My number" template.

Enhanced Anti-spam Settings

This version enables you to configure Anti-spam Configuration settings to specify sender IP addresses and/or subject keywords to skip matching email messages for database console.

Audience

ScanMail for IBM Domino documentation assumes a basic knowledge of security systems and administration of IBM Domino™ email and information sharing system functions. The Administrator's Guide and Domino-based online Help are designed for Domino and network administrators.
Document Conventions

To help you locate and interpret information easily, the ScanMail documentation (Help and Administrator’s Guide) uses the following conventions.

**TABLE 1-1. Conventions used in SMID documentation**

<table>
<thead>
<tr>
<th>CONVENTION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL CAPITALS</td>
<td>Acronyms, abbreviations, and names of certain commands and keys on the keyboard</td>
</tr>
<tr>
<td>Bold</td>
<td>Menus and menu commands, command buttons, tabs, options, and ScanMail tasks</td>
</tr>
<tr>
<td>Monospace</td>
<td>Examples, sample command lines, program code, and program output</td>
</tr>
<tr>
<td>Note:</td>
<td>Configuration notes</td>
</tr>
<tr>
<td>Tip:</td>
<td>Recommendations</td>
</tr>
<tr>
<td>WARNING!</td>
<td>Reminders on actions or configurations that should be avoided</td>
</tr>
</tbody>
</table>
Chapter 1

Introducing ScanMail for IBM Domino 5.8

ScanMail for IBM Domino (SMID) offers comprehensive virus protection and content security for the Domino environments, providing real-time scanning for viruses, adware, and spyware hidden within email attachments and databases. ScanMail for IBM Domino prevents viruses and other malicious code from entering your Domino environment.

ScanMail Suite for IBM Domino provides an added layer of protection through revolutionary anti-spam technologies and data loss prevention. ScanMail Suite for IBM Domino performs spam detection before it performs real-time mail scanning.

This chapter discusses the following topics:

- **Product Overview** on page 1-2
- **Types of Scans** on page 1-7
- **Understanding Policies, Rules, and Filters** on page 1-9
- **ScanMail Protection Strategy** on page 1-12
- **Planning for a Policy-Based Antivirus and Content Security Protection** on page 1-12
Product Overview

ScanMail for IBM Domino (SMID) works in real time to prevent viruses, malicious code (also known as malware), and unwanted content from entering your Domino environment through mail, replication, or infected documents. Malware scanning is performed in memory, which significantly increases the scanning speed.

ScanMail is designed to operate as a native Domino server application and thus provides administrators with a familiar, intuitive interface. The configuration interface for ScanMail is fully integrated with the Domino server and supports remote management from any IBM Notes workstation, Web browser, or Domino R8/R9/R10 Administration Client. This version of ScanMail for IBM Domino is designed to run on the Microsoft™ Windows™ and Linux.

The ScanMail Standard version provides security risk scanning in all modes and component update. The ScanMail Suite version additionally provides Web reputation, content and spam filtering, end-user quarantine functionalities. The Suite with Data Loss Prevention version provides all the features from Standard and Suite versions and additionally provides Data Loss Prevention.

ScanMail is fully compatible with Trend Micro Control Manager™, the Trend Micro centralized management console that lets you consolidate your antivirus and content security protection into a cohesive solution.

Administrators can specify which databases are to be scanned, and users are prevented from overwriting a clean document with an infected version. Manual database scanning cleans existing infections.

ScanMail helps administrators enforce company email policies, increase overall server efficiency, and minimize virus outbreaks. Administrators can create rules to block certain file types and block, delay, and prioritize messages. A corporate policy can be implemented to deal with malware incidents in several ways:

- Isolate the infected file for later cleaning or other action.
- Send the infected item to the intended recipient along with a notification that the file is infected and has not been cleaned.
- Delete the infected file.
- Block the infected file and prevent it from being delivered.
- Alert the administrator.
By using a multi-threaded scan engine and memory scanning, ScanMail is able to maximize efficiency and minimize impact on IBM Domino servers. Administrators can identify servers that don’t require scanning, thus eliminating redundant scanning.

To see where ScanMail fits in a comprehensive approach to protecting your environment, see:


ScanMail for IBM Domino Standard Features

ScanMail for IBM Domino Standard version features include:

- Support for true file formats for both malware scanning and attachment blocking.
- Support for multiple instances of ScanMail on multiple Domino servers.
- Real-time mail scanning, and real-time, manual, and scheduled database scanning.
- Customizable scanning options, such as limiting the extracted file size for compressed file scanning and enabling message body scanning.
- Advanced scanning options, which include:
  - An incremental scanning option that saves considerable server time and resources during manual and scheduled database scans because it allows selective scanning of new and newly modified documents.
  - Notes script scanning to eliminate malicious code at the source before it can do any damage.
  - Rich Text and Stored Form hot spot scanning.
  - Safeguard against Advance Persistent Threats (APTs) through latest technologies, such as Advanced Threat Scan Engine (ATSE) and Deep Discovery Advisor.
  - Ability to create policies and rules that define how ScanMail protects the Domino environment, updates components, sends notifications, and trusts cluster servers.
  - Scheduled and manual component updates.
  - ScanMail scan and update notifications.
  - Proactive outbreak prevention through Control Manager (CM).
  - Trusted server configuration for multi-server environments, which allows certain servers to be configured so that messages scanned on trusted servers will not be scanned again, thus saving server time and resources.
• A Quarantine database that allows easy viewing of quarantined email and attachment information.
• Complete logging and reporting capabilities, which include statistics and charting.
• Integration with Trend Micro Threat Connect information portal.

ScanMail for IBM Domino Suite Features
ScanMail for IBM Domino Suite version contains all the features of the Standard version and the following additional features:
• End-user quarantine
• Anti-spam filtering
• Filter message content by subject or body text
• Filter message by attachment content or attachment file name
• Scan attached MS Office documents, PDF, .txt, .html, and .rtf files
• Web reputation filtering
• Graymail filtering

ScanMail for IBM Domino Suite with DLP Features
ScanMail for IBM Domino Suite with Data Loss Prevention (DLP) version contains all the features of the Suite version and the Data Loss Prevention (DLP) Filtering.

ScanMail for IBM Domino Versions Comparison
A brief comparison of ScanMail Suite and Standard features is shown in Table 1-2.

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>STANDARD</th>
<th>SUITE</th>
<th>SUITE WITH DATA LOSS PREVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Anti-Spam</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Table 1-2. Comparison of Features for ScanMail for IBM Domino Standard and Suite Versions
Introducing ScanMail for IBM Domino 5.8

Note: Advance Persistent Threats (APT) Prevention Filtering is NOT supported on Windows 32-bit.

### TABLE 1-2. Comparison of Features for ScanMail for IBM Domino Standard and Suite Versions

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>STANDARD</th>
<th>SUITE</th>
<th>SUITE WITH DATA LOSS PREVENTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Reputation Service (WRS)</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Graymail filtering</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Active Update</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Control Manager Agent</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>End User Quarantine</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced Persistent Threats (APT) Prevention Filtering</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Threat Connect Integration</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Content Filtering**

| Subject/Attachment/Body/MS Office, PDF, .txt, .html, and .rtf files | No | Yes | Yes |

**Data Loss Prevention (DLP) Filtering**

| Subject/Attachment/Body/MS Office, PDF, .txt, .html, and .rtf files | No | No | Yes |

---

### How ScanMail Works

The Trend Micro scan engine uses both rule-based and pattern recognition technologies and includes MacroTrap technology, which detects and removes macro viruses. Frequent, automatic virus pattern and scan engine updates occur through a Web-based download mechanism, which does not require a shutting down ScanMail.

ScanMail scans and cleans attachments and document content on all entry points, as illustrated in Figure 1-1:
Email attachments are scanned in real time at the IBM Domino mail server.
Database events are monitored and attachments are scanned immediately.
Databases and modified data are scanned during replication.
Existing attachments in mailboxes and Domino databases are scanned to root out old infections.

ScanMail maintains a comprehensive activity log with detailed information for the infected file.
Java-based charts help administrators identify virus infections throughout the enterprise environment. Reports from different servers can be consolidated through Notes database replication.

**ScanMail Components**

The ScanMail Setup adds the following components to a Domino server after a successful installation:

- databases
Introducing ScanMail for IBM Domino 5.8

Types of Scans

ScanMail scans messages processed by the Domino mail router task, databases, documents, directories. ScanMail processes these items based on filters and rules that are defined in policies that you specify. See Planning for a Policy-based Antivirus and Content Security Protection on page 4-2.

Note: ScanMail provides a default policy to automatically protect Domino servers as soon as the installation finishes. The default policy cannot be deleted.

ScanMail does not scan the following:

- Encrypted mail messages and their attachments
- Password-protected files
- Files that contain more than 20 layers of compression
- Partial / incomplete messages

ScanMail provides the following types of scans:

- Real-time mail scanning
- Real-time database scanning
- Manual and scheduled database scanning

Real-time Mail Scanning

Real-time mail scanning allows ScanMail to scan all email transactions—messages to and from individual Notes Clients, and messages to and from a Notes Client and users not in the Domino network (those using the Internet, for example). ScanMail protects users against receiving malware from other Notes users and from outside sources.
Real-time Database Scanning

Real-time database scanning allows ScanMail to monitor all database document modifications as the documents are opened or updated in real time. ScanMail performs real-time monitoring on all or selected databases, and scans and filters databases that are designated for replication to or from other servers.

To maximize efficiency, ScanMail checks only those documents that have been modified and immediately scans them for malware. After scanning, ScanMail closes the document and the replicator task proceeds to the next document. Trend Micro uses this method because it is faster and more precise, which is especially important when Domino performs replication with remote servers through costly or slow telephone lines.

Real-time database scanning does not interrupt the entire replication process; rather, it prevents only the infected file from being saved, and replication of subsequent documents is unaffected.

Real-time database scanning can be time-consuming and processor intensive if your Domino server includes many databases and thousands of frequently updated files. To minimize overhead, you might want to activate real-time scanning only for the databases that are most vulnerable to virus infections. For example, user databases are probably more vulnerable to virus infections than Domino program databases. Documents and attachments in user mail files are protected by real-time message scanning and do not need to be rescanned.

To protect databases that are not modified frequently, use manual or scheduled database scanning.

Manual and Scheduled Database Scanning

Manual and scheduled scanning applies only to Notes databases. Although ScanMail does not scan other types of files on the hard drive:

- all file types contained within a Notes database can be checked for viruses, which includes OLE attachments and script bombs.
- all documents within the Notes database will be checked for content security.
- all documents within the Notes database, that match the selected forms, will be checked for data loss prevention.
Introducing ScanMail for IBM Domino 5.8

Note: ScanMail invokes the real-time mail scan task and applies its settings when manually scanning mailbox databases. If the real-time mail scan task is not running when a manual scan is invoked, a message appears on the Domino console and log file.

If you select the Incremental Scan option for scheduled and manual scanning operations, ScanMail scans only documents that are new or have been modified since the last manual or scheduled scan. By limiting the scan to these documents, you can save server resources and time.

WARNING! The scheduled or manual scan may not be able to detect malware if the virus pattern file used at the time of scanning is out-of-date. By enabling incremental scan in a scheduled database rule or manual scan, infected documents will never be rescanned and the malware will not be detected. Trend Micro recommends using the latest antivirus components to run a full manual scan at least once a week (preferably during non-peak hours).

See Understanding Threats in a Domino Environment on page A-1 for more information.

Understanding Policies, Rules, and Filters

ScanMail for IBM Domino (SMID) provides the ability to create policies that define how it protects the Domino environment, updates components, sends notifications, and trusts cluster servers. ScanMail implements one policy per server. ScanMail provides a default policy that includes a real-time mail scan rule that automatically protects all Domino servers that do not have an explicit policy implemented after a successful installation. Figure 1-2 depicts the relationship of a server policy and the rules and filters that make up the policy.

- A policy is composed of rules that define how ScanMail protects the Domino environment, updates components, sends notifications, and trusts cluster servers. ScanMail applies a policy to a server, which means it has the ability to share policies across applicable platforms (for example, Domino servers hosted on a Windows server can implement the same policy).

- Rules define:
  - how ScanMail scans mail in real-time
- how ScanMail performs real-time database scans
- when ScanMail initiates a scheduled database scan
- when updates occur for the antivirus and content security components
- how notifications are delivered

You can define unlimited rules per policy. However, the more rules that you have, the longer it takes to evaluate a given message.

- Rules contain *filters*, which actually define the scanning actions for messages and attachments.

![Policy-filter-rule relationship](image-url)
ScanMail Rules

ScanMail provides the rules described in Table 1-3, which define how ScanMail scans messages and databases.

Table 1-3. Types of ScanMail rules

<table>
<thead>
<tr>
<th>TYPE OF RULE</th>
<th>DEFINES HOW SCANMAIL…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail scan rule</td>
<td>scans and filters message content and attachments in real time. To create a real-time mail scan rule, see page 4-9.</td>
</tr>
<tr>
<td>Database scan rule</td>
<td>scans databases in real time. To create a real-time database scan rule, see page 4-14.</td>
</tr>
<tr>
<td>Scheduled scan rule</td>
<td>scans databases according to a schedule. To create a scheduled database scan rule, see page 4-16.</td>
</tr>
<tr>
<td>Scheduled update rule</td>
<td>updates antivirus and content security components. To create a scheduled update rule, see page 6-5.</td>
</tr>
<tr>
<td>Notification rule</td>
<td>delivers a notification. To create a notification rule, see page 7-2.</td>
</tr>
</tbody>
</table>

ScanMail Filters

Filters are subsets of a scan rule (mail scan, database scan, or scheduled scan) and actually define scanning actions for messages, attachments, and content. Types of filtering options include:

Table 1-4. ScanMail filtering options

<table>
<thead>
<tr>
<th>FILTERING OPTION</th>
<th>PROVIDES OPTIONS TO SET SPECIFIC SCANNING ACTION ON…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk Scan</td>
<td>virus and other malware types.</td>
</tr>
<tr>
<td>APT Prevention Filter</td>
<td>attachments with document exploits.</td>
</tr>
<tr>
<td>Scan Restrictions</td>
<td>compressed, encrypted, and other attachment types. Security Risk Scan must be enabled.</td>
</tr>
<tr>
<td>Message Filter</td>
<td>various message types.</td>
</tr>
<tr>
<td>Graymail Filter</td>
<td>unwanted marketing messages, social network updates, and other messages.</td>
</tr>
</tbody>
</table>
An organization must design a protection strategy that provides optimal protection for the enterprise. The key decision factors for selecting appropriate ScanMail protection strategies are:

- What is the overall corporate IT security strategy?
- What are the available resources (processor, memory) on the Domino servers?
- Where and how can malicious code enter the Domino environment (for example, email messages, attached files to documents in Domino databases, script bombs)?

### TABLE 1-4. ScanMail filtering options

<table>
<thead>
<tr>
<th>FILTERING OPTION</th>
<th>PROVIDES OPTIONS TO SET SPECIFIC SCANNING ACTION ON…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment Filter</td>
<td>unwanted attachments.</td>
</tr>
<tr>
<td>Content Filter</td>
<td>messages with unwanted content based on administrator-defined explicit rules.</td>
</tr>
<tr>
<td>Data Loss Prevention Filter</td>
<td>messages that violate custom data loss prevention rules.</td>
</tr>
<tr>
<td>Script Filter</td>
<td>messages with stored form or rich text hot spot content.</td>
</tr>
</tbody>
</table>

### ScanMail Protection Strategy

An organization must design a protection strategy that provides optimal protection for the enterprise. The key decision factors for selecting appropriate ScanMail protection strategies are:

- What is the overall corporate IT security strategy?
- What are the available resources (processor, memory) on the Domino servers?
- Where and how can malicious code enter the Domino environment (for example, email messages, attached files to documents in Domino databases, script bombs)?

### Planning for a Policy-Based Antivirus and Content Security Protection

Trend Micro recommends establishing and maintaining a standard antivirus and content security setting using the policy-based features. Policies allow you to:

- Automate redundant creation of antivirus and update settings, and other maintenance tasks
- Easily configure all of the servers in an environment from a single server

When planning for policy-based antivirus and content security protection, consider the following activities:

- Create group policies based on the ScanMail default policy.
Introducing ScanMail for IBM Domino 5.8

In a large network with multiple servers that perform common roles, creating a common set of protection settings once rather than repeatedly to each individual server saves configuration time and maintenance considerably.

By basing a policy on the default policy (see Understanding Policies, Rules, and Filters on page 1-9), you can easily and quickly create a common set of mail and database real-time and scheduled scanning protection settings once, rather than repeatedly to each individual server.

- Create group policies to assign settings applicable to all Domino servers in a specific geographical or administrative segment. In a multi-server environment, define server groups based on similar functions or characteristics to ensure that ScanMail applies the appropriate policy to all servers in a group.

- Create policies that have a common purpose. For example:
  - A policy for all Domino email servers that requires the same protection—real-time mail scanning
  - A policy for all servers that requires real-time and scheduled database scanning

Decide which servers belong together, and define the set of protection, update, and notification methods that apply to them. For example, you can create and then apply a policy protecting a mail server to other servers that also act as mail servers.

- Create unique policies to assign settings to specific Domino servers.

A unique policy assigns a default configuration to individual users, user groups, or servers. For example, to set scheduled scanning that will run only on certain days of the week, create a policy with a scheduled scan rule and then assign it to individual or groups of database servers.

Planning to Implement Rules and Filters in a Policy-Based Environment

Trend Micro recommends the following strategies for implementing rules and filters for optimal antivirus and anti-spam protection for a Domino environment:

- Create real-time mail scan rules for all messages and attachments.
- Implement filter rules for unauthorized attachment types and extensions (see Table 4-9, “Recommended file extensions to block,” on page 4-52 for the recommended list).
- Create real-time database scan rules for all databases.
Tip: Consider excluding user mail files (create real-time mail scan rules to scan messages), Domino system databases, and other large size databases that do not change often. This helps allocate server resource to databases that are constantly changing.

• Create a scheduled update rule for antivirus and content security components.
• Create a scheduled database scan rule of all Domino databases.
• Purchase ScanMail for IBM Domino Suite with Data Loss Prevention to implement prevention against unwanted spam or suspicious URL messages.
  • Enable comprehensive data loss prevention
  • Enable anti-spam protection and specify which actions to take.
  • Enable Web Reputation protection and specify which actions to take.
  • Set filter levels in accordance with IT security policies.
  • Enable and specify approved senders and blocked senders.

In addition, determine the appropriate number of scan tasks on your system. See Types of Scans on page 1-7 for details about the ScanMail scan tasks.
Chapter 2

Installing ScanMail for IBM Domino

This chapter guides you through installing ScanMail for IBM Domino (SMID). This chapter also lists the system requirements for SMID and contains post-installation configuration information and instructions on how to register and activate your software.

This chapter contains the following topics:
• Planning SMID Deployment on page 2-2
• Upgrading Domino Server on page 2-3
• Testing SMID at One Location on page 2-4
• Recommended System Requirements on page 2-5
• Installing SMID 5.8 on page 2-9
• Upgrading SMID on page 2-38
• Starting the Domino Server on page 2-62
• Registering and Activating SMID on page 2-63
• Testing Installation with EICAR on page 2-65
• Checking SMID Files and Folders on page 2-66
Planning SMID Deployment

Deployment is the process of strategically distributing SMID servers to provide optimal antivirus and content security protection for your Domino environment. Careful planning and assessment are required to deploy applications like SMID to a homogenous or heterogeneous environment.

Trend Micro recommends that you consider the following before deploying SMID to your network:

• Select a Domino server in your organization that will serve as the central SMID server.
• Install SMID on the central server and enable replication of SMID databases.
• Create replicas of newly installed *smconf.nsf* and *smvlog.nsf* databases for other Domino servers.
• To avoid replication conflicts, permit only the Domino administrator in charge of SMID policies to modify the Configuration database on each Domino server.
• Initiate push replication from the SMID Log database replicas to the master *smvlog.nsf* to centralize logging of virus and other malware incidents across the network.
• Decide whether to enable pull replication of the master Update database to replicas on other Domino servers so that only the central Domino server needs to connect to Trend Micro ActiveUpdate to download the latest component updates, and peripheral servers can select Replicated database as the update source (see Setting the Update Source starting on page 6-9).

**WARNING!** If you have version 5.8 and its previous version installed in the same network, you must disable the Design elements replication setting in the previous version to avoid user interface conflicts.
Upgrading Domino Server

If you are planning to upgrade the Domino server and you already have SMID installed, consider the following:

1. Back up the following SMID files to save the original configuration:
   • All program files in the following folder:
     • Windows: `C:\Program Files\Trend Micro\ScanMail for Domino`
     • Linux: `/opt/trend/SMID`
   • All data files in the following folder:
     • Windows: `C:\Program Files\IBM\Domino\data\smd`
     • Linux: `/local/notesdata/smd`

2. Upgrade the Domino server.

3. After you have completed the Domino server upgrade, verify if SMID works normally. If not, do the following:
   a. Stop the Domino server.
   b. Copy the files you backed up in Step 1 to their respective folders.
   c. Open the `notes.ini` file, and add the following:
      • At the end of `ServerTasks`, add the following:
        ```ini
        ,SMDemf,SMDreal,SMDsch,SMDmon,SMDcm
        ```
      • At the bottom of the file, add the following:
        ```ini
        EXTMRG_ADDINS=SMDext
        SmStopMail=1
        ScanMailInstallPath=c:\Program Files\Trend Micro\ScanMail for Domino
        SMLD_EQ_ENABLED=0
        SMDSkipTaskList=COMPACT,FIXUP,UPDALL,UPDATE
        ```

**Note:** `c:\Program Files\Trend Micro\ScanMail for Domino` is only an example here. Replace it with the original path where you have installed the SMID binaries.
4. Start the Domino server.

Testing SMID at One Location

Trend Micro recommends a pilot deployment of SMID before implementing it full scale. A pilot deployment:

- Allows you to gain familiarity with SMID.
- Allows you to develop or refine the company's network policies.
- Can give the IT department or installation team a chance to rehearse and refine the deployment process and test whether your deployment plan meets your organization's business requirements.
- Provides an opportunity to determine how features work and the level of support likely to be needed after full deployment.
- Can help determine which configurations need improvements.

To test SMID at one location:

1. Prepare for a test deployment (see Preparing for a Test Deployment on page 2-4).
2. Select a pilot site (see Selecting a Pilot Site on page 2-5).
3. Create a rollback plan (see Creating a Rollback Plan on page 2-5).
4. Deploy and evaluate the pilot (see Deploying and Evaluating SMID on page 2-5).

Preparing for a Test Deployment

During the preparation stage, complete the following activities:

- Decide on the SMID replication model for the test environment.
  A hub and spokes model is a common SMID replication model. In this model, the network administrator configures the SMID settings from the hub SMID server. Then, the other servers, or spokes, automatically pull the settings from the hub server.
- Evaluate the possible deployment methods to determine which are suitable for your particular environment.
- Establish TCP/IP connectivity among all systems in a heterogeneous trial configuration.
• Send a ping command to each agent system from the hub server and vice versa to verify bidirectional TCP/IP communications.

Selecting a Pilot Site
Select a pilot site that best matches your production environment, including other antivirus and management software installations such as Trend Micro™ ServerProtect™, Control Manager, and the services you plan to use. Try to simulate the topology that would serve as an adequate representation of your production environment.

Creating a Rollback Plan
Trend Micro recommends creating a contingency plan in case there are issues with the installation, operation, or upgrade of SMID. Consider your network’s vulnerabilities and how you can retain a minimum level of security if issues arise. Also take into account local corporate policies and IT resources.

Deploying and Evaluating SMID
Deploy and evaluate the pilot based on expectations regarding both antivirus and content security enforcement and network performance. Create a list of successes and failures encountered throughout the pilot process. Identify potential pitfalls and plan accordingly for a successful deployment.

This SMID test deployment and trial can be rolled into the overall production installation and deployment plan.

Recommended System Requirements
Individual company networks are as unique as the companies themselves. Different networks have different requirements depending on the level of network complexity. This section describes the recommended system requirements for SMID server.
SMID for Microsoft Windows

Table 2-5 lists the hardware and software requirements for ScanMail for IBM Domino 5.8 for Windows.

<table>
<thead>
<tr>
<th>Hardware / Software</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel™ Pentium™ or higher and compatibles (64-bit chips as appropriate), or equivalent</td>
</tr>
</tbody>
</table>
| Memory              | • 512-MB minimum  
                       | • 512-MB or more recommended per CPU |
| Disk Space          | 1.5-GB minimum per partition |
| Disk swap space     | Twice the physical RAM installed |
| Protocols           | • TCP/IP (includes IPv6) |
| Domino Server       | • Lotus Domino 8.0.1 (64-bit)  
                       | • Lotus Domino 8.0.2 (64-bit)  
                       | • Lotus Domino 8.5 (64-bit)  
                       | • Lotus Domino 8.5.2 (64-bit)  
                       | • Lotus Domino 8.5.3 (64-bit)  
                       | • IBM Domino 9.0 (64-bit)  
                       | • IBM Domino 9.0.1 (64-bit)  
                       | • IBM Domino 10.0 (64-bit)  
                       | • IBM Domino 10.0.1 (64-bit) |
| IBM Notes           | • Lotus Notes 8.0.1  
                       | • Lotus Notes 8.0.2  
                       | • Lotus Notes 8.5  
                       | • Lotus Notes 8.5.2  
                       | • Lotus Notes 8.5.3  
                       | • IBM Notes 9.0  
                       | • IBM Notes 9.0.1  
                       | • IBM Notes 10.0  
                       | • IBM Notes 10.0.1 |
Table 2-5 lists the hardware and software requirements for ScanMail for IBM Domino 5.8 for Linux.

**SMID for Linux**

Table 2-6 lists the hardware and software requirements for ScanMail for IBM Domino 5.8 for Linux.

### TABLE 2-6. SMID for Linux Hardware and Software Requirements

<table>
<thead>
<tr>
<th>Hardware / Software</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>Intel™ Pentium™ 4 Processor 1.3-GHz or higher</td>
</tr>
<tr>
<td>Memory</td>
<td>• 512 MB minimum</td>
</tr>
<tr>
<td></td>
<td>• 512 MB or more recommended per CPU</td>
</tr>
<tr>
<td>Disk Space</td>
<td>• 1.5-GB minimum per partition</td>
</tr>
<tr>
<td></td>
<td>• 500-MB for program files</td>
</tr>
<tr>
<td></td>
<td>• 450-MB for the /tmp folder</td>
</tr>
<tr>
<td>Disk swap space</td>
<td>• Equal to the physical RAM installed required</td>
</tr>
<tr>
<td></td>
<td>• Twice the physical RAM installed recommended</td>
</tr>
</tbody>
</table>
### TABLE 2-6. SMID for Linux Hardware and Software Requirements

<table>
<thead>
<tr>
<th>Hardware / Software</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocols</td>
<td>TCP/IP (includes IPv6)</td>
</tr>
</tbody>
</table>
| Domino Server       | • Lotus Domino 8.5 64-bit  
                      |   • Lotus Domino 8.5.1 64-bit  
                      |   • Lotus Domino 8.5.2 64-bit  
                      |   • Lotus Domino 8.5.3 64-bit  
                      |   • IBM Domino 9.0 64-bit  
                      |   • IBM Domino 9.0.1 64-bit  
                      |   • IBM Domino 10.0 64-bit  
                      |   • IBM Domino 10.0.1 64-bit |
| IBM Notes           | • Lotus notes 8.0.1  
                      |   • Lotus notes 8.0.2  
                      |   • Lotus notes 8.5  
                      |   • Lotus notes 8.5.1  
                      |   • Lotus notes 8.5.2  
                      |   • Lotus notes 8.5.3  
                      |   • IBM notes 9.0  
                      |   • IBM notes 9.0.1  
                      |   • IBM notes 10.0  
                      |   • IBM notes 10.0.1 |
| Platform            | • Novell SUSE Linux Enterprise Server (SLES) 10  
                      |   • Novell SUSE Linux Enterprise Server (SLES) 11  
                      |   • Novell SUSE Linux Enterprise Server (SLES) 12  
                      |   • Red Hat Enterprise Linux (RHEL) 5  
                      |   • Red Hat Enterprise Linux (RHEL) 6  
                      |   • Red Hat Enterprise Linux (RHEL) 7 |
| Browser             | • Microsoft Internet Explorer 7.0  
                      |   • Microsoft Internet Explorer 8.0 |
There are several pre-installation tasks that can help to make the installation process easier. Additionally, note the following points before installing SMID version 5.8:

- You cannot automatically roll back to SMID 5.6 SP1 after installing version 5.8. To roll back to SMID 5.6 SP1, remove SMID 5.8, and then perform a fresh installation of SMID 5.6 SP1. Refer to the SMID 5.6 SP1 documentation for details on how to install this version. See *Rolling Back to SMID 5.6 SP1* on page 10-16 for more information.

- You cannot install SMLD 5.0/5.5, SMID 5.6, SMID 5.6 SP1, and SMID 5.8 on the same physical machine. (Windows only)

- You must shut down the Domino server before installing or removing SMID.

- For partitioned servers, install only one version of SMID for all partitions. However, you can install separate binaries for each partition.

### TABLE 2-6. SMID for Linux Hardware and Software Requirements

<table>
<thead>
<tr>
<th>Hardware / Software</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| Trend Micro Control Manager | • Trend Micro Control Manager 5.0 with patch 8  
• Trend Micro Control Manager 5.5 with hotfix 1273  
• Trend Micro Control Manager 6.0  
• Trend Micro Control Manager 7.0 |

| Other | • compat-libstdc++-33-3.2.3-69.el6.i686.rpm (on RHEL6 64-bit)  
• glibc-2.12-1.107.el6.i686.rpm (on RHEL6 64-bit)  
• nss-softokn-freebl-3.12.9-11.el6.i686.rpm (on RHEL6 64-bit)  
• libgcc-4.8.5-28.el7.i686.rpm (on RHEL7 64-bit)  
• compat-libstdc++-33-3.2.3-72.el7.i686.rpm (on RHEL7 64-bit)  
• glibc-2.17-222.el7.i686.rpm (on RHEL7 64-bit)  
• nss-softokn-freebl-3.34.0-2.el7.i686.rpm (on RHEL7 64-bit) |

### Installing SMID 5.8

There are several pre-installation tasks that can help to make the installation process easier. Additionally, note the following points before installing SMID version 5.8:

- You cannot automatically roll back to SMID 5.6 SP1 after installing version 5.8. To roll back to SMID 5.6 SP1, remove SMID 5.8, and then perform a fresh installation of SMID 5.6 SP1. Refer to the SMID 5.6 SP1 documentation for details on how to install this version. See *Rolling Back to SMID 5.6 SP1* on page 10-16 for more information.

- You cannot install SMLD 5.0/5.5, SMID 5.6, SMID 5.6 SP1, and SMID 5.8 on the same physical machine. (Windows only)

- You must shut down the Domino server before installing or removing SMID.

- For partitioned servers, install only one version of SMID for all partitions. However, you can install separate binaries for each partition.
Pre-installation Tasks

Before installing SMID, perform the following tasks:

1. Log on the Windows platform as administrator or log on the Linux platform as root user.
2. Determine the `notes.ini` location(s) (including its location on partitioned servers, if applicable).
3. Determine the Domino Data and Domino Binary paths.
4. Ensure that the user/group that has the administrator authority used to manage the SMID databases exists. The default group is `LocalDomainAdmins`.
5. Check the available disk space to verify there is at least 1.5-GB of free space. See Recommended System Requirements on page 2-5 for the hardware and software requirements for your platform.
7. Close any open Notes account sessions.
8. Shut down all Domino servers installed on this machine completely before:
   - Upgrading from SMID 5.6 SP1
   - Installing SMID 5.8

Setup Modes

You can use the following methods to install SMID:

- **Wizard-based installation/upgrade** is an interactive process that requires user input when installing or upgrading SMID on a server. The wizard-based installation or upgrade provides a series of interfaces that help simplify the SMID installation or upgrade process. See Running a Wizard-Based Installation on page 2-11 and Running a Wizard-Based Upgrade on page 2-39.
- **Silent installation** requires no user intervention when installing SMID.
The silent installation makes use of a response file, which contains all of the information that Setup requires. Script files can help you quickly install SMID on multiple or partitioned Domino servers. See *Running a Silent Installation* on page 2-59.

### Setup Options

There are four Setup options:

- **Fresh install** installs SMID for the first time.
- **Install** installs the same SMID version to newly added Domino server(s).
- **Upgrade** upgrades an existing SMID installation to the latest version or build.
- **Install and Upgrade** installs SMID to additional Domino server(s) and upgrades an existing SMID installation to the latest version or build.

### Running a Wizard-Based Installation

Run the corresponding Setup program to initialize the wizard-based installation.

### Installing SMID for Windows

**To install SMID from a graphical user interface:**

1. To navigate to the Setup program, do one of the following:
   - If you are installing from the Trend Micro Enterprise Protection CD, go to the **SMID** folder on the CD.
   - If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your server.
2. Double-click **setup.exe**.
The InstallAnywhere screen appears (Figure 2-1.) followed by the SMID install screen.

![InstallAnywhere screen](image)

**FIGURE 2-1.** InstallAnywhere screen

After the SMID InstallAnywhere screen completes its progress, the SMID Welcome screen appears.

![SMID Welcome screen](image)

**FIGURE 2-2.** SMID Welcome screen
3. Click **Next**. The **License Agreement** screen appears.

![License Agreement Screen](image)

**FIGURE 2-3.** SMID License Agreement screen

Select **I accept the terms of the license agreement** to continue with the SMID installation. If you do not agree with the terms of the license, click **I do NOT accept the terms of the license agreement**; the installation then stops.
4. Click Next. The **Product Activation Code** screen then displays.

   ![Product Activation Code screen](image)

   **FIGURE 2-4. Product Activation Code screen**

5. On the **Product Activation Code** screen shown in Figure 2-4, you must enter the correct **SMID Activation Code** to activate SMID (see page 2-63).

   **Note:** Obtain the Activation Code to activate an SMID Trial, Standard, Suite, or Suite with Data Loss Prevention version for a new installation. You may use the same Activation Code used for SMLD 5.0/5.5 or SMID 5.6, if it has not yet expired.

   Type or paste the **SMID Activation Code** (see page 2-63) or click **Next**, to skip product activation. Do one of the following:

   - If you have not registered SMLD:
     i. Go the Trend Micro Product Registration Web site (https://olr.trendmicro.com/registration) and follow the on-screen instructions to register your product. Register your product to ensure you are eligible to receive the latest security updates and other product and maintenance services.
After registration is complete, Trend Micro sends the **SMID Activation Code (AC)** to the email address you specified during registration.

**ii. Use the Activation Code you have received from Trend Micro to activate SMID.**

- **If you have an Activation Code:**
  
  Type the Activation Code for SMID. To use SMID 5.8, you need to obtain a Standard, Suite or Suite with Data Loss Prevention Activation code (see page 2-63) to activate the software.

- **If you want to use the Configuration database to activate SMID later:**
  
  Leave the Activation Code field blank. Setup installs SMID; however, the SMID scan or update task will not load. Activate SMID immediately after installation to protect your Domino environment (see **SMID Activation Code** starting on page 2-63).

6. Click **Next**. The **Select Domino Server** screen then appears. Select the **notes.ini** server where you want to install SMID.

---

**Note:** If you have a partitioned server, install SMID on the partitions you want to protect.

---

![FIGURE 2-5. Select Domino Server screen](image)
FIGURE 2-6. Select correct location for notes.ini

WARNING! A warning message will display if you select a location where SMID is currently installed. Be sure to select a new location.

WARNING! A warning message will display if you select "notes.ini" for 32-bit domino server. Be sure to select "notes.ini" for 64-bit domino server.

After selecting the notes.ini path, click Add > Next. The Validate Domino Server screen displays.
7. From the **Validate Domino Server** screen, verify the domino and data directories path.

![Verify the Domino program and Data directories screen](image1)

**FIGURE 2-7.** Verify the Domino program and Data directories screen

8. Click **Next**. The **Analyze Domino Server** screen displays.

![Analyze Domino Server screen](image2)

**FIGURE 2-8.** Analyze Domino Server screen
9. After the configuration analysis screen progress completes, click **Next**. The **SMID Configuration** screen displays.

![SMID Configuration screen](image)

**FIGURE 2-9. SMID Configuration screen**

10. From the **SMID Configuration** screen, type or **Browse** for the location to install ScanMail for IBM Domino. If you clear the **Share single SMLD binary for all**
**Domino servers** option, the screen shown in Figure 2-10 appears.

![ScanMail for IBM Domino installation screen](image)

**FIGURE 2-10. Choose server install path**

**Note:** Trend Micro recommends that you do not install SMID product binaries in the Domino Data folder. Otherwise, SMID may generate extra logs.

11. If you cleared **Share single SMID binary for all Domino servers**, click ... as shown in Figure 2-10 to **browse** for a new server path.
12. Click Next. The **Database Replication Selection** screen appears.

   By default, Setup enables replicating all databases except the Quarantine database. If you want to change the default settings, select or deselect the SMID databases you want Setup to replicate.

   ![ScanMail database replication settings](image)

   **FIGURE 2-11. ScanMail database replication settings**

   If you plan to install SMID on several servers and replicate databases, you may want to disable replication of the Configuration database on subsequent servers. Select one server as the primary or administrative server to replicate to all other servers.

   **Note:** Remember to schedule the replication of the Configuration database after installing SMID so that all servers receive the default policy.

13. Click Next. The **Default Policy Selection** screen appears. Select which server(s) should get the default policy. If there are server(s) with SMID installed and the Configuration database is being replicated, you may skip this option on subsequent installations.
Installing ScanMail for IBM Domino

A single SMID server, central (hub) server, or the first server from a group of partitioned servers should always receive the default policy. If the default policy is not installed on a server, reload SMDReal on that server after you create a new policy.

**Note:** All servers must have a policy present for SMDReal to operate properly. Upon completion of installation, schedule replication of the Configuration database so that all servers will receive the default or other policy that you specify.

**FIGURE 2-12. SMID default policy screen**

14. Click Next. The ScanMail Administrator screen appears. Do one of the following:
   - Type a single administrator account / group that will have Manager access to all SMID databases.
   - If the target servers are partitioned servers and you have different administrator groups for each partition, specify different users or user groups for each partitioned server and then type the administrator account for each server in the Type the Administrator account field.
FIGURE 2-13. Specify user or group access screen

**Note:** If the account you specify does not exist, then create it when you complete the installation. Ensure that the account has administrator authority.
15. Click **Install**. The installation begins.

![Figure 2-14](image_url)

**Figure 2-14. Setup installs SMID on selected server(s).**

16. After the installation shown in Figure 2-14 completes, the **Installation Complete** screen displays.

![Figure 2-15](image_url)

**Figure 2-15. SMID Installation Complete screen**
17. Click **Next**. The **Introduce Control Manager Agent** screen displays.

![Introduce Control Manager Agent Screen](image)

**FIGURE 2-16. Introduce Control Manager Agent screen**

18. Click **Done** to close the Setup screen.

See *Testing Installation with EICAR* on page 2-65 to confirm that SMID has been successfully installed.

If you are running ServerProtect or another antivirus product on the Domino server where you will install SMID, see *Registering and Activating SMID* on page 2-63.
Installing SMID for Linux

To install SMID for Linux, perform the following steps:

1. Open Terminal. To navigate to installation program, do one of the following:
   • If you are installing from the Trend Micro Enterprise Protection CD, navigate to the SMID folder on the CD.
   • If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your server.

   **Note:** The installation file uses the `/tmp` file system as temporary folder by default. However, you can change the temporary folder by setting the `IATEMPDIR` environment variable to a different directory on a partition with enough free disk space.

   To set the variable, enter one of the following commands at the UNIX command line prompt before running the installation:
   • For Bourne shell (sh), Bourne-again shell (bash), Korn shell (ksh), and Z shell (zsh):
     
     ```
     $ IATEMPDIR=/your/directory/with/free/space
     $ export IATEMPDIR
     ```
   • For C shell (csh) and TC Shell (tcsh):
     
     ```
     $ setenv IATEMPDIR /your/directory/with/free/space
     ```
2. To make sure that the `install.bin` file has the execution privileges, type the following command:
   ```
   chmod 755 install.bin
   ```

3. Run the installation file `install.bin`, by typing the command:
   ```
   ./install.bin -i console
   ```
   The installer starts unpacking the file.

   ![FIGURE 2-17. Unpacking Installer file](image-url)
After unpacking of installation file is complete, the **Welcome** screen appears as shown in Figure 2-18.

**FIGURE 2-18. Welcome screen**

Press **Enter** to continue the installation. The **License Agreement** screen appears.

**FIGURE 2-19. License Agreement screen**
4. On the **Licence Agreement** screen, press **Enter** to continue scrolling to the next screen of **Licence Agreement**. If you want to move to the end of the agreement, type *skip* or *s* and press **Enter**.

![License Agreement screen](image)

**FIGURE 2-20. License Agreement screen**

5. At the end of the **License Agreement**, Type 1 if you agree and accept the terms of the license agreement. If you do not agree with the terms of the license, type 2; the installation then stops after confirmation.

![Figure 2-21. Product Activation screen](image)

7. On the Product Activation screen shown in Figure 2-21, you must type the correct SMID Activation Code to activate SMID (see page 2-63).

**Note:** Obtain the Activation Code to activate an SMID Trial, Standard, Suite, or Suite with Data Loss Prevention version for a new installation.

Do one of the following:

- If you have not registered SMID:
  - i. Go the Trend Micro Product Registration Web site (https://olr.trendmicro.com/registration) and follow the on-screen instructions to register your product. Register your product to ensure you are eligible to receive the latest security updates and other product and maintenance services.
    - After registration is complete, Trend Micro sends the SMID Activation Code (AC) to the email address you specified during registration.
  - ii. Use the Activation Code you have received from Trend Micro to activate SMID.
If you have an Activation Code:
Type the Activation Code for SMID. To use the full functionality of SMID 5.8, you need to obtain a Standard, Suite or Suite with Data Loss Prevention Activation Code (see page 2-63) and activate the software.

If you want to use the Configuration database to activate SMID later:
Leave the Activation Code field blank. Setup installs SMID; however, the SMID scan or update task will not load. Activate SMID immediately after installation to protect your Domino environment (see page 2-63).

8. Press Enter.

9. If you chose to proceed without the Activation Code, the setup will prompt for the confirmation. Do one of the following:
   a. To continue installing SMID without the Activation Code, type `y` and press Enter.
   b. If you want to type Activation Code at this point of installation:
      i. Type `n` and press Enter. The setup will prompt for the Activation Code.
      ii. Type the SMID Activation Code. and press Enter.

The Add or Remove Domino Server screen appears.

![Add or Remove Domino Server screen](image.png)

**FIGURE 2-22. Add or Remove Domino Server screen**
10. On the **Add or Remove Domino Server** screen shown in Figure 2-22, type 1 and press **Enter** to add *notes.ini* server where you want to install SMID.

**Note:** If you have a partitioned server, install SMID on the partitions you want to protect.

Accept current setting, and go to the next step option start the installation of selected Domino server (*notes.ini*). If you have not selected at least one *notes.ini*, Accept current setting, and go to the next step option would be ineffective. You must select at least one Domino server (*notes.ini*) before starting the installation process.

a. Press **Enter. Add Domino Server - Notes.ini Path [Step 1/4]** screen appears as shown in Figure 2-23. Type the path where *notes.ini* file is located.

---

**FIGURE 2-23. Domino server selection screen**

![Replication Settings screen]

**FIGURE 2-24. Replication Settings screen**

By default, Setup enables replicating all databases except the **Quarantine Database**. If you want to change the default settings, select or deselect the SMID databases you want Setup to replicate or ignore. To select or deselect SMID database, do the following:

i. Type the corresponding option number from 1 ~ 5 (for example, if you want to select **Quarantine Database**, type 4).

ii. Press Enter.

**Tip:** If you plan to install SMID on several servers and replicate databases, you may want to disable replication of the Configuration database on subsequent servers. Select one server as the primary or administrative server to replicate to all other servers.
Note: Remember to schedule the replication of the Configuration database after installing SMID so that all servers receive the default policy.

After making your selection, type 0 (zero) to accept setting, and proceed to next step.


![ScanMail Management screen](image)

**FIGURE 2-25. ScanMail Management screen**

The default administrator group is LocalDomainAdmins. If you want to specify another user or group for the administration tasks, type a single administrator account or group that will have Manager access to all SMID databases.

Note: If the account you specify does not exist, then create it when you complete the installation. Ensure that the account has administrator authority.

FIGURE 2-26. Installation Path selection screen

Type the installation path where you want the Setup to install the SMID. By default, Setup will install the SMID at /opt/trend.

**Note:** If SMID 5.8 has already been installed on one partition servers, the default installation path for the subsequent installation(s) will remain same and cannot be changed.
c. After typing the installation path, press Enter. The selection of one Domino Server completes and the **Add or Remove Domino Server** screen appears again, displaying the list of selected Domino server(s).

![Add or Remove Domino Server screen](image)

**FIGURE 2-27. Add or Remove Domino Server screen**

On the **Add or Remove Domino Server** screen shown in Figure 2-27, select one the following:

- Type 0 (zero) to select current settings and start the installation of selected Domino server(s).
- Type 1 to add another Domino server (*notes.ini*), and follow Substep a to Substep d of Step 10 on page 2-31.
- Type 2 to remove Domino server(s) previously selected.
11. Press **Enter**. The **Summary** screen appears. Type **Y** or **y** to start installing the selected Domino server(s).

![Installation Summary screen](image1.png)

**FIGURE 2-28. Installation Summary screen**

12. Press **Enter**. The installation begins.

![Setup installs SMID on selected server(s)](image2.png)

**FIGURE 2-29. Setup installs SMID on selected server(s)**
After the installation shown in Figure 2-29 completes, the **Installation Complete** message displays on the screen.

![Installation Complete Message](image)

**FIGURE 2-30. ScanMail Installation Complete screen**

**Note:** If this is the first time you install SMID, quit the current terminal session and start a new session.
Upgrading SMID

**WARNING!** Upgrading to SMID 5.8 cannot be automatically rolled back. However, you can perform a manual roll back if you need to revert to version 5.6 SP1. Backup the important SMID files before performing the upgrade, so that you can use those files to roll back to version 5.6 SP1, if and when required. Refer to **Important SMID Files to Back Up** on page 2-38 for the list of files.

Important SMID Files to Back Up

Before you can start upgrading SMID to version 5.8, Trend Micro strongly recommends backing up the following important SMID files, so that you can roll back to version 5.6 SP1, if and when required:

- **Windows**:
  - `C:\Windows\smdsys.ini`
  - SMID data directory under IBM data path. For example: `C:\Program Files\IBM\Domino\data\smd`
  - SMID binary directory. For example: `C:\Program Files\Trend Micro\ScanMail for Domino`
  - The following SMID binaries under IBM binary path (for example: `C:\Program Files\IBM\Domino`):
    - `nSMDupd.exe`
    - `nsmdTools.exe`
    - `nSMDsupp.exe`
    - `nSMDsch.exe`
    - `nSMDreal.exe`
    - `nSMDmon.exe`
    - `nSMDext.dll`
    - `nSMDEUQ.exe`
• nSMDemf.exe
• nSMDDTAS.exe
• nSMDdbs.exe
• nSMDcm.exe

• **Linux:**
  - `/etc/smdsysV3.ini`
  - SMID data directory under IBM data path.
    For example: `/local/notesdata/smd`
  - SMID binary directory.
    For example: `/opt/trend/SMID`
  - The following SMID binaries under IBM binary path (for example: `/opt/ibm/domino/notes/latest/linux`):
    - `libsmdext.so`
    - `smdcm`
    - `smddbs`
    - `smdtisas`
    - `smdemf`
    - `smdeuq`
    - `smdmon`
    - `smdreal`
    - `smdsch`
    - `smdsupp`
    - `smdupd`

**Running a Wizard-Based Upgrade**

Run the corresponding Setup program to initialize the wizard-based upgrade.
Upgrading SMID for Windows

To upgrade SMID from a graphical user interface:

1. To navigate to the Setup program, do one of the following:
   - If you are installing from the Trend Micro Enterprise Protection CD, go to the SMID folder on the CD.
   - If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your server.

2. Double-click setup.exe.

   The InstallAnywhere screen appears (Figure 2-31) followed by the SMID install screen.

   ![InstallAnywhere screen](image)

   **Figure 2-31. InstallAnywhere screen**
After the SMID InstallAnywhere screen completes its progress, the SMID Welcome screen appears.

![SMID Welcome screen](image)

**FIGURE 2-32.** SMID Welcome screen
3. Click Next. The License Agreement screen appears.

![FIGURE 2-33. SMID License Agreement screen](image)

4. Select I accept the terms of the license agreement to continue with the SMID installation. If you do not agree with the terms of the license, click I do NOT accept the terms of the license agreement; the installation then stops.

5. Click Next. The Select Domino Server screen then appears. Select the notes.ini server where you want to install SMID.
Note: If you have a partitioned server, install SMID on the partitions you want to protect.

Also, if you are upgrading from SMID 5.6 SP1, the existing `notes.ini` server file will display. This file cannot be removed, but you can Add other locations.

**FIGURE 2-34. Select correct location for notes.ini**

6. After selecting the `notes.ini` path, click Add > Next. The Validate Domino Server screen displays.
7. From the **Validate Domino Server** screen, verify the domino and data directories path.

**FIGURE 2-35. Verify the Domino program and Data directories screen**
8. Click **Next**. The **Analyze Domino Server** screen displays.

![Analyze Domino Server screen](Image)

**FIGURE 2-36. Analyze Domino Server screen**
9. After the configuration analysis screen progress completes, click **Next**. The **SMID Configuration** screen displays.

**FIGURE 2-37.** SMID Configuration screen
10. From the **SMID Configuration** screen, type or **Browse** for the location to install ScanMail for IBM Domino.

![Figure 2-38. Choose server install path](image)

**Note:** Trend Micro recommends that you do not install SMID product binaries in the Domino Data folder. Otherwise, SMID may generate extra logs.
11. Click **Next**. The **Database Replication Selection** screen appears. By default, Setup enables replicating all databases except the Quarantine database. If you want to change the default settings, select or deselect the SMID databases you want Setup to replicate.

**FIGURE 2-39. ScanMail database replication settings**

If you plan to install SMID on several servers and replicate databases, you may want to disable replication of the Configuration database on subsequent servers. Select one server as the primary or administrative server to replicate to all other servers.

**Note:** Remember to schedule the replication of the Configuration database after installing SMID so that all servers receive the default policy.
12. Click Next. The Default Policy Selection screen appears. Select which server(s) should get the default policy. If there are server(s) with SMID installed and the Configuration database is being replicated, you may skip this option on subsequent installations.

A single SMID server, central (hub) server, or the first server from a group of partitioned servers should always receive the default policy. If the default policy is not installed on a server, reload SMDReal on that server after you create a new policy.

**Note:** All servers must have a policy present for SMDReal to operate properly. Upon completion of installation, schedule replication of the Configuration database so that all servers will receive the default or other policy that you specify.

![SMID default policy screen](image)

**FIGURE 2-40.** SMID default policy screen
13. Click **Next**. The **ScanMail Administrator** screen appears.

14. Do one of the following:
   - Type a single administrator account / group that will have Manager access to all SMID databases.
   - If the target servers are partitioned servers and you have different administrator groups for each partition, specify different **users** or **user groups** for each partitioned server and then type the administrator account for each server in the **Type the Administrator account** field.

![Specify user or group access screen](image)

**FIGURE 2-41. Specify user or group access screen**

**Note:** If the account you specify does not exist, then create it when you complete the installation. Ensure that the account has administrator authority.
15. Click **Install**. The installation begins.

**FIGURE 2-42.** Setup installs SMID on selected server(s)
16. After the installation shown in Figure 2-42 completes, the **Installation Complete** screen displays.

![SMID Installation Complete screen](image)

**FIGURE 2-43.** SMID installation Complete screen
17. Click Next. The Introduce Control Manager Agent screen displays.

![Introduce Control Manager Agent screen]

**FIGURE 2-44. Introduce Control Manager Agent screen**

18. Click Done to close the Setup screen.
Upgrading SMID for Linux

To upgrade to SMID 5.8 from SMID 5.6 SP1, perform the following steps:

1. Open Terminal. To navigate to installation program, do one of the following:
   - If you are installing from the Trend Micro Enterprise Protection CD, navigate to the SMID folder on the CD.
   - If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your server.

   Note: The installation file uses the /tmp file system as temporary folder by default. However, you can change the temporary folder by setting the IATEMPDIR environment variable to a different directory on a partition with enough free disk space.

   To set the variable, enter one of the following commands at the UNIX command line prompt before running the installation:
   - For Bourne shell (sh), Bourne-again shell (bash), Korn shell (ksh), and Z shell (zsh):
     
     $ IATEMPDIR=/your/directory/with/free/space
     
     $ export IATEMPDIR
   - For C shell (csh) and TC Shell (tcsh):
     
     $ setenv IATEMPDIR /your/directory/with/free/space

2. To make sure that the install.bin file has the execution privileges, type the following command:

   chmod 755 install.bin

3. Run the installation file install.bin, by typing the command:

   ./install.bin -i console

   The installer starts unpacking the file.
After unpacking of installation file is complete, the **Welcome** screen appears as shown in Figure 2-45.

**FIGURE 2-45. Welcome screen**

4. Press **Enter** to continue the installation. The **License Agreement** screen appears.

**FIGURE 2-46. License Agreement screen**
5. On the **Licence Agreement** screen, press **Enter** to continue scrolling to the next screen of **Licence Agreement**. If you want to move to the end of the agreement, type *skip* or *s* and press **Enter**.

![Figure 2-47: License Agreement screen](image)

6. At the end of the **License Agreement**, Type 1 if you agree and accept the terms of the license agreement. If you do not agree with the terms of the license, type 2; the installation then stops after confirmation.
7. Press Enter. The setup provides options for upgrade or perform fresh installation.

![Image of setup mode selection](image)

**FIGURE 2-48. Select your setup mode**

8. To upgrade, type 2 and press Enter. The **Product Activation** screen appears.

---

**Note:** If you want to perform a fresh installation, type 1, press Enter, and then refer to the topic *Installing SMID for Linux* on page 2-25 for the installation procedure.
9. On the **Product Activation** screen, type a new Activation Code and press **Enter** to activate SMID. See **SMID Activation Code** on page 2-63 for details about SMID Activation Code. The **Summary** screen appears.

![Summary screen](image)

**FIGURE 2-49. Summary screen**

10. Type **Y** or **y** and press **Enter** to start installing the selected Domino server. The setup starts installing SMID.

After the installation completes, the **Installation Complete** message displays on the screen.

![Installation completed](image)
Running a Silent Installation

Silent SMID installation minimizes the number of installation steps, which simplifies installation. The script file, which is in a *.txt format, provides the required information necessary to complete an SMID installation.

Before you begin this installation process, do the following:

• Ensure that the required hardware and software components are in place and working. Refer to the hardware and software requirements for your platform as mentioned in the following table:

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>TABLE TITLES AND LOCATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>Refer to Table 2-5, “SMID for Windows Hardware and Software Requirements,” on page 2-6.</td>
</tr>
<tr>
<td>Linux</td>
<td>Refer to Table 2-6, “SMID for Linux Hardware and Software Requirements,” on page 2-7.</td>
</tr>
</tbody>
</table>

• Ensure that the Domino server is stopped and all other Notes applications are closed; otherwise, you may corrupt shared files, and Setup may not run properly.

• Prepare an installation script.

Use an installation script (that is, an answer or script file) to record a previous SMID installation and automate SMID installation on all the servers where you want to install SMID. Alternatively, use an installation script to customize the type of SMID setup or to specify options to install on the Domino server.

**Note:** Silent installation supports fresh SMID installation as well as upgrade to version 5.8. However, it will only install or upgrade SMID on the servers specified in the record script. If you want to do silent installation where a previous version of SMID is installed, make sure to add all the servers’ information in the script file.
Installing SMID for Windows in Silent Mode

To install SMID in the silent mode:

1. From the command console, type information as follows to record the silent installation script file while installing SMID to a single or multiple Domino server(s):

   `setup.exe -r "{script absolute path and file name}"`

   For example:

   `setup.exe -r "c:\smd_silent.txt"`

   **Note:** Run this command from a command line prompt opened in a graphical desktop environment when recording a script file for a silent SMID installation.

2. On the command console, type the following command to invoke silent installation:
Installing ScanMail for IBM Domino

**silentinstall.bat**

3. Open the silent installation log file for the Setup result, *smdins.log*, which is created in the user's default temp folder. You can access this folder by typing: "%windir%\temp" as the explorer address. Follow the steps in *Testing Installation with EICAR* on page 2-65 to check whether the SMID installation is successful.

### Installing SMID for Linux in Silent Mode

To install ScanMail in the silent mode:

1. From the Terminal console, type the following to record the silent installation script file while installing SMID to a single or partitioned Domino server:

   *.install.bin -i console -r {path and script file name}*

   For example:

   *.install.bin -i console -r /tmp/silent.txt*

2. On the Terminal console, type the following command to invoke silent installation:

   *.install.bin -i silent -f {path and script file name}*

   For example:

   *.install.bin -i silent -f /tmp/silent.txt*

3. Open the silent installation log file for the Setup result, *smdins.log*, which is created in /var/log folder. Follow the steps in *Testing Installation with EICAR* on page 2-65 to check whether the SMID installation is successful.
Starting the Domino Server

After installing SMID version 5.8, start the Domino server to launch the SMID tasks and test the installation with EICAR (page 2-65) to confirm whether SMID is successfully installed. Additionally, refer to Getting Started with SMID on page 3-1 for additional post-installation configuration.

To start the Domino server on Windows platform:
1. Make certain you are logged on as the Administrator.
2. Click Start > Programs > IBM Applications > Domino Server.

To start the Domino server on Linux:
1. If you have installed the SMID for the first time on the server computer, open a new Terminal (shell) session.
2. Make certain you are logged in with the Domino user account and not as root. Check this by issuing the command whoami or id.
3. Change to your Domino data directory (for example, local/notesdata), and then type the following command at the Terminal to start the Domino server:
   
   $ <Domino binary directory>/server –jc &

   **Tip:** If you have not customized your shell environment, run the following command to locate and execute the Domino startup script:

   <Domino binary directory>/server

   **Note:** Replace <Domino binary directory> with your actual Domino binary directory.

Refer to your Domino documentation for more information on how to start a Domino server.
SMID and Other Antivirus Products

If you are using another antivirus product (like ServerProtect) on the Domino server where you plan to install ScanMail, be sure to configure that antivirus product to exclude from scanning ScanMail "smd" and temporary directories for each partition. Otherwise, a scanning conflict may occur. Refer to Configuring Exceptions for Directories on page 12 for details.

Registering and Activating SMID

Use your Registration Key to register your product on the Trend Micro Online Registration Web site at the following:

https://olr.trendmicro.com/registration

Register your products to ensure eligibility to receive the latest security updates and other product and maintenance services. After completing the registration, Trend Micro sends an email that includes a SMID Activation Code, which you can then use to activate SMID.

SMID Activation Code

SMID has four types of Activation Codes:

- A Trial AC allows you to implement the full functionality of SMID. During the trial period, SMID performs malware and unwanted content filtering and scanning, as well as component update. When a Trial AC expires, all SMID functions are disabled, leaving your Domino environment unprotected.
- A Standard AC allows you to implement limited SMID functionalities. SMID Standard edition provides security risk scanning in all modes and component update. However, data loss prevention, content and spam filtering are unavailable.
- A Suite AC allows you to implement SMID, including content and spam filtering, Web Reputation and End User Quarantine (EUQ).
- A Suite with Data Loss Prevention AC allows you to implement ScanMail's full functionalities, including content and spam filtering, Web Reputation, End User Quarantine (EUQ) and Data Loss Prevention.
SMID displays the remaining number of days before a Trial version, Standard edition, Suite, or Suite with Data Loss Prevention edition expires via the Domino server console. Trend Micro recommends registering and obtaining a Suite or Suite with Data Loss Prevention AC before the expiration date to allow uninterrupted Domino environment protection.

**Obtaining an SMID Activation Code**

Activate the SMID server to keep your antivirus and content security updates current. To activate your product, register online and obtain an SMID Activation Code using your Registration Key.

If you have purchased the full version from a Trend Micro reseller, the Registration Key is included in the product package. Register online and obtain an Activation Code to activate the product.

**Activating SMID**

After you have obtained an Activation Code either from your product package or purchased through a Trend Micro reseller, activate SMID to use all of its functions, including downloading updated program components.

**To activate SMID:**

1. Open the SMID Configuration Database.
2. On the left menu, click Administration > Product License.
3. Creating a License Profile (see page 5-20).
4. Delete the license profile created during installation (see page 5-20).

**Convert to a Full Version**

Upgrade and activate the full version of SMID to continue using it beyond the trial period. Activate SMID to use all of its functions, including downloading updated program components.

**To convert to a full version:**

1. Purchase a full version Registration Key (from a Trend Micro reseller).
2. Register your software online.
3. Obtain and take note of the Activation Code.
4. *Creating a License Profile* (see page 5-20).
5. Delete the corresponding license profile for the trial version (see page 5-20).

**Renew SMID Maintenance**

Standard maintenance support is included in the initial purchase of product licenses and consists of one year of virus pattern updates, product version upgrades, and telephone and online technical support. Maintenance is due 12-months from the original purchase and every year thereafter.

**To renew product maintenance for a full version:**

1. Open the SMID Configuration Database.
2. On the left menu, click *Administration > Product License*.
3. On the working area, double-click the target *platform*; for example, Windows (all versions).
4. Click *View detailed license online*.
5. Follow the instructions in the *Existing user registration*.
6. Click *Save & Close*.

**Testing Installation with EICAR**

Trend Micro recommends testing SMID and confirming that it works by using the European Institute for Computer Antivirus Research (EICAR) test file. EICAR developed the test script as a safe way to confirm that your antivirus software is properly installed and configured.

---

**WARNING!** Never use real viruses to test your antivirus installation.

Use EICAR to trigger a virus incident and confirm that email notifications are correctly configured, and that there are no issues with logging.

---

**Note:** The EICAR file is a text file with a *.com* extension. It is inert. It is not a virus, it does not replicate, and it does not contain a payload.
To test the SMID installation with EICAR:

1. Open an ASCII text file and copy the following 68-character string to it.
   X5O!P%@AP[48]PZX54(P^)7CC)7$EICAR-STANDARD-ANTIVIRUS-TEST-FILE$H+H*

2. Save the file as eicar_test.com to a temp directory and then close it.

3. Attach eicar_test.com to an email and send it to yourself or a test mailbox.

Check the virus log in the SMID Log Database or check the notification sent to the administrator (if Notification is set).

Checking SMID Files and Folders

See the following appendices for details about SMID and Control Manager files and folders:

- *ScanMail for Windows* on page C-2
- *ScanMail for Linux* on page C-3
Chapter 3

Getting Started with SMID

This chapter presents post-installation and post-activation tasks that you need to perform to configure SMID.

This chapter includes the following topics:

• Understanding the SMID Interface on page 3-2
• Getting Help While Using ScanMail on page 3-3
• Running a Manual Scan After Installation on page 3-3
• Adding ScanMail Database Icons to the Notes Workspace on page 3-3
• Signing ScanMail Databases with a Different ID on page 3-4
• Defining Access and Roles to ScanMail Databases on page 3-4
• Accessing ScanMail Databases on page 3-6
Understanding the SMID Interface

The SMID interface layout is as follows:

![ScanMail Interface Diagram](image)

**FIGURE 3-1.** ScanMail interface

The interface contains the following areas:

**TABLE 3-7.** ScanMail interface layout description

<table>
<thead>
<tr>
<th>Area</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action buttons</td>
<td>allows you to perform specific actions, such as <strong>Edit</strong> the settings or navigate <strong>Back</strong> to the previous displayed document</td>
</tr>
<tr>
<td>Header section</td>
<td>includes links to the ScanMail Help Database, Trend Micro Web site, and other support tools</td>
</tr>
<tr>
<td>Left menu</td>
<td>provides shortcuts to each ScanMail feature and other ScanMail databases</td>
</tr>
<tr>
<td>Working area</td>
<td>is the central area of the ScanMail interface, and allows you to configure and set ScanMail options</td>
</tr>
</tbody>
</table>

**Tip:** ScanMail databases are best viewed using a screen area of 1024 x 768 pixels.
Getting Help While Using ScanMail

The ScanMail Help database contains information on all the ScanMail features and provides cross-reference links to related topics. Additionally, the How To sections often provide systematic solutions to common configuration questions. Consult this list when looking for information on how to perform an operation in ScanMail.

To get help while using ScanMail, do one of the following:

• Select Contents and Index from the list on the header section of ScanMail databases
• Click the underlined label or the help icon (?) that precedes an option for a tool-tip description of the options

Note: Tool-tips are not available when accessing ScanMail databases through a Web browser.

Running a Manual Scan After Installation

Trend Micro recommends running a manual scan (see Running Manual Scan on page 4-69) of all Notes databases to find and clean any existing viruses.

After performing the initial scan of all Notes databases, schedule ScanMail (see Creating Scheduled Database Scan Rules on page 4-16) to periodically scan the Notes databases on the local or remote hard disk.

Adding ScanMail Database Icons to the Notes Workspace

The Notes Workspace provides quick access to the ScanMail databases.

To add a ScanMail database icon to the Notes workspace:

1. From a Notes workspace, click File > Open > IBM Notes Application.
2. Enter the path and file name in the Filename field.
3. Click Open.
Refer to the Notes Workspace topic in the IBM Notes Help for more information on the Notes Workspace.

**Signing ScanMail Databases with a Different ID**

Sign ScanMail databases with a different ID if you want to:

- Replace the server.id used to sign databases during installation and assign another ID.

**To sign ScanMail databases with a different ID:**

1. On the IBM Notes Client, click Files > Security > Switch ID to switch to the ID that will be used to sign ScanMail databases.
2. Start the IBM Notes Administrator, select the Domino server where ScanMail has been installed; then, click the Files tab.
3. Select All database types from the Show me list.
4. Select the ScanMail databases from the list. Typically, ScanMail databases are found in the SMD folder.
5. Select Database > Sign from the list of available Tools.
6. On the Sign Database window, select All design documents.
7. Clear Update existing signatures only (faster) if this option is selected.
8. Click OK to complete the operation.

**Defining Access and Roles to ScanMail Databases**

Use a Notes Client to define accounts that can access ScanMail databases. These accounts have unlimited access to ScanMail functions.

**Note:** If an account is not included in the ScanMail databases accesses and roles, it will not be able to access the ScanMail functions, even if the account has administrator privileges.
To define access to ScanMail databases:

1. From a Notes Workspace, select the ScanMail icon.
2. Click File > Application > Access Control…
3. On the Basics tab of the Access Control List window, change the database's default access to No Access.
   Set the following options:
   - User type: Unspecified
   - Access: No Access
   The ScanMail administrator should appear as a Person or Group in the same list as -Default-, along with the ScanMail server, LocalDomainServers, and OtherDomainServers.
4. If either the ScanMail administrator, ScanMail server, LocalDomainServer, or OtherDomainServer do not appear in People, Servers, Groups, click Add… and then .
   a. In the Names window, select an address book from the box in the upper left corner.
   b. Select a person from the list displayed in the left pane.
   c. Click Add > to add the name to the list. Repeat until you have found all the names.
   d. Click OK when finished.
5. Back in the Basics tab, highlight the ScanMail administrator's name. Assign the ScanMail administrator the following rights:
   - User type: Person or Person Group
   - Access: Editor or higher
6. Assign the ScanMail administrator Delete documents privilege, and continue assigning access rights as specified in Table 3-8.
ScanMail requires at least Editor access to perform manual and scheduled scans of the Notes databases, and Delete documents privilege to delete logs older than the specified number of days (see page 8-8). Do not select any check boxes for the Default user.

7. On the Roles group, click the [PolicyCreator], [PolicyModifier], and [PolicyReader] roles to enable access to ScanMail database components with restricted access.

8. Click OK.

For more information on assigning roles and refining Notes database access, refer to the Notes help—Restricting access to documents and local databases.

### Accessing ScanMail Databases

There are two ways to access a ScanMail database:

- Using a Notes Client
- Using a compatible Web browser
Accessing ScanMail Databases Using a Notes Client

The Notes Client provides quick, easy access to ScanMail features.

To access a ScanMail database using a Notes Client:

1. Open a Notes Client.
2. Click File > Open > IBM Notes Application.
3. In the Server text box, specify the Domino server where you installed ScanMail.
4. In the Database list, locate the ScanMail Configuration Database (*smconf.nsf*).
5. Click Open.

![FIGURE 3-2. The Configuration Database displays Server Summary as the default first page](image)

IBM Notes creates a database icon for ScanMail in the Notes Workspace.
Accessing ScanMail Databases Using a Web Browser

The ScanMail Configuration, Quarantine, Log, Update, and Help databases are accessible through a Web browser for those who are using Domino server and running the Notes / Domino HTTP task, provided that the Domino Server document has been configured to allow database access with a Web browser.

Domino provides password security for ScanMail. System administrators can configure the password (see Set the Internet Password for ScanMail Database Access through a Web Browser on page 3-9) for each person under the HTTP password in the Address Book. The Access Control List, as set from the Notes Workspace, can further control access.

To access a ScanMail database using a Web browser:

1. Open a Web browser.
2. In the Address text box (or similar), type the following Web address:

   http://{Domino server}/smd/smconf.nsf

   where {Domino server} represents the Domino server's host name or IP address.

   ![FIGURE 3-3. Access ScanMail databases using a Web browser](image-url)
Limitations when Accessing ScanMail Databases Using a Web Browser

There are limitations when using a Web browser to access ScanMail:

• You must save a policy, rule or filter that you have created before you can configure it.

• When accessing the ScanMail Configuration database, the following options are unavailable:
  • ScanMail Databases
  • Domino Administrator

• Some elements to view and operate Data Loss Prevention Filtering, and Local Smart Scan Sources are not fully supported. Additionally, some elements to view and operate Content Filtering for Database scan is not fully supported.

• When accessing the ScanMail Log Database, the following options are unavailable:
  • Statistics > Database scan history
  • Log Maintenance > Deletion Settings > Manual deletion

Set the Internet Password for ScanMail Database Access through a Web Browser

Set an Internet password to securely access ScanMail from a Web browser. ScanMail uses Domino’s own password schema for restricting database access.

To set the Internet password for accessing a ScanMail database:

1. Open the Address Book and select the Person you will grant access.
2. Type a password in the Internet password field.
3. Click Save and Close.

For additional information regarding Internet passwords, consult the IBM Notes / Domino documentation.
Accessing other ScanMail Databases through the Configuration Database

Use the Configuration Database to access other ScanMail databases.

**To access other ScanMail databases through the Configuration database:**

1. Open the ScanMail Configuration database.
2. Click the corresponding link to access:
   - Log database
   - Quarantine database
   - Update database
   - Filter list database
Chapter 4

Configuring Scan Tasks

This chapter explains how to set up policies for different individuals and groups in your organization to enforce real-time and scheduled malware and unwanted content protection. In addition, it provides manual scanning instructions.

This chapter contains the following topics:

- Planning for a Policy-based Antivirus and Content Security Protection on page 4-2
- Managing Policies on page 4-3
- Creating Rules on page 4-9
- Organizing Rules on page 4-19
- Introducing ScanMail Filters on page 4-20
- Configuring the Scan and Filter Settings on page 4-25
- Running Manual Scan on page 4-69
Planning for a Policy-based Antivirus and Content Security Protection

Trend Micro recommends that you use the policy-based features in SMID to establish and maintain a standard antivirus, data loss prevention, and content security setting. Policies allow you to:

- Automate redundant creation of antivirus and update settings, and other maintenance tasks
- Easily configure all of the servers in an environment from a single server

When planning for policy-based antivirus and content security protection, consider the following activities:

- Create group policies based on the ScanMail default policy.
  In a large network with multiple servers that perform common roles, you can save considerable configuration time and maintenance when you base a policy on the default policy (see Understanding Policies, Rules, and Filters on page 1-9). You can easily and quickly create a common set of mail real-time and scheduled scanning protection settings once rather than repeatedly for each individual server.

- Create group policies to assign settings applicable to all Domino servers in a specific geographical or administrative segment.
  In a multi-server environment, defining server groups based on similar functions or characteristics ensures that ScanMail applies the appropriate policy to all servers in a group.

Create policies that have a common purpose. For example:

- A policy for all Domino email servers that require the same protection—real-time mail scanning
- A policy for all servers that require real-time and scheduled database scanning

Decide which servers belong together, and define the set of protection, update, and notification methods that apply to them. For example, you can create and then apply a policy that protects a mail server to other servers that act as mail servers.

- Create unique policies to assign settings to specific Domino servers.
  A unique policy assigns a default configuration to individual users, user groups, or servers. For example, to set scheduled scanning that will run only on certain days of the week, create a policy with a scheduled scan rule and then assign it to individual or groups of database servers.
How Policy-based Protection Works

Policy-based protection works when you do the following:

1. Create policies for ScanMail scan tasks, notifications, updates, and general options. See Understanding Policies, Rules, and Filters on page 1-9.

2. Create server settings for each server in your environment. See Configuring the Server Settings Menu Options on page 5-3.

3. Set synchronization schedule and enable policies to replicate to other servers in your environment.

After all the policy documents and server profiles have been created, you will need to include the ScanMail Configuration Database (smconf.nsf) in your replication schedule for the servers in your environment. View the status of all servers in the Summary view. See Viewing the Summary of All Servers.

Note: To replicate successfully between servers, add the target server to the database’s ACL list and grant manager access. See Creating and Applying a New Access Control (ACL) Entry on page 5-19.

Managing Policies

This section describes how to use the ScanMail Configuration database to manage policies.

Creating Policies

Use the ScanMail Configuration database to create policies.

To create policies:

1. Open the ScanMail Configuration Database (See Accessing ScanMail Databases on page 3-6).

2. From the left menu, click Configuration > Policies.
3. From the working area, click **Create New Policy**.
4. Type the **Policy Name**.

5. Select from **This policy applies to server/server groups** the server or server groups that should apply the policy.
Configuring Scan Tasks

4-5

Note: The server group type should be set to multi-purpose when using Domino version R8.

6. Click Copy Settings to copy the scan, update, or notification rule from the list of available policies.

Note: Copy Settings creates a policy that is the same as the source policy, with exceptions such as the Policy Name and the servers or server groups that apply.

7. Create a real-time mail scan rule (See Creating Real-time Mail Scan Rules on page 4-9).
8. Create a real-time database scan rule (See Creating Real-time Database Scan Rules on page 4-14).
9. Create a scheduled database scan rule (See Creating Scheduled Database Scan Rules on page 4-16).
10. Define how ScanMail delivers notifications (See Defining How ScanMail Delivers Notifications on page 7-7).
11. Define cluster trusting (See Managing the Trusted Cluster Servers for a Policy on page 4-7).
12. Click Save & Close.

ScanMail adds the new policy in the Policies view.

Modifying Policies

Use the ScanMail Configuration database to modify policies.

To modify policies:

1. Open the ScanMail Configuration Database (see page 3-6).
2. On the left menu, click Configuration > Policies.
3. On the working area, double-click a policy.
4. Modify the Mail Scan (page 4-9), Database Scan (page 4-14), Scheduled Scan (page 4-16), Scheduled Update (page 6-5), Notifications (page 7-8), or Cluster Trusting (page 4-7) tab settings.
5. Click Save & Close.

Deleting Policies

Use the Policies view to delete a policy.

To delete a policy:

1. Open ScanMail Configuration Database (See Accessing ScanMail Databases on page 3-6).
3. Select the policy that you want to delete.
4. On the working area, click Delete Policy.

Note: The ScanMail default policy cannot be deleted.

Prioritize Policies

Use Prioritize Policies view to select the order of precedence for all policies (see Figure 4-1).

To prioritize policies:

1. Open ScanMail Configuration Database (See Accessing ScanMail Databases on page 3-6).
2. From the left menu, click Configuration > Policies. The Policies view appears.
3. From the working area, click Prioritize Policies. The Policy Organizer appears.
4. Select the policy for which you want to change priority; then, click Increase Priority or Decrease Priority as appropriate.
5. Repeat as needed until all priorities are set.
6. Click Close.
Managing the Trusted Cluster Servers for a Policy

Use the Cluster Trusting tab to view the cluster server(s) to which the selected policy applies and select the trusted servers in a cluster group.

Note: The Default policy can never belong to a specific cluster group. Therefore, it cannot be used in the Cluster Trusting tab.

To manage trusted cluster server(s) for a policy:

1. Create or modify a policy (See Creating Rules on page 4-9) or (See Modifying Policies on page 4-5) for more information.
2. Click the Cluster Trusting tab.
3. Do one of the following:
   - When the Cluster Trusting table is empty, click Update to resolve the cluster server grouping and refresh the view.
   - When the Cluster Trusting table lists the applicable servers, select a server to include in the trusted cluster group.
Note: The Cluster Trusting table has two columns: In This Policy and Not In This Policy. The servers listed in the In This Policy column are the ones that apply the selected policy. Consider Figure 4-4.

In Figure 4-4, the cluster named ASD_DOM1 has three servers: CN=ASD_S1, CN=ASD_S2, and CN=ASD_S3. The policy named test is applied only to CN=ASD_S1. In the Cluster Trusting table, the servers CN=ASD_S1 and CN=ASD_S3 are selected. Therefore, CN=ASD_S1 will trust CN=ASD_S3 and CN=ASD_S2 will not be trusted.

4. Click Save & Close.
Creating Rules

Create mail and database rules to define how ScanMail filters and scans messages and databases in real time. Alternatively, create scheduled database scan rules to schedule periodic scanning of Notes databases.

**Note:** Always ensure that smdreal has started and that its status is Idle before you create rules.

**Tip:** If a rule has too many conditions, it can become unpredictably complex. Trend Micro recommends creating multiple simple rules rather than one or two complex rules per policy.

Creating Real-time Mail Scan Rules

Real-time mail scan rules define how ScanMail scans and filters incoming and outgoing messages.

**To create a mail scan rule:**

1. Create or modify a policy (See *Creating Rules* on page 4-9) or (See *Modifying Policies* on page 4-5) for more information.
2. From the working area, click the **Mail Scan** tab.
3. Select **Apply the strictest rule to all recipients with conflicting rules** to implement the strictest mail scan rule when multiple rules are triggered during mail scanning. See **Apply the Strictest Rule** on page 4-12 for details.

4. If you have the Suite or Suite with Data Loss Prevention edition, select **Enable Trend Micro Anti-spam** and click **Configure** to specify anti-spam settings (See **Configure Anti-Spam Filtering** on page 4-26).

5. If you have the Suite or Suite with Data Loss Prevention edition, select **Enable Web reputation** and click **Configure** to enable specify Web reputation settings.

6. Click **Create New Rule**.

7. On the New Mail Rule screen, select **Stop processing succeeding rules if the mail matches this rule (enable Exit Flag)** to instruct ScanMail to stop processing other rules and finalize the action on the message when it matches one of the rules.

---

**Tip:** To improve performance when ScanMail scans messages, enable **Stop processing succeeding rules if the mail matches a rule in a mail scan rule**.

8. On the **General** tab, specify the **rule name**.
9. Set general settings (See *Configure General Mail Scan Rule Settings* on page 4-13).

10. Click the **Scan Options** tab to set how ScanMail scans and filters messages:
   - Security Risk Scan (See *Configuring Security Risk Scan* on page 4-41)
   - APT Prevention Filter (See *Configuring APT Prevention Filter* on page 4-45)
   - Scan Restrictions (See *Configuring Scan Restrictions* on page 4-47)
   - Message Filter (See *Configuring the Message Filter* on page 4-48)
   - Graymail Filter (See *Configuring the Graymail Filter* on page 4-50)
   - Attachment Filter (See *Configuring the Attachment Filter* on page 4-52)
   - Content Filter (See *Create a New Content Filter* on page 4-56)
   - Data Loss Prevention Filter (See *Configuring Data Loss Prevention Filter Options* on page 4-64)
   - Script Filter (See *Configuring Script Filter* on page 4-66)

**Tip:** When creating a rule, Trend Micro recommends that you save a copy of blocked messages to the Quarantine Database rather than deleting them. Once you have verified that the new rule is free of unintended consequences, modify and change the scan action.

11. Set the scan notification (See *Setting the Scan Notifications* on page 7-9).

12. Configure **Redirect Options** (See *Configuring Redirect Options* on page 4-67).

13. Insert disclaimers (See *Inserting Disclaimers* on page 4-68).

14. Set the rule schedule (See *Setting the Rule Schedule* on page 4-68).

15. Click **Save & Close**.
Apply the Strictest Rule

The option **Apply the strictest rule to all recipients with conflicting rules** instructs ScanMail to apply the strictest mail scan rule to all recipients with conflicting rules.

Consider the following example:

- **Mail scan rule A** has the following settings:

<table>
<thead>
<tr>
<th>General:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include specified recipients = All of Accounting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scan Options &gt; Attachment Filter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable attachment filtering by size = 10MB</td>
</tr>
<tr>
<td>Action = Block mail</td>
</tr>
</tbody>
</table>

- **Mail scan rule B** has the following settings:

<table>
<thead>
<tr>
<th>General:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include specified recipients = <a href="mailto:user@domain.com">user@domain.com</a></td>
</tr>
<tr>
<td><a href="mailto:user@domain.com">user@domain.com</a> is a member of the All of Accounting group.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Scan Options &gt; Attachment Filter:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable attachment filtering by size = 5MB</td>
</tr>
<tr>
<td>Action = Block mail</td>
</tr>
</tbody>
</table>

When an incoming message with a 7-MB attachment addressed to **All of Accounting** and **user@domain.com** arrives:

- All users in the **All of Accounting** group will not receive the message if **Apply the strictest rule...** is enabled.
- All users, excluding user@domain.com, will receive both the message and the attachment if **Apply the strictest rule...** is disabled.

Disabling this option allows ScanMail to apply the strictest mail scan rule to a specific user in a group.

**Tip:** Defining accurate and complete address groups ensures that ScanMail applies the appropriate policies to individuals in those groups.
Configure General Mail Scan Rule Settings

Use the **Mail Scan General** tab to set the included and excluded senders and recipient for a mail scan rule.

**To configure the general mail scan rule settings:**

1. Click the **General** tab.
2. Under **Rule Identifier**, type a name for the rule.

---

**Tip:** Trend Micro recommends using a name that appropriately describes the rule (for example, *finance_confidential*).

3. Specify the senders or recipients that will be the target of this rule. Choose from the following:
   - Under the **Senders** section, choose the target senders:
     i. Select which senders to **include**:
        - Click **All senders** to apply the rule to all senders belonging to the servers specified.
        - Click **Specified senders** to apply the rule to specific senders.
        Do one of the following:
        - Type or click to select the Notes user or group from the list (for example, user@domain.com).
        - Type parts of the user or group and use the wildcard characters * or ? (for example, *@domain).
     ii. Specify the senders to **exclude**.
   - Under the **Recipients** section, choose the target recipients:
     i. Select which recipient to **include**:
        - Click **All recipients** to apply the rule to all recipients belonging to the servers specified
        - Click **Specified recipients** to apply the rule to specific recipients
        Do one of the following:
        - Type or click to select the Notes user or group from the list (for example, user@domain.com)
Trend Micro™ ScanMail™ for IBM Domino™ Administrator’s Guide

- Type parts of the user or group and use the wildcard character * or ? (for example, *@domain)

  ii. Specify the recipients to exclude.

**Note:** If you specified both sender(s) and recipient(s), select the operator (see page 4-20) that ScanMail will use when processing this rule.

4. From the **Action when Sender and Recipients Match** section, select the action when the sender and/or recipient match: **Block** or **Deliver**.
   
   For the **Deliver** option, choose whether to **Set to low priority** or **Hold mails to be delivered at a time range**.

**Note:** By default, Domino R8 servers route low priority messages between 12 AM and 6 AM.

5. From the **Notification** section, select **Notify sender** to send notification to the message sender.
   
   a. Type a name in the **Subject** field.
   
   b. Type a new message or click **Add >>** to add tags to the message field.

6. Click **Save & Close**.

   Settings such as a rule name, priority, sender and recipient inclusion/exclusion, schedule, and Exit Flag settings, and the **Scan Options** enabled are available in the **Mail Scan** tab view.

**Creating Real-time Database Scan Rules**

Real-time database scan rules define how ScanMail scans Notes databases.

**To create a database scan rule:**

1. Create or modify a policy (See **Creating Rules** on page 4-9) or (See **Modifying Policies** on page 4-5) for more information.

2. On the working area, click the **Database Scan** tab.
3. Select **Enable database scan** to enable database scan functionality.

4. Click **Create New Rule**. The **New Database Scan Rule** screen appears.

5. From the **Rule Identifier** section, type a name for the new rule in the **Name** field.

**Note:** The **Priority** for the rule is assigned automatically. See *Changing a Rule’s Priority* on page 4-19 for information about how to modify the priority settings.

6. Click the **Databases to scan** tab to set which database(s) to scan:
   - **All databases**—ScanMail scans all databases stored on the Domino server.
   - **Scan selected databases only**—ScanMail scans specific database(s) based on the directory and database list.
   - **Exclude selected databases from scanning**—ScanMail skips scanning of specified database(s).

   Use the **Add**, **Remove**, and **Remove All** buttons to manipulate the database(s) in the list.

7. Click the **Scan Options** tab and set how ScanMail scans databases according to the following:
8. Set the scan Notification (See Setting the Scan Notifications on page 7-9).
9. Set the rule schedule (See Setting the Rule Schedule on page 4-68).
10. Click Save & Close.

Tip: To configure ScanMail to perform a real-time scan whenever a database file is opened, instead of only when it is modified, set SMDEnableOpenEvent=1 in notes.ini.

Creating Scheduled Database Scan Rules

Scheduled scan rules define how ScanMail scans Notes databases at a specific time.

To create a scheduled scan rule:

1. Create or modify a policy (See Creating Rules on page 4-9) or (See Modifying Policies on page 4-5) for more information.
2. On the working area, click the Scheduled Scan tab.

3. Click Create New Rule.
4. On the New Scheduled Scan Rule document, specify the general settings in the General tab:
   a. Specify the rule name.
   b. Select the scan condition:
      - Enable incremental scan— instructs ScanMail to scan only updated and new documents since the last scan
        Incremental scanning can save considerable server time and resources. ScanMail scans only files that have been modified since the last complete scan.
      - Scan all documents if the pattern file has been updated— instructs ScanMail to scan all documents when ScanMail updates to a new pattern file
      - Scan all documents if the scan engine has been updated— instructs ScanMail to scan all documents when ScanMail updates to a new scan engine
        Type an integer that corresponds to the minimum number of days before ScanMail should perform scanning. For example, if the minimum number of days is 4, ScanMail will run a scheduled scan on the fourth day after the last scan.
        The minimum number of days setting applies to both pattern file and scan engine update condition.

Note: The conditions Scan all documents if the pattern file / scan engine has been updated follow the incremental scan setting.

   c. Under the Apply To group, select All server(s) of the parent policy or select Specified server, and click  to choose server(s) from the list.

Note: The Apply To option is ONLY available in Scheduled Scan.

5. Click the Databases to scan tab to set which database(s) to scan:
   - All databases— ScanMail scans all databases on the Domino server
• **Specified databases**—ScanMail performs or excludes from scanning specific mail file(s) or database(s)
  
  Use the Add, Remove, and Remove All buttons to manipulate the database(s) in the list.

6. Click the **Scan Options** tab to set the following scan options:
   - Security Risk Scan (See Configuring Security Risk Scan on page 4-41)
   - APT Prevention Filter (See Configuring APT Prevention Filter on page 4-45)
   - Scan Restrictions (See Configuring Scan Restrictions on page 4-47)
   - Attachment Filter (See Configuring the Attachment Filter on page 4-52)
   - Content Filter (See Create a New Content Filter on page 4-56)
   - Data Loss Prevention Filter (See Configuring Data Loss Prevention Filter Options on page 4-64)
   - Script Filter (See Configuring Script Filter on page 4-66)

7. Set the scan notification (See Setting the Scan Notifications on page 7-9).

8. Set the schedule.
   a. Type the time in the **Run at time** field that corresponds to the time when the schedule scan rule will be run. For example, 06:00 AM.

   **Note:** If the **Run at time** field is left blank, the scheduled scan rule will be invalid.

   b. Type how long the scan will run in the **Duration of scan** field. 0 (zero) will instruct ScanMail to stop only when scanning is finished completely.

   c. Type or click ⬤ to select the **days of the week** when the rule will be run.

9. Click **Save & Close**.

   **Note:** Whenever creating a new rule, Trend Micro recommends saving a copy of blocked email messages to the Quarantine Database rather than deleting them. Once you have verified that the new rule is free of unintended consequences, modify and change the scan action.
Organizing Rules

Use the Rule Organizer to organize mail scan, database scan, or scheduled scan rules.

![Table of rules]

**Figure 4-8.** Click ▲ or ▼ to modify a rule's priority.

Use the Activate Rule or Deactivate Rule button to enable or disable a rule.

Trend Micro recommends the following guidelines when organizing rules:

- Give your broadest rules, and those with the greatest likelihood of matching, the highest priority.

  ScanMail checks each message (and/or attachment) against the entire list of active rules, from priority 1 to priority X. If **Stop processing succeeding rules if the mail matches this rule** is enabled, further rule comparisons stop and the action specified (typically quarantine) is enacted once a match occurs.

  For example, if a rule with a 50% probability of matching occurs at the end of a list of 12 active rules, each of the 11 rules before it would be checked before the match occurs on rule 12. By moving such a rule to priority 1, the match would be found immediately; the processing of the 11 rules would be saved.

- Create and apply many narrowly focused rules rather than a few very broad rules.

  Create one rule for each condition you want to check, or each blocking action you want to take, rather than 2 or 3 rules with every option filled out.

Changing a Rule’s Priority

Use the Rule Organizer document to modify the order by which ScanMail applies mail, database, scheduled scan, and scheduled update rules. The Rule Organizer also provides a shortcut to enable or disable a rule.
To change a rule’s priority:

1. Under the Mail Scan, Database Scan, Scheduled Scan, or Scheduled Update tab, click the Organize Rules button.
2. Change a rule’s priority:
   • Click ![Up Arrow](image) to promote a rule
   • Click ![Down Arrow](image) to demote a rule
3. Click Close.

Rule Operators

The OR operator is always implied as the connector between senders and recipients list within a rule.

The AND operator is implied within a given list. In other words, all items on the same line, delimited with a comma, are connected. For example, the entry:

1@domain.com, 2@domain.com, 3@domain.com

means 1@domain.com AND 2@domain.com AND 3@domain.com.

Introducing ScanMail Filters

Filters are subsets of a scan rule, which actually define the scanning and filtering behavior of ScanMail through the Scan Options.

Filter Execution Order

The Scan Options tabs allow you to create filters that make up the database and mail scan rules.
Use the following table to define how ScanMail scans or filters messages, attachments, and content (in the following order):

<table>
<thead>
<tr>
<th>ORDER</th>
<th>FILTER</th>
<th>PROVIDES OPTIONS TO SET SPECIFIC SCANNING ACTION ON…</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Message Filter</td>
<td>Various message types</td>
</tr>
<tr>
<td>2</td>
<td>Attachment Filter</td>
<td>Unwanted attachments</td>
</tr>
<tr>
<td>3a</td>
<td>Scan Restrictions</td>
<td>Compressed, encrypted, and other attachment types</td>
</tr>
<tr>
<td>3b</td>
<td>Security Risk Scan</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>APT Prevention Filter</td>
<td>Suspicious attachments</td>
</tr>
<tr>
<td>5</td>
<td>Content Filter</td>
<td>Messages with unwanted content based on administra-</td>
</tr>
<tr>
<td></td>
<td></td>
<td>tor-defined explicit rules</td>
</tr>
<tr>
<td>6</td>
<td>Data Loss Prevention Filter</td>
<td>Messages that violate custom data loss prevention rules (see Table 1-4 on page 1-11)</td>
</tr>
<tr>
<td>7</td>
<td>Script Filter</td>
<td>Messages with stored form or rich text hot spot con-</td>
</tr>
<tr>
<td>8</td>
<td>Graymail Filter</td>
<td>Unwanted marketing messages, social network updates,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>and other messages</td>
</tr>
</tbody>
</table>

**Note:** When spam filtering is set, a mail scan rule executes the following filter order:

1. Spam filtering (Configure Anti-Spam Filtering on page 4-26) of incoming messages based on Approved Senders and Blocked Senders (when enabled) or the Trend Micro Anti-Spam engine.

2. Web Reputation (Configure Web Reputation on page 4-36).

3. General settings (Configure General Mail Scan Rule Settings on page 4-13).

4. Scan Options filter enabled.
Spam Filtering (Suite Edition or Suite Edition with Data Loss Prevention only)

The Trend Micro Anti-Spam engine (TMASE) provides spam filtering of incoming messages. Incoming messages refer to those messages sent by SMTP protocol. Spam filtering allows ScanMail to block unwanted messages based on the following components:

<table>
<thead>
<tr>
<th>ORDER</th>
<th>COMPONENT</th>
<th>SOURCE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Approved Senders</td>
<td>User-defined</td>
<td>A list of people and/or organizations from whom messages will be accepted. Other messages take the Action on unwanted messages.</td>
</tr>
<tr>
<td>2</td>
<td>Blocked Senders</td>
<td>User-defined</td>
<td>A list of people and/or organizations from whom messages will be blocked. Other messages will be accepted.</td>
</tr>
<tr>
<td>3</td>
<td>Rule files</td>
<td>Trend Micro</td>
<td>Consist of heuristic and URL signature files. The Trend Micro Anti-Spam engine uses these files to filter for spam messages when there are no approved and blocked senders defined.</td>
</tr>
</tbody>
</table>

**Note:** If there are no approved senders or blocked senders set, TMASE will use the Trend Micro rule files.

TMASE provides three filter levels. The following table shows an example of when and how TMASE tags messages as spam:

<table>
<thead>
<tr>
<th>FILTER LEVEL/SENSITIVITY</th>
<th>THRESHOLD LEVEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>High (Rigorous filtering)</td>
<td>4.0</td>
</tr>
<tr>
<td>Medium (Default filtering)</td>
<td>5.0</td>
</tr>
<tr>
<td>Low (Lenient filtering)</td>
<td>8.0</td>
</tr>
</tbody>
</table>
where:

- **Filter level** defines the TMASE sensitivity when filtering for spam
- **Threshold level** defines the maximum allowable spam score

If the total spam score is equal or greater than the threshold level, then TMASE tags a message as spam. Otherwise, if the total spam score is less than the threshold level, ScanMail proceeds to the next filter execution order (see page 4-20).

**Note:** SMLD 5.0 and above has a dynamic threshold level, which changes according to different spam rules.

For example:

![FIGURE 4-10. Sample spam scores](image)

In this example, the filter level is set to Medium. The highlighted items refer to the spam scores. The first spam score, 15.20, is greater than the threshold level (that is, 5). This instructs TMASE to tag the message as spam. On the other hand, the second spam score, 3.726, is less than the threshold level. This prevents TMASE from tagging the message as spam.

To configure the filter level or Approved and Blocked Senders lists, see page 4-26.
Content Filtering (Suite Edition, or Suite Edition with Data Loss Prevention only)

Content filters define how ScanMail filters message contents based on explicit rules defined by administrators.

Content security can take many forms, including checking for leaked corporate secrets, offensive or inappropriate language, or even questionable contact with competitor corporations or hostile countries.

The Content Filter tab allows you to define general and advanced rules.

Create general content filter rules to:

• Quickly create a rule (without first creating an Expression).
• Filter messages based on the text appearing in the Subject.
• Filter messages based on the text appearing in the Body (all or some keywords).
• Filter messages based on file attachment name.

Create advanced content filter rules to:

• Create complex filters, including one or more Expressions.
• Create filters using multiple Expressions, linked via the OR operator.
• Scan the message body only.
• Scan attachment content only.
• Focus your search on a particular message header field: Subject, To, CC, From.
• Set up a match threshold for the occurrence of a particular attachment (for example, do not block a message unless X matches of the specified attachment has occurred. This is useful, for example, for mass mailing threats that tend to propagate widely and may include attachments of a common name).
• Include additional values for .OCCUR.
• Include additional values for .NEAR.

Expressions

Expressions are words or phrases ScanMail uses to filter message content based on headers and actual content.

When creating or modifying content filter expressions, refer to the help section at the bottom of the New Expression workspace for details on how to use logical operators.
Leave a space before and after each operand in the expression. Do not insert line breaks or carriage returns within a single expression. Create two expressions, instead.

For example, to create an expression to distinguish between “apple” fruit and “apple” computer, you may want to construct a rule such as the following:


This rule triggers a match if:
- The word Apple occurs two or more times in a document, and within 25 words in either direction of the word computer
- The word Macintosh occurs in a document

However, if the word eat also occurs in the document—a match is not triggered.

Trend Micro recommends keeping expressions simple and narrowly defined. Instead of one complex rule as shown above, create two simpler expressions and attach each to a mail scan rule.

Expression 1: $. ( .OCCUR. apple .). .AND. (. apple .NEAR. computer .).$
Expression 2: (. apple .NEAR. macintosh .). .AND. (. .NOT. (. .OCCUR. eat .). ).

When you configure multiple expressions to a mail scan rule, the OR operator is used between them. To create expressions, see page 4-59.

**Configuring the Scan and Filter Settings**

Use the **Scan Options** tabs to configure scan restrictions and filter settings.

---

**Note:** The Anti-spam Filter, Web Reputation Filter, Data Loss Prevention Filter, Content Filter, and End User Quarantine (EUQ) features are available only in the SMID Suite. See **SMID Activation Code** on page 2-63 for details. In addition, the ScanMail spam filtering only applies to mail scan rules.

*Data Loss Prevention* is only available for Suite with Data Loss Prevention.
Configure Anti-Spam Filtering

Use the **Anti-spam Configuration** screen to configure how the Trend Micro Anti-Spam engine filters unsolicited or unwanted messages (see page 4-22). The Anti-Spam Configuration screen provides options that define the heuristic detection level or the Approved Senders and Blocked Senders lists, which ScanMail uses to filter for unwanted messages.

**To configure Anti-spam filtering:**

1. On the **Mail Scan** tab, select **Enable Trend Micro Anti-spam**, and then click **Configure**. The Trend Micro Anti-spam Configuration Window appears.

![Trend Micro Anti-spam Configuration screen](image)

**FIGURE 4-11. Trend Micro Anti-spam Configuration screen**
2. On the Trend Micro Anti-spam Configuration window, select the anti-spam mail filter level:
   • **High**—the most rigorous level of spam detection
     ScanMail monitors all messages for suspicious files or text, but there is a greater chance of false positives. False positives are email messages that ScanMail filters as spam when they are actually legitimate messages.
   • **Medium**—the default setting
     ScanMail monitors at a high level of spam detection with a moderate chance of filtering false positives.
   • **Low**—the 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.

3. In **Action on Spam**, select the action to take for unwanted messages: **Pass**, **Quarantine**, or **Block**.

4. Select **Insert the stamp as a subject prefix**, and then type the **stamp** if you want to add eye-catching notices or keywords in the subject header.

5. Enable **Approved Senders** and **Blocked Senders**, and then specify the senders for these lists to help minimize false positives.
   • Select the **Approved Senders** check box to configure email addresses/domains that you trust.
     Type the **email addresses/domains** that you want ScanMail to exempt from blocking and then click **Add** or click an address/domains from the list or click an address/domains from the list and click **Remove**

   **WARNING!** Experience caution in configuring Approved Senders list. ScanMail will NOT send messages received from the email addresses/domains configured in the Approved Senders list to Trend Micro Anti-spam engine. Therefore, no action will be taken on such messages by Anti-spam engine to reduce false positives.

   • Select the **Blocked Senders** check box to configure email addresses/domains that you always want to tag as spam.
     Type the **email addresses/domains** that you want ScanMail to block and then click **Add** or click an address/domain from the list and click **Remove**.
WARNING! Experience caution in configuring Blocked Senders list. ScanMail will ALWAYS consider messages received from the email addresses/domains configured in the Blocked Senders list as spam, and takes configured action against these messages WITHOUT sending these messages to Trend Micro Anti-spam engine. This is done to catch spam from known sources.

**Note:** Enabling the Approved Senders and Blocked Senders lists and customizing the senders that belong to each list helps reduce false-positives. See Spam Filtering (Suite Edition or Suite Edition with Data Loss Prevention only) on page 4-22 for details on how ScanMail applies the Trend Micro rules and user-defined lists.

**Note:** The approved sender, blocked sender, and approved URL lists are stored in the same database (smlists.nsf). Each of the lists can be managed in the database. See Managing the Filter Lists on page 5-17 for details on how to manage the lists.

6. Save the spam filter settings by clicking:
   - OK on the upper-right corner of the Anti-spam Configuration screen, and then clicking Save & Close (IBM Notes console interface)
   - or -
   - Save (Web interface)
Anti-spam filtering with EUQ enabled:

1. From the Mail Scan tab, select Enable Trend Micro Anti-spam and click Configure. The Trend Micro Anti-spam Configuration screen appears.

   ![Anti-spam Configuration Screen](image)

   **FIGURE 4-12. Anti-spam Configuration Screen**

2. Under the Action section, choose Quarantine as the action on unwanted messages.

3. Click OK.
4. Select **Allow spam mails but move them to the receiver’s Junk folder**.

**End User Quarantine**

The end-user quarantine (EUQ) feature supports both the anti-spam and graymail filtering. EUQ enables you to choose whether to quarantine spam and graymail and move them to end users’ Junk folder.

![Enable End-User Quarantine](image.png)

**WARNING!** If EUQ is enabled and the mail template replication is also enabled on the Domino server, the mail template will be replicated automatically between all the servers. That is, the mail template will also be replicated on the servers where SMID is not installed or using an older version of SMID.
To enable end user quarantine:

1. From the Mail Scan tab, select Enable End User Quarantine.
2. Click Configure. Select the All recipients or Selected users/groups option.

3. Click Save & Close.

To deploy EUQ to a user’s mailbox:

1. On the Domino server console, deploy EUQ to the target mail template:
   - To deploy EUQ to the default mail template, run `load smdeuq -install`.

---

**FIGURE 4-14. Configuring End User Quarantine**

**FIGURE 4-15. Deploying EUQ to the default mail template**
• To deploy EUQ to a specified mail template, run load smdeuq -install ${mail template file path}.

```
load smdeuq -install mail85.ntf
```

**FIGURE 4-16. Deploying EUQ to a specified mail template**

**Note:** You must configure the specified mail template under the Domino Data folder.

2. Run load design on the Domino server console. Or, you can accept the defaults, and the change will take effect at 01:00 a.m.

```
load design
```

**FIGURE 4-17. Load Design screen**

**Note:** After EUQ is deployed, check the user's mailbox. The Junk folder should contain two menu items: Manage Junk Mail Senders List and Manage Approved Mail Sender List. All users will have the two menu items in their mailboxes regardless of whether you select All recipients or Selected users/groups.
Note: If the mail template does not contain a Junk folder, spam mails will be moved to the user's Inbox folder.

**FIGURE 4-18. Manage Mail Screen**

To add a sender to the approved mail sender list:

1. From the junk folder, right-click a mail message, and select **Add sender to approved mail sender list**.

**FIGURE 4-19. Add Sender to Approved List**

2. Choose from the following:
   - **Add mail address only**
• Add mail address domain

**FIGURE 4-20. Add Mail Address or Mail Address Domain**

*Note:* To remove the mail address from the approved mail address list, click *Manage Approved Mail Sender List* on the menu bar.

To manage graymail categories:
1. From the junk folder, click *Manage Your Graymail* on the menu bar.

**FIGURE 4-21. Managing graymail**

2. Select one or multiple graymail categories from the following:
   • Marketing graymail
   • Social network graymail
• Other graymail

![Image of graymail categories]

**FIGURE 4-22. Selecting graymail categories**

3. Click **OK**.

**Note:** To change your selections, click **Manage Your Graymail** again on the menu bar.

To disable end user quarantine:

1. On the Domino server console, disable EUQ for the target mail template:
   - To disable EUQ for the default mail template, run `load smdeuq -uninstall`.

   ![Image of load smdeuq command]

   **FIGURE 4-23. Disabling EUQ for the default mail template**

   - To disable EUQ for a specified mail template, run `load smdeuq -uninstall ${mail template file path}`.

   ![Image of load smdeuq command for specified mail template]

   **FIGURE 4-24. Disabling EUQ for a specified mail template**

2. Run `load design` on the Domino server console. Or, you can accept the defaults, and the change will take effect at 01:00 a.m.

3. On the **Mail Scan** tab, clear the **Enable End User Quarantine** check box.
Configure Web Reputation

Use the **Web Reputation Configuration** screen to configure how the Trend Micro URL filtering engine protects against dangerous URLs in email according to their Web reputation rating.

Local and Global Smart Protection

This version of SMID provides two options for determining the reputation and safety of URLs; these options are: the Global Smart Protection Network, and the Local Smart Protection Server. The Global Smart Protection Network sends requests to the Trend Micro Smart Protection Network to examine the reputation of URLs. The Local Smart Protection Server sends these requests to your local smart protection server. The Local Smart Protection Server will provide more privacy and improve the processing speed. Protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for those who use it. The smart scan solution uses the Smart Protection Network for in-the-cloud protection.
To configure Web reputation:

1. On the **Mail Scan** tab, select **Enable Web reputation**, and then click **Configure**. The Trend Micro Web Reputation window appears.

![Trend Micro Web Reputation Configuration screen](image)

**FIGURE 4-25. Trend Micro Web Reputation Configuration screen**

2. From the **Trend Micro Web Reputation Configuration** window, select the Scan Services method you would like to use on the **General** tab:
   - Trend Micro Smart Protection Network
   - Local Smart Protection Server
Note: If you select Local Smart Protection Server, you can also select Do not allow Smart Protection Server to make external queries to Smart Protection Network.

This feature only works if you are using Smart Protection Server 2.1 or older.

Note: You must also configure Smart Protection Server to stop sending external queries to Smart Protection Network. Refer to the Smart Protection Server documentation for the procedure.

3. On the **Trend Micro Web Reputation Configuration** window, select a Security Level on the **General** tab:
   - **High**– Blocks a greater number of Web threats, but increases the risk of false positives.
     ScanMail monitors all messages for suspicious URLs, but there is a greater chance of false positives. False positives are email messages that ScanMail filters as containing dangerous URLs when they are actually legitimate.
   - **Medium**– Blocks most Web threats while keeping the false positive count low.
     ScanMail monitors at a high level of detection with a moderate chance of filtering false positives.
   - **Low**– Blocks fewer Web threats, but reduces the risk of false positives.
     ScanMail will only filter the most obvious and common Web threats and there is a very low chance that it will filter false positives.

4. Select the type of messages that will be scanned:
   - **Both SMTP and IBM Notes mails**
   - **SMTP mails only**

5. Select the message part(s) that will be scanned:
   - **Mail Body**
   - **Mail Attachment**

6. In the **Action** section, select the **Action on unwanted messages**: **Pass**, **Quarantine**, or **Block**.
7. Select **Stamp subject prefix**, and then type a **stamp** label to add eye-catching notices or keywords in the subject header.

**Note:** If you believe a URL is misclassified, use the following link to notify Trend Micro:

http://global.sitesafety.trendmicro.com

8. In the **Notification** section, select the notification options to apply when an URL is identified by the Web Reputation filter.

9. On the **Approved URL List** tab, select **Enable approved URL list**, and then Add, Import, Export, or Remove URLs to the list to help minimize false positives by doing the following:
   - Type a URL in the Add field and click **Add**.
   - Click **Import** to import a list of URLs from a text file (*.txt), and click **Add**.
   - Click **Export** to export a list of URLs to a text file (*.txt).
   - To remove a single URL, select the URL and click **Remove**.
   - To remove All URLs, click **Remove All**.

10. On the **Notification Template** tab, configure the notification template.

11. After you complete all settings, click **OK** to save and exit.

**Note:** The approved URL list can be managed in the *smlists.nsf* database. See *Managing the Filter Lists* on page 5-17 for details on how to manage the list in the database.
Optimizing Web Reputation

You can optimize the performance of Web Reputation scanning by configuring your settings accordingly. Consider implementing the following to optimize your version of Web Reputation:

• Add your company’s internal URL to the **Approved URL List**. This allows 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 **Server Settings > Local Smart Scan Source**.

• 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.

Troubleshooting Web Reputation Performance Issues

If Web Reputation is performing slowly, 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 that provides Web Reputation services. Enable the alert **Send notification when Web reputation service becomes: Unavailable/Available** so that you will 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 may have stability issues.
Configuring Security Risk Scan

Use the **Security Risk Scan** tab to define how ScanMail scans documents for viruses and other malware.

![FIGURE 4-26. Scan Options > Security Risk Scan screen](image)

---

4-41
To configure security risk scan options:

1. Under Scan Options click the Security Risk Scan tab.
2. Under Scan Mode Settings section of the Security Risk Scan tab, click Enable Advance Threat Scan Engine.

**Note:** Advanced Threat Scan Engine checks files for less conventional threats, including document exploits. However, it may detect some files that are actually safe. Therefore, further observation and analysis is required in a virtual environment, which is provided by Deep Discovery Advisor. Refer to the topic Configuring Deep Discovery Advisor Settings on page 5-15 for the configuration procedure.

The Advanced Threat Scan Engine is not supported on Windows 32-bit version.

3. Under the Files to Scan section, configure the security risk scan options as follows:
   a. Select which files to scan from the following options:
      • **All** (recommended) scans all documents except file types, names, or specified extensions.
         To define exclusions by true file type, type the file name or extension in the **Exclude files by true file type** field or click to select from the available list. You can also specify exclusions according to file name or extension, type the file name or extension in the **Exclude files by file name** or **extension** field or click to select from the available list.
      • **Selected files** scans documents based on file names or extension names.
         A default list of file extension names is presented. To define new file names or extensions to scan, type the file name or extension in the **Scan files by file name** or **extension field** or click to select from the list.

4. Under the Advanced Options section, configure the settings according to the following:
   • **Compressed files** scans compressed files.
      ScanMail contains a default list of compressed file types to scan. You can select the number of layers of compression to scan via the Scan Restrictions tab. When you select **Clean compressed files**, ScanMail extracts compressed files for scanning, which can consume a large amount of disk space.
Note: Refer to the Trend Micro Knowledge Base for the list of compressed file types that the ScanMail can support.

- **Embedded objects** scans OLE.
  ScanMail can scan embedded objects in IBM Notes mails.

- **Macros in Microsoft Office files** uses heuristic scanning to detect macro viruses/malware in Microsoft Office files (for example, *.*.doc and *.*.xls).
  Heuristic scanning is an evaluative method of using pattern recognition and rules-based technologies to detect malicious macros.
  After you select **Macros in Microsoft Office files**, choose from the following:
  - **All** takes actions against all macros detected.

  Note: This setting will apply to all Microsoft Office files containing macros, even if they are not malicious.

- **Equal to and below heuristic level** takes action against macros detected with the specified or a lower heuristic level.
  When you select **Equal to and below heuristic level**, you also need to choose a heuristic level.

  Note: Before choosing a heuristic level, read the following information:
  - Level 1 uses the most specific criteria, but detects the least macros.
  - Level 4 detects the most macros, but uses the least specific criteria, and may falsely identify safe macros as harboring malicious macros.
  - Trend Micro recommends level 2. This level provides a high detection level and a fast scanning speed. It uses only the necessary rules to detect macro virus/malware strings and has a low level of false identification.

5. In the **IntelliTrap** section, you can enable or disable scanning by IntelliTrap.
Note: 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 email attachments with real-time compressed executable files and pairing them with other malware characteristics.

6. Under the **Action** section, set the scan action on infected files according to the following:

   • **Use ActiveAction (intelligent actions based on the virus pattern file)** identifies malware types and uses the Trend Micro pattern file to automatically recommend scan or filter actions based on how each type infects a computer system or environment. **Quarantine** is the default action for items that are uncleanable.

   When you select **ActiveAction**, you will also need to choose an action to perform on uncleanable Microsoft Office files. Microsoft Office files can contain macros that cannot be stripped, which means that these files will be scanned as uncleanable. The action that you select for **Action on uncleanable virus** will be applied to Microsoft Office files only; the actions defined in the pattern file will be applied to all other file types.

   • **Specified actions** allows you to select the action ScanMail takes according to the malware type.

   **Note:** If the **Clean compressed files** action is disabled, ScanMail applies the action for a detected malware to the entire compressed file that contains the malware. If the **Clean compressed files** action is enabled, ScanMail applies the action only to the specific file harboring the malware.

   If there is no threat and specific action enabled under **Action on other malware**, ScanMail applies the **Action on cleanable virus** or **Action on uncleanable virus** for all detected threats. To customize the **Action on other malware**, enable the threat and then select the corresponding action.

   **Note:** If **Mass-mailing virus** is enabled and the **Delete** action is selected, ScanMail will automatically delete a detected mass-mailing virus.

7. Under the **Notification** section, select the notification options for when malware is detected, uncleanable, or a scan action was applied on infected file(s).
8. Under the Email Stamp section, select and enter the appropriate options.
9. Click Save & Close.

Configuring APT Prevention Filter

Use the APT Prevention Filter tab to configure the ScanMail actions for suspicious files for advanced persistent targeted attacks and latest or unknown security threats.

**Note:** You MUST configure and start the Deep Discovery Advisor before configuring APT Prevention Filter. See Configuring Deep Discovery Advisor Settings on page 5-15 and See Starting Deep Discovery Advisor Agent on page 4-47 for the procedures.

To configure APT Prevention Filter options:

1. Under Scan Options click the APT Prevention Filter tab.
2. Select Send messages to Deep Discovery Advisor for analysis.

**Note:** The Deep Discovery Advisor uses simulators to identify potentially harmful behaviors shown by suspicious files. It can identify files used in advanced persistent targeted attacks and latest or unknown security threats.

3. In the Scan Settings section of the APT Prevention Filter tab, configure the APT prevention filter options as follows:
   • Select which messages to scan from the following options:
     • Incoming messages only (recommended)
     • Incoming and outgoing messages
   • Select which attachments to scan from the following options:
     • Highly recommendable file types
       • Suspicious files detected by Advanced Threat Scan engine (ATSE)
Note: To use APT Prevention Filter option, you must enable Advanced Threat Scan Engine in Security Risk Scan tab. See Configuring Security Risk Scan on page 4-41 for the procedure.

The APT Prevention Filter is not supported on Windows 32-bit version.

- Microsoft Office files with macros
- Scripts (such as JavaScript and others)
- Microsoft Windows executable files (.exe)
- Files with specified types—ScanMail can open, organize, and scan the contents of more than 200 file formats—including Notes database formats, the wide variety of file types that may be attached therein. Selecting Files with specified types allows you to:
  - Click Edit to modify the file type groups in ScanMail File Types database.
  - Specify which file types to scan: Archives, Executables and applications, Pictures, Audio/Video, Flash files, Documents, Others.
  - Type new file types or click ✋ to select types for True file type(s).

Note: Be aware that modifying the file type groups in APT Prevention Filter will also update the file type groups information in Attachment Filter.

4. In the Security Level section, select the security level for SMID to apply actions from the following options:
   - High: Apply action on all messages exhibiting any suspicious behavior
   - Medium: Apply action on messages with a moderate to high probability of being malicious
   - Low: Apply action only on messages with a high probability of being malicious

5. In Action section, select the filtering action: Pass, Quarantine, Block, or Delete attachment.
6. In the Notification section, select the notification options for when a suspicious file is identified by the APT prevention filter.

7. In the Email Stamp section, define the email stamp settings for notification emails.

8. Click Save & Close.

**Starting Deep Discovery Advisor Agent**

**To start Deep Discovery Advisor Agent manually**

- Type and run the following command on the Domino console:

  ```
  load smddtas
  ```

**To start Deep Discovery Advisor Agent automatically with Domino server**

1. Using a text editor, open the `notes.ini` of the Domino server where SMID is installed, and then add the following item in the ServerTasks:

  ```
  SMDdtas
  ```

2. Save and close `notes.ini`.

**Configuring Scan Restrictions**

Use the Scan Restrictions tab to configure the ScanMail actions for compressed files and files with special or unknown behavior.

**To configure scan restrictions:**

1. Under Scan Options, click the Scan Restrictions tab.

2. Select the scan action for compressed file, special, or unknown file behavior:

   - **Exceed maximum extracted file size**—restricts ScanMail to scan compressed files that matches the Maximum extracted file size setting
     
     Specify the Maximum extracted file size in kilobytes (KB).

   - **Exceed maximum compression level**—restricts ScanMail to scan compressed files that match the Maximum compression level setting.
     
     Select the limit of compression layers to scan by choosing the Maximum compression layer. For example, if you want ScanMail to scan only files that have been compressed and then recompressed (compression layer is equals 2), set the Maximum compression layer to 3.
Note: ScanMail can scan up to 20-layers of compression.

- **Password-protected files**—restricts ScanMail to scan files that are password-protected.
- **Unknown reason(s) why attachments could not be scanned**—allows ScanMail to perform a scan action for unscannable files automatically.

3. In the **Notification** section, select the notification options for when a file matches the attachment filters.
4. In the **Email Stamp** section, define the safe email stamp settings.
5. Click **Save & Close**.

### Configuring the Message Filter

Use the **Message Filter** tab to define how ScanMail treats messages.

**To configure message filter options:**

1. Under **Scan Options**, click the **Message Filter** tab.
2. Select the **Enable message filter** check box.
3. In the **Action** section, define the scan actions for encrypted messages that meet any of the following conditions:
   - **Exceed message size limit**—allows ScanMail to bypass scanning and automatically perform the specified action for messages matching the specified limit.
     Set the size limit in bytes (B), kilobytes (KB), or megabytes (MB).
   - **Encrypted message within domain**—allows ScanMail to bypass scanning and automatically perform the specified action for encrypted messages whose sender and recipients are within the same domain.
   - **Encrypted incoming message**—allows ScanMail to bypass scanning and automatically perform the specified action for encrypted incoming messages.
   - **Encrypted outgoing message**—allows ScanMail to bypass scanning and automatically perform the specified action for encrypted outgoing messages.
   - **Partial message**—allows ScanMail to bypass scanning and automatically perform the specified action for incomplete messages.
• **Message with character sets**— allows ScanMail to bypass scanning and automatically perform the specified action for messages with the specific character sets.

4. In the **Notification** section, select the notification options for when a file matches the notification filters.

5. In the **Email Stamp** section, define the safe email stamp settings.

6. Click **Save & Close**.
Configuring the Graymail Filter

Configure all the inbound gateway IP addresses of the organization in ScanMail. The graymail filter must have this information to correctly analyze the incoming email messages.

Configure the following in ScanMail:
• Inbound gateway IP addresses list
• Graymail filter scan options
• End User Quarantine (EUQ) settings if EUQ is enabled

Configuring Inbound Gateway IP Address List

Configure inbound gateway IP address for ScanMail for IBM Domino to obtain sender’s IP address. Refer to Configuring Inbound Gateway IP Addresses on page 5-7 for the detailed procedure.

Configuring Graymail Filter Scan Options

Configure graymail filter scan options to define the graymail filter behaviors for each graymail category.

To configure graymail filter scan options:
1. From the left menu, click Configuration > Policies.
2. Double-click a policy for the target server and choose Edit.
3. Click the Mail Scan tab.
4. Double-click the rule to be edited from the rule list.
5. Click Scan Options.
6. Click **Graymail Filter**.

   ![Graymail Filter Configuration](image)

   **FIGURE 4-27. Configuring graymail filter actions**

7. Select the **Enable graymail detection** check box.

8. In the **Action** section, select the action to take for each graymail category: **Pass**, **Quarantine**, or **Block**.

9. Select the **Insert the stamp as a subject prefix** check box.
   The defined prefix content will be added to the beginning of each detected email message’s subject.

10. Click **Save & Close**.

   **Note:** Make sure that all inbound gateway IP addresses have been added to the gateway IP address list. For detailed procedure, see **Configuring Inbound Gateway IP Addresses** on page 5-7.

**Graymail filtering with EUQ enabled:**

**Note:** If EUQ is enabled, graymail messages will be quarantined to end users’ junk folder, which allows end users to check the quarantined graymail. For details on how to enable EUQ, see **End User Quarantine** on page 4-30.

1. From the **Mail Scan** tab, double-click the rule to be edited from the rule list.
2. Click **Scan Option**.
3. Click **Graymail Filter**.
4. In the **Action** section, select **Quarantine** as the action for each graymail category.
5. Click **Save & Close**.

**Note:** It is recommended that you select the **Insert the stamp as a subject prefix** check box. Both spam and graymail messages will be quarantined to end users’ junk folder. With stamped prefixes, you can easily differentiate the quarantined messages.

### Configuring the Attachment Filter

Use the **Attachment Filter** tab to define how ScanMail filters message attachments.

Trend Micro recommends blocking the following attachments on the ScanMail server:

**TABLE 4-9. Recommended file extensions to block**

<table>
<thead>
<tr>
<th>EXTENSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>.386</td>
<td>Windows Enhanced Mode Driver or Swap File</td>
</tr>
<tr>
<td>.ACM</td>
<td>Audio Compression Manager Driver (Windows) and Windows System File</td>
</tr>
<tr>
<td>.ASP</td>
<td>Active Server Page</td>
</tr>
<tr>
<td>.AVB</td>
<td>Inoculan Anti-Virus virus infected file</td>
</tr>
<tr>
<td>.BAT</td>
<td>Batch Processing</td>
</tr>
<tr>
<td>.BIN</td>
<td>Binary File</td>
</tr>
<tr>
<td>.CLA</td>
<td>Java Class File (usually *.CLASS but can be shortened)</td>
</tr>
<tr>
<td>.CLASS</td>
<td>Java Class File</td>
</tr>
<tr>
<td>.CMD</td>
<td>OS/2, Windows NT Command File, DOS CP/M Command File, dBase II Program File</td>
</tr>
<tr>
<td>.CNV</td>
<td>MS Word Data Conversion File</td>
</tr>
<tr>
<td>.COM</td>
<td>Executable File</td>
</tr>
<tr>
<td>.CS*</td>
<td>Corel Script</td>
</tr>
<tr>
<td>.DLL</td>
<td>Dynamic Link Library</td>
</tr>
<tr>
<td>.DRV</td>
<td>Device Driver</td>
</tr>
<tr>
<td>.EXE</td>
<td>Executable File</td>
</tr>
</tbody>
</table>
## TABLE 4-9.  Recommended file extensions to block

<table>
<thead>
<tr>
<th>EXTENSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>.GMS</td>
<td>Corel Global Macro Storage</td>
</tr>
<tr>
<td>.HLP</td>
<td>Windows Help File</td>
</tr>
<tr>
<td>.HTA</td>
<td>Hypertext Application (runs applications from HTML files)</td>
</tr>
<tr>
<td>.HTM .HTML</td>
<td>Hypertext Markup Language</td>
</tr>
<tr>
<td>.HTT</td>
<td>Hypertext Template</td>
</tr>
<tr>
<td>.INF</td>
<td>Information or Setup File</td>
</tr>
<tr>
<td>.INI</td>
<td>Initialization/Configuration file</td>
</tr>
<tr>
<td>.JS* .JS .JSE</td>
<td>JavaScript Source Code</td>
</tr>
<tr>
<td>.LNK</td>
<td>Linker File, Windows Shortcut File</td>
</tr>
<tr>
<td>.MHT*</td>
<td>Microsoft MHTML Document (Archived Web Page)</td>
</tr>
<tr>
<td>.MPD</td>
<td>Mini Port Driver</td>
</tr>
<tr>
<td>.OCX</td>
<td>Object Linking and Embedding (OLE) Control Extension</td>
</tr>
<tr>
<td>.OV*</td>
<td>Program Overlay File (.OVL)</td>
</tr>
<tr>
<td>.PIF</td>
<td>Windows Program Information File</td>
</tr>
<tr>
<td>.SCR</td>
<td>Screen Saver Script</td>
</tr>
<tr>
<td>.SHS</td>
<td>Shell Scrap Object File</td>
</tr>
<tr>
<td>.SYS</td>
<td>System Device Driver</td>
</tr>
<tr>
<td>.TLB</td>
<td>Remote Automation Truelib Files</td>
</tr>
<tr>
<td>.TSP</td>
<td>Windows Telephony Service Provider</td>
</tr>
<tr>
<td>.VBS</td>
<td>Visual Basic Script</td>
</tr>
<tr>
<td>.VBE</td>
<td>Visual Basic Script Encrypted</td>
</tr>
<tr>
<td>.VXD</td>
<td>Virtual Device Driver</td>
</tr>
<tr>
<td>.WBT</td>
<td>WinBatch Script</td>
</tr>
<tr>
<td>.WIZ</td>
<td>Wizard File</td>
</tr>
</tbody>
</table>
To configure attachment filter options:

1. Click Scan Options > Attachment Filter tab.
2. Select Enable attachment filter.
3. In the Filter Attachment by File Size section, select Enable attachment filtering by size to filter attachments according to file size.

   **Note:** You can specify the file size per attachment or the total file size of all attachments in a message. Set the size limit in bytes (B), kilobytes (KB), or megabytes (MB). Select Single attachment file size or Sum of all attachments (collective total file size of all attachments).

4. Select the filtering Action for Filter Attachment by File Size by choosing one of the following: Pass, Quarantine, Delete attachment, Block mail, Redirect mail for approval, or Send at a time range.

   **Note:** When selecting Send at a time range, choose the Days of week and Time to send.

5. In the Filter Attachment by File Type section, select the Enable attachment filtering by file type check box.

   ScanMail can open, organize, and scan the contents of more than 200 file formats—including Notes database formats, the wide variety of file types that may be attached therein.

   a. Specify which file type to scan: All file types, Specified, or All except specified.

       Selecting Specified or All except specified allows you to:

       • Edit the ScanMail File Types database.

       • Type new entries or click to select types according to true file type, true file type groups, or extension name.

**TABLE 4-9. Recommended file extensions to block**

<table>
<thead>
<tr>
<th>EXTENSION</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>.WSH</td>
<td>Windows Script Host Settings File</td>
</tr>
</tbody>
</table>

4-54
Configuring Scan Tasks

Note: Be aware that Domino sometimes stores the attachment's file name within the body text of messages. A body text search will find the specified word within a file name.

b. Select the filtering action: Pass, Quarantine, Delete attachment, Block mail, or Redirect mail for approval.

c. Select Enable attachment filtering within compressed files to instruct ScanMail to filter compressed files. By default, this option is disabled to optimize server performance.

6. In the Exception section Allowed attachments field, type the attachment file name that will be excluded from filtering. You may use the wildcard characters (*) or (?) to specify multiple file names or extension names. Separate multiple entries with semicolons (;).

The file names or extension names specified in the Allowed attachments field overrides the attachment filtering criteria.

7. In the Notification section, select the notification options for when a file matches the attachment filters.

8. In the Email Stamp section, define the safe email stamp settings.

9. Click Save & Close.

Configuring Content Filter

Content filters define how ScanMail filters message contents based on explicit rules defined by administrators.

Content security can take many forms, including checking for leaked corporate secrets, offensive or inappropriate language, or even questionable contact with competitor corporations or hostile countries.

Note: Scanning support for Microsoft Office and Adobe Portable Document Format

The Content Filter tab allows you to define general and advanced rules (see page 4-24 for details).
To configure content filter options:

1. Under Scan Options, click the Content Filter tab.
2. Select the Enable mail scan rule check box.
   • Select the Stop processing succeeding rules if the mail matches this rule (enable Exit Flag) check box to stop processing other rules after a match.
3. Select the Enable content filter check box.
4. In the Content Filter section, select Create New Content Filter (page 4-56) or Add Existing Content Filter (page 4-58).
5. In the Action section, select the Action on mails with unwanted content to specify the scan action.
6. In Notification section, select the appropriate notification and filtering options for messages.
   Insert a filter description in the notification to include additional instructions or descriptions.
   For example: Contact the Domino Administrator for more details.
7. Click Save & Close.

Create a New Content Filter

Use the Content Filter tab to create a new content filter.

To create a new content filter:

1. From the Content Filter tab, click Create New Content Filter.
2. In the Filter Name field, type a name for the content filter.
3. From the Select the message part(s) that will be compared against the available expressions section, select the part of the message, (Subject, From, To, CC, Mail body, Attachment content, and Attachment file name) that ScanMail will
compare against the expressions (see Expressions starting on page 4-24 for details).

4. Select All selected message part(s) have to match to instruct ScanMail to return a match only when all selected parts match the content filter expression.

5. From the Select the expression(s) used to filter message content section, create or add expressions that ScanMail will use for content filtering. See Create New Expressions on page 4-59 or Add New Expressions Based on Existing Expressions on page 4-60 for more information.
   - Type an integer in the Content filter matches if the number of expressions in the message exceeds threshold field to instruct ScanMail to perform the action on unwanted content if the number of expressions in a message exceeds the specified value.
   - Specify a new integer in the Additional value for .OCCUR. field to instruct ScanMail to perform the action on unwanted content when the total number of expressions in a message is equal to the specified value.
• Specify a new integer in the Additional value for .NEAR. field to instruct ScanMail to perform the action on unwanted content when the number of words between expressions in a message exceeds to the specified value.

Note: ScanMail applies the logical operator AND if .OCCUR. and .NEAR. is used in an expression.

6. Click Save & Close.

Remove Content Filter(s)
Use Remove Content Filter to remove all or a specific content filter.

To remove content filter(s):
1. Click the filter to be removed.
2. Click Remove Content Filter.
3. To remove all content filters, click Remove All.

ScanMail removes the content filter and instructs the real-time mail scan task of the changes.

Add New Content Filters Based on Existing Filters
You can create content filters that define what portions of the message to scan, and use them as elements for other content filters. For example, create a content filter for scanning the Subject header, another for Attachments, and another to include all parts of the mail; then, use these filters as building blocks for your content filter.

To add a new content filter:
1. From the content filter workspace, click Add Expression.
2. From the Add Expressions window, click the expressions you want to add. You can select multiple expressions.
3. Click OK.

Note: Too many expressions in a content filter can cause it to become unpredictably complex. Trend Micro recommends including one or two expressions per content filter.
Create New Expressions

Create a new expression for each word, phrase, or concept you want to filter. Alternatively, you can include multiple search criteria into a single compound expression.

**Tip:** Having too many conditions in a content filter often causes it to become unpredictably complex. Trend Micro recommends creating one or two expressions per content filter.

**To create new expressions:**
1. From the content filter rule workspace, click **Create New Expression**. The **New Expression** screen appears.
2. Type the expression (that is, word or phrase) you want to filter, connected by logical operators in the **Definition** section **Expression** field. Refer to the help section at the bottom of the **New Expression** screen for details on how to use logical operators.
   
   **Note:** This version of SMID enables you to use Regular Expressions in your content filtering. For example, if you want to filter a specific Social Security Number or Bank Card, you can use .REG. and type:

   For SSN
   
   `.REG.(0[0-1-9]|01-9|0-9|1[1-6]|0[0-9]|7[0-3]|0-3|7[56]|0-9|77[0-2])[ ]?d(4)`

   For Visa, MC, Discover, Switch/Solo, and JCB
   
   `.REG.(6011|5[1-5]|d(2)|4\d(3)|67\d(2))([ ]?d(4))`  
   `.REG.(6011|5[1-5]|d(2)|4\d(3)|67\d(2))([ ]?d(4))`  
   `.REG.(6011|5[1-5]|d(2)|4\d(3)|67\d(2))([ ]?d(4))`  
   `.REG.(6011|5[1-5]|d(2)|4\d(3)|67\d(2))([ ]?d(4))`  
   `.REG.(6011|5[1-5]|d(2)|4\d(3)|67\d(2))([ ]?d(4))`  

3. Select **Enable** or **Disable** case sensitive matching.
4. Click **Save & Close**.

**Tip:** Before enabling a new expression in a Mail Scan rule, always test it first to be sure there are no unexpected consequences and choose to **Quarantine** rather than **Delete**.
Add New Expressions Based on Existing Expressions

Adding new expressions to a content filter based on existing expressions allows you to re-use these items as a template.

To add new expressions:

1. From the Content Filter tab, select one of the existing content filters; then, click Add Existing Content Filter.
2. In the Add Content Filter window, select the content filters you want to use. You can select multiple expressions.
3. Click OK.

Tip: Too many content filters in a mail scan rule can cause it to become unpredictably complex. Trend Micro recommends including one or two content filters per mail scan rule.

Configuring Data Loss Prevention Filter

The Data Loss Prevention (DLP) filtering is used to detect sensitive data in Mail Content. Compliance Patterns are best used with structured content, like Social Security Numbers (SSN), credit card numbers (CCN) and telephone numbers.

For example, credit card numbers are typically presented in 16-digit format, “xxxx-xxxx-xxxx-xxxx”, making them good candidates for pattern-based detection.

The DLP rules define different parts of an email message or a database document to be scanned. The DLP filter can perform logical operations of multiple rules to fulfill complicated DLP requirements. Besides, SMID integrates the latest Trend Micro DLP scan engine, which provides more than 200 predefined DLP templates.

Note: Scanning support for Microsoft Office and Adobe PDF.

Data Loss Prevention enables you to manage DLP rules, templates, and data identifiers.
Data Loss Prevention Rule Management

You can create, remove, and view data loss prevention rules from: Configuration > Data Loss Prevention > DLP Rules.

**To create a DLP rule:**
1. Click Configuration > Data Loss Prevention > DLP Rules.
2. Click Add > DLP Rule for Mail Document or DLP Rule for Non-mail Document.
3. Specify a rule name.
4. Select the parts of documents to be scanned.
5. Under Select Data Loss Prevention template, select the templates to match the selected email parts.
6. Click Save & Close.

**Note:** A DLP rule does not work until the rule is added to an effective DLP Filter. See Configuring Data Loss Prevention Filter Options on page 4-64.

**To delete a DLP rule:**
1. Click Configuration > Data Loss Prevention > DLP Rules.
2. Select a rule and click Delete.

**To view a DLP rule:**
1. Click Configuration > Data Loss Prevention > DLP Rule.
2. Double-click a DLP rule to view its details.

Data Loss Prevention Template Management

You can add, delete, copy, import, export and view data loss prevention templates from: Configuration > Data Loss Prevention > DLP Templates. You can create a custom template using expressions and keywords. This template may include multiple expressions and keywords.

**To add a custom template:**
1. Click Configuration > Data Loss Prevention > DLP Templates.
2. Click Add.
3. Type a Name and Description.

4. Under Matching Condition, choose a Data Identifier: Expression, or Keyword.

5. Select existing, Import, or Add a new Keyword or Expression and click >> to add it to the Matching Condition window.

6. Click Add to Template Definition.

7. Click Save & Close.

To delete a DLP template:
1. Click Configuration > Data Loss Prevention > DLP Templates.
2. Select a custom template and click Delete.

To copy a DLP template:
1. Click Configuration > Data Loss Prevention > DLP Templates.
2. Select one or more templates and click Copy.

To import a DLP template:
1. Click Configuration > Data Loss Prevention > DLP Templates.
2. Click Import and select a template in .dat format.

To export a DLP template:
1. Click Configuration > Data Loss Prevention > DLP Templates.
2. Click Export.

To view a DLP template:
1. Click Configuration > Data Loss Prevention > DLP Templates.
2. Double-click the template you want to view.

Note: You can only modify custom DLP templates. The pre-defined templates cannot be modified.

Data Identifiers

You can add, delete, copy, import, export and view keywords and expressions from:
Configuration > Data Loss Prevention > Data Identifiers.
To add a keyword:
1. Click Configuration > Data Loss Prevention > Data Identifiers.
2. Click Add and choose Keyword.
3. Type a Name and Description.
4. Select the appropriate Conditions.
5. Under the Sub Keyword section, type a Name and Description.
6. Select Case Sensitive as required.
7. Click Add.
8. Repeat to add additional sub-keywords. You can click import to bring in additional sub-keywords.
9. Select a keyword(s) and click Remove or Remove All to remove sub-keywords.
10. Click Save & Close.

To add an expression:
1. Click Configuration > Data Loss Prevention > Data Identifiers.
2. Click Add and choose Expression.
3. Type a Name and Description.
4. Select the appropriate Type.
5. Type the Expression and choose whether Case Sensitive.
6. Type the Expression for Display and Examples.
7. Choose the appropriate Validation.
8. Click Save & Close.

To copy a keyword or expression:
1. Click Configuration > Data Loss Prevention > Data Identifiers.
2. Select one or more Keyword(s)/Expression(s).
3. Click copy.

To import a keyword or expression:
1. Click Configuration > Data Loss Prevention > Data Identifiers.
2. Click Import and select the .dat file.
To export a keyword or expression:
1. Click Configuration > Data Loss Prevention > Data Identifiers.
2. Click Export.

**Note:** All keywords and expressions are combined during export.

To set View By parameters for keyword(s) or expression(s):
1. Click Configuration > Data Loss Prevention > Data Identifiers.
2. Click Viewed By and choose the appropriate option: Identifiers, Expression, or Keyword.

To view a DLP template:
1. Click Configuration > Data Loss Prevention > Data Identifiers.
2. Select one Keyword or Expression and double-click it to open.

**Note:** You can only modify custom DLP templates. The pre-defined templates cannot be modified.

### Configuring Data Loss Prevention Filter Options

This section describes the steps required to configure Data Loss Prevention Filter options.

**To configure data loss prevention filter options:**
1. Under Scan Options, click the Data Loss Prevention Filter tab.
2. Select the Enable data loss prevention filter check box.
3. In the Data Loss Prevention Filter section choose from the following options:
   - Create DLP Filter...
   - Add Existing DLP Filter...
   - Remove Filter...
   - Remove All...
4. To create a DLP filter:
   a. Under **Data Loss Prevention Filter**, click **Create DLP Filter**. The DLP filter screen appears.
   b. In the **Filter Name** field, type a new name for your filter.
   c. Select a rule that you want to use in this filter from the left window and click **And >>**.
      - To combine the current rule with another rule, select another rule and click **And >>**.
      - To combine the current rule with another rule to exclude it from the current filter (perform "AND NOT" operation on the rule), select another rule and click **And Not>>**.
      - To remove a rule from the right window, select the rule and click **<<**.
   d. Click **Save & Close**.

5. For manual scan or scheduled scan, in the **Scan Documents with forms** section, select **Scan All documents** in the database or select **Scan documents with specified forms**, and select the target forms.

6. In the **Exception** section, type the name of the file(s) you want to exclude from the DLP filter.

7. In the **Action** section, select the **Action on mails with unwanted content** to specify the scan action: **Pass**, **Quarantine**, **Block**, **Redirect mail for approval**, **Mask content and pass**.

   **Note:** The action **Mask content and pass** only works when the subject or the body of email message matches the DLP filter setting. ScanMail for IBM Domino will mask the sensitive content in the subject or body of an email message starting from the first character but will show the last four characters. It will consider all characters in the original sensitive content as sensitive and will replace these contents including blanks with an asterisk ".*".

8. In **Notification** section, select the appropriate notification and filtering options for messages.

   **Insert a filter description in the notification** to include additional instructions or descriptions.
For example: Contact the Domino Administrator for more details.

9. Click Save & Close.

Configuring Script Filter

Use the Script Filter tab to define how ScanMail filters IBM Notes scripts.

To configure script filter options:

1. Click Scan Options > Script Filter tab.
2. Select the Enable script filter check box.
3. From the String List section, type the stored form and rich text hotspot scripts to filter as follows:
   - @Function strings may contain any valid IBM Notes function in Formula language. For example: \texttt{prompt}
   - @Command strings may contain any valid IBM Notes formatted command in Formula language. For example: \texttt{[Execute]} or \texttt{[FileDatabaseDelete]}
   - Script strings may contain any valid LotusScript command from your operating system. For example: \texttt{shell}, \texttt{getobject}, \texttt{kill}, \texttt{rmdir}, or \texttt{activate}
   - @URLOPEN URLs can open any valid URLOPEN command in Formula language.
4. From the Action section, select the Action on items as appropriate.
5. Click \texttt{ } to set the filter action for Stored form hotspots and events and the action for Rich text hotspots.

\textbf{Note:} The Auto-clean action for rich text hotspots instructs ScanMail to delete the code segment that contains the malicious string. Consequently, the whole document containing the hotspot will be quarantined completely to allow document restoration of false-positive detections. If the Replace hotspot with pop-up message is selected, rich text hotspots will be replaced with a pop-up message.

6. In the Notification section, select the notification options for when a file matches the notification filters.
7. In the **Email Stamp** section, define the safe email stamp settings.
8. Click **Save & Close**.

### Configuring Redirect Options

Use the **Redirect Option** tab to set where ScanMail will redirect email messages for approval. The designated approver decides whether a message is fit for delivery.

**To configure redirect options:**

1. Under a mail scan rule, click the **Redirect Options** tab.

2. Under the **Administrator** section, click ![ ] to specify the approver's email address in the **Redirect original message to** field.

   **Note:** Even if an account has administrator privileges, it will not be able to access the ScanMail functions if that account is not included in the ScanMail databases accesses and roles.

   Ensure the account specified has the appropriate ScanMail database access. See *Defining Access and Roles to ScanMail Databases* on page 3-4 to learn more about defining ScanMail database access.

   **Tip:** Trend Micro recommends ensuring the availability of the designated approver. Set another email address where ScanMail can redirect email messages if the designated approver will be unavailable.

   In addition, you may want to designate at least two accounts that will approve redirected messages. In the absence of one approver, the other designated account can still attend to the redirected messages. This prevents messages from getting lost or being forgotten.

3. Under the **Notification** section, type the notification subject when an approver rejects or approves a message.

4. Click **Save & Close**.
Inserting Disclaimers

Use the Disclaimer tab to insert disclaimers for a mail scan notification and define the actual disclaimer message.

**Note:** ScanMail can insert disclaimers to an Internet mail on Domino. However, when there are identical disclaimer names, ScanMail uses and inserts only the first disclaimer.

**To insert disclaimers:**
1. Under a mail scan rule, click the Disclaimer tab.
2. Select Enable disclaimer.
3. Set the disclaimer position.

**Note:** When ScanMail inserts filter notifications in a message, disclaimers that should be positioned *At the beginning of the message body* are placed after the filter notification. In addition, ScanMail inserts subject disclaimers after the original message subject.

4. Type a name for the disclaimer in the Disclaimer name field.

**Note:** ScanMail will insert disclaimers with the same disclaimer names only once.

5. Type the appropriate naming information in the Subject disclaimer and Message body disclaimer fields.
6. Click Save & Close.

Setting the Rule Schedule

Use the Scan Schedule tab to set the schedule of a mail or database scan rule.

**To set the schedule:**
1. Under a scan rule, click the Scan Schedule tab.
2. Specify the rule schedule:
   - *Always*—ScanMail applies the rule 24x7.
• **Specified**—ScanMail applies the rule during or except the specified day, time, and time zone.

3. Click **Save & Close**.

### Running Manual Scan

Any database on the local Domino server, or remote clients with drives or directories mapped to the local server, can be scanned for viruses.

There are two ways to run a manual scan:

- Use the Domino server console
- Use the Configuration Database

See the next sections for details on how to invoke a manual scan.

### Running Manual Scan Using the Domino Server Console

You can scan Notes databases manually from a Domino server console or use the ScanMail interface.

Any Notes databases on a local or mounted hard drive, including network drives, can be included in a manual or scheduled scan.

**To scan databases from the Domino server console:**

Type and enter the following:

```bash
load SMDdbs -manual {directory name and database.nsf}
```

where `{directory name and database.nsf}` represents the database or directory you want to scan.

ScanMail searches specified databases or respective directories under the Directory section of `notes.ini` and follows the manual scan settings available in the Configuration database.

**Tip:** Separate multiple databases with semicolons. For example:

```bash
load SMDdbs -manual database.nsf;database2.nsf;database3.nsf;folder/database4.nsf
```
Running Manual Scan Using the Configuration Database

Use the Configuration database to invoke manual database scanning.

To run Scan Now:

1. Open the ScanMail Configuration Database.
2. From the left menu, click Actions > Manual Scan.
3. On the working area, click Edit.
4. Click the General tab.
5. Under the Condition section, select Enable incremental scan.
6. Under the Duration section, specify the number of minutes that corresponds to the duration of the scan.

Note: If the scan duration is set to zero (0), the manual scan task will stop once it finishes scanning all databases.

7. Click the Databases to scan tab to set which database(s) to scan according to the following:
   • All databases– ScanMail scans all databases stored on the \Domino Data\ directory, including databases found in its sub-directories.
   • Specified databases– ScanMail scans specific database(s) based on the directory and database list.
     Select Include sub-directories to include folders under directories specified.
   • Exclude selected databases from scanning– ScanMail skips scanning of specified database(s)
     Use the Add, Remove, and Remove All buttons to manipulate the database(s) in the list.

8. Click the Scan Options tab to configure the options as required.
9. Define the notification template.
10. Click **Scan Now**.

![Image of Scan Now configuration settings]

**FIGURE 4-29.** The ID used to run **Scan Now** must have the appropriate access right to submit server console command.

11. Click **Save & Close** to save the manual scan settings.

**Stopping the Manual Scan Manually**

When you want to stop manual database scanning before it automatically finishes, issue the following command to gracefully terminate the scan task at the Domino server console:

```
tell SMDdbs quit
```

Scanning will stop after the current document has been scanned.
Performing Administrative Tasks

The Summary, Server Settings, CM Agent Settings and Administration options are found in the Configuration Database. These options allow you to determine the ScanMail server information, and configure functions to optimize the ScanMail database manageability and performance.

This chapter includes the following topics:

- Viewing the Summary of All Servers on page 5-2
- Configuring the Server Settings Menu Options on page 5-3
- Configuring CM Agent Settings on page 5-14
- Configuring Deep Discovery Advisor Settings on page 5-15
- Managing the Filter Lists on page 5-17
- Configuring the Administration Menu Options on page 5-18
Viewing the Summary of All Servers

The Configuration Database provides a summary of the scan task status, and the ScanMail and operating system information.

To view the summary of all servers:

1. Open the ScanMail Configuration Database (see Accessing ScanMail Databases on page 3-6).

2. From the left menu, click Summary.

3. Do any of the following:
   - Click Display Summary of All Servers to display a summary of all available servers.
   - Press F9 to refresh the displayed information.
Performing Administrative Tasks

**Tip:** If Control Manager exists in your environment, you can also use the management console > **Product Status** tab to view the ScanMail status.

### Configuring the Server Settings Menu Options

Use **Server Settings** in the Configuration Database to define the following settings for a Domino server or groups of Domino servers:

- Directory used for detaching temporary files for scanning
- Memory size used for scanning
- Proxy server settings for component download and product activation
- Local Smart Scan sources used to configure Web Reputation
- Type of ScanMail event and if they will be displayed through the Domino server console
- Notification to inform administrator(s) if a ScanMail task has ended abnormally
- Default character set used when ScanMail cannot detect the character set used for disclaimers
- Other miscellaneous settings, such as multi-threaded scanning, trusted antivirus servers, warning image, and message routing

### Creating a Server Setting Rule

Use the ScanMail Configuration Database **Server Settings** menu to create a server settings rule.

**Tip:** Create server setting rules per server or groups of servers.

**To create a server settings rule:**

1. Open the ScanMail Configuration Database (see *Accessing ScanMail Databases* on page 3-6).
2. On the left menu, click **Configuration > Server Settings**.
3. From the working area, click **Create Server Settings**.
4. Specify which Server or Server Groups should apply the server settings rule.
5. Set directories used for scanning (see Set a Scanning Directory on page 5-5).
6. Set the memory size used for scanning (see Set the Memory Size for Scanning on page 5-5).
7. Configure the proxy server settings that ScanMail will use for component download and product activation (see Configure the Proxy Server Settings on page 5-6).
8. Configure inbound gateway IP address for ScanMail for IBM Domino to obtain sender's IP address (see Configuring Inbound Gateway IP Addresses on page 5-7).
9. Configure the Local Smart Scan Sources (see Configure Local Smart Scan Sources on page 5-8).
10. Select the event that will trigger ScanMail to display notification via the Domino server console (see Monitor Server Events on page 5-11).
11. Enable server task monitoring (see Enable Server Task Monitoring on page 5-11).
12. Specify the default character set that ScanMail should use when it cannot detect the character set of a message (see Specify the Default Character Set on page 5-12).
13. Configure miscellaneous settings (see Configure Miscellaneous Settings on page 5-12).
14. Click Save & Close.

Modifying a Server Settings Rule

Use the ScanMail Configuration Database Server Settings menu to modify a server settings rule.

To modify a server settings rule:
1. Open the ScanMail Configuration Database (see Accessing ScanMail Databases on page 3-6).
2. From the left menu, click Configuration > Server Settings.
3. From the working area, double-click a server settings rule document or click Edit.
4. Modify settings.
5. Click Save & Close.
Configuring a Server Settings Rule

Use the Temporary Directory, Scan Memory, Proxy Settings, Local Smart Scan Sources, Event Log, Task Monitoring, Regional Option, and Misc tabs to set the properties of a Server Setting rule.

Set a Scanning Directory

Use the Temporary Directory tab to set the directories that ScanMail should use when detaching temporary files for scanning.

To set a temporary directory:
1. Create or modify a server settings rule (see Creating a Server Setting Rule on page 5-3) or (Modifying a Server Settings Rule on page 5-4).
2. From the working area, click the Temporary Directory tab.
3. Type the directories related to the Domino Data directory.
4. Click Save & Close.

Set the Memory Size for Scanning

Use the Scan Memory tab to set the size of memory, which ScanMail tasks allocate to scan files in memory.

Use the following guidelines as a starting point to determine the appropriate memory for memory-based scanning:

- Dedicate the amount of memory that is adequate for most messages and document attachments in your environment.
  If you find that 90% of attachments in your organization are below 2-MB, you can allocate only 2-MB to each memory-based scanning task. Do not use the average message size for this sizing as you will not get optimal results.
- If your organization is limiting the maximum attachment size, you can use this value.
- Compressed files must be decompressed before scanning.
  Dedicate an appropriate amount of memory for the decompressed files, not the compressed attachments.
- Consider the total amount of memory that will be used by all ScanMail tasks on the Domino server.
For example, if you are running three SMDreal tasks with 5-MB dedicated memory, ScanMail is using 15-MB of memory. At the time of scheduled scans (SMDdbs), you must also add this memory to the total amount.

- Check the size and utilization of memory on the Domino server (refer to the Domino documentation for more information on how to determine memory utilization.

In memory starved environments, the negative impact of dedicating memory for ScanMail will be far greater than the performance improvement of memory-based scanning.

For most organizations, the default value of 5-MB for each ScanMail task is suitable.

**To set scan memory size:**

1. Create or modify a server settings rule (see *Creating a Server Setting Rule* on page 5-3) or *(Modifying a Server Settings Rule* on page 5-4).
2. From the working area, click the **Scan Memory** tab.
3. For each scan type, type an integer that corresponds to the **memory size** in megabytes (MB).
4. Click **Save & Close**.

**Configure the Proxy Server Settings**

Use the **Proxy Settings** tab to configure the proxy server used for Web Reputation, CM Agent, component download and product activation.

**Note:** You can specify another proxy server for CM Agent or component download in the scheduled update or manual update document. See *Defining the Proxy Server Settings for Component Download* on page 6-11.

**To configure the proxy server settings:**

1. Create or modify a server settings rule (see *Creating a Server Setting Rule* on page 5-3) or *(Modifying a Server Settings Rule* on page 5-4).
2. From the working area, click the **Proxy Settings** tab.
3. Select **Use a proxy server**.
4. Select the proxy server **Protocol**, (for example, HTTP, Socks4, Socks5, or HTTPS).
5. Type the proxy server **Address** or host name.
6. Type the proxy server **Port** number.
7. Type a **User name** and **Password** used for proxy authentication.
8. Click **Save & Close**.

### Configuring Inbound Gateway IP Addresses

The graymail filter uses the configured gateway IP addresses to check the reputation of the sender’s IP address and identify graymail messages.

**To configure Inbound Gateway IP addresses:**
1. From the left menu, click **Configuration > Server Settings**.
2. Double-click the settings of the target server and choose **Edit**.
3. Click the **Inbound Gateway IP Addresses** tab.

![FIGURE 5-30. Adding inbound gateway IP addresses](image-url)
4. Add all the inbound gateway IP addresses of your organization into the gateway IP address list.

**Note:** Add all of the inbound gateway IP addresses used in the organization to the list. If a gateway IP address is not added to the list, ScanMail may consider inbound email messages from that IP address as spam.

5. (Optional) Select **Notify the administrator of unknown gateway IP addresses**. Configure the following:
   a. In the **Subject** field, specify the notification email subject.
   b. In the **Content** field, specify the notification email content.
   c. In the **Interval** field, specify the notification interval.

**Note:** If all of the following conditions are met, ScanMail sends notifications to the administrator email addresses predefined on the **Notification** tab page:
   - Graymail detection is enabled in at least one rule of the active policy.
   - The **Notify the administrator of unknown gateway IP addresses** check box is selected in target server settings.
   - Any unknown gateway IP address is found during the specified interval.

6. Click **Save & Close**.

**Configure Local Smart Scan Sources**

Use the Local Smart Scan Sources tab to configure local the smart scan source used for Web Reputation.

**To add local smart protection server filter options:**

1. Click **Server Settings** to open the server settings options.
2. Click the **Local Smart Scan Sources** tab.
3. Click **Add** and choose from the following options:
   - Type the local Web Reputation server name or IP address in the **Server name or address** field.
   - Type the server port in the **Web Reputation Service Port** field (default port is 5274).
Performing Administrative Tasks

To edit local smart protection server options:
1. Click Server Settings to open the server settings options.
2. Click the Local Smart Scan Sources tab.
3. Double-click one of the available servers in the Smart Protection Server List.
   - Modify the local Web Reputation server name or IP address in the Server name or address field.
   - Modify the server port in the Web Reputation Service Port field (default port is 5274).
4. Click Save & Close.

To delete local smart protection server options:
1. Click Server Settings to open the server settings options.
2. Click the Local Smart Scan Sources tab.
3. Click Delete, select the server, and click OK.
4. Click Save & Close.

To change local Web reputation server priority options:
1. Click Server Settings to open the server settings options.
2. Click the Local Smart Scan Sources tab.
3. Select the server priority you want to change and click Move To Top.
4. Click Save & Close.

To configure notification mail:
1. Click Server Settings to open the server settings options.
2. Click the Local Smart Scan Sources tab.
3. Type or choose the name of the admin user from the To field.
4. Select from the following to Send notification when Web reputation service becomes:
   - Unavailable
   - Available
5. Use the default Subject or customize it as required.
6. Click Save & Close.
To configure proxy settings:
1. Click Server Settings to open the server settings options.
2. Click the Local Smart Scan Sources tab.
3. Select from the following:
   • Do not use proxy server
   • Use proxy server of server setting
   • Use following proxy server setting
4. If you chose: Use following proxy server setting:
   • Select the proxy server Protocol (HTTP, Socks4, or Socks5).
   • Type the proxy server Address or Host name, and Port used.
   • Type the User name and Password for proxy authentication as required.
5. Click Save & Close.

Note: Local Web reputation does not support proxy server with HTTPS protocol.
Performing Administrative Tasks

Monitor Server Events

Use the Event Log tab to monitor events and display or write them to the Domino server console according to the following:

- **Virus found**– provides information when ScanMail detects viruses and other malware types.
- **New settings applied**– provides information when ScanMail applies new settings to its databases.
- **New components downloaded**– provides information when ScanMail finishes downloading antivirus or content security components.
- **New components applied**– provides information when ScanMail finishes applying/deploying components.

**To monitor server events:**
1. Create or modify a server settings rule (see Creating a Server Setting Rule on page 5-3) or (Modifying a Server Settings Rule on page 5-4).
2. From the working area, click the Event Log tab.
3. Select which Event(s) ScanMail should monitor and whether logs will be displayed on the Domino server console.
4. Click Save & Close.

Enable Server Task Monitoring

Use the Task Monitoring tab to define whether ScanMail should send a notification to administrator(s) if a task ended abnormally.

**To enable server task monitoring:**
1. Create or modify a server settings rule (see Creating a Server Setting Rule on page 5-3) or (Modifying a Server Settings Rule on page 5-4).
2. From the working area, click the Task Monitoring tab.
3. Select Send a notification message to the administrator if a task ended abnormally.
4. In the Administrator field, type or click to determine the administrator(s) you wish to receive notification.
5. In the Subject and Body fields, type the appropriate information regarding the notification message.
6. Click Save & Close.

Specify the Default Character Set

Use the Regional Option tab to specify the default character set that ScanMail should use when it cannot detect the character set for disclaimers.

To insert disclaimers, see Inserting Disclaimers on page 4-68.

**To specify the default character set:**
1. Create or modify a server settings rule (see Creating a Server Setting Rule on page 5-3) or (Modifying a Server Settings Rule on page 5-4).
2. On the working area, click the Regional Option tab.
3. Select the appropriate Default character set from the list.
4. Click Save & Close.

Configure Miscellaneous Settings

Use the Misc tab to configure multi-threaded scanning, trusted antivirus server(s), warning image, and mail routing settings.

**To configure miscellaneous settings:**
1. Create or modify a server settings rule (see Creating a Server Setting Rule on page 5-3) or (Modifying a Server Settings Rule on page 5-4).
2. From the working area, click the Misc tab.
3. Under the Multi-threaded scanning group, type the integer that corresponds to the used for mail and database scanning according to the following:
   - Number of threads for real-time mail scanning
   - Number of threads for real-time database scanning
   - Number of threads for on-demand database scanning

   **Tip:** Set the value per scan to be between 1 and 20, inclusive. The sum of both the real-time mail and real-time database scanning threads cannot exceed 20.

   Trend Micro recommends five (5) threads per scan.

4. Under the Trusted Antivirus Servers group:
Performing Administrative Tasks

- **SMTP servers**: type the IP address(es) or server name(s) of SMTP servers
- **Domino servers**: type the server name(s) or click and choose from the menu.

**Note:** Verify that trusted servers have antivirus and content security protection to prevent viruses and other malware from spreading to other Domino servers.

**WARNING!** A warning bitmap will NOT appear when an attachment is removed.

5. Under the **Mail Routing** group, select **Do not deliver mails when the mail scan task is not running** to disable mail routing when the ScanMail real-time task is not running.

**Tip:** Trend Micro recommends enabling this option. See the following **Warning** and **Note** information:

**WARNING!** The ScanMail Setup enables this option by default. If the ScanMail tasks failed to load or **SMDreal** was unintentionally unloaded, the Domino server will continue to deliver messages. Messages that are not scanned may contain viruses and other threats, which can lead to outbreaks.

**Note:** When **Do not deliver mails when the mail scan task is not running** is disabled and SMDreal is not yet loaded, the Domino router delivers messages that are not yet scanned. This can lead to virus and other threat outbreaks.

6. Under the **Exclude tasks** group, type the Domino tasks names excluded from real-time database scan. For example: compact; fixup; updall; update

**Tip:** Use this option to help improve scanning performance.
7. Click **Save & Close**.

### Configuring CM Agent Settings

The communication between SMID and Control Manager uses a new protocol as SMID no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of SMID and Control Manager. The Control Manager Agent can be registered after completing the SMID installation. The following describes how to configure the CMAgent settings:

**Note:** CMAgent is automatically installed during the installation process.

**To create or modify CM Agent Settings:**

1. From the left menu, select **Configuration > CM Agent Settings**.
2. From the working area, click **Create CM Agent Settings**.

**Note:** To modify an existing setting, double-click the setting and click **Edit** on the Control Manager settings screen.

3. Type the server name in the **Applied to** field, or click to choose.
4. Under the **Control Manager Settings** group, select **Register ScanMail for IBM Domino to Control Manager Server**.
5. Under the **Control Manager Server** group, type the **Server Address** and **Port** number in the appropriate fields.
6. Under the **Web server authentication** group, type the **User name** and **Password** if used.
7. If a proxy server is used, under the **Proxy Settings** group, select **Use a proxy server to connect to the Control Manager server** and choose from the following options:
   a. **Use proxy server of server settings** to use the proxy server configured for Server Settings.
   b. **Use another proxy server** to choose a proxy server different from that configured for Server Settings as follows:
Performing Administrative Tasks

• Select the proxy server Protocol, (for example, HTTP, Socks4, Socks5, or HTTPS).
• Type the proxy server Address or host name.
• Type the proxy server Port number.
• Type a User name and Password used for proxy authentication.

8. Click Save & Close.

FIGURE 5-2. Control Manager settings screen

Configuring Deep Discovery Advisor Settings

The communication between SMID and Deep Discovery Advisor uses standard HTTPS protocol with an API Key for authorization. This section describes how to configure the Deep Discovery Advisor Settings in SMID.

To configure Deep Discovery Advisor:

1. Open the ScanMail Configuration Database (see Accessing ScanMail Databases on page 3-6).
2. From the left menu, click Configuration > Deep Discovery Advisor Settings.
3. From the working area, click **Create Deep Discovery Advisor**.

**Note:** To modify an existing setting, double-click the setting and click **Edit** on the Deep Discovery Advisor setting screen.

4. Type the server name in the **Applied to** field, or click **Choose** to choose.

5. Select **Register ScanMail for IBM Domino to Deep Discovery Advisor**.

6. In the **Deep Discovery Advisor** section, type the **Server Address**, **Port number** and **API Key** in the appropriate fields.

**Note:** If you do not have the Deep Discovery Advisor API Key, then contact your Deep Discovery Advisor administrator to obtain the API Key.

7. In the **Notification** section, select from the following to **Send notification when Deep Discovery Advisor becomes**:
   - **Unavailable**
   - **Available**

Use the default **Subject** or customize it as required.

8. If you want to use a proxy server, then under the **Proxy Settings** section select **Use a proxy server to connect to the Deep Discovery Advisor** and then select from the following options:
   - **Use proxy server of server setting**
   - **Use another proxy server**
     - If you chose: **Use another proxy server**, then:
       - Select the proxy server **Protocol** (HTTP, Socks4, or Socks5, HTTPS)
       - Type the proxy server **Address** or host name, and **Port** used.
       - Type the **User name** and **Password** for proxy authentication as required.

9. In the **Exception Handling** section, set the **Maximum wait time for analysis ratings** and click **Choose** to choose the **Action on unanalyzed risks**.

10. Click **Save & Close**.
Performing Administrative Tasks

Managing the Filter Lists

ScanMail for IBM Domino (SMID) 5.8 uses the Filter Lists Database (smlists.nsf) to store the filter lists, including the anti-spam approved and blocked sender lists and the Web Reputation approved URL list. This section describes how to manage the filter lists in the database.

To manage the filter lists:

1. Open the ScanMail Configuration Database (see Accessing ScanMail Databases on page 3-6).
2. From the left menu, click Filter Lists Database to open the Filter Lists Database.
3. Click Web Reputation Approved URLs, Anti-spam Blocked Senders, Anti-spam Approved Senders, Graymail Gateway IP List, or DLP Database Scan Target Forms.

4. Do any of the following:
   - Click Add to add information to the filter list.
   - Click Delete to delete information from the filter list.
   - Click Import to import approved URLs or graymail gateway IP addresses.
   - Click Export to export approved URLs or graymail gateway IP addresses.
Applying the Notes Database Properties to ScanMail Databases

The Administration > ScanMail Databases option provides shortcuts to database properties.

Use the Configuration database to set and apply the following properties to ScanMail databases:

- **Show in the Open Database Dialog**
  Enable/Disable this option to include/exclude ScanMail database in the list of databases displayed in the Open Database dialog.

- **List in Database Catalog**
  Enable/Disable this option to include/exclude ScanMail databases in the Notes Database Catalog Search.

- **Web access: Require SSL connection**
  Notes R8 and above supports Secure Sockets Layer (SSL) version 2.0 and above for secure communication. Instead of using the Database Properties dialog, use the Configuration database to enable this option to use SSL to access ScanMail databases through the Web.

- **Replication**
  Select this option to enable ScanMail database replication to other servers.
Performing Administrative Tasks

To set and apply Notes database properties to ScanMail databases:

1. Open the ScanMail Configuration Database (see Accessing ScanMail Databases on page 3-6).
2. From the left menu, click Administration > ScanMail Databases.
3. From the working area, type or click to select Domino server(s).
4. Select whether to Enable, Disable, or Do not change the property for each ScanMail database.
5. Click Save, and then click Apply Settings.

Note: The settings in the Configuration database overwrite the last saved settings.

Creating and Applying a New Access Control (ACL) Entry

Use the Configuration database to create and apply access control for ScanMail databases on Domino server(s).

To create and apply a new ACL entry:

1. Open the ScanMail Configuration database (see Accessing ScanMail Databases on page 3-6).
2. From the left menu, click Administration > Access Control.
3. From the working area, click Create New Entry.
4. Type or click to specify the ACL entry to a Domino server or groups of Domino servers.
5. Select a User type from the list.
6. Select a ScanMail database and set the permission(s).
7. Click Advanced to select the access level from the list and enable read or write public documents.
8. Click Save & Close; then, click Apply Settings to ACL.
Allowing Tasks to be Viewed through the Domino Administrator

Use the Configuration database to enable ScanMail tasks to be viewed through the Domino Administrator.

To allow tasks to be viewed through the Domino Administrator:
1. Open the ScanMail Configuration database (see Accessing ScanMail Databases on page 3-6).
2. From the left menu, click Administration > Domino Administrator.
3. From the working area, click Copy to domadmin.nsf.

Creating a License Profile

Use the Configuration database to create a license profile to activate a full version of ScanMail or renew its maintenance.

To create a license profile:
1. Open the ScanMail Configuration database (see Accessing ScanMail Databases on page 3-6).
2. Click Administration > Product License.
3. From the working area, click Create License Profile.
4. Type or copy the SMID Activation Code on page 2-63 in the field provided.
5. Click Save & Close.

Deleting a License Profile

Use the Configuration database to delete the license profile of an old or expired ScanMail version.

Note: To convert a trial version to a full version, create a new license profile first before deleting the old profile. See Convert to a Full Version on page 2-64.
To delete a license profile:

1. Open the ScanMail Configuration database (see Accessing ScanMail Databases on page 3-6).
2. Click Administration > Product License.
3. From the working area, select the license profile to be removed.
4. Click Delete License Profile.

A message displays confirming the profile deletion. Click OK to go back to the License Profile view.

**Tip:** When a profile has been accidentally deleted, restore it by creating a new profile using the Activation Code of the deleted profile.
Chapter 6

Updating Components

ScanMail allows you to update antivirus and content security components automatically or manually.

This chapter includes the following topics:

• Understanding the Antivirus and Content Security Components on page 6-2
• Updating Components on page 6-3
• Configuring Update Settings on page 6-8
• Loading Components Manually on page 6-12
Understanding the Antivirus and Content Security Components

The following ScanMail antivirus and content security components are listed according to the frequency of recommended update:

- **Virus pattern file** detects and cleans malicious file infections.

  If a particularly damaging malware is discovered “in the wild,” or actively circulating, Trend Micro releases a new pattern file as soon as a detection routine for the threat is available (usually within a few hours).

  As virus authors and malicious content writers release new viruses to the public, Trend Micro collects their telltale signatures and incorporates the information into the virus pattern file. Because new and virulent viruses are discovered every day, Trend Micro frequently makes available new versions of the virus pattern, often 2-3 times a week depending on the need and threat-risk.

- **Spyware pattern** detects hidden programs that secretly collect confidential information.

- **IntelliTrap pattern** detects viruses that attempt to circumvent virus filtering by using real-time compression algorithms. IntelliTrap helps reduce the risk of such viruses entering your network by blocking email attachments with real-time compressed executable files and pairing them with other malware characteristics.

- **IntelliTrap exception pattern** detects added exceptions to the IntelliTrap pattern.

- **Virus scan engine** detects all virus and malware known to be “in the wild,” or actively circulating.

- **Anti-spam engine** detects unsolicited commercial or bulk email messages (UCEs, UBEs).

- **Anti-spam pattern** detects unwanted content based on an updatable file containing spam definitions.

  The 32/64-bit, multi-threaded scan engine checks files in real-time using the process called pattern matching. The virus scan engine also employs a number of heuristic scanning technologies that even allows it to detect new viruses, not yet seen in the wild. In addition to viruses, the scan engine protects against mass mailing worms, macro and polymorphic viruses, Trojans, and Distributed Denial of Service (DDoS) attacks.

- **URL filtering engine** detects dangerous or unwanted URLs contained in email.
The scan engine includes an automatic clean-up routine for old virus pattern files, to help manage disk space. It also features incremental pattern updates to help manage bandwidth.

- The **Advanced Threat Scan Engine** detects files for less conventional threats, including document exploits.
- The **ScanMail** application refers to product specific components (for example, Service Pack releases).

**Tip:** Trend Micro recommends updating the antivirus and content security components to remain protected against the latest virus and malware threats.

However, only registered users are eligible for components update. For more information, see *Registering and Activating SMID* on page 2-63.

**Updating Components**

There are two ways to update the ScanMail components:

- Manually
- Automatically

**Updating Components Manually**

Use Update Now in the Configuration Database to run a manual update.

**To update components manually:**

1. Open the ScanMail Configuration Database (see *Accessing ScanMail Databases* on page 3-6).
2. From the left menu, click **Actions > Manual Update**.
3. From the working area, click **Edit**.
4. Under the **Update Components** group, select which component(s) to update.
5. Under the Options group, select the appropriate options for **Component update**, and **Download components for platforms**.
6. Click the **Source** tab.
7. Under the **Update Source** group, select the appropriate options.
8. Click the **Proxy Settings** tab.
9. Under the **Proxy Settings** group, configure the proxy server settings for component download.
10. Click the **Notifications** tab.
11. Under the **Notify administrator** group, define the notification settings as appropriate.
12. Click **Save** to save the manual update settings.
13. Click **Update Now**.

FIGURE 6-1. Click **Update Now** to download the latest antivirus and content security components.
Updating Components Automatically Using Scheduled Update Rules

Create scheduled update rules to update components automatically. Scheduled update rules define how ScanMail downloads the latest components at a specific time.

To update components automatically:

1. Create or modify a policy (see Creating Policies on page 4-3) or (Modifying Policies on page 4-5).
3. Select Enable scheduled update.
4. Set which components to deploy automatically (see Deploy Specific Components Automatically on page 6-7).
5. Click Create New Rule.
6. On the New Scheduled Update Rule document, specify the general settings on the General tab:
   • Under the Rule Identifier group, specify the scheduled update name in the Name field.
   • Under the Apply To group, select All server(s) of the parent policy or select Specified server, and click to choose server(s) from the list.
7. Click the Components tab.
8. Under the **Update Components** group, select which components to update.

   ![Image](image.png)

   **FIGURE 6-2.** Creating a scheduled update rule > defining the components to update

9. Click the **Source** tab.

10. Under the **Update Source** group, select the appropriate options. (see *Setting the Update Source* on page 6-9).

11. Click the Proxy Settings tab.

12. Under the **Proxy Settings** group, configure the proxy server settings for component download. (see *Defining the Proxy Server Settings for Component Download* on page 6-11).

13. Click the **Notifications** tab.

14. Under the **Notify administrator** group, define the notification settings as appropriate (see *Setting the Update Notifications* on page 7-9).

**Note:** ScanMail sends scheduled update rule notifications to the email address(es) set in the policy **Notifications** tab.
15. Click the Update Schedule tab to set the Run at times, Repeat interval of, and Days of the week when the scheduled update should occur.

16. Click Schedule Replication in the work area to launch the Notes Address Book and configure the schedule replication (refer to the Setting options on the Replicator topic in the Notes Help).

17. Click Save & Close. ScanMail updates components based on the schedule.

**Deploy Specific Components Automatically**

Depending on the Update Source and download options, ScanMail can deploy all the latest available components automatically. To instruct ScanMail to deploy only specific components, select Enable component deployment and set components to deploy.

ScanMail downloads and deploys the latest components as follows:

1. ScanMail checks for and downloads the latest components from the Update Source.
2. If updated components are available, ScanMail downloads these components to the Update Database.
3. ScanMail deploys the latest components from the Update Database to the servers specified in the Apply To General setting.

**To deploy specific components automatically:**

1. Create or modify a policy (see Creating Policies on page 4-3) or (Modifying Policies on page 4-5).
3. Select Enable component deployment, and then click Configure.
4. From the Component Deployment Configuration window, under the Deploy Components group, select which component(s) you want to deploy automatically.
5. Under the Options group, type values in the Retain pattern file history: ["x" pattern files] and Retain scan engine history: ["x" scan engines] fields to indicate the number of pattern files and scan engines ScanMail will save.
Note: Because virus pattern and scan engine files can take up disk space, Trend Micro recommends keeping three (3) previous pattern file and two (2) previous scan engine versions on hand (in addition to the current version). As subsequent pattern file or scan engine updates occur, the oldest component is deleted for each new one added.

6. Click OK to close the window.
7. Click Save & Close to apply the deployment settings.

**Configuring Update Settings**

Update settings include the configuration of:

- Components to update
- Update source
- Proxy server for component download

**Selecting Components to Update**

Use the Components tab to select which components to update.

**To select components to download:**

1. From the schedule update rule or manual update document, click the Components tab to set which components to download (see *Automatically* on page 6-3) or *(Manually* on page 6-3).
2. Under the Update Components group, select the components to download.
3. Under the Options group, type values in the Retain pattern file history ["x" pattern files] and Retain scan engine history ["x" scan engines] fields to indicate the number of files ScanMail will save.
Note: Because pattern files and scan engine can take up disk space, Trend Micro recommends keeping three (3) previous pattern file and two (2) previous scan engine versions on hand (in addition to the current version). As subsequent pattern file or scan engine updates occur, the oldest component is deleted for each new one added.

4. Under Component update, select how ScanMail applies the program update: Download only or Download and apply.

Tip: Use care when applying these options alternately. If you use the Download only option, and then run an update, the latest component will be downloaded to the Update Database. If you then decided to change the setting to Download and apply, ScanMail will not download any components because the ones in the Update Database are already the latest. This prevents ScanMail from applying the latest components to the servers in the Apply To General setting. In this case, use Replicated database as the Update Source to download and apply the latest components to other servers.

5. Select the appropriate options from Download components for platforms.
6. Click Save and Close.

Setting the Update Source

Use the Source tab to set which components to download.

To set the update source:

1. From the scheduled update rule or manual update document, click the Source tab to select one of the following update sources (see Automatically on page 6-3) or (Manually on page 6-3):
   - Replicated database—ScanMail servers automatically replicate (pull) the new pattern files from the central ScanMail server.
     In this model, a hub ScanMail server downloads the new updates and then all spoke ScanMail servers automatically pull the updates from the hub server. Even if Download only is set, ScanMail will still deploy (that is, apply) components to the spoke servers.
Note: IBM Domino does not replicate the Update Database automatically. Create a connection document in the Domino directory and specify the direction of the replication and the central server, which will download the components from the ActiveUpdate server.

- **ActiveUpdate server** – ScanMail servers automatically download the latest component from the Trend Micro ActiveUpdate server.

  Note: By default, ScanMail implements digital signature checking whenever it downloads components from the Trend Micro ActiveUpdate server. The signature files (*.sig) ensures secure component download from the Trend Micro ActiveUpdate server.

Using the ActiveUpdate server is the simplest way to update components. In a multi-server environment, you can configure every ScanMail server to independently poll for component updates using ActiveUpdate, or designate a single ScanMail server to act as a hub server for downloading updates and then have your spoke ScanMail servers pull in the update using replication.

  **Tip:** See *Update Issues* starting on page 11-3 to troubleshoot update issues.

- **Other Internet source** – ScanMail servers can download the pattern file and scan engine from another non-Trend Micro Web site (for example, your local Intranet Web site).

  Type the **URL** or **UNC path** of your own "ActiveUpdate" server in the **Address** field.
Updating Components

**Note:** The UNC source only applies to ScanMail for IBM Domino for Windows. Updating from another source requires having the corresponding signature files (*.sig) saved in the location where the latest components are located. Otherwise, the absence of the *.sig file will lead to an unsuccessful update.

To disable checking for the signature files, open the Domino console, and type the following command and press Enter:

```
set configuration disablesecureupdate=1
```

2. Click **Save & Close**.

**Defining the Proxy Server Settings for Component Download**

Use the **Proxy Settings** tab if the ScanMail server needs a proxy server to access the Internet.

**To define proxy server settings:**

1. From the schedule update rule or manual update document, click the **Proxy Settings** tab.
2. Under the **Proxy Settings** group, select **Use Proxy** if connecting to the Internet requires a proxy server.
3. Select whether to **Use proxy server of Server Settings** or **Use another proxy server**.
4. If using another proxy server, select the proxy server **Protocol**, and:
   a. Specify the proxy server **Address** or **Host** name, and **Port** used.
   b. Type the **User name** and **Password** used for proxy authentication.
5. Click **Save & Close**.
Loading Components Manually

If for some reason a Domino server is not able to update the ScanMail components via the Web or replicate from other servers due to network restrictions or network configuration errors (for example, intermittent network connection), use the Update Database to load components manually.

Note: Trend Micro recommends trying the automatic methods before attempting to load a component manually. If the automatic methods fail, first open the ScanMail configuration database and go to Actions > Manual Update > Source and verify you have selected Replicated database as the manual update source.

To load the latest virus pattern file:

1. Locate the latest virus pattern file and number from the activeupdate server.ini file at:
   
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/server.ini

2. Open the file, and locate the latest zip file name for the virus pattern: for example:
   
   vsapi945.zip

3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:
   
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/pattern/vsapi945.zip

4. Open the ScanMail Update Database (see Accessing ScanMail Databases on page 3-6 or Accessing other ScanMail Databases through the Configuration Database on page 3-10).

5. On the left menu, click Virus Pattern File.

6. On the working area, click Edit.

7. Modify the Pattern version.

8. Attach the latest version pattern file to the Pattern file field.

9. Click Save & Close.

10. Load SMDupd at the Domino server console:
    
    load SMDupd -realtime
Note: When manually loading a Controlled Pattern Release (CPR), the Status Summary screen may not reflect the latest pattern file version. As a workaround, unload SMDreal, load the CPR, and then reload SMDreal.

WARNING! Unloading SMDreal leaves the Domino environment temporarily unprotected.

To load the latest spyware patterns:
1. Locate the latest spyware pattern file name and number from the activeupdate server.ini file at:
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/server.ini
2. Open the file, and locate the latest zip file name for the spyware pattern; for example: ssaptn.zip.
3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:
4. Open the ScanMail Update Database (see Accessing ScanMail Databases on page 3-6 or Accessing other ScanMail Databases through the Configuration Database on page 3-10).
5. On the left menu, click Spyware Pattern.
6. On the working area, click Edit.
7. Modify the Spyware Pattern version.
8. Attach the latest spyware pattern file to the Spyware pattern field.
9. Click Save & Close.
10. Load SMDupd at the Domino server console:
    load SMDupd -realtime

To load the latest anti-spam pattern:
1. Locate the latest anti-spam pattern version number from the activeupdate server.ini file at:
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/server.ini
2. Open the file, and locate the latest zip file name for the anti-spam pattern: for example: **ias9899.zip**.
3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:
   
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/antispam/ias9899.zip
4. Download, save, and extract the content(s) of the zip file to a temporary directory.
5. Open the ScanMail Update Database (see *Accessing ScanMail Databases* on page 3-6 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-10).
6. On the left menu, click Anti-spam Pattern.
7. On the working area, click Edit.
8. Attach the latest version to the Anti-spam pattern field.
9. Update the Anti-spam pattern version.
10. Click Save & Close.
11. Load SMDupd at the Domino server console:

   ```
   load SMDupd -realtime
   ```

**To load the latest anti-spam engine:**

1. Locate the latest anti-spam engine version number from the activeupdate server.ini file at:

   http://smid56-p.activeupdate.trendmicro.com/activeupdate/server.ini
2. Open the file, and locate the latest zip file name for the anti-spam engine: for example: **tmaseng.zip**.
3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:

4. Download, save, and extract the content(s) of **tmaseng.zip** to a temporary directory.
5. Open the ScanMail Update Database (see *Accessing ScanMail Databases* on page 3-6 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-10).
6. On the left menu, click **Anti-spam Engine**.
7. On the working area, double-click the corresponding platform for the anti-spam engine.
8. On the Spam Engine Database document, click **Edit**.
9. Attach the latest version to the **Anti-spam engine** field.
10. Update the **Anti-spam engine version**.
11. Click **Save & Close**.
12. Load **SMDupd** at the Domino server console:
   
   ```
   load SMDupd -realtime
   ```

**To load the latest Intellitrap pattern file:**

1. Locate the latest IntelliTrap pattern version number from the activeupdate **server.ini** file at:
   
   ```
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/server.ini
   ```

2. Open the file, and locate the latest zip file name for IntelliTrap: for example: **tmblack.zip**.

3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:
   
   ```
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/pattern/tmblack.zip
   ```

4. Save and extract the content(s) of the zip file to a temporary directory.

5. Open the ScanMail Update Database (see **Accessing ScanMail Databases** on page 3-6 or **Accessing other ScanMail Databases through the Configuration Database** on page 3-10).

6. On the left menu, click **IntelliTrap Pattern**.
7. On the working area, click **Edit**.
8. Attach the latest version to the **IntelliTrap pattern** field.
9. Update the **IntelliTrap pattern number**.
10. Click **Save & Close**.
11. Load **SMDupd** at the Domino server console:

    ```
    load SMDupd -realtime
    ```

**To load the latest Intellitrap exception pattern file:**

1. Locate the latest IntelliTrap exception pattern version number from the activeupdate **server.ini** file at:
   
   ```
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/server.ini
   ```
2. Open the file, and locate the latest zip file name for IntelliTrap: for example:
   `tmwhite.zip`.
3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:
   ```
   ```
4. Save and extract the content(s) of the zip file to a temporary directory.
5. Open the ScanMail Update Database (see Accessing ScanMail Databases on page 3-6 or Accessing other ScanMail Databases through the Configuration Database on page 3-10).
6. On the left menu, click **IntelliTrap Exception**.
7. On the working area, click **Edit**.
8. Attach the latest version to the **IntelliTrap Exception pattern** field.
9. Update the **IntelliTrap Exception pattern number**.
10. Click **Save & Close**.
11. Load **SMDupd** at the Domino server console:
    ```
    load SMDupd -realtime
    ```

**To load the latest scan engine:**
1. Download the latest scan engine from [www.trendmicro.com](http://www.trendmicro.com).
2. Check the Domino server console to determine if there is no scheduled scan running.
3. Extract the engine under the Domino directory (for example, `c:\IBM\Domino`).
4. Open the ScanMail Update Database (see Accessing ScanMail Databases on page 3-6 or Accessing other ScanMail Databases through the Configuration Database on page 3-10).
5. On the left menu, click **Virus Scan Engine**.
6. On the working area, double-click the corresponding platform for the scan engine.
7. On the Scan Engine document, click **Edit**.
8. Update the **Scan engine version**.
9. Attach the latest version to the **scan engine field** at the bottom of the screen.
10. Click **Save & Close**.
11. Load **SMDupd** at the Domino server console:
    ```
    load SMDupd -realtime
    ```
To load the ScanMail database templates:

1. Using Windows Explorer, navigate to the Domino directory where you installed ScanMail.
2. Overwrite the old ScanMail database templates with the latest versions.

Note: If the Anti-spam Engine, Scan Engine, or Application document becomes corrupted, delete and then replace the corrupted document by using Add Anti-spam Engine, Add Scan Engine, or Add Application, respectively. Contact Trend Micro Support for details.
Chapter 7

Sending ScanMail for IBM Domino Notifications

When ScanMail detects a virus or other threat infection in a mail, attachment, or document, ScanMail can automatically alert, by email or IBM Instant Messaging and Web Conferencing, the persons you designate. For example, the Domino administrator or other individuals who need to know when infected files are found, the sender, and/or the recipient(s).

This chapter includes the following topics:

• Understanding ScanMail Notifications on page 7-2
• Using Email Stamps (Safe Stamps) on page 7-6
• Setting ScanMail Notifications on page 7-7
Understanding ScanMail Notifications

Whenever ScanMail discovers a malware in a message or database, it can automatically notify whomever you specify: a Domino administrator, an internal or external sender, an internal or external recipient, a database owner, or other Internet mail addresses or members of the Address book.

**Note:** Use the notification of external senders with caution as it may contribute to the problem of spam.

SMID has the following notification categories:

- **Scan notifications** are sent whenever a message or database triggers a mail scan, database scan, or scheduled scan rule.
- **Update notifications** are sent whenever ScanMail performs scheduled update or you run manual update.
- **Web Reputation server status notification**

ScanMail sends a separate notification to an administrator, sender, or recipient (recipient's notification is merged to the original message if Domino can send the original message to the recipient).

The notification message can include event-specific information based on tags you set. For example, a scan notification can include the malware name, action ScanMail took, and name of the infected file.
## Customizing Notifications

ScanMail uses two types of notification tags:

- Filter-based tags are available in **Scan Options** tabs.

Use the following tags to customize filter notifications:

<table>
<thead>
<tr>
<th><strong>Scan Options</strong></th>
<th><strong>Tags</strong></th>
<th><strong>Returns What</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Risk Scan</strong></td>
<td>%FILE%</td>
<td>File name of the infected file</td>
</tr>
<tr>
<td></td>
<td>%DETECTION%</td>
<td>Name of the malware detected</td>
</tr>
<tr>
<td></td>
<td>%ACTION%</td>
<td>Scan action</td>
</tr>
<tr>
<td><strong>APT Prevention Filter</strong></td>
<td>%FILE%</td>
<td>File name of the infected file</td>
</tr>
<tr>
<td></td>
<td>%DETECTION%</td>
<td>Name of the malware detected</td>
</tr>
<tr>
<td></td>
<td>%ACTION%</td>
<td>Scan action</td>
</tr>
<tr>
<td><strong>Scan Restrictions</strong></td>
<td>%FILE%</td>
<td>File name of the infected file</td>
</tr>
<tr>
<td></td>
<td>%CAUSE%</td>
<td>Matching scan restriction option</td>
</tr>
<tr>
<td></td>
<td>%ACTION%</td>
<td>Scan action</td>
</tr>
<tr>
<td><strong>Message Filter</strong></td>
<td>%CAUSE%</td>
<td>Matching message filter option</td>
</tr>
<tr>
<td></td>
<td>%ACTION%</td>
<td>Filter action</td>
</tr>
<tr>
<td><strong>Graymail Filter</strong></td>
<td>%GATEWAY_ADDRESSES%</td>
<td>Top three IP addresses recommended</td>
</tr>
<tr>
<td><strong>Attachment Filter</strong></td>
<td>%FILE%</td>
<td>File name of the infected attachment</td>
</tr>
<tr>
<td></td>
<td>%CAUSE%</td>
<td>Matching attachment filter option</td>
</tr>
<tr>
<td></td>
<td>%ACTION%</td>
<td>Filter action</td>
</tr>
<tr>
<td><strong>Content Filter</strong></td>
<td>%CONTENT_FILTER_NAME%</td>
<td>Matching content filter</td>
</tr>
<tr>
<td></td>
<td>%MAILPART%</td>
<td>Message part that matches the content filter: Header, message body, or attachment</td>
</tr>
<tr>
<td></td>
<td>%ACTION%</td>
<td>Filter action</td>
</tr>
<tr>
<td><strong>Script Filter</strong></td>
<td>%FORM_PART%</td>
<td>Message part that matches the script filter</td>
</tr>
<tr>
<td></td>
<td>%KEYWORDS%</td>
<td>Matching keyword(s)</td>
</tr>
<tr>
<td>SCAN OPTIONS</td>
<td>TAGS</td>
<td>RETURNS WHAT</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Data Loss Prevention Filter</td>
<td>%DLP_FILTER_NAME</td>
<td>Matching data loss prevention filter</td>
</tr>
<tr>
<td></td>
<td>%MAILPART%</td>
<td>Message part that matches the content filter: Header, message body, or attachment</td>
</tr>
<tr>
<td></td>
<td>%ACTION%</td>
<td>Filter action</td>
</tr>
</tbody>
</table>
• Rule-based tags are used by ScanMail rules.

Use the following tags to customize the notification template used by mail, database, or scheduled scans, and scheduled update rules.

<table>
<thead>
<tr>
<th>TAGS</th>
<th>RETURNS WHAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>%DATABASE%</td>
<td>Database name</td>
</tr>
<tr>
<td>%version%</td>
<td>Pattern/Engine version</td>
</tr>
<tr>
<td>%SERVER%</td>
<td>Domino/ScanMail server</td>
</tr>
<tr>
<td>%SENDER%</td>
<td>Sender of the message that matched a scan rule</td>
</tr>
<tr>
<td>%RECIPIENTS%</td>
<td>Recipient(s) of the message that matched a scan rule</td>
</tr>
<tr>
<td>%SUBJECT%</td>
<td>Subject header of the message that matched a scan rule</td>
</tr>
<tr>
<td>%SEND_TIME%</td>
<td>Time (in hh:mm format) when the message was sent</td>
</tr>
<tr>
<td>%FINAL_ACTION%</td>
<td>Final scan/Filter action taken</td>
</tr>
<tr>
<td>%MATCHING_FILTER%</td>
<td>Matching filter</td>
</tr>
<tr>
<td>%SCAN_TIME%</td>
<td>Time (in hh:mm format) when ScanMail scanned a message</td>
</tr>
<tr>
<td>%PRODUCTVERSION%</td>
<td>ScanMail for IBM Domino version</td>
</tr>
<tr>
<td>%PATTERNVERSION%</td>
<td>Virus pattern file version</td>
</tr>
<tr>
<td>%SCANENGINEVERSION%</td>
<td>Scan engine version</td>
</tr>
<tr>
<td>%RULENAME%</td>
<td>Rule name</td>
</tr>
<tr>
<td>%RULENUMBER%</td>
<td>Rule priority</td>
</tr>
<tr>
<td>%ADMIN_FILTER_INFORMATION%</td>
<td>Consolidates selected filter-based tags () for notifications sent to administrators</td>
</tr>
<tr>
<td>%OWNER_FILTER_INFORMATION%</td>
<td>Consolidates selected filter-based tags for notifications sent to database owners</td>
</tr>
<tr>
<td>%INTERNAL_FILTER_INFORMATION%</td>
<td>Consolidates selected filter-based tags for notifications sent to senders or recipients belonging to the Domino address book</td>
</tr>
<tr>
<td>%EXTERNAL_FILTER_INFORMATION%</td>
<td>Consolidates selected filter-based tags for notifications sent to senders or recipients not belonging to the Domino address book</td>
</tr>
<tr>
<td>%OS%</td>
<td>Platform (for example, Windows)</td>
</tr>
<tr>
<td>%COMPONENT%</td>
<td>Antivirus or content security component</td>
</tr>
</tbody>
</table>
Note: A Notification Template consolidates the specified filter-based tags and then uses the policy notification settings to deliver notification (see Defining How ScanMail Delivers Notifications on page 7-7). Do not insert characters such as << and >> in the Notification Template as these characters will result in a parsing error and the content contained within these characters will not display in the notification.

Using Email Stamps (Safe Stamps)

Aside from ScanMail notifications, defining email stamps is another way to immediately notify users of any ScanMail action.

Email stamps are appended in the Subject header as regular texts. You can customize the subject header of a message, for example:

[ScanMail Stamp] ScanMail found this email to be virus-free.

Depending on the Scan Options tab available in a scan or update rule, you can define email stamps as part of the message subject or body:

<table>
<thead>
<tr>
<th>Scan Options Tab</th>
<th>Available Email Stamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Risk Scan</td>
<td>You can: • Insert warning to the original mail if a security risk is detected • Insert message to the original mail if mail is malware-free</td>
</tr>
<tr>
<td></td>
<td>Insert email stamps at the end of the subject header or message body.</td>
</tr>
<tr>
<td>APT Prevention Filter</td>
<td>You can Insert the stamp as a subject prefix.</td>
</tr>
<tr>
<td>Scan Restrictions</td>
<td>You can Insert the stamp as a subject prefix.</td>
</tr>
<tr>
<td>Message Filter</td>
<td>You can Insert the stamp as a subject suffix.</td>
</tr>
<tr>
<td>Graymail Filter</td>
<td>You can Insert the stamp as a subject suffix.</td>
</tr>
<tr>
<td>Attachment Filter</td>
<td>You can Insert the stamp as a subject suffix.</td>
</tr>
</tbody>
</table>
Check the following links to define safe stamps for applicable filters:

- **Spam filter** stamp, see page 4-27
- **Web Reputation** stamp, see page 4-27
- **Security Risk Scan** stamp, see page 4-45
- **APT Prevention Filter** stamp, see page 4-47
- **Scan Restrictions** stamp, see page 4-48
- **Message Filter** stamp, see page 4-49
- **Graymail Filter** stamp, see page 4-52
- **Attachment Filter** stamp, see page 4-55
- **Script Filter** stamp, see page 4-67

### Setting ScanMail Notifications

Configure ScanMail to send notifications whenever it detects threats or unwanted contents, or when it updates antivirus or content security components to the latest version.

Refer to the next sections for details on how to set ScanMail notifications.

### Defining How ScanMail Delivers Notifications

ScanMail can send notification through email or IBM Instant Messaging and Web Conferencing. Use the **Notifications** tab to define the medium that ScanMail uses to deliver notifications. ScanMail can also send the notifications to the Windows Event Logs.
To define how ScanMail delivers notifications:

1. Create or modify a policy (see Creating Policies on page 4-3) or (Modifying Policies on page 4-5).
2. From the working area, click the Notifications tab.
3. Double-click the document or click Edit to configure the following settings:
   a. Under the Settings group, click or type the address in the Return address field.
   b. Type the Sametime server DNS/IP address to instruct ScanMail to send notification to an IBM Instant Messaging and Web Conferencing account.
   c. Type the Sametime sender user name for the account.
   d. Type the Sametime sender password for the account.
   e. Under the Administrator group, select Set recipients for each filter to send notifications to various email and IBM Instant Messaging and Web Conferencing recipient(s) when a message matches a filter setting. Otherwise, ScanMail will only send notifications to the Administrator's email address(es) and IBM Instant Messaging and Web Conferencing account(s).
4. Click Save & Close.

Configuring ScanMail for Windows Event Logs

You can configure ScanMail to write the notifications to the Application category in the Windows Event Logs.

To configure ScanMail to deliver the notifications to Windows Event Logs:

- Open the Domino console, and type the following command:
  
  set config SMDWriteOSEventLog=1

**Note:** If you modify the notes.ini file using a text editor, you must restart the Domino server for the changes to take effect.
Setting the Scan Notifications

Use the Notification Template tab to define the contents of ScanMail notifications. Define notification templates for each rule.

To set the scan notifications:

1. From a mail, database, or scheduled scan rule, click the Notification Template tab.
2. Click Add >> to include tags for the Administrator, Internal sender and recipient(s), and External sender and recipient(s) notifications.

   Note: ScanMail sends administrator notifications to email address(es) set in the policy Notifications tab (see Defining How ScanMail Delivers Notifications on page 7-7).

   ScanMail allocates “n/a” as values for the antivirus and content security variables in some scan notifications. When a component has an “n/a” value, this means that the filter did not use such component during a database or message scanning. For example, the Attachment Filter neither uses the scan engine nor virus pattern file when filtering messages. Therefore, when a message matches an Attachment Filter setting and you have set a scan notification with %PATTERNVERSION%, “n/a” becomes the value for this variable.

3. Click Save & Close.

Setting the Update Notifications

Use the Notifications tab to instruct ScanMail to send a notification whenever it updates a component.

To set the update notifications:

1. From the schedule update rule or manual update document, click the Notification tab (see Updating Components Automatically Using Scheduled Update Rules on page 6-5 or Updating Components Manually on page 6-3).

2. Type or click ☑ to select the recipient(s) of the update notification in the Administrator field.

3. Select the component(s) that when updated, will trigger ScanMail to send the update notification:
• Select the antivirus or content security component(s) (see Understanding the Antivirus and Content Security Components on page 6-2).

• Select Update has been unsuccessful to trigger ScanMail to send a notification when it cannot update the component selected.

  Type the **Number of attempts** that ScanMail will try to download the component. ScanMail will send a notification if it has exceeded the number of attempts.

  **Note:** ScanMail allots 120 seconds duration per attempt.

4. Type the message content in the **Subject** field for the update notification.

5. Click **Save & Close**.
Chapter 8

Using the Log and Quarantine Databases

This chapter covers viewing and deleting ScanMail virus and quarantine logs, and provides information on generating virus statistics.

Topics included are:

• Using the Log Database on page 8-2
• Using the Quarantine Database on page 8-13
• Understanding Deep Discovery Advisor Quarantine Database on page 8-19
Using the Log Database

ScanMail keeps a log of all its activities and writes them to the Log Database (smvlog.nsf).

Logs represent a valuable source of system information. Examine all (or selected) log entries to learn what type of malware ScanMail detected in messages, shared databases, and replication transactions.

Depending on the volume of traffic a server handles and the number of malware it encounters, the Log Database may grow quite large. Delete logs manually or schedule ScanMail to delete logs automatically.

You can view Mail Scan Logs and Database Scan Logs by selecting from the ScanMail Log Database left menu.

An aggregate view of ScanMail activity is available in the Statistics screen.
Note: In a multi-server environment, you may prefer to have a single, central server that consolidates logs from all the ScanMail servers. Trend Micro recommends setting up pull-only replications from the peripheral servers to the central Domino server.

Accessing Trend Micro Threat Connect Portal

Threat Connect is a cloud based service powered by Trend Micro global intelligence network, designed to enrich Trend customers with relevant and actionable intelligence.

In this version, you can access the Trend Micro Threat Connect portal by clicking Detail link in the virus log to get the latest information about the threat. By associating the threat with Trend Micro global threat intelligence, you will be able to take proper actions relevant to the attack profile.

FIGURE 8-2. SMID Virus Log

| Rule number | 1 |
| Rule description | Default Mail Scan |
| Matching policy | Default |
| Date scanned | 09/30/2013 14:42:09 |
| Virus | EXPL_ARTIFICIAL |
| File | 2004-05-01.doc |
| Notes UNID | ER90CA0A171897C57857E600234ABEC |
| Sender | jzon@zen.com |
| Recipient | zdvon <zdvon@gmail.com> |
| Filter | Security First Scan Filter |
| Engine | Advanced Threat Scan Engine |
| Action | Block |
| Scanner | SMIDreal |
| Server | CN=smidG=smid |
FIGURE 8-3. Virus details on the Threat Connect portal

Managing ScanMail Logs

The ScanMail Log Database provides options that allow you to set the number of days to keep virus logs, schedule regular log maintenance, manually delete virus and quarantine logs, or set up a log replication connection to replicate your virus logs to a hub server.

Use the ScanMail Log Database to access and view ScanMail logs.
Searching for Logs

Use the Log database to search for logs by configurable search conditions.

To configure a log search task:

1. Do one of the following to open the Log database:
   - From the ScanMail Configuration left menu, click Log Database.
   - Open smvlog.nsf.
2. Choose Log Query > Search.

3. On the Search Condition tab page, set the search conditions:

   **FIGURE 8-4. Setting Search conditions**
- **Search Status** section: shows the status of a search task, including *None*, *Task running*, and *Task finished*.
- **Condition Setting** section: adds conditions to the condition list.
  To add a condition, select a field option, type a value, click **Add** to add the value, and then click **Add to Condition List**.
- **Condition List** section: lists the conditions set for the current search.
  To remove a condition, select the condition from the condition list and click **Remove**. To remove all existing conditions, click **Remove All**.

4. On the **Notification** tab page, enable mail notification.
   a. Select the **Notify the administrator when the search is completed** check box.
   b. Select recipients for the notification mail.
   c. Type the subject and content for the notification mail.

   ![FIGURE 8-5. Enabling mail notification](image)

   **To search for logs:**
   1. On the action bar, click **Search**.
   2. Click **Refresh** to check whether the search is completed.
   3. When the search is completed, click **Check Results** to view search results.
      To clear the results, click **Clear Results**.
Note: The log search function allows you to run only one search task at a time. That is, if a task is running, another task cannot start. When you start a second task, the search results for the previous task will be removed automatically.

Enabling/Disabling Log Deletion

Use the Log database to enable or disable log deletion. When a log is enabled for deletion, ScanMail can delete it automatically.

To delete logs automatically:

1. Do one of the following to open the Log database:
   • From the ScanMail Configuration left menu, click Log Database.
   • Open smvlog.nsf.
2. Select which logs you want to enable or disable for deletion.
3. Click Enable Log Deletion or Disable Log Deletion.

FIGURE 8-6. Enabling/disabling log deletion from the Log database
Note: Before enabling the deletion of a number of logs, Trend Micro recommends reviewing them to verify that they are expendable.

Deleting Virus Logs Automatically

Use the Log database to schedule ScanMail to delete virus logs older than the specified number of days automatically. This is especially useful if a Domino server handles a large amount of traffic.

Note: ScanMail automatically deletes logs enabled for deletion.

To delete virus logs automatically:

1. Do one of the following to open the Log Database:
   - From the ScanMail Configuration left menu, click Log Database.
   - Open smvlog.nsf

2. From the left menu of the Log database, click Log Maintenance > Deletion Settings. The Automatic / Manual Deletion Settings screen appears (Figure 8-7).

3. On the Automatic Deletion Settings section, select Delete log files after.
4. Type the **number of days** that corresponds to the age of logs that ScanMail will save.

5. Type the **Number of deletion records** that corresponds to the number of deletion records that ScanMail will keep.

6. Click **Save & Close**.

**Deleting Virus Logs Manually**

Use the Log database to delete virus logs manually.

**To delete virus logs manually:**

1. Do one of the following to open the Log database:
   - From the ScanMail Configuration left menu, click **Log Database**.
   - Open **smvlog.nsf**.

2. From the left menu of the Log database, click **Log Maintenance > Deletion Settings**. The Automatic / Manual Deletion Settings screen appears (see Figure 8-7).

3. On the Manual Deletion section, do one of the following:
   - Select **Delete all virus log files** to delete all existing logs available on the Log database.
   - Select **Delete selected virus log files** to delete selected logs.
     i. Click **Browse** to launch the Log Files window.
     ii. Select which logs to delete.
     iii. Click **OK**.

4. Click **Delete Now**.

---

**Note:** ScanMail only deletes virus logs that are enabled for deletion.

**Viewing Statistics and Charting**

The **Statistics** option enables you to generate a numerical summary of the email and database virus logs on the server. It includes the aggregate number of malware cleaned, deleted, quarantined, and passed. It also includes options to generate statistics regarding
the results of security risk scanning, APT prevention filtering, message filtering, attachment filtering, content filtering, script filtering, spam filtering, Web reputation, data loss prevention filtering, outbreak prevention filtering, and redirected messages.

Generating, Viewing, and Exporting Statistics

Use the Log database to generate and view log statistics.

To generate, view, and export log statistics:

1. Do one of the following to open the Log database:
   - From the ScanMail Configuration left menu, click Log Database.
   - Open smvlog.nsf.

2. From the left menu of the Log database, click Statistics > Log Report.

3. From the working area, select all statistics or a specific statistic to view.

4. Select which tables to show from Show table(s):
   - All
   - Security Risk Scan
   - APT Prevention Filter
   - Message Filter
   - Attachment Filter
   - Content Filter
   - Data Loss Prevention Filter
   - Script Filter
   - Spam Filter
   - Web Reputation
   - Outbreak Prevention Filter
   - Redirected Messages
   - Graymail Filter

5. Select the Server(s) where the logs you want are located.

6. Select a Range: All, Today, Last 7 days, Last 30 days, or Specific date.

7. Click Calculate to begin compiling a summary report for the logs you selected.

8. From the working area, click Export to export the raw data to a *.csv file.
Using the Log and Quarantine Databases

Using Microsoft Excel™ to View *.csv Exported Logs

Microsoft Excel displays the exported ScanMail logs in a more useful form.

To use Excel to view *.csv ScanMail exported logs:

1. Open Microsoft Excel.
2. Open the exported *.csv.
3. Highlight the first column of data by clicking the column header.
4. From the main menu, choose Data > Text to columns... and follow the Wizard that appears.
   • Select Delimited and then click Next.
   • Clear the Tab checkbox. Choose Comma, and then for the Text Qualifier, choose None.
   • Without making any changes in the last Wizard screen, click Finish.
5. Save the document as an Excel file (*.xls) so you do not need to import and reformat again.

Generating and Viewing Charts

The Statistics > Top 10 option allows you to generate any of the following charts in a column layout:

• Detection Chart– provides the top 10 viruses detected.
• Server Chart– provides information of the top 10 servers where most infections are detected.
• User Chart– provides information of the top 10 users who sent the most viruses via email.
• Database Chart– provides information of the top 10 infected databases.

To generate and view log statistics:

1. Do one of the following to open the Log Database:
   • From the ScanMail Configuration left menu, click Log Database.
2. Open smvlog.nsf
3. From the Log Database left menu, click Statistics > Top 10.
4. From the working area, select the chart type to generate and view.
5. Select a date, either All or a Date Range.
6. Click Generate Chart.

The screen displays a column-type chart with the top ten values corresponding to the selected chart’s total percentage count. If there are no logs in the Log database, no data will be available in a column type chart.

<table>
<thead>
<tr>
<th>Virus</th>
<th>Number</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>NE_TEST_VIRUS</td>
<td>94</td>
<td>35.03%</td>
</tr>
<tr>
<td>TRZL_SUBFR.ZA.DPR</td>
<td>30</td>
<td>11.21%</td>
</tr>
<tr>
<td>EICAR_TEST_FILE</td>
<td>26</td>
<td>9.53%</td>
</tr>
<tr>
<td>JOKE_TEST_VIRUS</td>
<td>27</td>
<td>7.96%</td>
</tr>
<tr>
<td>JOKE_WOW</td>
<td>17</td>
<td>6.59%</td>
</tr>
<tr>
<td>Trojan_Test_Virus</td>
<td>17</td>
<td>6.59%</td>
</tr>
<tr>
<td>EICAR_TEST_VIRUS</td>
<td>17</td>
<td>6.59%</td>
</tr>
</tbody>
</table>

**FIGURE 8-8. A sample Detection Chart**
Using the Quarantine Database

The ScanMail Quarantine database (`smquar.nsf`) stores copies of messages quarantined for content, malware, or spam violations.

Depending on the volume of traffic a server handles and the amount of malware ScanMail encounters, the Quarantine database may grow quite large. If malware is detected, ScanMail will quarantine infected emails and attachments, which are stored as a new document in the `smquar.nsf` database.

Configure ScanMail to delete quarantined items every "x" days automatically (see Deleting Quarantined Items Automatically starting on page 8-17). Alternatively, you can manually delete quarantined items from the Quarantine database (see Deleting Quarantined Items Manually starting on page 8-18).

Viewing Quarantined Messages, Documents and Attachments

Use the ScanMail Quarantine database to access and view quarantined items.

To view quarantined attachments for Mail Scan:

1. Do one of the following to open the Quarantine database:
   - From the Configuration database left menu, click Quarantine Database.
   - Open `smquar.nsf`. 
2. From the left menu, select **Mail Scan** for the items you want to view according to the following criteria:
   - By Date: displays according to the date, all messages that ScanMail quarantined.
   - By Sender: displays according to the sender, all messages that ScanMail quarantined.
   - By Recipient: displays according to the recipient, all messages that ScanMail quarantined.
   - By Filter: displays according to the filter, all messages that ScanMail quarantined.

**To view quarantined attachments for Database Scan:**

1. Do one of the following to open the Quarantine database:
   - From the Configuration database left menu, click **Quarantine Database**.
   - Open `smquar.nsf`.
2. From the left menu, select **Database Scan** for the items you want to view according to the following criteria:
   - By Date: displays according to the date, all messages that ScanMail quarantined.
   - By Database: displays according to the database, all messages that ScanMail quarantined.
   - By Filter: displays according to the filter, all messages that ScanMail quarantined.

### Resending Quarantined Messages

*Quarantined messages* refer to messages quarantined by ScanMail Real-time Mail scan task. ScanMail can resend quarantined messages.

**To resend quarantined messages:**

1. Do one of the following to open the Quarantine database:
   - From the Configuration database left menu, click **Quarantine Database**.
   - Open `smquar.nsf`.
2. From the Quarantine Database left menu, select **Mail Scan > By Date, By Sender, By Recipient, or By Filter.**
3. Select the quarantined Mail Scan message(s) you want to resend.

4. From the working area, click **Enable Resend**.

5. The icon 🚭 represents a message enabled for resending. If the icon 🚭 is missing, it indicates the item is disabled for resending.

6. Click **Resend** to resend a message.

### Restoring Quarantined Documents

*Quarantined documents* refer to documents quarantined by the ScanMail Real-time, Manual, or Scheduled database scan task. ScanMail can restore quarantined documents.

**WARNING!** Use care when restoring documents. Documents containing malicious threats may be restored and then opened, which can cause a virus outbreak.

#### To restore quarantined documents:

1. Do one of the following to open the Quarantine database:
   - From the Configuration database left menu, click **Quarantine Database**.
   - Open `smquar.nsf`.

2. From the Quarantine Database left menu, select **Mail Scan** or **Database Scan**.
   - For Mail Scan, select **By Date, By Sender, or By Filter**.
   - For Database Scan, select **By Date, By Database, or By Filter**.

3. From the working area, select a quarantined document; click **Enable Resend**, and then click **Resend**.

### Enabling/Disabling Quarantined Item Deletion

Use the Quarantine database to enable or disable quarantined item deletion. When an item is enabled for deletion, ScanMail can delete it automatically.

#### To delete quarantined items automatically:

1. Do one of the following to open the Quarantine Database:
   - From the Configuration database left menu, click **Quarantine Database**.
• Open **smquar.nsf**.
2. Select the quarantined item you want to enable or disable for deletion.
3. Click **Enable Deletion** or **Disable Deletion**.

![FIGURE 8-10. Enabling/Disabling quarantined item for deletion](image)

**Note:** Before enabling deletion, Trend Micro recommends reviewing documents to make sure they are indeed expendable.

**Deleting Quarantined Items Automatically**

Use the Quarantine database to schedule ScanMail to delete quarantine items older than the specified number of days automatically. This feature is especially useful if a Domino
server handles a large amount of traffic (see Figure 8-11).

![Automatic and Manual deletion screen](image)

**FIGURE 8-11. Automatic and Manual deletion screen**

**Note:** ScanMail automatically deletes quarantine items enabled for deletion.

**To automatically delete quarantined items from Mail Scan and Database Scan:**

1. Do one of the following to open the Quarantine database:
   - From the Configuration database left menu, click **Quarantine Database**.
   - Open `smquar.nsf`.
2. From the Quarantine Database left menu, click **Maintenance > Deletion Settings**.
3. Select **Enable automatic deletion**; then, choose from the following:
   - Select **Delete quarantined mail older than**, and type the number of days that ScanMail will keep mail before it is deleted.
   - Select **Delete quarantined database documents older than**, and type the number of days that ScanMail will keep database documents before they are deleted.
4. In the **Keep number of deletion records** field, type then number of deletion records (0-100) that ScanMail will keep in the Deletion Records folder.
5. Click Save & Close.

Deleting Quarantined Items Manually

Use the Quarantine Database to delete quarantine items manually.

**To delete quarantined items manually:**

1. Do one of the following to open the Quarantine database:
   - From the Configuration database left menu, click **Quarantine Database**.
   - Open **smquar.nsf**.
2. From the Quarantine Database left menu, click **Maintenance > Deletion Settings**.
3. From the working area, do one of the following:
   - Select **Delete all quarantine documents** to delete existing logs available in the Quarantine database.
   - Select **Delete selected quarantine documents** to delete selected logs.
     i. Click **Browse** to launch the Log Files window.
     ii. Select which quarantine items ScanMail will delete.
     iii. Click **OK**.
4. Click **Delete Now**.

**Note:** ScanMail only deletes quarantine items enabled for deletion.
Understanding Deep Discovery Advisor Quarantine Database

ScanMail for IBM Domino Advance Persistent Threat (APT) Prevention scanning tasks use the SMID Deep Discovery Advisor Quarantine Database (smddtas.nsf) for temporarily storing messages with suspicious attachments. Meanwhile, the APT Prevention Filter uploads the suspicious attachments to the Deep Discovery Advisor for analysis, and then takes the preconfigured action on messages or attachments according to the analysis results.

**Note:** Trend Micro recommends that you do not manually delete the messages in this temporary quarantine database as this may cause the loss of data.

Viewing Quarantined Messages

Use the Deep Discovery Advisor Quarantine database to access and view quarantined items.

**To view quarantined attachments for Mail Scan or Database Scan:**

1. Open ScanMail Deep Discovery Advisor Quarantine Database (smddtas.nsf) in smd folder.
2. From the left menu, select **Mail Scan** or **Database Scan** to view temporarily quarantined messages.
3. Double-click a record to view its details.
Chapter 9

Using ScanMail for IBM Domino with Trend Micro Control Manager

Trend Micro Control Manager™ is a centralized system that unites Trend Micro antivirus products and services into a cohesive virus security and content management solution.

This chapter discusses the following topics:

- Introducing Control Manager on page 9-2
- Introducing the Control Manager Management Communication Protocol on page 9-3
- Introducing Outbreak Prevention Services on page 9-4
- Using Control Manager to Administer ScanMail on page 9-5
Introducing Control Manager

Trend Micro Control Manager is a central management console that manages Trend Micro and third-party antivirus and content security products and services 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.

Control Manager is available in Standard and Enterprise editions to better satisfy the needs of different enterprises.

- The Standard edition provides powerful management and configuration features that allow you to manage your corporate antivirus and content security.
- The Enterprise edition is for large enterprises and xSPs. This edition adds a variety of advanced features to the Standard edition—such as cascading console support and reporting functions.

Key Features

Key features of Control Manager include:

- Centralized management, which allows administrators to configure, monitor, and maintain Trend Micro software installed on the network from a single console—regardless of location or platform.
- Flexible and scalable configuration, which simplifies the administration of a corporate virus and content security policy.
- A hierarchical structure for job delegation so administrators can determine access control—different users can be assigned separate access to individual branches of the hierarchy.
- Outbreak Prevention Services that provides proactive attack protection service and blocks malicious code by file name or specific file details while new pattern files are being developed that can detect and clean the new threat.
- Vulnerability Assessment, a service that assesses network security risk and scans for system vulnerabilities that are associated with known virus and malware attacks and recommends actions to take to eliminate the vulnerabilities.
Agent-free Damage Cleanup Services (DCS), a comprehensive cleaning service that offers infection assessment and system repair for malicious remnants, such as Worms and Trojans. The service provides system administrators an easy approach for system cleaning without the use of any software locally installed on the client machines.

Using ScanMail with Control Manager

Control Manager is a useful tool for organizations with multiple Domino servers or for organizations using other Trend Micro products in addition to ScanMail. The main advantages of using Control Manager with ScanMail for IBM Domino are:

- Centralized virus logging
- Powerful reporting and analysis options
- Faster response to virus outbreak prevention using Outbreak Prevention Services
- Centralized license management console
- Centralized distribution of components

Introducing the Control Manager Management Communication Protocol

The communication between SMID and the Control Manager uses a new protocol called the Trend Micro Control Manager Management Communication Protocol (MCP). SMID no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of SMID and the Control Manager.

The Control Manager Agent can be registered after installing SMID. SMID supports Web console redirection from the Control Manager. Access the SMID product console directly from the Control Manager product console using a separate user name and password for the SMID product console.
Introducing Outbreak Prevention Services

Note: ScanMail does not apply Outbreak Prevention Services if the real-time scan is not enabled.

The Outbreak Prevention phase is the critical period when managed products have identified a virus outbreak and a pattern file is not yet available. During this crucial time, system administrators must endure a chaotic, time-consuming process of communication—often to global and decentralized groups within their organizations.

Outbreak Prevention Services delivers notification of new threats and continuous and comprehensive updates on system status as an attack progresses. The timely delivery of detailed virus data coupled with predefined, threat-specific action and scanning policies delivered immediately after a new threat identification allows enterprises to quickly contain viruses and prevent them from spreading.

Additionally, by centrally deploying and managing policy recommendations, Outbreak Prevention Services helps eliminate the potential for miscommunication, applies policies, and deploys information regarding attacks as they are occurring.

By providing automatic or manual download and deployment of policies via Trend Micro Control Manager, Outbreak Prevention Services import knowledge to critical access points on the network directly from experts at TrendLabs, Trend Micro’s global security research and support network.

This subscription-based service requires minimal up-front investment and provides enterprise-wide coordination and outbreak management via Trend Micro products, which reside across critical points on the network including the Internet gateway, mail server, file server, caching server, client, remote and broadband user, and third-party enterprise firewalls.
Using Control Manager to Administer ScanMail

Access the Control Manager management console to configure the ScanMail managed product from any computer on the network.

Accessing the Control Manager Management Console

There are two ways to access the management console:

- Locally on the Control Manager server
- Remotely using any compatible browser

To access the management console locally from the Control Manager server:

1. Click Start > Programs > Trend Micro Control Manager > Trend Micro Control Manager.
2. Provide the Username and Password in the fields provided.
3. Click Enter.

To access the console remotely:

1. Type the following at your browser's address field to open the sign in page:
   - For TMCM 5.0: https://{host name}/webapp/login.aspx
   - For TMCM 6.0/TMCM 7.0: https://{host name}/webapp/login.aspx
   where {host name} is the Control Manager server’s fully qualified domain name (FQDN), IP address, or server name.
2. Type the Username and Password in the fields provided.
3. Click Enter.

Managing ScanMail from the Control Manager Management Console

The Control Manager management console is a Web-based console that lets you use a compatible Web browser to administer the Control Manager network from any machine. For the list of compatible browsers, refer to the Control Manager Getting Started Guide or online help.
The Control Manager agent for ScanMail accepts commands from the Control Manager server and instructs ScanMail to perform them. For example, when you select **Tasks > Deploy engine** on the Control Manager management console, the Control Manager agent instructs ScanMail for IBM Domino to deploy the latest scan engine.

**To manage ScanMail from the management console:**
1. Access the Control Manager management console (see *Accessing the Control Manager Management Console* on page 9-5).
2. From the main menu, click **Products**.
3. Under Product Directory, expand the SMID folder to perform the following:

**To check ScanMail status:**
1. From the working area, click **Status**, to update the currently displayed status.

   The Product Status screen displays the **Product Information**, **Component Status**, **Operating System Information**, **Agent Environment Information**, and **Product License Information**.

**To configure ScanMail:**
1. From the working area, click **Configuration**.
2. Choose ScanMail from the product list that appears. The ScanMail Configuration Database Web console appears.

   **Note:** If necessary, type the **Username** and **Password** to access the Configuration database. Contact your administrator for the password set for ScanMail.

3. Configure ScanMail as you would from a Notes Client interface.

**To deploy anti-spam pattern, scan engine, license profiles, or pattern files:**
1. From the working area, click **Tasks**.
2. Select one of the following tasks from the list:
   - Deploy Anti-spam patterns
   - Deploy Engines
   - Deploy license profiles
   - Deploy pattern files/cleanup templates
3. Select the appropriate options and click **Deploy Now**.
4. Click **OK**.

**To view security and data loss prevention logs:**

1. From the working area, click **Logs**.
2. Select the type of logs you want to view:
   - **Security Threat Information** include all virus log incidents, content security violations, spam violation log, and viruses found in email and databases.
   - **Data Loss Prevention Information** includes data loss prevention incidents found in real-time email and in databases where emails are stored.
      i. Provide the search parameters (for example, Severity, Incident) after selecting the type of logs you want to view.
      ii. Click **Query** to begin query.
      iii. Click **Export Logs into CSV** to export the on-screen data to a comma separated values file.
   - Export logs into **CSV format**

**To export logs into CSV format:**

1. Click **Export to CSV**.
2. **File Download** dialog-box pops up.
3. Click **Save**.
4. On the **Save As** screen, specify the location where you want to keep the file.
5. Click **Save**.

Use an electronic spreadsheet application (for example, Microsoft Excel™) to open *.*CSV files.

**Viewing an Active Outbreak Prevention Policy**

**Note:** ScanMail does not apply Outbreak Prevention Services if the real-time scan is not enabled.

There are two methods to view an active Outbreak Prevention Policy:

- Through the Configuration database
  a. Open the ScanMail Configuration database.
b. On the left menu, click **Configuration > Outbreak Prevention**.
Details of the active Outbreak Prevention Policy should display on the working area.

- Through the Control Manager management console > **Outbreak Prevention** page.
  - For TMCM 6.0: **Management > Outbreak Prevention**.
  a. Access the Control Manager management console (see page 9-5).
  b. Click **Services** on the main menu.
  c. From the left menu under Services, click **Outbreak Prevention**.

This page automatically refreshes to ensure that the top threat and status information is current.
Chapter 10

Removing SMID

This chapter provides information on how to remove ScanMail components from a Domino environment.

This chapter includes the following topics:
- Removing ScanMail Automatically on page 10-2
- Removing a Single or Shared ScanMail Installation Manually on page 10-9
- Rolling Back to SMID 5.6 SP1 on page 10-16
Removing ScanMail

ScanMail can be removed either automatically or manually on all platforms on which it is installed.

- You can use a wizard to uninstall ScanMail.
- Although an automatic uninstall is recommended, you can remove ScanMail manually.

Before removing ScanMail:

1. Disable End User Quarantine (EUQ). Otherwise, the changes applied to the mail database template file may not be rolled back during uninstallation on the Windows 64-bit operating system.
2. Shut down the Domino server.

Removing ScanMail Automatically

The following uninstall procedure applies depending on the operating system hosting ScanMail.

Running a Wizard-based Uninstallation

The wizard-based ScanMail uninstallation uses steps that guide you with the uninstallation process.
Removing SMID 5.8 for Windows

To run an automatic ScanMail uninstallation using a graphical desktop environment:

1. Click Start > Programs > Trend Micro ScanMail for IBM Domino > Uninstall ScanMail for IBM Domino 5.8. The uninstallation progress screen appears.

   ![Uninstallation progress screen](image1)

   **FIGURE 10-1. Uninstallation progress screen**

2. After the uninstallation progress screen completes, the Welcome to Trend Micro ScanMail for IBM Domino Uninstaller screen appears. Click Next; the wizard proceeds to Choose Domino Server step.

   ![Welcome Screen](image2)

   **FIGURE 10-2. Welcome Screen**
3. On the **Choose Domino Server** step, select the server(s) from which to remove ScanMail and click **Uninstall**.

![Select server from which to uninstall SMID](image1.png)

**FIGURE 10-3. Select server from which to uninstall SMID**

4. After you execute the uninstall process, the **Uninstalling** progress screen displays.

![Uninstalling ScanMail for IBM Domino](image2.png)

**FIGURE 10-4. Uninstalling ScanMail for IBM Domino**
5. When the **Uninstalling** process finishes, the **Uninstall Complete** screen appears. Click **Done**. See Figure 10-5.

![Figure 10-5. Uninstallation complete](image)

**Note:** On the Windows platform, you may also remove ScanMail by selecting **ScanMail for Domino** from the Windows **Start > Control Panel > Add/Remove Programs**.
Removing SMID 5.8 for Linux

To remove SMID 5.8, perform the following steps:

1. Open Terminal, and navigate to the uninstall folder under SMID installation path (for example, /opt/trend/SMID/uninstall).

2. Run the uninstallation file (uninstaller) using command `./uninstaller`.

![FIGURE 10-6. Running the uninstallation file](image1.png)

The SMID uninstall Welcome screen appears.

![FIGURE 10-7. Welcome screen](image2.png)

![Select Domino Server screen showing installed Domino server(s)](image)

**FIGURE 10-8.** Select Domino Server screen showing installed Domino server(s)

On the screen shown in Figure 10-8, the list of all Domino servers installed is displayed. Select or deselect the domino server(s) you want to remove or keep.

To select or deselect the Domino server:

a. Type the corresponding number. For example, if you want to select the server named as BIF65x64/biftest from the list shown on the screen in Figure 10-8, type 2.

b. Press Enter.

4. Type 0 (zero) to accept current settings and start the uninstallation of selected Domino server(s).
5. Press Enter. The Summary screen appears, showing the list of selected Domino server(s) to be uninstalled.

![Summary screen](image)

**FIGURE 10-9. Summary screen**

6. Type Y or y and press Enter. The uninstallation begins. After the uninstallation process completes, **Uninstallation Completed** message appears on the screen.

![Uninstallation Completed](image)

**FIGURE 10-10. Uninstallation Completed**
Removing a Single or Shared ScanMail Installation Manually

If you are unable to remove ScanMail automatically, you can manually remove ScanMail. However, Trend Micro recommends trying the automatic methods before attempting to manually remove the product.

If the server has multiple installations of ScanMail and you want to manually uninstall all these instances, the procedure is similar to manually removing ScanMail on a single installation.

The installation information and file paths for each instance are all recorded in `smdsys.ini` (for Windows) or `smdsysV3.ini` (for Linux), which will also have multiple instances of `[SMDConfX]`.

Removing a Single or Shared ScanMail Installation on Windows

To manually remove a single or shared ScanMail installation:

**Tip:** Refer to Table C-1 on page C-2 in Appendix C, Program File and Folder Lists for the list of ScanMail files and folder structures.

1. On the server where ScanMail is installed, search for `smdsys.ini`, and then use a text editor to open it. Keep the file open for reference when performing the succeeding steps.

   Parameters that will be referred to in the succeeding steps include:
   - `DomSvr{X}DominoBinPath`
   - `DomSvr{X}DataPath`
   - `DomSvr{X}NotesIniPath`
   - `ProductPath`
Note: \texttt{DomSvr\{X\}} represents the ScanMail instance where \{X\} is the number corresponding to the ScanMail installation.

If the target server has only a single ScanMail installation, \texttt{DomSvr\{X\}} is \texttt{DomSvr0}. For multiple ScanMail installation, \texttt{DomSvr\{X\}} increments by 1. \texttt{DomSvr0} is the first instance, \texttt{DomSvr1} is the second instance, and so forth.
Here is a sample of `smdsys.ini` for a Windows server that has multiple instances of ScanMail:

```ini
[SMDConf] \indicates the first ScanMail instance
ProductPath=C:\TrendMicro\1\ScanMail for Domino
DomSvrISMDCount=2 \indicates the partition server number of first ScanMail instance
ProductVersion=V5.8 \indicates ScanMail version is 5.8
InstallType=64-bit \indicates it is a 64-bit ScanMail
DomSvrISMDSecs=DomSvr0,DomSvr1 \indicates partition servers of first ScanMail instance
[DomSvr0] \indicates the first partition server of first ScanMail instance
DomSvr0NotesIniPath=C:\IBM\Domino1\Data1\notes.ini
DomSvr0DominoBinPath=C:\IBM\Domino1
DomSvr0DataPath=C:\IBM\Domino1\Data1
DomSvr0DominoVersion=0
DomSvr0SMDVersion=5.8
[DomSvr1] \indicates the second partition server of first ScanMail instance
w=C:\IBM\Domino1\Data2\notes.ini
DomSvr1DominoBinPath=C:\IBM\Domino1
DomSvr1DataPath=C:\IBM\Domino1\Data2
DomSvr1DominoVersion=0
DomSvr1SMDVersion=5.8

[SMDConf0] \indicates the second ScanMail instance
ProductPath=C:\TrendMicro\2\ScanMail for Domino
DomSvrISMDCount=1 \indicates the partition server number of second ScanMail instance
ProductVersion=V5.8
DomSvrISMDSecs=DomSvr2 \indicates partition servers of second ScanMail instance
[DomSvr2] \indicates the first partition server of second ScanMail instance
DomSvr2NotesIniPath=C:\IBM\Domino2\Data1\notes.ini
DomSvr2DominoBinPath=C:\IBM\Domino2
DomSvr2DataPath=C:\IBM\Domino2\Data1
DomSvr2DominoVersion=0
DomSvr2SMDVersion=5.8
```
2. If the SMID instance is removed from all the partition servers that share the Domino binary, then navigate to the directory specified in \DomSvr\DominoBinPath, and then search for and delete the corresponding ScanMail files:
   - DomSvr\DominoBinPath ScanMail files on a Windows server (see Table C-1 on page C-2).
3. Navigate to the directory specified in \DomSvr\DataPath, and then delete the ScanMail installation and temporary folders (see Table C-1 on page C-2).
4. Using a text editor, open the notes.ini specified in \DomSvr\NotesIniPath, and then perform the following:
   a. Look for the ServerTasks section, and then delete the following items:
      - SMDemf
      - SMReal
      - SMDsch
      - SMDmon
      - SMDCm
   b. Look for the EXTMR_ADDINS section, and then delete the item SMDext.
   c. Look for the ScanMailInstallPath section, and then delete the whole line (including the file path).
5. Save and close notes.ini.
6. Delete smd.ini. This file is located in the path specified in \DomSvr\DominoBinPath.
7. If the SMID instance is removed from all the partition servers that share the SMID binary, delete the folder specified in ProductPath. This folder contains other ScanMail files, including the virus pattern and scan engine files for VSAPI and Trend Micro Anti-Spam.
8. Navigate to the folder where the ScanMail installation logs are located (see Locating Installation and Uninstallation Logs on page 11-2) and delete the log files.
9. For ScanMail installed on a Windows server, complete the following tasks:
   a. Open the Registry, and then delete the uninstall key:
      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\ScanMail for Domino
b. Delete the Trend Micro ScanMail for IBM Domino folder from `C:\Documents and Settings\All Users\Start Menu\Programs`. This action removes the ScanMail program folder from the Start menu.

c. Close the registry editor

10. Delete and modify the information of partition server which installs the specified SMID instance in `smdsys.ini`.
   - DomSvrISMDCount
   - DomSvrISMDSecs
   - DomSvrX (delete the related information of the partition server of ScanMail instance)

   If the SMID instance is removed from all the partition servers that share the SMID binary, delete the SMDConfX instance in `smdsys.ini`.

   If all SMID instances are removed from the target server, delete `smdsys.ini`.

11. Restart the Domino server.

Removing a Single or Shared ScanMail Installation on Linux

Tip: Refer to Table C.2 on page C-3 in Appendix C, Program File and Folder Lists for the list of ScanMail files and folder structures.

1. On the server where ScanMail is installed, search for `smdsysV3.ini`, and then use a text editor to open it. Keep the file open for reference when performing the succeeding steps.

   Parameters that will be referred to in the succeeding steps include:
   - DomSvr{X}
   - ProductPath

Note: DomSvr{X} represents the ScanMail instance where {X} is the number corresponding to the ScanMail installation.

   If the target server has only a single ScanMail installation, DomSvr{X} is DomSvr0.

   For multiple ScanMail installation, DomSvr{X} increments by 1. DomSvr0 is the first instance, DomSvr1 is the second instance, and so forth.
Here is a sample of `smdsysV3.ini` for a Linux server that has multiple instances of ScanMail:

```ini
[SMDConf] \ indicates the first ScanMail instance
ProductPath=/ibm2/linux/trend/SMID
ProductVersion=V5.8 \ indicates ScanMail version is 5.8
InstallType=64-bit \ indicates it is a 64-bit ScanMail
DomSvrISMDCount=1 \ indicates the partition server number of first ScanMail instance
DomSvrISMDSecs=DomSvr0 \ indicates partition servers of first ScanMail instance
DomSvr0=/ibm2/linux/notesdata0/notes.ini

[SMDConf0] \ indicates the second ScanMail instance
ProductPath=/ibm1/trend/SMID
ProductVersion=V5.8
InstallType=64-bit
DomSvrISMDCount=2 \ indicates the partition server number of second ScanMail instance
DomSvrISMDSecs=DomSvr1,DomSvr2 \ indicates partition servers of second ScanMail instance
DomSvr1=/ibm1/notesdata1/notes.ini
DomSvr2=/ibm1/notesdata0/notes.ini

[SMDConf1] \ indicates the third ScanMail instance
ProductPath=/ibm2/trend/SMID
ProductVersion=V5.8
InstallType=64-bit
DomSvrISMDCount=1 \ indicates the partition server number of third ScanMail instance
DomSvrISMDSecs=DomSvr3 \ indicates partition servers of third ScanMail instance
DomSvr3=/ibm2/notesdata0/notes.ini
```

2. If the SMID instance is removed from all the partition servers that share the Domino binary, then navigate to the Domino Binary directory, and then search for and delete the corresponding ScanMail files:
   - ScanMail files in the Domino Program directory (`ibmpow`) on a Linux server (see Table C-2 on page C-3).

3. Navigate to the Domino Data directory, and then delete the SMID installation and temporary folders.
4. Using a text editor, open the `notes.ini` specified in DomSvr{X}, and then perform the following:
   a. Look for the `ServerTasks` section, and then delete the following items:
      - SMDemf
      - SMDreal
      - SMDsch
      - SMDmon
      - SMDcm
   b. Look for the `EXTMGR_ADDINS` section, and then delete the item `SMDext`.
   c. Look for the `ScanMailInstallPath` section, and then delete the whole line (including the file path).

5. Save and close `notes.ini`.

6. If the SMID instance is removed from all the partition servers that share the SMID binary, delete the folder specified in `ProductPath`. This folder contains other ScanMail files, including the virus pattern and scan engine files for VSAPI and Trend Micro Anti-Spam.

7. Navigate to the folder where the ScanMail installation logs are located (see Locating Installation and Uninstallation Logs on page 11-2) and delete the log files.

8. Delete and modify the information of partition server which installs the specified SMID instance in `smdsysV3.ini`.
   - DomSvrISMDCount
   - DomSvrISMDSecs
   - DomSvrX (delete the related information of the partition server of ScanMail instance)

If the SMID instance is removed from all the partition servers that share the SMID binary, delete the `SMDConfx` instance in `smdsysV3.ini`.

If all SMID instances are removed from the target server, delete `smdsysV3.ini`.

9. Restart the Domino server.
Rolling Back to SMID 5.6 SP1

If you need to roll back to SMID 5.6 SP1, you can perform the procedure manually. SMID 5.8 does not provide an automatic procedure for the rollback.

Rolling Back to SMID 5.6 SP1 on Windows

To manually roll back to SMID 5.6 SP1:

1. Stop the Domino server.
2. Replace the following files with the original files that you backed up before upgrading to SMID 5.8 (see Important SMID Files to Back Up on page 2-38):
   - SMID data directory under IBM data path.
     For example: C:\Program Files\IBM\Domino\data\smd
   - SMID binary directory.
     For example: C:\Program Files\Trend Micro\ScanMail for Domino
   - The following SMID binaries under IBM binary path (for example: C:\Program Files\IBM\Domino):
     • nSMDupd.exe
     • nsmdTools.exe
     • nSMDsupp.exe
     • nSMDsch.exe
     • nSMDreal.exe
     • nSMDmon.exe
     • nSMDext.dll
     • nSMDEUQ.exe
     • nSMDemf.exe
     • nSMDDTAS.exe
     • nSMDdbs.exe
     • nSMDcm.exe
3. Update smdsys.ini:
   a. Open C:\Windows\smdsys.ini in a text editor.
   b. Look for the section \SMDC\Conf, and change \ProductVersion back to V5.6.1.
   c. Look for the section \DomSvr, and change the \DomSvr0\SMD\Version field back to 5.6.1.
   d. Save and close smdsys.ini.
4. Start the Domino server.

Rolling Back to SMID 5.6 SP1 on Linux

To manually roll back to SMID 5.6 SP1:

1. Stop the Domino server.
2. Replace the following files with the original files that you backed up before upgrading to SMID 5.8 (see Important SMID Files to Back Up on page 2-38):
   • SMID data directory under IBM data path.
     For example: /local/notesdata/smd
   • SMID binary directory.
     For example: /opt/trend/SMID
   • The following SMID binaries under IBM binary path (for example:
     /opt/ibm/domino/notes/latest/linux):
     • libsmdext.so
     • smdc
     • smddbs
     • smddtas
     • smdemf
     • smdeuq
     • smdmon
     • smdreal
     • smdsch
     • smdsupp
3. Update smdsysV3.ini:
   a. Open `/etc/smdsysV3.ini` in a text editor.
   b. Look for the section `SMDConf`, and change `ProductVersion` back to V5.6.1.
   c. Save and close `smdsysV3.ini`.
4. Start the Domino server.
Chapter 11

Troubleshooting

This chapter describes how to troubleshoot problems that may occur with ScanMail for IBM Domino.

This chapter discusses the following topics:

- Locating Installation and Uninstallation Logs on page 11-2
- Held Mail Issues on page 11-2
- Update Issues on page 11-3
- Scheduled Scan/Update Issue on page 11-4
- Recovering a Corrupt ScanMail Database on page 11-5
- Using the Database Templates to Recreate ScanMail Databases on page 11-6
- Deep Discovery Advisor Agent Issue on page 11-7
- Debugging ScanMail Tasks on page 11-7
- Understanding ScanMail Error Messages on page 11-9
Locating Installation and Uninstallation Logs

The following are the ScanMail installation and uninstallation logs:

**TABLE 11-10. Installation and uninstallation logs**

<table>
<thead>
<tr>
<th>PLATFORM</th>
<th>LOCATION AND FILE NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td>%windir%temp\smdins.log</td>
<td>ScanMail installation log</td>
</tr>
<tr>
<td></td>
<td>%windir%temp\smdunins.log</td>
<td>ScanMail uninstallation log</td>
</tr>
<tr>
<td>Linux</td>
<td>/var/log/smdins.log</td>
<td>ScanMail installation log</td>
</tr>
<tr>
<td></td>
<td>/var/log/smdunins.log</td>
<td>ScanMail uninstallation log</td>
</tr>
</tbody>
</table>

Held Mail Issues

This section provides information on how to handle various held mail issues.

General Held Message Issues

To help quickly resolve held mail issues, determine and collect the following information:

- Mail.box(es)
- ScanMail Temporary Files (check Configuration Database > Server Settings screen for the exact path of the temporary directory)
- **SMDreal** debug files
- Number of SMDreal tasks running

Scanning for and Releasing Held Mail in the System Mailbox

In some circumstances, such as when **SMDreal** is manually halted, some unscannable email messages may be held in the system mailbox, mail.box. If this occurs, manually scan the system mailbox and release the held messages.
To scan the system mailbox and release the held email messages:

1. Load the SMDreal server task and verify its status is idle.
2. Go to Actions > Manual Scan > Databases to scan and add mail.box to the list.
3. Click Scan Now or load smddbs on the Domino console. All messages in the system mailbox will be scanned and all held messages will be released.

**Note:** A manual scan of the system mailbox will use the rules set in the currently active Mail Scan policy.

**Update Issues**

If you configured the update source to download antivirus and content security components from the update source, and updated components cannot be downloaded. See Setting the Update Source on page 6-9 and Understanding the Antivirus and Content Security Components on page 6-2.

Perform the following steps to help troubleshoot the cause of the issue:

- If **Other Internet source** is enabled as the update source, check whether the folder containing the latest components has the corresponding signature files for secure digital download. The absence of the *.sig file will cause an unsuccessful component download and update.

- If **Trend Micro ActiveUpdate** is enabled as the update source, check the connection from the Domino server to the ActiveUpdate server.
  a. Use nslookup to verify that the Domino server can resolve the ActiveUpdate server’s FQDN.
  b. Ping the following from the Domino server:
     smid56-p.activeupdate.trendmicro.com
  c. Telnet the ActiveUpdate server at port 80 to make sure the Domino server can connect via HTTP.
  d. If an HTTP proxy is being used to update from the Internet, access the following URL to test the connection:
     
     http://smid56-p.activeupdate.trendmicro.com/activeupdate/server.ini
The Internet browser will either display the content of *server.ini* file or ask you permission to download it to the computer. Check the Domino console to see whether SMDupd returns an error message.

If ScanMail still cannot update components, enable SMDupd debugging and then contact Trend Micro Support (see *Debugging ScanMail Tasks* on page 11-7).

**Scheduled Scan/Update Issue**

An SMID scheduled scan/update cannot be re-run if the scheduler failed to start at the scheduled time. A workaround for this issue is:

1. Add SMDdbs/SMDupd as a startup server task in *notes.ini*.
   
   Example: `ServerTasks=XXXX,XXXX,XXXX,XXXX,SMDdbs,SMDupd`

   **Note:** The *XXXX* in this example represents already existing task names in *notes.ini*.

2. Use the same settings that are specified in the Scheduled Scan/update settings to configure the Manual Scan/update settings.

![FIGURE 11-1. Manual Scan settings](image)
FIGURE 11-2. Scheduled Scan settings

When the Domino server encounters a restart, such as a nightly backup, smddbs/smdupd will run the same scan/update tasks as the scheduled scan/update.

Recovering a Corrupt ScanMail Database

If for some reason, a ScanMail database becomes corrupted, you can try to recover the database by performing a consistency check on the database. To do this, type the following command at the Domino server console:

```bash
load fixup {database path and file name}
```

For example, if the administrator wants to recover a corrupted Configuration Database, the following command should be issued from the Domino server console:

```bash
load fixup smd\smdconf.nsf
```

If the database can no longer be recovered, you may opt to recreate the database (see Using the Database Templates to Recreate ScanMail Databases on page 11-6).
Note: Recreating a database does not restore its original contents.

Using the Database Templates to Recreate ScanMail Databases

If the ScanMail database becomes corrupted and is irrecoverable, use the corresponding ScanMail database templates to recreate these databases.

Note: Recreating a ScanMail database does not restore the original database contents. If the corrupted database was the Configuration database, then the administrator needs to redefine the policies, rules, and filters (or replicate the configuration database from another ScanMail server after the local Configuration Database is recreated).

To recreate a ScanMail database:

1. Obtain a *.NTF copy of the database you would like to replace and place it in the Domino Data directory.
2. Launch a Notes Client, and then open the Workspace tab containing the ScanMail databases (see Adding ScanMail Database Icons to the Notes Workspace on page 3-3 for details on how to add ScanMail icons to the Notes Workspace).
3. Select the ScanMail database to recover.
4. On the main menu, click to File > Application > Replace Design. The Replace Database Design window appears.
5. Click Template Server.
6. Click the corresponding server from the list; then, click OK.
7. Select the Show advanced templates check box.
8. From the templates list, select the corresponding ScanMail template to replace the corrupted database.
9. Click Replace. If the template file had not been signed using the ID used during ScanMail installation; then, sign the new database with this ID.
Deep Discovery Advisor Agent Issue

If the Deep Discovery Advisor Agent does not connect with Deep Discovery Advisor, then perform the following steps:

1. Make sure that the SMID server is connected with the Deep Discovery Advisor.
2. Verify the API key in Deep Discovery Advisor Settings. See Configuring Deep Discovery Advisor Settings on page 5-15 for the detailed configuration steps.

**Note:** If you do not have the Deep Discovery Advisor API Key, then contact your Deep Discovery Advisor administrator to obtain the API Key.

Debugging ScanMail Tasks

Do one of the following debug procedures:

**To debug ScanMail SMDreal, SMDdbs, SMDmon, SMDsch, or SMDcm tasks:**

Type and run the following commands on the Domino console:

```
tell {scan task} quit
load {scan task} -debug {level}
```

where `{level}` can be 1, 2, or 3.

**To debug ScanMail EMfilter tasks:**

a. Open *notes.ini* using a text editor (for example, *notepad.exe*).

**Tip:** Use care when modifying Domino or ScanMail *.*.ini files. To ensure that you can rollback to the original settings, back up *notes.ini*.

b. Add this parameter as the last *notes.ini* entry:

```
SMDMDEBUG=1
```

c. Save and close *notes.ini*. 
Debug Levels

The ScanMail scanning tasks uses the following debug levels:

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Shows fatal errors only</td>
</tr>
<tr>
<td>2</td>
<td>Shows abbreviated debug information</td>
</tr>
<tr>
<td>3</td>
<td>Shows detailed debug information</td>
</tr>
</tbody>
</table>

**Note:** Debug levels for the Extension Manager and Extension Manager filter cannot be set.

Debug Results

For scan task debugging, ScanMail writes logs to files with the following naming convention:

```
{servertaskname}_{yyyymmdd}.dbg
```

where:

- `{servertaskname}` is the name of the ScanMail task
- `{yyyymmdd}` is the year, month, and day the log file is generated

Examples:

- **Windows:** nsMdeadl_20040211.dbg

Other debug logs are:

- `SMDEXT.dbg` for Extension Manager task
- `SMDEMF.dbg` for Extension Manager filter task (SMDEMF)
- `<Domino Data>\SMDTemp\dbsetup.log` for ScanMail database setup debug logs

ScanMail saves all debug files to the `\SMDtemp` folder under the Domino Data directory.
# Understanding ScanMail Error Messages

The following table explains the most common ScanMail messages that may appear on the Domino server console:

<table>
<thead>
<tr>
<th>MESSAGE</th>
<th>CAUSE</th>
<th>WHAT TO DO</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMDreal: Unable to create message queue. Restart Domino server.</td>
<td>Domino server may not be running properly.</td>
<td>Restart the Domino server.</td>
</tr>
<tr>
<td>SMDreal: Unable to initialize common message. Unload and then reload SMDreal.</td>
<td>Message files are missing.</td>
<td>Uninstall, and then re-install ScanMail.</td>
</tr>
<tr>
<td>SMDreal: Unable to initialize scan engine. Check the scan engine and pattern file.</td>
<td>The scan engine or pattern file is missing.</td>
<td>Uninstall, and then re-install ScanMail. Create a policy in smconf.nsf, and then load smdreal again</td>
</tr>
<tr>
<td>SMDreal: Missing Extension Manager in notes.ini. Re-install ScanMail.</td>
<td>ScanMail was installed using a wrong installation package. Alternatively, ScanMail was removed manually.</td>
<td>Uninstall, and then re-install ScanMail.</td>
</tr>
<tr>
<td>SMDreal: Invalid Activation Code. Activate ScanMail via the Configuration Database and then reload SMDreal.</td>
<td>Activation Code (AC) was not entered during ScanMail installation. Alternatively, an invalid AC was entered.</td>
<td>Enter a valid AC using the ScanMail Configuration Database &gt; Administration &gt; Product License document. See Registering and Activating SMID on page 2-63.</td>
</tr>
<tr>
<td>SMDreal: The trial period has expired. Obtain a Registration Key and then activate ScanMail.</td>
<td>An AC trial version was entered during installation, and the AC already expired.</td>
<td>See Renew SMID Maintenance on page 2-65</td>
</tr>
<tr>
<td>SMDreal: Unable to load policy. Check Configuration Database and then reload SMDreal.</td>
<td>The Configuration Database might be corrupt.</td>
<td>Reinstall ScanMail.</td>
</tr>
<tr>
<td>SMDreal: Unable to load Message Database. Check smmsg.nsf and then reload SMDreal.</td>
<td>smmsg.nsf (ScanMail Message Database) might be corrupt.</td>
<td></td>
</tr>
</tbody>
</table>
## Trend Micro™ ScanMail™ for IBM Domino™ Administrator's Guide

**Message** | **Cause** | **What To Do**
---|---|---
**SMDdbs: Invalid database list settings.** Check the database list in the Manual or Scheduled scan rule setting. | The format of the database list in the Configuration Database is incorrect. | Check Databases to Scan list in the Real-time Database Scan, Scheduled Scan, or Manual Scan documents. Use semicolons to separate multiple entries. |
**SMDreal: Unable to read Domino directory. Check server status.** | The fully qualified name (FQDN) of the Domino server is empty. Alternatively, other Domino configuration is wrong. | Correct the Domino settings. |
**SMDreal: Cannot open database {database name}. Check the database name in the Configuration Database.** | ScanMail cannot open the database when trying to scan the special document in that database. Probably, the database was deleted before ScanMail was able to scan it. | No action needed. |
**SMDdbs: Cannot read Database Scan settings. Check Configuration Database.** | Database Scan setting is incorrect. | Check database scan rule (see Creating Real-time Database Scan Rules on page 4-14). |
**SMDupd: Unable to run multiple instances** | Scheduled update, manual update, or update task from the Control Manager server are running at the same time. | Wait until an update is finished, then run another update task. |
## Troubleshooting

### SMDupd: Invalid parameter

The Update task only accepts 4 kinds of format parameter, which represent update that was triggered from 3 different sources. If the parameter did not follow the required format, this message will be displayed.

- **Check the manual scan document or scheduled update rule (see Running Manual Scan on page 4-69 or Updating Components on page 6-3).**

### SMDupd: Unable to initialize the update task

Unable to obtain the correct update settings or ActiveUpdate cannot be invoked.

- **Check the network connection and the proxy server connection and configuration. Refer to <ScanMail Installation Path>\AU_Log\TmuDump.txt for details.**

### SMDupd: Unable to set up connection. Check network connection. Refer to ScanMail Help > Troubleshooting section for details.

Connection to the ActiveUpdate server cannot be established.

- **Check the network connection and the proxy server connection and configuration. Refer to <ScanMail Installation Path>\AU_Log\TmuDump.txt for details.**

### SMDupd: Unable to download components. Check server status or refer to ScanMail Help > Troubleshooting section for details.

Network congestion or unable to perform integrity checking for the downloaded component.

- **Refer to <ScanMail Installation Path>\AU_Log\TmuDump.txt for details.**

### SMDupd: Unable to update component(s), the Activation Code already expired.

AC already expired.

- **See Renew SMID Maintenance on page 2-65**

### SMDupd: Unable to update to the latest version. Refer to ScanMail Help > Troubleshooting for details.

Connection to the ActiveUpdate server cannot be established or unable to perform integrity checking for the downloaded component.

- **Check the network connection and the proxy server connection and configuration. Refer to <ScanMail Installation Path>\AU_Log\TmuDump.txt for details.**

### SMD Loader: The executable file exceeds the allowable maximum size (maximum size)

The path name of executable file is too long. This could be caused by multiple cascading subdirectories or long file names.

- **Reinstall ScanMail on a directory with a short path name.**

<table>
<thead>
<tr>
<th>MESSAGE</th>
<th>CAUSE</th>
<th>WHAT TO DO</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMDupd: Invalid parameter</td>
<td>The Update task only accepts 4 kinds of format parameter, which represent update that was triggered from 3 different sources. If the parameter did not follow the required format, this message will be displayed.</td>
<td>Check the manual scan document or scheduled update rule (see Running Manual Scan on page 4-69 or Updating Components on page 6-3).</td>
</tr>
<tr>
<td>SMDupd: Unable to initialize the update task</td>
<td>Unable to obtain the correct update settings or ActiveUpdate cannot be invoked.</td>
<td>Check the network connection and the proxy server connection and configuration. Refer to &lt;ScanMail Installation Path&gt;\AU_Log\TmuDump.txt for details.</td>
</tr>
<tr>
<td>SMDupd: Unable to set up connection. Check network connection. Refer to ScanMail Help &gt; Troubleshooting section for details.</td>
<td>Connection to the ActiveUpdate server cannot be established.</td>
<td>Check the network connection and the proxy server connection and configuration. Refer to &lt;ScanMail Installation Path&gt;\AU_Log\TmuDump.txt for details.</td>
</tr>
<tr>
<td>SMDupd: Unable to download components. Check server status or refer to ScanMail Help &gt; Troubleshooting section for details.</td>
<td>Network congestion or unable to perform integrity checking for the downloaded component.</td>
<td>Refer to &lt;ScanMail Installation Path&gt;\AU_Log\TmuDump.txt for details.</td>
</tr>
<tr>
<td>SMDupd: Unable to update component(s), the Activation Code already expired.</td>
<td>AC already expired.</td>
<td>See Renew SMID Maintenance on page 2-65</td>
</tr>
<tr>
<td>SMDupd: Unable to update to the latest version. Refer to ScanMail Help &gt; Troubleshooting for details.</td>
<td>Connection to the ActiveUpdate server cannot be established or unable to perform integrity checking for the downloaded component.</td>
<td>Check the network connection and the proxy server connection and configuration. Refer to &lt;ScanMail Installation Path&gt;\AU_Log\TmuDump.txt for details.</td>
</tr>
<tr>
<td>SMD Loader: The executable file exceeds the allowable maximum size (maximum size)</td>
<td>The path name of executable file is too long. This could be caused by multiple cascading subdirectories or long file names.</td>
<td>Reinstall ScanMail on a directory with a short path name.</td>
</tr>
</tbody>
</table>
Configuring Exceptions for Directories

If you install ScanMail for Domino on the server, where another anti-virus software is also installed, the other anti-virus software may prevent SMID from implementing anti-virus processes correctly. To let SMID perform proper scanning, you need to configure the other anti-virus software to exclude the Domino server and the following SMID directories out of the scope of anti-virus detection process.

- ScanMail for Domino management database:
  C:\Program Files\IBM\Domino\data\smd

- ScanMail for Domino working directory:
  Select the target server from ScanMail Configuration > Configuration > Server Settings. The path shown in Temporary Directory is the temporary directory to be used by SMID for scanning.

- Notes Temporary Directory:
  C:\Windows\Temp\notes***

IBM Notes may create temporary files in the temporary directory, and may conflict with the scan performed by another product.
- Temporary Directory for recording log files or updating components:
  C:\Program Files\IBM\Domino\data\smdtemp

**Note:** SMID creates the `smdtemp` directory during installation. If an anti-virus software, such as ServerProtect, scans the `smdtemp` directory, it may affect SMID performance.
Trend Micro is committed to providing service and support that exceeds our users’ expectations. This chapter contains information on how to get technical support. Remember, you must register your product to be eligible for support.

This chapter includes the following topics:

- **Before Contacting Technical Support** on page 12-2
- **Contacting Technical Support** on page 12-2
- **Reporting Spam and False Positives to Trend Micro** on page 12-3
- **Introducing TrendLabs** on page 12-3
- **Other Useful Resources** on page 12-4
Before Contacting Technical Support

Before contacting technical support, two things you can quickly do to find a solution to your problem:

- **Check your documentation:** the manual and online help provide comprehensive information about ScanMail. Search both documents to see if they contain your solution.
- **Visit our Technical Support Web site:** our Technical Support Web site contains the latest information about all Trend Micro products. The support Web site has answers to previous user inquiries.

To search the Knowledge Base, visit

http://esupport.trendmicro.com/support/supportcentral/supportcentral.do

Contacting Technical Support

In addition to phone support, Trend Micro provides the following resources:

- **Email support**
  
  support@trendmicro.com

- **Help database-** configuring the product and parameter-specific tips

- **Readme-** late-breaking product news, installation instructions, known issues, and version specific information

- **Knowledge Base-** technical information procedures provided by the Support team:
  
  http://esupport.trendmicro.com/support/supportcentral/supportcentral.do

- **Product updates and patches**
  
  http://www.trendmicro.com/download/

To locate the Trend Micro office nearest you, open a Web browser to the following URL:

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

To speed up the problem resolution, when you contact our staff please provide as much of the following information as you can:

- **Product Activation Code**
• ScanMail Build version
• Exact text of the error message, if any
• Steps to reproduce the problem

**Reporting Spam and False Positives to Trend Micro**

To report a spam email message, forward the message, including all headers, to:
spam@support.trendmicro.com

To report messages that ScanMail incorrectly identified as spam (a false positive), forward the message, including all headers, to:
false@support.trendmicro.com

Trend Micro regularly updates the anti-spam rule and engine with information from the messages you provide. Your assistance helps reduce future spam and false positive messages.

**Introducing TrendLabs**

Trend Micro TrendLabs is a global network of antivirus research and product support centers that provide continuous 24 x 7 coverage to Trend Micro customers around the world.

Staffed by a team of more than 250 engineers and skilled support personnel, the TrendLabs dedicated service centers in Paris, Munich, Manila, Taipei, Tokyo, and Irvine, CA. ensure a rapid response to any virus outbreak or urgent customer support issue, anywhere in the world.

The TrendLabs modern headquarters, in a major Metro Manila IT park, has earned ISO 9002 certification for its quality management procedures in 2000 - one of the first antivirus research and support facilities to be so accredited. Trend Micro believes TrendLabs is the leading service and support team in the antivirus industry.
Other Useful Resources


Internet-based tools and services include:

• Virus Map—monitors virus incidents around the world
• HouseCall™—Trend Micro online virus scanner
• Virus risk assessment— the Trend Micro online virus protection assessment program for corporate networks
Appendix A

Understanding Threats in a Domino Environment

ScanMail stops the spread and acquisition of computer malware (both known and unknown) in an IBM Notes environment.

This appendix includes the following sections:

• Understanding Malware on page A-2
• How Malware Spreads in a Notes Environment on page A-5
Understanding Malware

Malware refers to any program that executes and performs activities that are outside of the user's consent. A virus is a form of malware. Other examples of malware include Trojans, Worms, Backdoors, Denial of Service attacker agents, Joke programs, and several other smaller categories of malicious code.

Viruses are just part of a large of group of malicious programs called malware, coined from the two words “malicious software”. When we say “malicious”, we mean that the program is doing something outside of our knowledge or consent. Calling every type of malware a virus would be like calling every kind of vehicle that you see on the street a car, when in fact some are not.

We often associate the term “viruses” with any type of malicious code. That is incorrect, as not every malicious code is a virus.

In fact, malware is the best term to describe malicious code. Malware has many sub-categories including:

- Viruses
- Worms
- Trojans
- Joke programs

Descriptions for each sub-category are provided below.

Viruses

A computer virus is a segment of code that has the ability to replicate. Viruses usually replicate by infecting files. When a virus infects a file, it attaches a copy of itself to the file in such a way that when the former is executed, the virus is also run. When this happens, the infected file also becomes capable of infecting other files.

Generally, there are three kinds of viruses:

- File
  File viruses may come in different types—there are DOS viruses, Windows viruses, macro viruses, and script viruses. All of these share the same characteristics of viruses except that they infect different types of host files or programs.
• Boot

Boot viruses infect the partition table of hard disks and boot sector of hard disks and floppy disks.

• Script

Script viruses are viruses 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 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 can be activated simply by double-clicking a *.vbs or *.js file from Windows Explorer.

What is so special about script viruses? Unlike programming binary viruses, which require assembly-type programming knowledge, virus authors programs script viruses 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 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, 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. These types of viruses can infect files belonging to different platforms (for example, Windows and Linux). However, such viruses are very rare and seldom achieve 100% functionality.
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 via network connections or email attachments. Unlike viruses, 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 also use chat applications such as ICQ, AIM, mIRC, or other Peer-to-Peer (P2P) programs to spread copies of themselves.

Trojan Horses

A Trojan horse is a destructive program that comes concealed in software that not only appears harmless, but also comes in a particularly attractive form (such as a game or a graphics application). There may be instances when a Trojan does not have a destructive payload. Instead, it may contain routines that can compromise the security of your system or the entire network. These types of Trojans are often referred to as Backdoor Trojans.

Trojans are non-replicating malware – they do not replicate by themselves and they rely on the user to send out copies of the Trojan to others. They sometimes achieve this by hiding themselves inside desirable software (that is, computer games or graphics software), which novice users often forward to other users.

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.

Web Reputation

The Web Reputation features now provided with ScanMail for IBM Domino help ensure that Web pages users access are safe and free from Web threats, like malware, spyware, and phishing scams, which are designed to trick users into providing personal information. The Web Reputation functionality contained in SMID identifies unsafe URLs in email according to their reputation rating. Additionally, the administrator can add additional URLs to this list. See Configure Web Reputation on page 4-36.

When enabled, Web Reputation queries Trend Micro servers to obtain ratings, which are correlated with 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. Web Reputation queries Trend Micro servers for the reputation rating when an email message with a URL in the message body is received. Depending on the configuration, Web Reputation can quarantine, delete, or tag the email message that contains these URLs.

How Malware Spreads in a Notes Environment

ScanMail provides constant detection and protection of the three points of entry where the Notes Client environment is most vulnerable:

- Email transmissions—ScanMail performs real-time scanning on all incoming and outgoing email messages and their attachments to stop malware from entering your system, or infecting someone else’s (for example, a customer)

- Client database accesses—ScanMail monitors database files that are modified in real time to prevent viruses from being archived among your stored database documents
• Replications—ScanMail checks all files modified through the Notes database replicator in real time to keep viruses from being replicated from other Notes servers.

**FIGURE A-1.** A virus infected document spreading in a Notes environment.

In addition to real-time scan, ScanMail helps end the cycle of recurring infections with manual or scheduled sweeps of the entire database and mail message attachments. See *Types of Scans* for introduction to ScanMail scanning.
Appendix B

ScanMail for IBM Domino Best Practices

This appendix provides the best practices for optimized operations and maximum performance of ScanMail. This includes:

- *Tuning the Domino Server* on page B-2
- *Performance Recommendations* on page B-2
Tuning the Domino Server

Trend Micro recommends the following settings for servers running ScanMail for IBM Domino:

- (Windows only) Set HKEY_Local_Machine\System\CurrentControlSet\Control\PriorityControl\Win32PrioritySeparation to 0 rather than the default value of 24, in accordance with IBM recommendations for better server performance.
- (All platforms) Create two Mail.box databases (mail routing databases) to load balance message throughput based on workload
  
  Review Domino documentation for additional recommendations.

Performance Recommendations

Using the ScanMail for IBM Domino memory-based scanning feature improves scanning performance. Memory can be allocated to ScanMail for real-time replication, email, and database scanning, and manual and scheduled database scanning.

When scanning, detecting, and cleaning viruses, at least two SMDreal tasks are recommended for most environments. When enabling spam scanning and filter policies, additional SMDreal tasks are recommended.

Note: Trend Micro continually assesses whether different filtering rule structures have different performance ramifications.

The recommendations found in this Appendix are subject to change without prior notice. Please consult Trend Micro support to ensure up-to-date information.
Appendix C

Program File and Folder Lists

This appendix provides a list of the ScanMail files and folder structures. These files and folders are available upon a successful application installation.

For the list of installation and uninstallation logs, see Locating Installation and Uninstallation Logs on page 11-2.
### ScanMail for Windows

Refer to Table C-1 for the list of files created by a successful ScanMail and Control Manager agent installation on a Windows server.

<table>
<thead>
<tr>
<th>FILE/FOLDER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>...\IBM\Domino ndbsetup.exe nSMDcm.exe nSMDdbs.exe nSMDDTAS.exe nSMDEUQ.exe nSMDemf.exe nSMDext.dll nSMDmon.exe nSMDrreal.exe nSMDsch.exe nSMDaupp.exe nSMDupd.exe smd.ini</td>
<td>Contains the ScanMail loader, filter, extension manager, end-user quarantine, dbsetup, and ScanMail configuration files.</td>
</tr>
<tr>
<td>...WINDOWS\smdeys.ini</td>
<td>The main ScanMail for IBM Domino configuration file</td>
</tr>
<tr>
<td>...\Program Files\Trend Micro\ScanMail for Domino</td>
<td>The ScanMail for IBM Domino default installation folder</td>
</tr>
<tr>
<td>...\engine</td>
<td>Contains the TMASE and virus scan engine folders</td>
</tr>
<tr>
<td>...\engine\atse</td>
<td>Contains the Trend Micro Advanced Threat Scan engine</td>
</tr>
<tr>
<td>...\engine\tmase</td>
<td>Contains the Trend Micro Anti-spam Engine (TMASE)</td>
</tr>
<tr>
<td>...\engine\tmufe</td>
<td>Contains the Trend Micro tmufe engine</td>
</tr>
<tr>
<td>...\engine\vsapi</td>
<td>Contains the Trend Micro scan engine</td>
</tr>
<tr>
<td>...\pattern</td>
<td>Contains the TMASE and virus scan rule/pattern folders</td>
</tr>
<tr>
<td>...\pattern\tmase</td>
<td>Contains the TMASE rule files</td>
</tr>
<tr>
<td>...\pattern\vsapi</td>
<td>Contains the virus pattern file, spyware pattern and Intellitrap pattern files</td>
</tr>
<tr>
<td>...\program</td>
<td>Contains the ScanMail readme file and the binary and configuration file folders</td>
</tr>
<tr>
<td>...\program\V5.#.#.#####</td>
<td>Contains the ScanMail binary and configuration files</td>
</tr>
</tbody>
</table>
ScanMail for Linux

Refer to Table C-2 for the list of files created by a successful ScanMail and Control Manager agent installation on a Linux server.

**Table C-2. ScanMail files and folders available on a Linux server**

<table>
<thead>
<tr>
<th>FILE/FOLDER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>...\Uninstall</td>
<td>Contains the ScanMail uninstall program</td>
</tr>
<tr>
<td>...IBM\Domino\Data\smd</td>
<td>Contains the ScanMail databases and templates under the Domino Data directory</td>
</tr>
<tr>
<td>...IBM\Domino\Data\smd\temp</td>
<td>Contains the Setup <em>dbsetup.log</em> and the temporary files used by the ScanMail scan tasks under the Domino Data directory.</td>
</tr>
<tr>
<td>...IBM\Domino\Data\smd\temp</td>
<td>The ScanMail folder used to extract temporary files for scanning.</td>
</tr>
</tbody>
</table>

**Table C-1. ScanMail files and folders available on a Windows server**

<table>
<thead>
<tr>
<th>FILE/FOLDER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>...\Uninstall</td>
<td>Contains the ScanMail uninstall program</td>
</tr>
<tr>
<td>...IBM\Domino\Data\smd</td>
<td>Contains the ScanMail databases and templates under the Domino Data directory</td>
</tr>
<tr>
<td>.../engine/atse</td>
<td>Contains the Trend Micro Advanced Threat Scan engine</td>
</tr>
<tr>
<td>.../engine/tmase</td>
<td>Contains the Trend Micro Anti-spam Engine (TMASE)</td>
</tr>
<tr>
<td>.../engine/vsapi</td>
<td>Contains the Trend Micro scan engine</td>
</tr>
<tr>
<td>.../pattern/tmase</td>
<td>Contains the TMASE rule files</td>
</tr>
<tr>
<td>.../pattern/vsapi</td>
<td>Contains the virus, spyware, and Intellitrap pattern files</td>
</tr>
<tr>
<td>.../engine/tmufe</td>
<td>Contains the Trend Micro tmufe engine</td>
</tr>
<tr>
<td>.../program</td>
<td>Contains the ScanMail readme file and the binary and configuration file folders</td>
</tr>
</tbody>
</table>
### TABLE C-2. ScanMail files and folders available on a Linux server

<table>
<thead>
<tr>
<th>FILE/FOLDER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| .../program/V5.#.#.#### | Contains the ScanMail binary and configuration files. Where:  
  - .#.# (the first two) indicate the minor version  
  - #### (the last four #) indicate the build number |
| /opt/lotus/notes/latest/ibm-pow  
  ...libsmdext.a  
  ...smdcm  
  ...smdubs  
  ...smdtas  
  ...smdueq  
  ...smdemf  
  ...smdmon  
  ...smdreal  
  ...smdsch  
  ...smdsupp  
  ...smdupd | Contains the ScanMail configuration, binary, and database files under the Domino Program directory. The Domino Program directory can however, be any other folder. |
| .../smd | Contains the ScanMail databases and templates under the Domino Data directory |
| .../smdtemp | Contains the Setup `dbsetup.log` and the temporary files used by the ScanMail scan tasks under the Domino Data directory. |
| .../smd/smdtemp | The ScanMail default folder used to extract temporary files for scanning which is under the Domino Data directory. |
Appendix D

SMID 5.6 SP1 and SMID 5.8 Feature Comparison

The following table presents a comparison of Trend Micro ScanMail for IBM Domino (SMID) 5.6 SP1 and SMID 5.8.
# TABLE D-1. SMID 5.6 SP1 and SMID 5.8 feature comparison

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>INSTALLATION/PLATFORM SUPPORT</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supports Domino 6.5.x</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports Domino 6.0.x</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports Domino 5.0.13a, 5.0.12, 5.0.11</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports Domino 7.0.2, 7.0.3, 8.0</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Supports Domino 8.0.1, 8.0.2, 8.5, 8.5.1, 8.5.2, 8.5.3, 8.5.4, Domino 9, and Domino 9.0.1</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Domino 10, and Domino 10.0.1</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Linux 32-bit</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Supports Linux 64-bit</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Windows 32-bit</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Supports Windows 64-bit</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports cluster server (full support with task on each server and trusting)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports partitioned servers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Simultaneous installation on multiple partitions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scripted/silent installation on all platforms</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Preparation for replication during installation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configuration of ACL during installation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Database signing during installation</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Database signing with alternate ID/password or skip signing</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Replicates Configuration database across platforms</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports installation parameterization</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multi-instance support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### TABLE D-1. SMID 5.6 SP1 and SMID 5.8 feature comparison (Continued)

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supports new CM and Management Communication Protocol (MCP) Agents</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SUPPORTED DOMINO APPLICATIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Domino Database (.nsf)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IBM Domino Web Access (formerly iNotes Web Access)</td>
<td>Limited</td>
<td>Limited</td>
</tr>
<tr>
<td>Native 64-bit support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>PRODUCT ACTIVATION</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trend Micro Online Registration system</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>One Activation Code (either for ScanMail for IBM Domino or ScanMail for IBM Domino Suite)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Activation Code (Suite with Data Loss Prevention)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SCANNING (GENERAL)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multi-threaded scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multi-threaded scan tasks</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Separate actions for Adware/Spyware</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>MAIL SCANNING</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time scan</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced Threat scan</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mail scan rule based on mail sender/recipient</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Different scan settings for users/groups with exceptions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduled scanning with different settings at different times</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Virus cleaning upon detection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable action upon detection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Nested compressed file scanning with selectable scanning depth</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### TABLE D-1. SMID 5.6 SP1 and SMID 5.8 feature comparison (Continued)

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>MIME/HTML body scanning for script viruses</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Malicious notes script, hot spots, and URL scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Signature-based scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports trusted antivirus server(s) to avoid rescanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Selectively scans embedded OLE objects</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IntelliTrap support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Office 2007 support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Office 2010 support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Decompression algorithm support RAR, SFX, CHM, NSIS, and ZIP SFX files</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**ANTI-SPAM**

| Anti-spam support                                                       | Yes          | Yes      |
| End User Quarantine                                                    | Yes          | Yes      |
| Enables End User Quarantine for specified users/groups                  | Yes          | Yes      |
| Deploys End User Quarantine to mail templates                          | Yes          | Yes      |

**GRAYMAIL FILTERING**

| Graymail support                                                       | Yes          | Yes      |
| Enables End User Quarantine for graymail                               | Yes          | Yes      |
| Gateway IP address notification                                         | Yes          | Yes      |

**WEB REPUTATION**

| Web reputation support                                                 | Yes          | Yes      |
| Local Web reputation support                                            | Yes          | Yes      |
| Web reputation notification                                             | Yes          | Yes      |
| Supports the “Ransomware” category                                      | No           | Yes      |

**ADWARE DETECTION**
### TABLE D-1.  SMID 5.6 SP1 and SMID 5.8 Feature Comparison (Continued)

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configurable action upon detection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>SPYWARE DETECTION</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Configurable action upon detection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>MAIL/BANDWIDTH MANAGEMENT</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Redirects email for approval</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports selectable grouping of file types</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>APT Prevention Filter</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable attachment blocking by true file type (individual file types)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable action for Microsoft Office macros</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable attachment blocking by extension or filename</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable attachment blocking by true file type (group)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Strips macros from Microsoft Office documents</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Delays mail according to a specific schedule</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blocks mail depending on size</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Lower priority setting</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blocks mail based on the attachment’s true file type</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Blocks mail based on the attachment’s file or extension name</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>CONTENT FILTERING (REQUIRES ScanMail for IBM Domino Suite / eManager)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message header field scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Filters for text in message body</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Filters for text in message attachment</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Regular expression support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Office 2007 file support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### TABLE D-1. SMID 5.6 SP1 and SMID 5.8 feature comparison (Continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Office 2010 file support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Additional OLE layer scanning support for a maximum of 20-layers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses heuristics technology</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Approved/Blocked Senders lists</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable filter sensitivity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses rule file</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Real-time scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduled scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable time period for multiple real-time scanning config</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Script scanning support in real-time scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduled scanning within defined time periods (maximum duration)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for several scheduled scans with different settings</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resume a scan that did not finish</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Script scanning support in scheduled scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable scan schedule through Configuration database</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>Data Loss Prevention Filtering</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Message header field scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Filters for text in message body</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Filters for text in message attachment</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Office 2007/2010 file support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Additional OLE layer scanning support for a maximum of 20-layers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
**TABLE D-1. SMID 5.6 SP1 and SMID 5.8 feature comparison (Continued)**

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Uses heuristics technology</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Specify file names to be excluded from all data loss prevention filters</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable filter sensitivity</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Uses rule file</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Real-time scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduled scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DLP rule support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DLP logical operation</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Non-email documents scanning support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports &quot;Mask content and pass&quot; action</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Manual scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable time period for multiple real-time scanning configurations</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Script scanning support in real-time scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Scheduled scanning within defined time periods (maximum duration)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Support for several scheduled scans with different settings</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Resume a scan that did not finish</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Script scanning support in scheduled scanning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable scan schedule through configuration database</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**ADMINISTRATION**

<table>
<thead>
<tr>
<th>Feature</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full integration with R6/5 Administrator Client and Notes Client</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Lotus Notes 7/8 support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IBM Notes 9 support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### TABLE D-1.  SMID 5.6 SP1 and SMID 5.8 feature comparison (Continued)

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Notes 10 support</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote administration through a Web interface</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Remote administration through a Notes Client</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User interface uses frames and follows the latest Trend Micro standard</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server status monitoring available through user interface</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Server task watch dog</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Task status monitoring</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Share server settings and antivirus policies between servers and groups of servers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>User-defined and controlled rules to define actions</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Ability to define rules based on users and groups</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Configurable server settings that are policy-independent</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Role-based access configurable through the Notes interface</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>One-button information collector (Support Tool)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Antivirus and Content Security Component Updates

<table>
<thead>
<tr>
<th>Feature</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual update</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Select components and set recurring scheduled updates</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automated pattern update through ActiveUpdate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automated scan engine update through ActiveUpdate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automated program updates through ActiveUpdate</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Pattern/Engine integrity check after update</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Product integrity check after update</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Table D-1. SMID 5.6 SP1 and SMID 5.8 feature comparison (Continued)

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>SMID 5.6 SP1</th>
<th>SMID 5.8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full and Small pattern download support for TMASE.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>IntelliTrap pattern update support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>NOTIFICATION OPTIONS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customized notifications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Notifications via IBM Instant Messaging (ScanMail for Domino for Windows only)</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Sender, recipient, or administrator notifications</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Separate notifications to internal/external users</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Rich text configurable message</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports notification insertion in a MIME email</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Safe stamp in the message subject</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Safe stamp in Notes message body</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Safe stamp in SMTP message body</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Multiple disclaimer support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Single disclaimer inserted when an email passes multiple servers</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports disclaimer positioning</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>QUARANTINE</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Automatically deletes quarantined logs based on type, age, and records to retain</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports resend/restore of quarantined items</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports forwarding of quarantined items</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>LOGGING/STATISTICS</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exports statistics to a Microsoft Excel spreadsheet</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Automatically deletes logs</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Identify the sender of an infected message</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>FEATURE</td>
<td>SMID 5.6 SP1</td>
<td>SMID 5.8</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------</td>
<td>----------</td>
</tr>
<tr>
<td>Identify infected file</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports Threat Connect information portal access</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Records the recipient information</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Records the action taken on a threat</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Graphical email statistics/reports</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Log search</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Index

A
accessing help 3
ACL entry 19
action on
  cleanable virus 44
  other malware 44
  specific threats 44
  uncleanable virus 44
anti-spam engine 3
anti-spam rule 2
antivirus. See components
audience cxii
character set 12
charts 9
checking debug logs 8
components 2
  anti-spam engine 3
  anti-spam rule 2
  program files 3
  scan engine 2
ScanMail for Domino application 3
signature file. See also virus pattern file
spyware pattern 2
unable to download 3
virus pattern file 2
anti-spam filtering 26, 36
attachment filtering 52
content filtering 55, 64
general mail scan rule settings 13
message filtering 48
redirect options 67
scan restrictions 47
script filtering 66
security risk scanning 41
expressions 24
content security. See components
Control Manager
  agent 3
  agent for ScanMail 3
  Enterprise edition 2
  features 2
  manage ScanMail 5
  OPP 7
  outbreak prevention 4
  server 2
  Standard edition 2
  using 5
  using ScanMail with 2
convention
document cxii
creating
  content filter 56
  expressions 59
  policies 3
  rules 9
  server settings rule 3
customizing notifications 3
database
  log 2
  quarantine 13
A
accessing help 3-3
ACL entry 5-19
action on
cleanable virus 4-44
other malware 4-44
specific threats 4-44
uncleanable virus 4-44
anti-spam engine 6-3
anti-spam rule 6-2
antivirus. See components
audience 1-clxxix
C
character set 5-12
charts 8-9
checking debug logs 11-8
components 6-2
anti-spam engine 6-3
anti-spam rule 6-2
program files 6-3
scan engine 6-2
ScanMail for Domino application 6-3
signature file. See also virus pattern file
spyware pattern 6-2
unable to download 11-3
virus pattern file 6-2
configuring
anti-spam filtering 4-26, 4-36
attachment filtering 4-52
content filtering 4-55, 4-64
general mail scan rule settings 4-13
message filtering 4-48
redirect options 4-67
scan restrictions 4-47
script filtering 4-66
security risk scanning 4-41
content filter 4-24
expressions 4-24
content security. See components
Control Manager
agent 9-3
agent for ScanMail 9-3
Enterprise edition 9-2
features 9-2
manage ScanMail 9-5
OPP 9-7
outbreak prevention 9-4
server 9-2
Standard edition 9-2
using 9-5
using ScanMail with 9-2
customizing notifications 7-3
D
database
log 8-2
quarantine 8-13
Database Catalog 5-18
databases
recovering 11-5
recreating 11-6
debug logs 11-8
checking 11-8
debugging 11-7
levels 11-8
results 11-8
ScanMail tasks 11-7
deleting logs
automatically 8-8
manually 8-9
digital signature 6-10
disclaimers 4-68
document conventions 1-clxxx

E
email stamps 7-6
error messages 11-9
exporting
charts 8-11
statistics 8-10
expressions 4-24

F
false positives 4-27, 4-38, 12-3
filtering
anti-spam 4-26, 4-36
content 1-12, 4-21
message 1-11, 4-21
order 4-20
script 1-12, 4-21
filters 1-11, 4-20

H
help 3-3

I
incoming messages 4-22
inserting disclaimers 4-68
installing
ScanMail 2-1
interface 3-2

J
joke programs A-4

L
loading components 6-12
Log Database 8-2
logs 8-2
  deleting virus logs 8-8
  automatically 8-8
manually 8-9
managing 8-4

M
mail scan rules 4-13
general settings 4-13
malware A-2
  joke programs A-2
  spread A-5
  trojans A-2
  viruses A-2
    boot A-3
    file A-2
    script A-3
  worms A-2
management console 9-5
manual 1-8
manual scan 4-70
  ending manually 4-71
  terminating 4-71
  via Configuration Database 4-70
  via Domino server console 4-69
manual scanning 3-3, 4-69
memory size 5-5
Message Filter 1-11, 4-21
Microsoft Excel 8-11
miscellaneous settings 5-12
modifying
  server settings rule 5-4
monitoring server events 5-11

N
notes
  administrator notification 7-9
  attachment file name 4-46, 4-55
  attempt downloading components 7-10
  auto-clean action 4-66
  automatic log deletion 8-8, 8-17
  Cluster Trusting 4-8
compression layer 4-48
converting to full version 5-20
converting trial version 5-20
Copy Settings 4-5
corrupted document 6-17
creating a new rule 4-18
creating policies 4-5
debug levels 11-8
default policy 1-7, 4-6
deleting default policy 4-6
disclaimer names 4-68
disclaimers 4-68
Download only 6-9
downloading component 7-10
EICAR 2-65
expressions 4-58, 4-66
Extension Manager 11-8
filter order 4-21
history 6-8–6-9
inserting disclaimers 4-68
loading components manually 6-12
log deletion 8-8, 8-16
logical operator 4-58
multi-server environment 8-3
Notes database properties 5-19
Notification Template 7-6
partitioned server 2-16
pattern file condition 4-17
proxy server 5-6
recreating ScanMail databases 11-6
removing ScanMail manually 10-10, 10-13
replicating Update Database 6-10
replication schedule 2-21
rich text hotspots 4-66
routing low priority messages 4-14
scan duration 4-70
scan engine condition 4-17
scan engine history 6-8
ScanMail Suite edition 4-25
scheduled update notifications 6-6
tooltip 3-3
trusted servers 5-13
update source 6-9
virus pattern file history 6-8
notifications 7-1
about 7-2
customizing 7-3
delivery 7-7
for scan actions 7-2
for update actions 7-2
scan notifications 7-9
setting 7-9
tags 7-3
filter-based tags 7-3
rule-based tags 7-5
templates 7-9
update notifications 7-9
O
Open Database Dialog 5-18
OPP. See Outbreak Prevention Policy
OPS. See Outbreak Prevention Services
other Internet source 6-10
outbreak prevention 9-4
Outbreak Prevention Policy 9-7
viewing 9-7
Outbreak Prevention Services 9-4
P
policies
creating 4-3
modifying 4-5
planning 4-2
understanding 1-9
preface 1-clxxv
proxy server
component download 6-11
proxy server settings 5-6
proxy. See proxy server settings

Q
Quarantine Database 8-13
quarantined messages
  resending 8-14
  viewing 8-13

R
real-time database scanning 1-8
real-time mail scanning 1-7
recovering corrupt databases 11-5
recreating databases 11-6
redirecting messages 4-67
resending quarantined messages 8-14
rules
  creating 4-9
  database scan 1-11
  mail scan 1-11
  notification 1-11
  real-time database scan 4-14
  schedule 4-68
  scheduled scan 1-11
  scheduled update 1-11
  server settings 5-3

S
scan engine 6-2
scan restrictions 1-11, 4-21
ScanMail
  about 1-1–1-2
  components 1-6, 6-1
databases
  recovering 11-5
  recreating 11-6
error messages 11-9
features 1.3–1-9
interface 3-2
logs 8-4
notifications 7-1
scan types 1-7
versions comparison 1-4
server events 5-11
Server Settings 5-1
  about 5-3
server task monitoring 5-11
setting
database properties 5-18
rule schedule 4-68
scan notifications 7-9
tasks viewing 5-20
update notifications 7-9
setting rule schedule 4-68
sig 6-10
signature file. See also virus pattern file
signature files 6-10
smquar.nsf 8-13
smvlog.nsf 8-2
source. See updating
spread A-5
spyware pattern 6-2
statistics 8-9

T
tags 7-3
tags. See notification tags
temporary directories 5-5
threats. See malware
tips
  address groups 4-12
  applying the strictest rule 4-12
  components 6-3
  conditions 4-59
content filters 4-60
creating mail scan rules 4-10
creating rules 4-9
deleted license profiles 5-21
Domino threats 1-9
expressions 4-59
improving ScanMail performance 4-10
license profile 5-21
modifying configuration files 11-7
multiple databases 4-69
naming a rule 4-13
new rule 4-11
rule condition 4-59
rule conditions 4-9
rule name 4-13
scan and filter action 4-11
ScanMail action 4-11
scanning messages 4-10
strictest rule 4-12
testing expressions 4-59
threats 1-9
troubleshooting update issue 6-10
update issues 6-10
updating components 6-3
viewing ScanMail databases 3-2
TrendLabs 12-3
trojans A-4
troubleshooting 11-1
trusted cluster servers 4-7

U
uninstalling
ScanMail
automatic 10-2
Update Now 6-3
update source 6-9
updating
antivirus components 6-3
automatically 6-5
content security components 6-3
loading components manually 6-12
manually 6-3
proxy server settings 6-11
select components 6-8
source 6-9
updating components 6-3

V
verifying
Control Manager agent installation 2-66
viewing
charts 8-11
quarantined messages 8-13
statistics 8-10
summary 5-2
virus pattern file 6-2
viruses A-2

W
warning
delivering mails 5-13
mail task not running 5-13
restoring quarantined documents 8-15
Web access 5-18
ScanMail databases 3-8
Web reputation
about A-5
configuration 4-36
what’s new 1-clxxvii
who should read this document
audience 1-clxxix
worms A-4