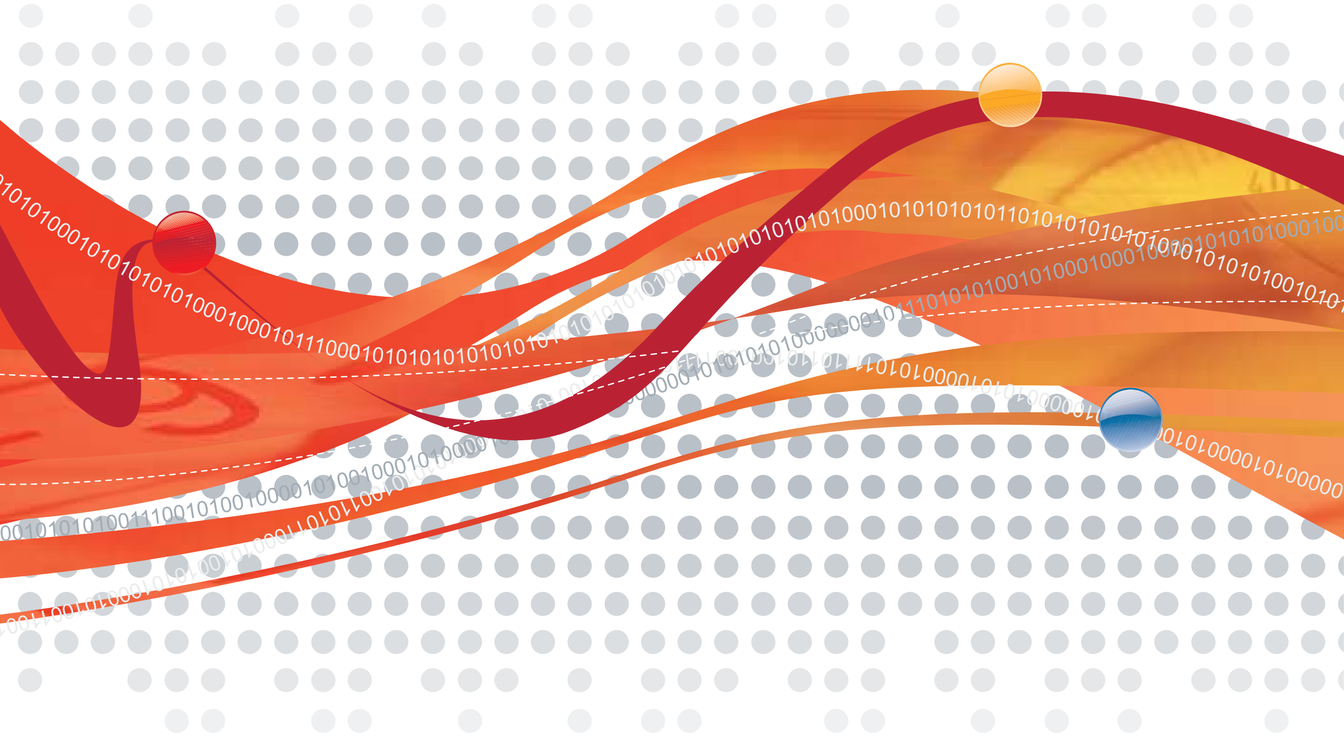
ScanMail™ for Lotus Domino 5

Proactive Antivirus and Content Security for the Domino Environment

Administrator's Guide



Messaging Security

Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the Administrator's Guide, which are available from the Trend Micro Web site at:

www.trendmicro.com/download/documentation/

NOTE: A license to the Trend Micro Software usually includes the right to product updates, pattern file updates, and basic technical support for one (1) year from the date of purchase only. Maintenance must be renewed on an annual basis at the Trend Micro then-current Maintenance fees.

This product includes software developed by the University of California, Berkeley and its contributors.

Document Part No. SNEM53989_90107

Release Date: January 2010

Protected by U.S. Patent Nos. 5,951,698 and 5,889,943

The Administrator's Guide for ScanMail for Lotus 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 Lotus Domino collects and provides detailed instructions on how to disable the specific features that feedback the information.

https://success.trendmicro.com/data-collection-disclosure

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

https://www.trendmicro.com/en_us/about/legal/privacy-policy-product.html

Preface

Preface

This Administrator's Guide describes ScanMail for Lotus Domino (SMLD) version 5.0 and provides installation and uninstallation instructions, with information to help you configure SMLD functions for your specific needs.

The ScanMail *Administrator's Guide* discusses the following topics:

- *Introducing ScanMail and ScanMail Suite for Lotus Domino 5.0* provides an overview of the product and description of all new features in this release.
- *Installing ScanMail for Lotus Domino* provides step-by-step instructions on installing ScanMail for Lotus Domino 5.0.
- *Getting Started with ScanMail* provides recommended procedures to configure SMLD after you have installed it.
- *Configuring Scan Tasks* provides procedures to create policies, rules, or expressions that SMLD 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 Lotus 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 Lotus Domino with Trend Micro Control Manager* provides details on how to use Trend Micro Control Manager™ to manage ScanMail.
- *Removing SMLD* provides procedures for removing ScanMail for Lotus Domino.
- *Troubleshooting* provides troubleshooting tips.
- *Getting Support* provides guidelines to get more information.

In addition, 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 Lotus Domino Best Practices* provides the best practices for optimized operations and maximum performance for SMLD.
- *Program File and Folder Lists* provides a list of the SMLD and Control Manager files and folder structures that are available upon a successful application installation.
- *SMD 3.0 and SMLD 5.0 Feature Comparison* provides a comparison of ScanMail for Domino (SMD) 3.0 and ScanMail for Lotus Domino 5.0 features.

What's New in Version 5.0

ScanMail for Lotus Domino represents a significant advancement in antivirus and content security for Lotus Domino environments. ScanMail Suite for Lotus Domino provides state-of-the-art detection based on heuristic rule-based scanning, recognition of Approved / Blocked Senders lists and signature databases. It includes modifiable anti-spam and content filtering functionality, which may be applied according organizational needs. Configuration improvements in version 5.0 make ScanMail more flexible and scalable than ever before.

- *New Functionality for Web Reputation*
- *Standardized Installation*
- *New Active Update (AU) Engine Support*
- *Enhanced Virus Scan Engine*
- *Enhanced Content Filtering*
- *Enhanced Anti-Spam Functionality*
- *Support New CM and Management Communication Protocol (MCP) Agents*
- *New Software / Hardware Requirements*
- *Lotus Domino 8.5 DAOS Support*

New Functionality for Web Reputation

Many emails contain URLs that may be dangerous. This release provides Web Reputation support to examine emails that contain dangerous URLs. To use this feature, you must have Anti-Spam enabled. Web reputation assigns a reputation rating to Web pages according to the assigned rating. It queries Trend Micro servers for these ratings, which are correlated from multiple sources, including Web page links, domain and IP address relationships, spam sources, and links in spam messages. By obtaining ratings online, Web reputation uses the latest available information to detect harmful URLs contained in email. The administrator can modify the Web reputation setup to determine the action to take on unsafe URLs, whether Quarantine, Block, or Pass. For more information see *Configure Web Reputation* on page 4-30, and *Web Reputation* on page A-5.

Standardized Installation

A new installation development tool has been implemented to enable a standardized installation process that looks and feels the same across all platforms. The flow of the installation remains the same as that used in previous versions. This Standardized Installation has the following features:

- Installation parameterization: this feature enables the administrator to select the path and location where ScanMail for Lotus Domino will be installed.
- Multi-instance support: SMLD 5.0 support using the Domino DPARs mode to create multiple domino versions on one machine. For example, Domino 8.5 and Domino 8.0.2 can be installed on one machine, and SMLD 5.0 will support both versions.
- Database migration from SMLD 3.0 to SMLD 5.0 (Windows only): during installation, the database schema will be updated in from SMLD 3.0 to SMLD 5.0 and includes a UI update with new replicate IDs.

New Active Update (AU) Engine Support

SMLD 5.0 provides full 64-bit processing and also provides the following Active Update support:

- Small and Full pattern download support for TMASE. Provides functionality to enable recognizing the version of all pattern updates.
- IntelliTrap pattern update support, provides functionality to allow updating IntelliTrap pattern files.

Enhanced Virus Scan Engine

- IntelliTrap support. 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.
- Microsoft Office 2007 support (Windows only). File scanning support will be added during the installation process.
- Decompression algorithm support for RAR SFX, CHM, NSIS, and ZIP SFX files. This new feature provides a broader range of support for scanning these file types.

Enhanced Content Filtering

- Regular expression support for content filter. Regular expressions like (badda|wham), will match the expression "baddabing." Enhanced Content Filtering provides functionality to use a new operator like: ".REG.". Any tokens that are followed by, ".REG." will be interpreted as a regular expression. See *Create New Expressions* on page 4-41 for more information.
- Microsoft Office 2007 file support. This release provides scanning the content of Office 2007 files.
- Additional OLE layer scanning support for a maximum of 20-layers, a minimum of one-layer, with three-layer scanning being the default.

Enhanced Anti-Spam Functionality

- New Spam categories added to both Domino console log and debug log, which include: Phishing, Malware, Suspicious, and Spam. See *Configure Anti-Spam Filtering* on page 4-27.

Support New CM and Management Communication Protocol (MCP) Agents

- Integration for TMCM MCP 5.0 agent. This feature allows all products to register to the same server, which enables users to manage SMLD functionality from a single server. After installing SMLD 5.0, the CM agent settings can be configured as follows:
  - **a.** CM Server (FQDN or IP address)
  - **b.** Port (80 for HTTP or 443 for HTTPS)
  - **c.** Web server authentication
  - **d.** Proxy

Note: Integration for TMCM MCP 5.0 agent replaces Trend Micro Infrastructure (TMI), which is not supported by SMLD 5.0.

New Software / Hardware Requirements

- Information regarding both software and hardware requirements. See *Recommended System Requirements* starting on page 2-5.

Lotus Domino 8.5 DAOS Support

- This release provides support for Lotus Domino Attachment and Object Service (DAOS).

Audience

ScanMail for Lotus Domino documentation assumes a basic knowledge of security systems and administration of Lotus™ 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 SMLD documentation

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

Contents

Preface

Chapter 1: Introducing ScanMail and ScanMail Suite for Lotus Domino 5.0

Chapter 2: Installing ScanMail for Lotus Domino

Chapter 4: Configuring Scan Tasks

Chapter 5: Performing Administrative Tasks

Chapter 6: Updating Components

Chapter 7: Sending ScanMail for Lotus Domino Notifications

Chapter 8: Using the Log and Quarantine Databases

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

Chapter 10: Removing SMLD

Chapter 11: Troubleshooting

Chapter 12: Getting Support

Appendix A: Understanding Threats in a Domino Environment

Appendix B: ScanMail for Lotus Domino Best Practices

Appendix C: Program File and Folder Lists

Appendix D: SMD 3.0 and SMLD 5.0 Feature Comparison

Chapter 1

Introducing ScanMail and ScanMail Suite for Lotus Domino 5.0

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

ScanMail Suite for Lotus Domino provides an added layer of protection through revolutionary anti-spam technologies and systematic content filtering. ScanMail Suite for Lotus 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 1-6*
- *Understanding Policies, Rules, and Filters* on page 1-9
- *ScanMail Protection Strategy* on page 1-11
- *Planning for a Policy-Based Antivirus and Content Security Protection* on page 1-12

Product Overview

ScanMail for Lotus Domino (SMLD) 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 Lotus Notes workstation, Web browser, or Domino R8 Administration Client. This version of ScanMail for Lotus Domino is designed to run on the Microsoft^{TM} Windows^{TM} and IBM^{TM} AIX^{TM} 64-bit platform.

The ScanMail Standard version provides virus scanning in all modes and component update. The ScanMail Suite version additionally provides content and spam filtering functionality.

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 Lotus 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:

http://www.trendmicro.com/en/products/global/enterprise.htm

ScanMail for Lotus Domino 5.0 Standard Features

ScanMail for Lotus Domino 5.0 Standard version features for Windows and IBM AIX includes:

- Multi-threaded in-memory scanning process for fast performance.
- 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.
- 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, and support for Lotus Instant Messaging and Web Conferencing notification.
- 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.

ScanMail for Lotus Domino 5.0 Suite Features

ScanMail for Lotus Domino 5.0 Suite version contains all the features of the Standard version and the following additional features:

- anti-spam filtering
- the ability to filter message content by subject or body text
- the ability to scan content of attached MS Office 2007 document (Windows only), PDF, .txt, .html, and .rtf files
- web reputation filtering

A brief comparison of ScanMail Suite and Standard features is shown in *Table 1-1*.

TABLE 1-1. Comparison of Features for ScanMail for Lotus Domino Standard and Suite Versions

FEATURE	STANDARD	SUITE
Antivirus	Yes	Yes
Anti-Spam	No	Yes
Web Reputation Service (WRS)	No	Yes
Content Filtering		
Subject/Body/MS Office 2007, PDF, .txt, .html, and .rtf files **Note:** Content Filtering of MS Office and Adobe PDF files are not supported in IBM AIX 64-bit.	No	Yes
Active Update	Yes	Yes
Control Manager Agent	Yes	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 Lotus Domino mail server.
- Database events are monitored and attachments are scanned immediately before a document is closed.
- Databases and modified data are scanned during replication.
- Existing attachments in mailboxes and Domino databases are scanned to root out old infections.

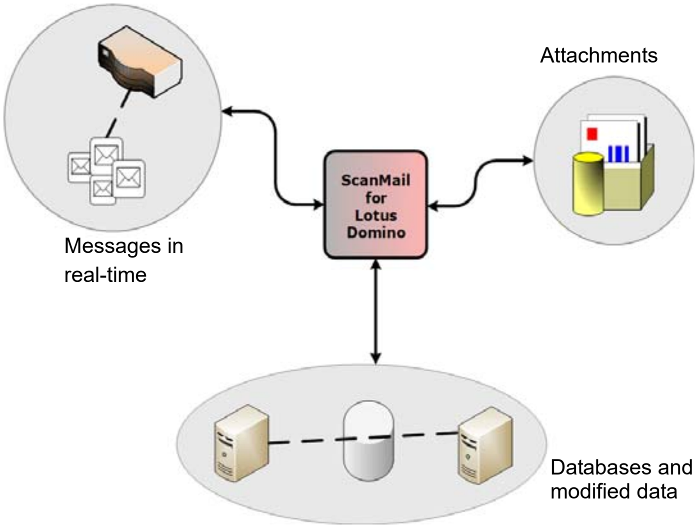


FIGURE 1-1. ScanMail detects and removes threats before infections can spread to the desktop.

ScanMail maintains a comprehensive activity log, detailing the following for each infected file:

- the origin, name, and destination of the file
- date the file was received
- identity of any virus found
- the action taken

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
- database templates
- tasks
- notes.ini entries

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, including OLE attachments and script bombs.

Note: ScanMail invokes the real-time mail scan task and applies its settings when manually scanning mail.box 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 Lotus Domino (SMLD) 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.

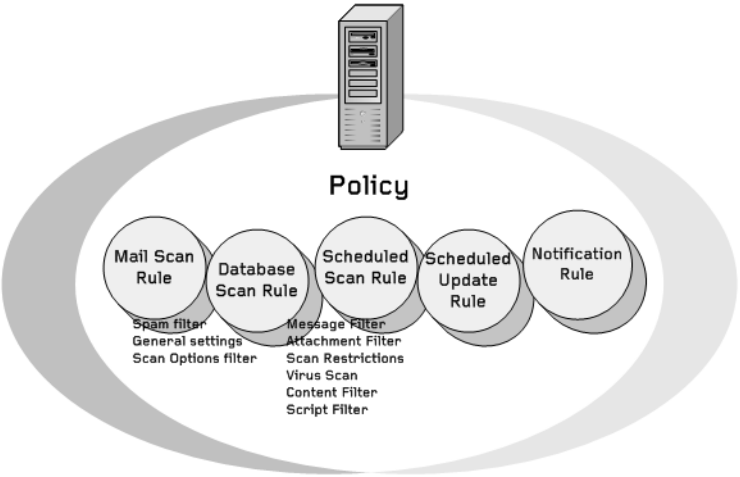


FIGURE 1-2. Policy-filter-rule relationship

ScanMail Rules

ScanMail provides the **rules** described in *Table 1-2*, which define how ScanMail scans messages and databases.

TABLE 1-2. Types of ScanMail rules

TYPE OF RULE	DEFINES HOW SCANMAIL…
Mail scan rule	scans and filters message content and attachments in real time. To create a real-time mail scan rule, see page 4-10.
Database scan rule	scans databases in real time. To create a real-time database scan rule, see page 4-15.
Scheduled scan rule	scans databases according to a schedule. To create a scheduled database scan rule, see page 4-17.
Scheduled update rule	updates antivirus and content security components. To create a scheduled update rule, see page 6-4.

TABLE 1-2. Types of ScanMail rules

TYPE OF RULE	DEFINES HOW SCANMAIL…
Notification rule	delivers a notification. To create a notification rule, see page 7-2.

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 1-3. ScanMail filtering options

FILTERING OPTION	PROVIDES OPTIONS TO SET SPECIFIC SCANNING ACTION ON…
Message Filter	various message types.
Attachment Filter	unwanted attachments.
Virus Scan	virus and other malware types.
Scan Restrictions	compressed, encrypted, and other attachment types. Virus Scan must be enabled.
Content Filter	messages with unwanted content based on administrator-defined explicit rules.
Script Filter	messages with stored form or rich text hot spot content.

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 in SMLD 5.0. 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, 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 4-8, "Recommended file extensions to block," on page 4-43* 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 Lotus Domino Suite to implement protection against unwanted spam or suspicious URL messages.
  - 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 1-6* for details about the ScanMail scan tasks.

Chapter 2

Installing ScanMail for Lotus Domino

This chapter guides you through installing ScanMail for Lotus Domino (SMLD) on Microsoft$^{\text{TM}}$ Windows$^{\text{TM}}$ and IBM$^{\text{TM}}$ AIX$^{\text{TM}}$ platforms. This chapter also lists the system requirements for ScanMail and contains post-installation configuration information and instructions on how to register and activate your software.

This chapter contains the following topics:

- *Planning ScanMail Deployment* on page 2-2
- *Testing ScanMail at One Location* on page 2-3
- *Upgrading from ScanMail 3.0 (Windows Only)* on page 2-4
- *Recommended System Requirements* on page 2-5
- *Installing ScanMail* on page 2-8
- *Starting the Domino Server* on page 2-43
- *Registering and Activating ScanMail* on page 2-44
- *Testing Installation with EICAR* on page 2-47
- *Checking ScanMail Files and Folders* on page 2-48

Planning ScanMail Deployment

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

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

- Select a Domino server in your organization that will serve as the central ScanMail server.
- Install ScanMail on the central server and enable replication of ScanMail 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 ScanMail policies to modify the Configuration database on each Domino server.
- Initiate push replication from the ScanMail 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 6-8).

Testing ScanMail at One Location

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

- Allows you to gain familiarity with ScanMail.
- 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 ScanMail at one location:

1. Prepare for a test deployment.
2. Select a pilot site.
3. Create a rollback plan.
4. Deploy and evaluate the pilot.

Preparing for a Test Deployment

During the preparation stage, complete the following activities:

- Decide on the ScanMail replication model for the test environment.

  A *hub and spokes* model is a common ScanMail replication model. In this model, the network administrator configures the ScanMail settings from the hub ScanMail 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 5.0, 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 ScanMail. 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 ScanMail

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 ScanMail test deployment and evaluation can be rolled into the overall production installation and deployment plan.

Upgrading from ScanMail 3.0 (Windows Only)

To upgrade from ScanMail 3.0 to 5.0, perform the following tasks:

1. Close any opened Notes account session.
2. Back up the ScanMail databases to save the original configuration.
3. If you are using Control Manager, remove the existing CMAgent installation.

Note: ScanMail 5.0 uses the same activation code as that used for ScanMail 3.0.

4. During installation, specify all partitioned servers on the target server with ScanMail 3.0 installed.

Note: Setup will convert ScanMail 3.0 components to ScanMail 5.0 to avoid program conflicts.

Upgrade from ScanMail 3.0 to ScanMail 5.0 is only available for Windows platform.

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 SMLD server.

ScanMail for Microsoft Windows

Table 2-4 lists the hardware and software requirements for ScanMail for Lotus Domino 5.0 for Windows.

TABLE 2-4. ScanMail for Windows Hardware and Software Requirements

Hardware / Software	***Requirement***
Processor	Intel Pentium or higher and compatibles (32-bit and 64-bit chips as appropriate), or equivalent
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	• NetBIOS over IP (32-bit processor only, only Microsoft IP is supported) • NetBIOS over IPX (32-bit processor only) • TCP/IP (includes IPv6)

TABLE 2-4. ScanMail for Windows Hardware and Software Requirements

Hardware / Software	***Requirement***
Domino Server	• Lotus Domino 8.0.1 (32/64-bit) • Lotus Domino 8.0.2 (32/64-bit) • Lotus Domino 8.5 (32/64-bit)
Platform	• MS Windows 2003 Server Standard Edition • MS Windows 2003 Server Enterprise Edition, Service Pack 2 • MS Windows 2003 Server x64 Edition
Lotus Notes	• Lotus Notes 8.0.1 • Lotus Notes 8.0.2 • Lotus Notes 8.5
Browser	• Microsoft Internet Explorer 6.0 SP2 • Microsoft Internet Explorer 7.0
Trend Micro Control Manager	• Trend Micro Control Manager 3.5 with patch 6 • Trend Micro Control Manager 5.0 with patch 3 and hotfix 1728 **Note:** Support MCP CM agent

ScanMail for IBM AIX

Table 2-4 lists the hardware and software requirements for ScanMail for Lotus Domino 5.0 for IBM AIX.

TABLE 2-5. ScanMail for IBM AIX Hardware and Software Requirements

Hardware / Software	***Requirement***
Processor	Power 4 and higher
Memory	• 512 MB minimum • 512 MB or more recommended per CPU
Disk Space	• 1.5-GB minimum per partition • 1.5 GB or more recommended per partition • 500-MB for program files • 400-MB for ***/tmp*** file system
Disk swap space	• Equal to physical RAM installed required • Twice the physical RAM installed recommended
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 8.5.1 64-bit
Lotus Notes	• Lotus notes 8.0.1 • Lotus notes 8.0.2 • Lotus notes 8.5 • Lotus notes 8.5.1
Platform	• 64-bit IBM AIX 5.3, TL7 0815 (5300-07-04-0815) • 64-bit IBM AIX 6.1, Service Pack 4, APAR IZ10223, APAR IZ09961, APAR IZ10284, APAR IZ08022

TABLE 2-5. ScanMail for IBM AIX Hardware and Software Requirements

Hardware / Software	*Requirement*
Browser	• Microsoft Internet Explorer 6.0 SP2 • Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0
Trend Micro Control Manager	• Trend Micro Control Manager 3.5 with patch 6 • Trend Micro Control Manager 5.0 with patch 4 and hotfix 1824 **Note:** Support MCP CM agent
Other	• XL C/C++ runtime lib 9.0.0.1 or later

Installing ScanMail

Read the following sections before installing ScanMail for Lotus Domino.

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

- You cannot automatically roll back to ScanMail 3.0 after installing version 5.0 (Windows only).

  To roll back to ScanMail 3.0, remove ScanMail 5.0, and then perform a fresh installation of ScanMail 3.0. Refer to the ScanMail 3.0 documentation for details on how to install this version.
- You cannot upgrade ScanMail 3.0 for AIX to ScanMail 5.0 for AIX. Consequently, you cannot roll back ScanMail 5.0 for AIX to ScanMail 3.0 for AIX.
- You cannot install both ScanMail 3.0 and ScanMail 5.0 on the same physical machine.
- You must shut down the Domino server before installing or removing SMLD.
- For partitioned servers, install a copy of ScanMail on each partition.

Pre-installation Tasks

Before installing ScanMail, perform the following tasks:

1. Log on the Windows platform as administrator or IBM AIX 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 ScanMail 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 Table 2-4, "ScanMail for Windows Hardware and Software Requirements," on page 2-5 if installing ScanMail on Windows platform. If installing ScanMail on IBM AIX platform, see Table 2-5, "ScanMail for IBM AIX Hardware and Software Requirements," on page 2-7.
6. Close any open Notes Clients.
7. Close any open Notes account sessions.
8. Shut down all Domino servers installed on this machine completely before:
   - Installing ScanMail 5.0 for the first time
   - Upgrading from ScanMail 3.0 (Windows only)
   - Removing ScanMail 5.0
9. Prepare the ScanMail Activation Code. See *ScanMail Activation Code* on page 2-45.

Once you have verified that the target server is ready, install the ScanMail program files and set up the ScanMail databases.

Setup Modes

You can use the following methods to install ScanMail:

- **Wizard-based installation** is an interactive installation that requires user input when installing SMLD on a server.

  The wizard-based installation provides a series of interfaces that help simplify the ScanMail installation. See *Running a Wizard-Based Installation* on page 2-10.

- **Silent installation** requires no user intervention when installing SMLD.

  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 ScanMail on multiple or partitioned Domino servers. See *Running a Silent Installation* on page 2-41.

Setup Options

There are four Setup options:

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

Running a Wizard-Based Installation

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

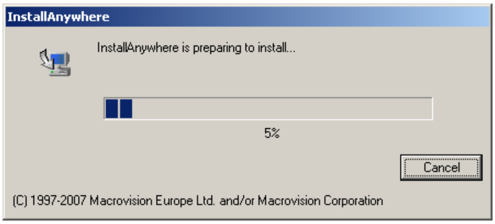
Installing ScanMail for Windows

Note: If you are upgrading from ScanMail 3.0, you must uninstall Trend Micro Management Infrastructure (TMI), before you begin the installation process.

To install ScanMail 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 **SMLD** 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 SMLD install screen.

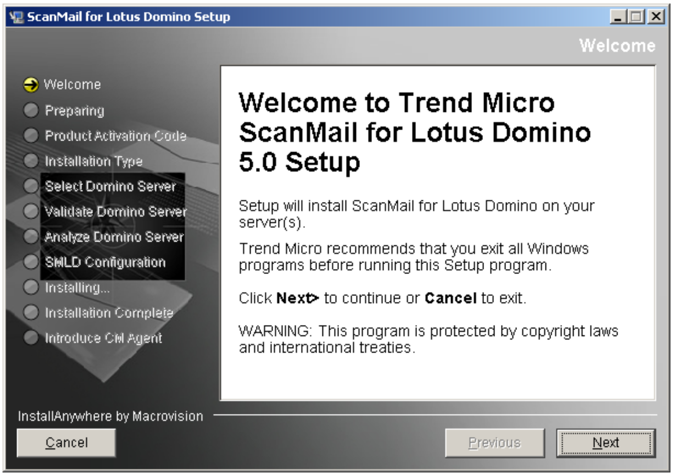


InstallAnywhere is preparing to install...

(C) 1997-2007 Macrovision Europe Ltd. and/or Macrovision Corporation

FIGURE 2-1. InstallAnywhere screen

3. After the SMLD InstallAnywhere screen completes its progress, the SMLD **Welcome** screen appears.



Welcome to Trend Micro ScanMail for Lotus Domino 5.0 Setup

Setup will install ScanMail for Lotus Domino on your server(s).

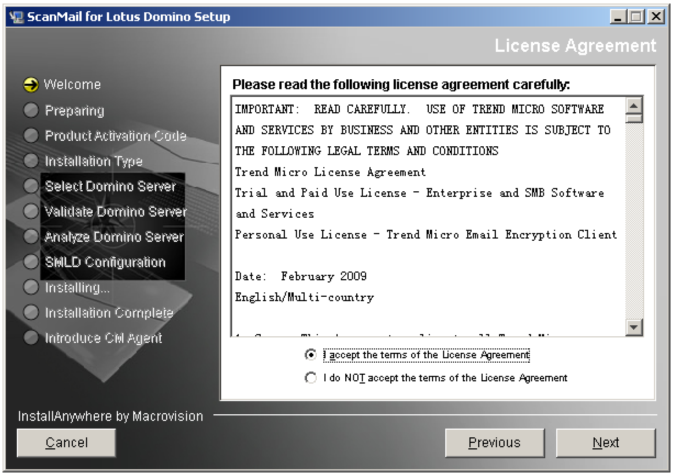
Trend Micro recommends that you exit all Windows programs before running this Setup program.

Click **Next>** to continue or **Cancel** to exit.

WARNING: This program is protected by copyright laws and international treaties.

FIGURE 2-2. SMLD Welcome screen

4. Click **Next**. The **License Agreement** screen appears.



Please read the following license agreement carefully:

```
IMPORTANT:  READ CAREFULLY.  USE OF TREND MICRO SOFTWARE
AND SERVICES BY BUSINESS AND OTHER ENTITIES IS SUBJECT TO
THE FOLLOWING LEGAL TERMS AND CONDITIONS
Trend Micro License Agreement
Trial and Paid Use License - Enterprise and SMB Software
and Services
Personal Use License - Trend Micro Email Encryption Client

Date:  February 2009
English/Multi-country
```

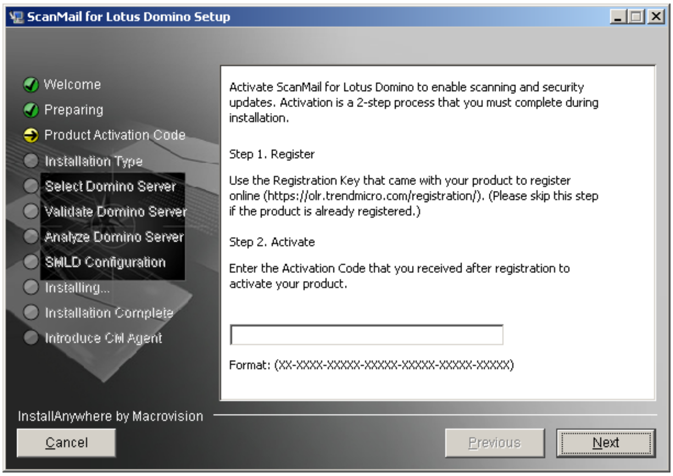
● I accept the terms of the License Agreement

○ I do NOT accept the terms of the License Agreement

FIGURE 2-3. SMLD License Agreement screen

Select **I accept the terms of the license agreement** to continue with the SMLD 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 **Product Activation Code** screen then displays.



Activate ScanMail for Lotus Domino to enable scanning and security updates. Activation is a 2-step process that you must complete during installation.

Step 1. Register

Use the Registration Key that came with your product to register online (https://olr.trendmicro.com/registration/). (Please skip this step if the product is already registered.)

Step 2. Activate

Enter the Activation Code that you received after registration to activate your product.

Format: (XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

FIGURE 2-4. Product Activation Code screen

6. On the **Product Activation Code** screen shown in Figure 2-4, you must enter the correct *ScanMail Activation Code* to activate ScanMail (see page 2-45).

Note: Obtain the Activation Code to activate a ScanMail Evaluation, Standard, or Suite version for a new installation. You may use the same Activation Code used for ScanMail 3.0 if it has not yet expired.

Type or paste the *ScanMail Activation Code* (see page 2-45) or click **Next**, to skip product activation. Do one of the following:

- If you have not registered ScanMail:

  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.

ii. After registration is complete, Trend Micro sends the *ScanMail Activation Code* (AC) to the email address you specified during registration. Use this Activation Code to activate ScanMail.

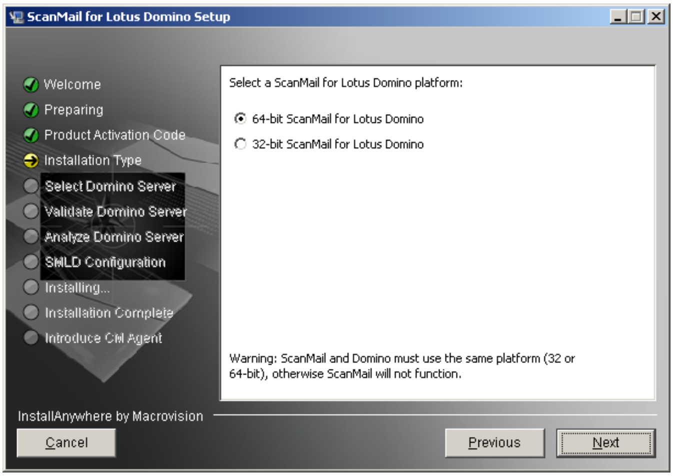
- If you have an Activation Code:

  Type the Activation Code for ScanMail. To use the full functionality of ScanMail 5.0, you need to obtain a Standard or Suite Activation Code (see page 2-45) and activate the software.

- If you want to use the Configuration database to activate ScanMail later:

  Leave the Activation Code field blank. Setup installs ScanMail; however, the SMLD scan or update task will not load. Activate SMLD immediately after installation to protect your Domino environment (see page 2-45).

7. Click **Next**. The **Installation Type** screen then displays.



Select a ScanMail for Lotus Domino platform:

● 64-bit ScanMail for Lotus Domino

○ 32-bit ScanMail for Lotus Domino

Warning: ScanMail and Domino must use the same platform (32 or 64-bit), otherwise ScanMail will not function.

FIGURE 2-5. Installation Type screen

From the Installation Type screen, select from the following:

- 64-bit ScanMail for Lotus Domino
- 32-bit ScanMail for Lotus Domino

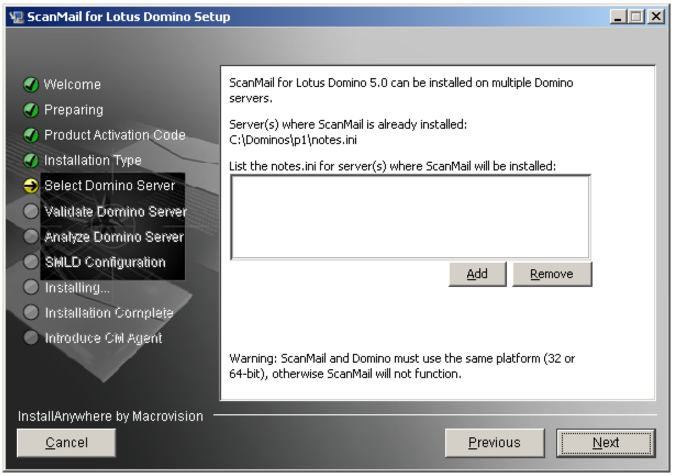
Note: The Installation Type screen (Figure 2-5) will not display if you install ScanMail to a Windows 32-bit Operating System or if you are upgrading from ScanMail 3.0.

WARNING! **The Domino server platform must match the SMLD installation type, otherwise ScanMail will not function. For example, if the Domino server is 32-bit, you must install SMLD 32-bit. If the Domino server is 64-bit, you must install SMLD 64-bit.**

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

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

Also, if you are upgrading from SMD 3.0, the existing **`notes.ini`** server file will display. This file cannot be removed, but you can **Add** other locations.



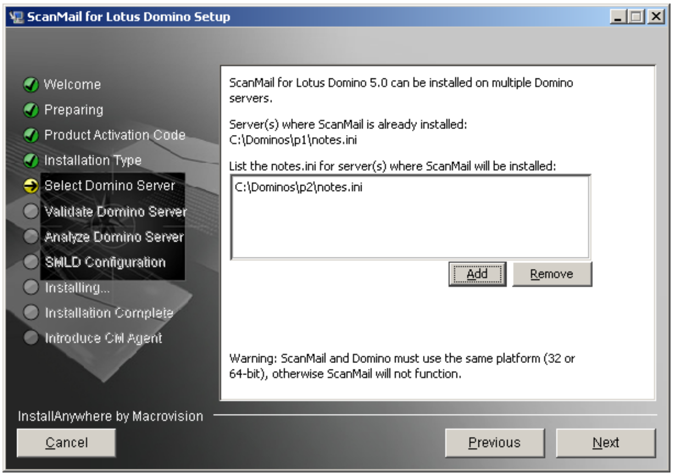
ScanMail for Lotus Domino 5.0 can be installed on multiple Domino servers.

Server(s) where ScanMail is already installed:
C:\Dominos\p1\notes.ini

List the notes.ini for server(s) where ScanMail will be installed:

Warning: ScanMail and Domino must use the same platform (32 or 64-bit), otherwise ScanMail will not function.

FIGURE 2-6. Select Domino Server screen



ScanMail for Lotus Domino 5.0 can be installed on multiple Domino servers.

Server(s) where ScanMail is already installed:
C:\Dominos\p1\notes.ini

List the notes.ini for server(s) where ScanMail will be installed:
C:\Dominos\p2\notes.ini

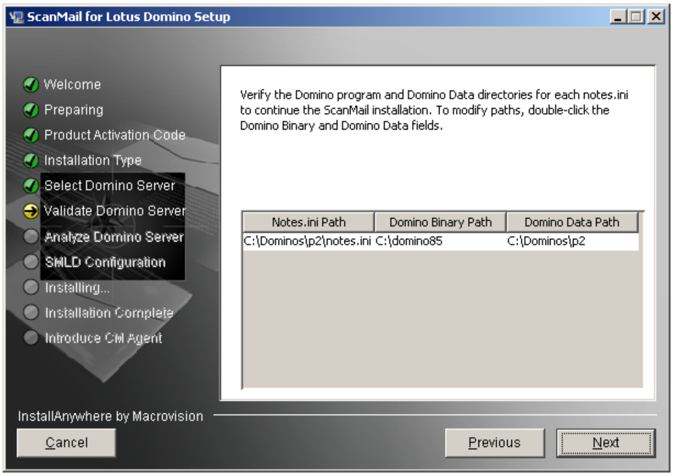
Warning: ScanMail and Domino must use the same platform (32 or 64-bit), otherwise ScanMail will not function.

FIGURE 2-7. Select correct location for notes.ini

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

After selecting the ***`notes.ini`*** path, click **Add > Next.** The **Validate Domino Server** screen displays.

9. From the **Validate Domino Server** screen, verify the domino and data directories path.

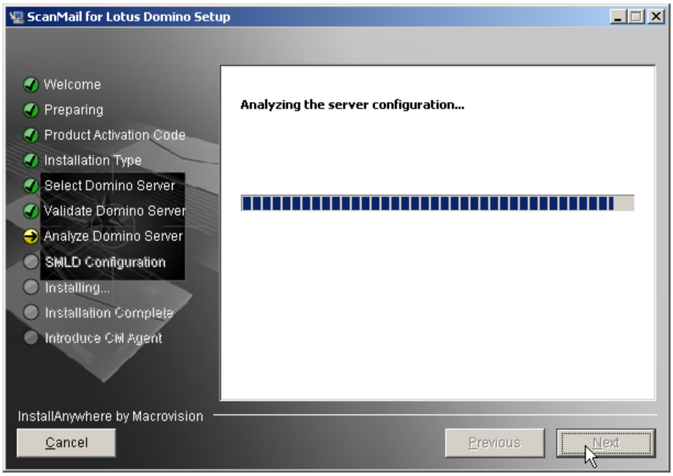


Verify the Domino program and Domino Data directories for each notes.ini to continue the ScanMail installation. To modify paths, double-click the Domino Binary and Domino Data fields.

Notes.ini Path	Domino Binary Path	Domino Data Path
C:\Dominos\p2\notes.ini	C:\domino85	C:\Dominos\p2

FIGURE 2-8. Verify the Domino program and Data directories screen

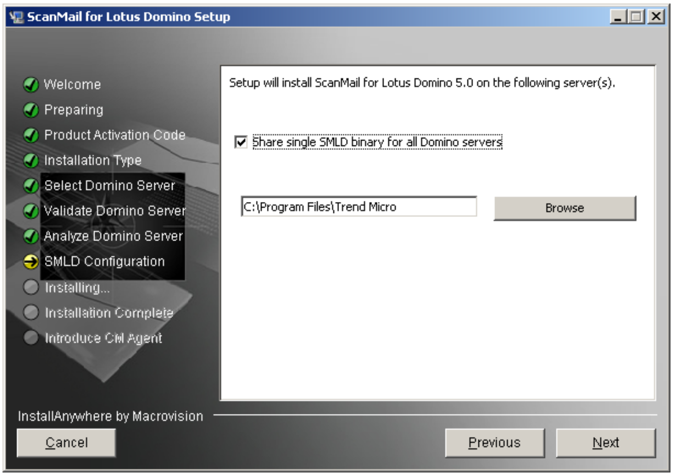
Double-click the Domino Binary Path to modify the path if necessary and click **Next**. The **Analyze Domino Server** screen displays.



Analyzing the server configuration...

FIGURE 2-9. Analyze Domino Server screen

10. After the configuration analysis screen progress completes, click **Next**. The **SMLD Configuration** screen displays.



ScanMail for Lotus Domino Setup

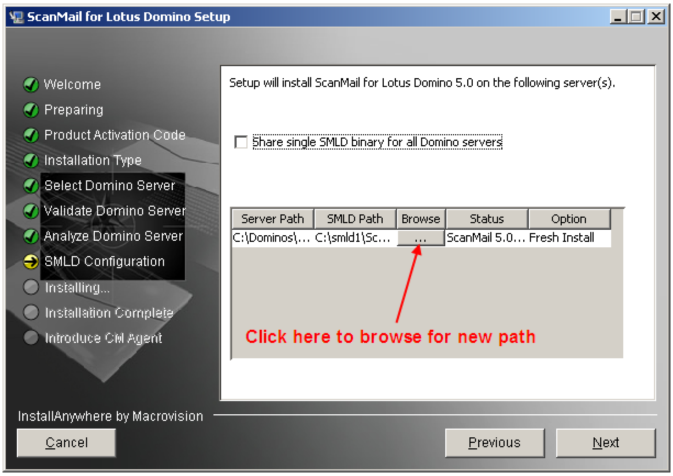
Setup will install ScanMail for Lotus Domino 5.0 on the following server(s).

☑ Share single SMLD binary for all Domino servers

C:\Program Files\Trend Micro

FIGURE 2-10. SMLD Configuration screen

11. From the **SMLD Configuration** screen, type or **Browse** for the location to install ScanMail for Lotus Domino. If you clear the **Share single SMLD binary for all Domino servers** option, the screen shown in Figure 2-11 appears.



Setup will install ScanMail for Lotus Domino 5.0 on the following server(s).

□ Share single SMLD binary for all Domino servers

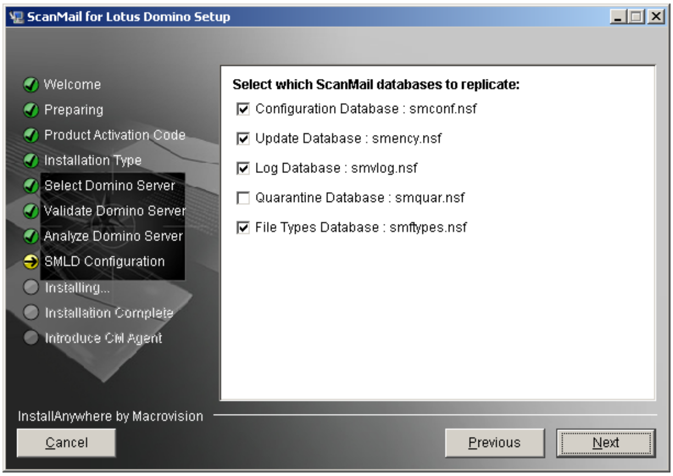
Server Path	SMLD Path	Browse	Status	Option
C:\Dominos\...	C:\smld1\Sc...	...	ScanMail 5.0...	Fresh Install

Click here to browse for new path

FIGURE 2-11. Choose server install path

12. If you cleared **Share single SMLD binary for all Domino servers**, click **...** as shown in Figure 2-11 to browse for a new server path.
13. 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 ScanMail databases you want Setup to replicate.



Select which ScanMail databases to replicate:

☑ Configuration Database : smconf.nsf

☑ Update Database : smency.nsf

☑ Log Database : smvlog.nsf

□ Quarantine Database : smquar.nsf

☑ File Types Database : smftypes.nsf

FIGURE 2-12. ScanMail database replication settings

If you plan to install ScanMail 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.

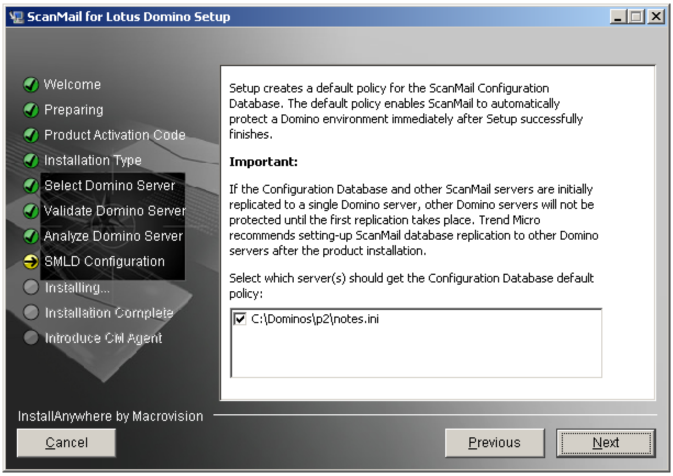
Note: Remember to schedule the replication of the Configuration database after installing ScanMail so that all servers receive the default policy.

---

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

A single ScanMail 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.



Setup creates a default policy for the ScanMail Configuration Database. The default policy enables ScanMail to automatically protect a Domino environment immediately after Setup successfully finishes.

Important:

If the Configuration Database and other ScanMail servers are initially replicated to a single Domino server, other Domino servers will not be protected until the first replication takes place. Trend Micro recommends setting-up ScanMail database replication to other Domino servers after the product installation.

Select which server(s) should get the Configuration Database default policy:

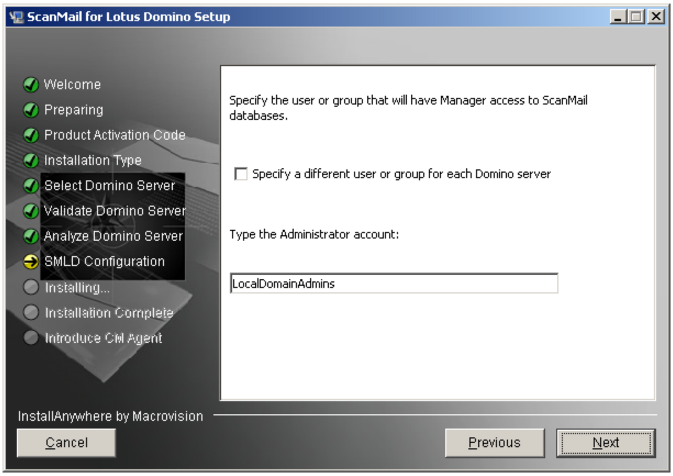
☑ C:\Dominos\p2\notes.ini

FIGURE 2-13. ScanMail default policy screen

15. 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 ScanMail 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 **Administrator** field



Specify the user or group that will have Manager access to ScanMail databases.

□ Specify a different user or group for each Domino server

Type the Administrator account:

LocalDomainAdmins

FIGURE 2-14. 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.

16. Click **Next**. The **ScanMail Database Signing** screen, shown in Figure 2-15, appears.

    Do one of the following:

    - Select **Skip database signing** to prevent Setup from signing ScanMail databases. Sign ScanMail databases manually after the installation.

    WARNING! **Do not select "Skip database signing" when upgrading from SMD 3.0 to SMLD 5.0 and the server ID requires a password. You must enter the correct password to continue with a successful installation. Additionally, if you skip database signing in this case the upgrade will be unsuccessful.**

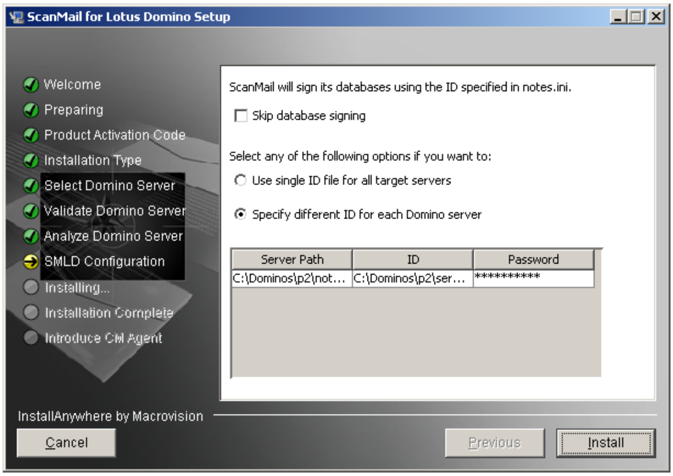
    - Select **Use single ID file for all target servers** to sign ScanMail databases with a single ID.

Type the ID (including full path) under **ID** column or click **Browse** to specify the path of the target ID, and then type the **password**.

- Select **Specify different ID for each Domino server** to sign ScanMail databases on each Domino server with a different ID.

WARNING! **If you select, "Specify different ID for each Domino server," you must enter the correct password for the signing ID. If you enter the incorrect password, or leave the field blank, the upgrade will be unsuccessful.**

Type the ID (including its full path) under the **ID** column or click **Browse** to specify the path to the target ID.



ScanMail for Lotus Domino Setup

ScanMail will sign its databases using the ID specified in notes.ini.

□ Skip database signing

Select any of the following options if you want to:

○ Use single ID file for all target servers

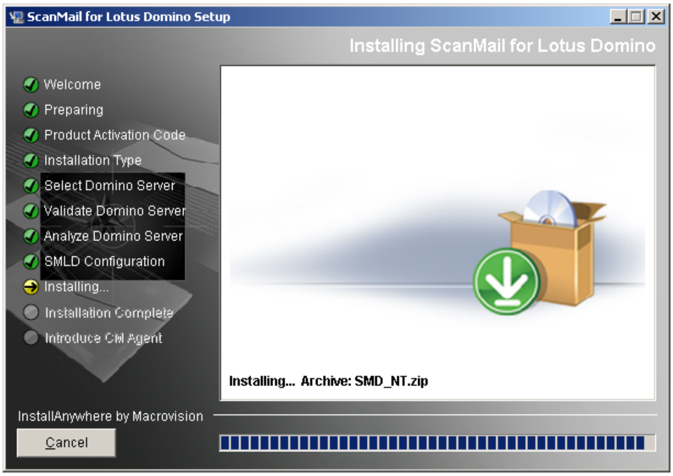
● Specify different ID for each Domino server

Server Path	ID	Password
C:\Dominos\p2\not...	C:\Dominos\p2\ser...	***********

InstallAnywhere by Macrovision

FIGURE 2-15. ScanMail database signing screen

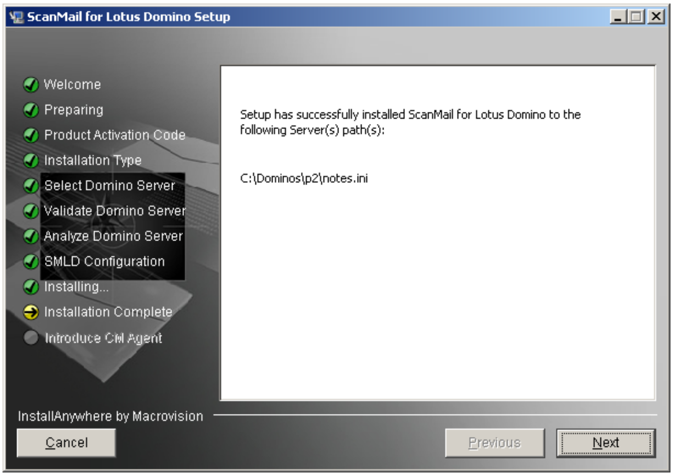
17. Click **Install**. The installation begins.



Installing... Archive: SMD_NT.zip

FIGURE 2-16. Setup installs ScanMail on selected server(s).

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

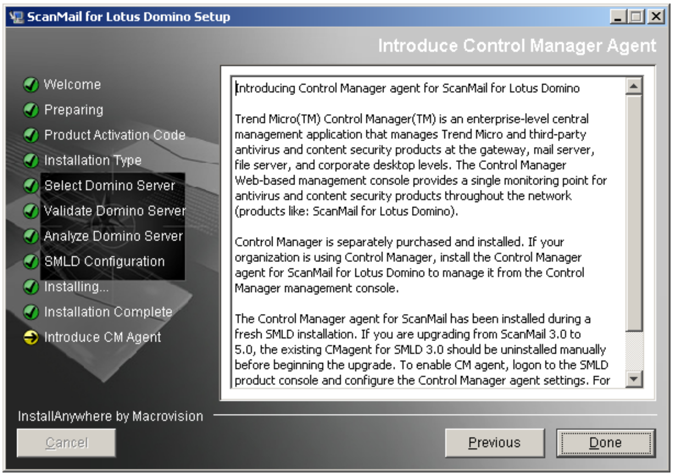


Setup has successfully installed ScanMail for Lotus Domino to the following Server(s) path(s):

C:\Dominos\p2\notes.ini

FIGURE 2-17. ScanMail Installation Complete screen

19. Click **Next**. The **Introduce CM Agent** screen displays.



Introducing Control Manager agent for ScanMail for Lotus Domino

Trend Micro(TM) Control Manager(TM) is an enterprise-level central management application that manages Trend Micro and third-party antivirus and content security products at the gateway, mail server, file server, and corporate desktop levels. The Control Manager Web-based management console provides a single monitoring point for antivirus and content security products throughout the network (products like: ScanMail for Lotus Domino).

Control Manager is separately purchased and installed. If your organization is using Control Manager, install the Control Manager agent for ScanMail for Lotus Domino to manage it from the Control Manager management console.

The Control Manager agent for ScanMail has been installed during a fresh SMLD installation. If you are upgrading from ScanMail 3.0 to 5.0, the existing CMagent for SMLD 3.0 should be uninstalled manually before beginning the upgrade. To enable CM agent, logon to the SMLD product console and configure the Control Manager agent settings. For

FIGURE 2-18. Introduce CM Agent screen

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

See *Testing Installation with EICAR* on page 2-47 to confirm that ScanMail has been successfully installed.

If you are running ServerProtect or another antivirus product on the Domino server where you will install ScanMail, see *SMLD and Other Antivirus Products* on page 2-44.

Installing ScanMail for AIX

To install ScanMail, 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 SMLD 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):

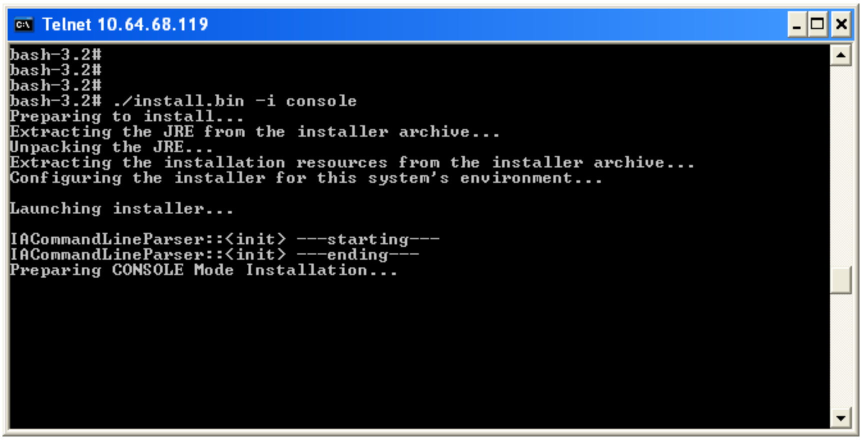
  $ IATEMPDIR=/your/directory/with/free/space

  $ export IATEMPDIR

- For C shell (csh) and TC Shell (tcsh):

  $ setenv IATEMPDIR /your/directory/with/free/space

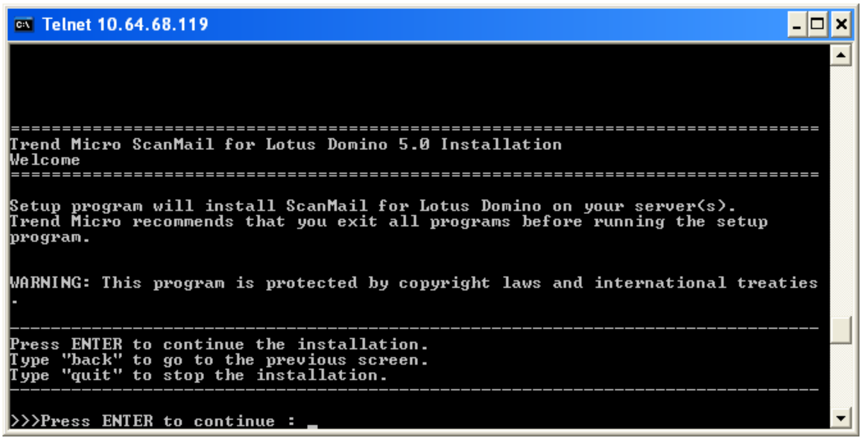
2. Run the installation file (***`SMLD5SetupAIX.bin`***) by typing the command: **./SMLD5SetupAIX.bin -i console**. The installer starts unpacking the file.



```
bash-3.2#
bash-3.2#
bash-3.2#
bash-3.2# ./install.bin -i console
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...

IACommandLineParser::<init> ---starting---
IACommandLineParser::<init> ---ending---
Preparing CONSOLE Mode Installation...
```

FIGURE 2-19. Unpacking Installer file

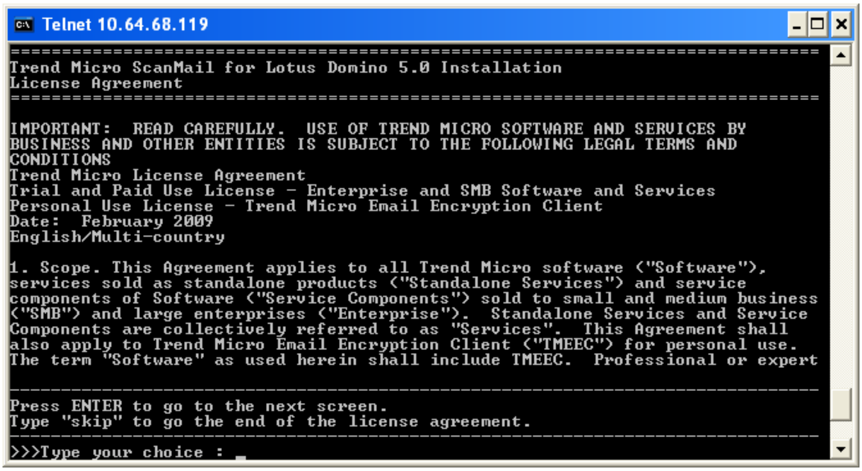
After unpacking of installation file is complete, the **Welcome** screen appears as shown in Figure 2-20.



```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Welcome
================================================================================

Setup program will install ScanMail for Lotus Domino on your server(s).
Trend Micro recommends that you exit all programs before running the setup
program.

WARNING: This program is protected by copyright laws and international treaties
.
--------------------------------------------------------------------------------
Press ENTER to continue the installation.
Type "back" to go to the previous screen.
Type "quit" to stop the installation.
--------------------------------------------------------------------------------
>>>Press ENTER to continue : _
```

FIGURE 2-20. Welcome screen

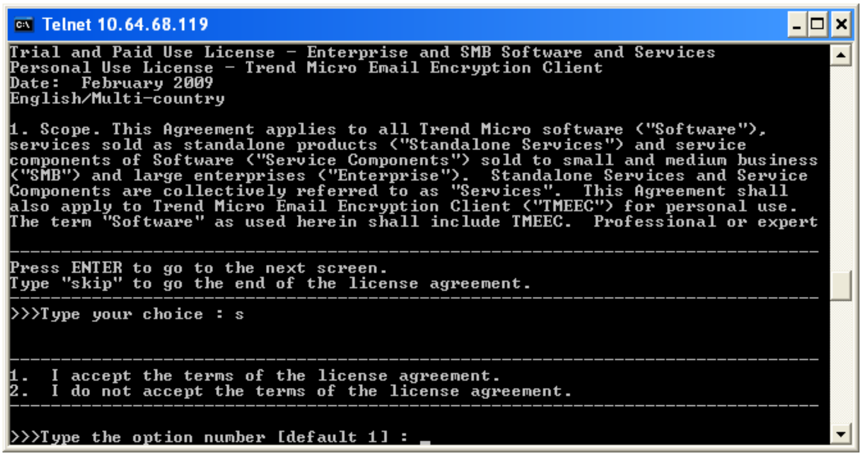
Press **Enter** to continue the installation. The **License Agreement** screen appears.



```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
License Agreement
================================================================================

IMPORTANT:  READ CAREFULLY.  USE OF TREND MICRO SOFTWARE AND SERVICES BY
BUSINESS AND OTHER ENTITIES IS SUBJECT TO THE FOLLOWING LEGAL TERMS AND
CONDITIONS
Trend Micro License Agreement
Trial and Paid Use License - Enterprise and SMB Software and Services
Personal Use License - Trend Micro Email Encryption Client
Date:  February 2009
English/Multi-country

1. Scope. This Agreement applies to all Trend Micro software ("Software"),
services sold as standalone products ("Standalone Services") and service
components of Software ("Service Components") sold to small and medium business
("SMB") and large enterprises ("Enterprise").  Standalone Services and Service
Components are collectively referred to as "Services".  This Agreement shall
also apply to Trend Micro Email Encryption Client ("TMEEC") for personal use.
The term "Software" as used herein shall include TMEEC.  Professional or expert

--------------------------------------------------------------------------------
Press ENTER to go to the next screen.
Type "skip" to go the end of the license agreement.
--------------------------------------------------------------------------------
>>>Type your choice : _
```

FIGURE 2-21. License Agreement screen

3. 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**.

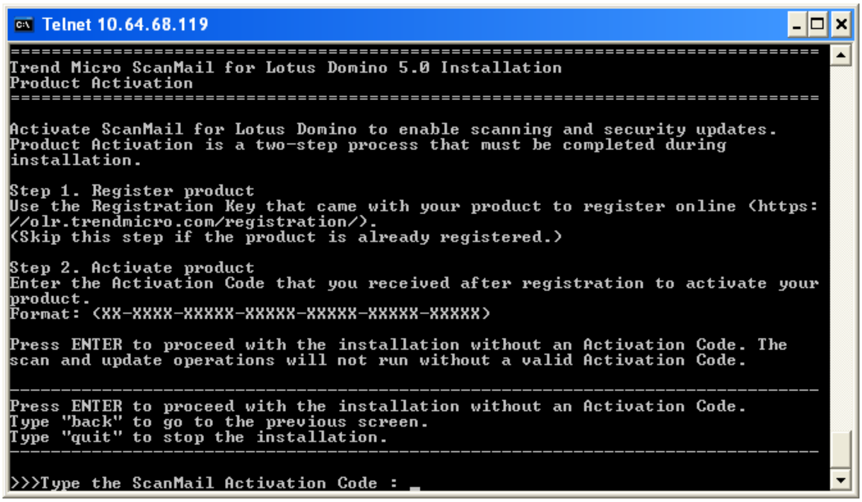


```
Trial and Paid Use License - Enterprise and SMB Software and Services
Personal Use License - Trend Micro Email Encryption Client
Date:  February 2009
English/Multi-country

1. Scope. This Agreement applies to all Trend Micro software ("Software"),
services sold as standalone products ("Standalone Services") and service
components of Software ("Service Components") sold to small and medium business
("SMB") and large enterprises ("Enterprise").  Standalone Services and Service
Components are collectively referred to as "Services".  This Agreement shall
also apply to Trend Micro Email Encryption Client ("TMEEC") for personal use.
The term "Software" as used herein shall include TMEEC.  Professional or expert

--------------------------------------------------------------------------------
Press ENTER to go to the next screen.
Type "skip" to go the end of the license agreement.
--------------------------------------------------------------------------------
>>>Type your choice : s


--------------------------------------------------------------------------------
1.  I accept the terms of the license agreement.
2.  I do not accept the terms of the license agreement.
--------------------------------------------------------------------------------

>>>Type the option number [default 1] : _
```

FIGURE 2-22. License Agreement screen

4. 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.

5. Press **Enter**. The **Product Activation** screen appears.



```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Product Activation
================================================================================

Activate ScanMail for Lotus Domino to enable scanning and security updates.
Product Activation is a two-step process that must be completed during
installation.

Step 1. Register product
Use the Registration Key that came with your product to register online (https:
//olr.trendmicro.com/registration/).
(Skip this step if the product is already registered.)

Step 2. Activate product
Enter the Activation Code that you received after registration to activate your
product.
Format: (XX-XXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX)

Press ENTER to proceed with the installation without an Activation Code. The
scan and update operations will not run without a valid Activation Code.

--------------------------------------------------------------------------------
Press ENTER to proceed with the installation without an Activation Code.
Type "back" to go to the previous screen.
Type "quit" to stop the installation.
--------------------------------------------------------------------------------

>>>Type the ScanMail Activation Code : _
```

FIGURE 2-23. Product Activation screen

6. On the **Product Activation** screen shown in Figure 2-23, you must type the correct *ScanMail Activation Code* to activate ScanMail (see page 2-45).

Note: Obtain the Activation Code to activate a ScanMail Evaluation, Standard, or Suite version for a new installation.

Do one of the following:

- If you have not registered ScanMail:

  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.

  ii. After registration is complete, Trend Micro sends the *ScanMail Activation Code* (AC) to the email address you specified during registration. Use this Activation Code to activate ScanMail.

- If you have an Activation Code:

  Type the Activation Code for ScanMail. To use the full functionality of ScanMail 5.0, you need to obtain a Standard or Suite Activation Code (see page 2-45) and activate the software.

- If you want to use the Configuration database to activate ScanMail later:

  Leave the Activation Code field blank. Setup installs ScanMail; however, the SMLD scan or update task will not load. Activate SMLD immediately after installation to protect your Domino environment (see page 2-45).

Press **Enter**.

7. If you chose to proceed without the Activation Code, the setup will prompt for the confirmation. Do one of the following:

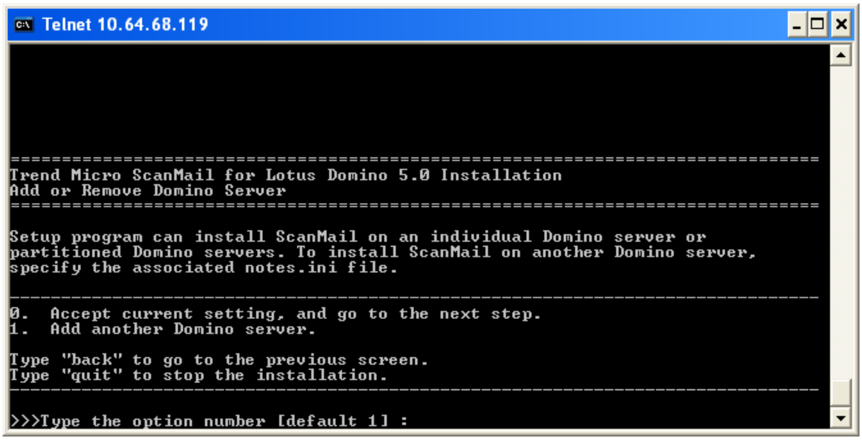
a. To continue installing ScanMail without the Activation Code, type *y* and press **Enter**.

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 **ScanMail Activation Code**. and press **Enter**.

The **Add or Remove Domino Server** screen appears.



```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Add or Remove Domino Server
================================================================================

Setup program can install ScanMail on an individual Domino server or
partitioned Domino servers. To install ScanMail on another Domino server,
specify the associated notes.ini file.

--------------------------------------------------------------------------------
0.  Accept current setting, and go to the next step.
1.  Add another Domino server.

Type "back" to go to the previous screen.
Type "quit" to stop the installation.
--------------------------------------------------------------------------------
>>>Type the option number [default 1] :
```

FIGURE 2-24. Add or Remove Domino Server screen

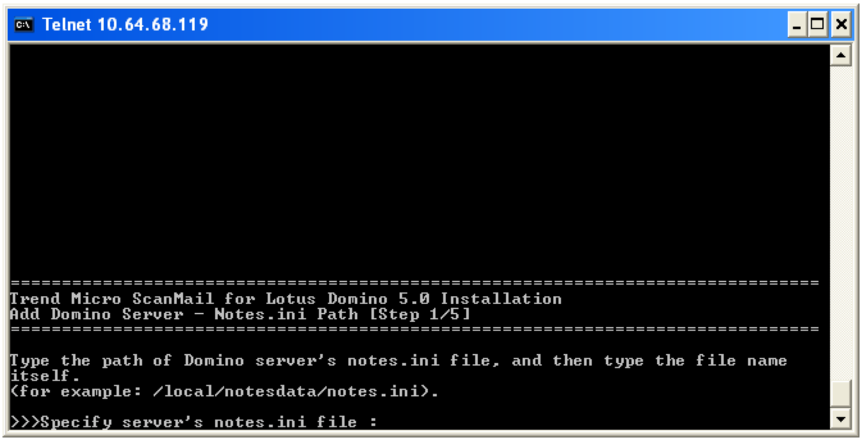
8. On the **Add or Remove Domino Server** screen shown in Figure 2-24, type `1` to add **`notes.ini`** server where you want to install SMLD.

Note: If you have a partitioned server, install ScanMail 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 1/5]** screen appears as shown in Figure 2-25. Type the path where **`notes.ini`** file is located.

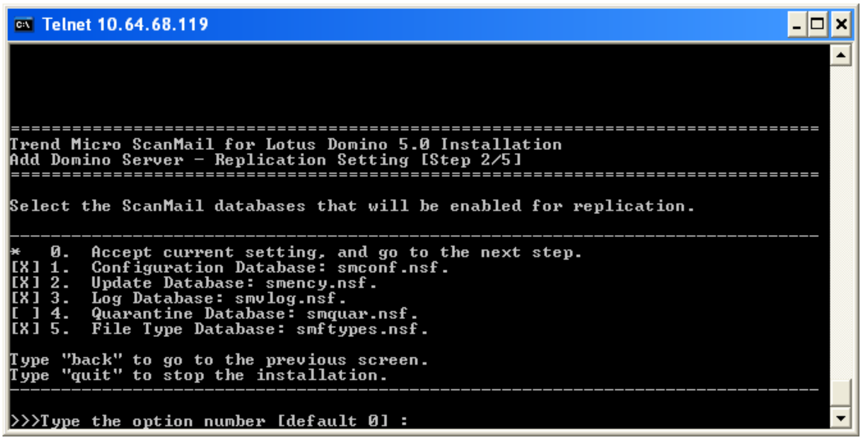


Telnet 10.64.68.119

```
==============================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Add Domino Server - Notes.ini Path [Step 1/5]
==============================================================================

Type the path of Domino server's notes.ini file, and then type the file name
itself.
(for example: /local/notesdata/notes.ini).

>>>Specify server's notes.ini file :
```

FIGURE 2-25. Domino server selection screen

b. Press **Enter**. **Add Domino Server - Replication Setting [Step 2/5]** screen appears.



```
===============================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Add Domino Server - Replication Setting [Step 2/5]
===============================================================================

Select the ScanMail databases that will be enabled for replication.

-------------------------------------------------------------------------------
*    0.  Accept current setting, and go to the next step.
[X] 1.  Configuration Database: smconf.nsf.
[X] 2.  Update Database: smency.nsf.
[X] 3.  Log Database: smvlog.nsf.
[ ] 4.  Quarantine Database: smquar.nsf.
[X] 5.  File Type Database: smftypes.nsf.

Type "back" to go to the previous screen.
Type "quit" to stop the installation.
-------------------------------------------------------------------------------

>>>Type the option number [default 0] :
```

FIGURE 2-26. 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 ScanMail databases you want Setup to replicate or ignore. To select or deselect ScanMail database, do the following:

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

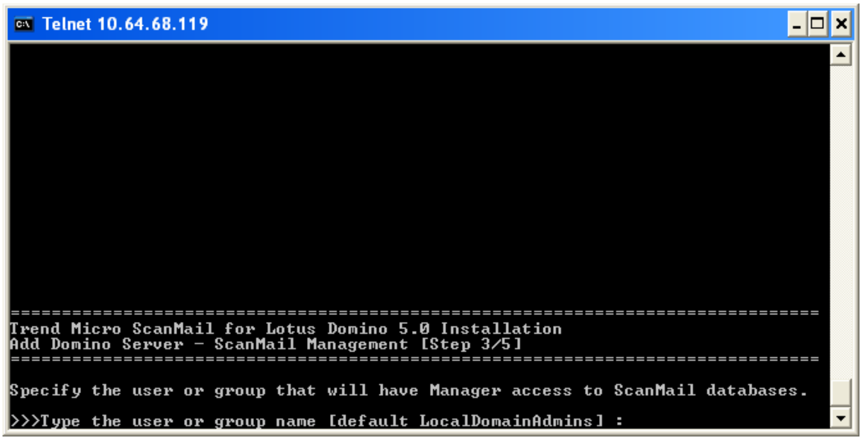
ii. Press **Enter**.

Tip: If you plan to install ScanMail 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 ScanMail so that all servers receive the default policy.

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

c. Press **Enter**. The **Add Domino Server - ScanMail Management [Step 3/5]** screen appears.



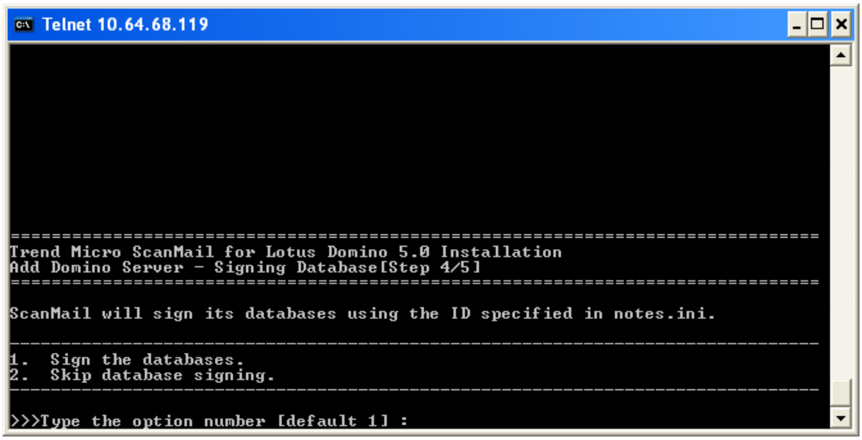
```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Add Domino Server - ScanMail Management [Step 3/5]
================================================================================

Specify the user or group that will have Manager access to ScanMail databases.

>>>Type the user or group name [default LocalDomainAdmins] :
```

FIGURE 2-27. 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 ScanMail 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.

d. Press **Enter**. The **Add Domino Server - Signing Database[Step 4/5]** screen appears.



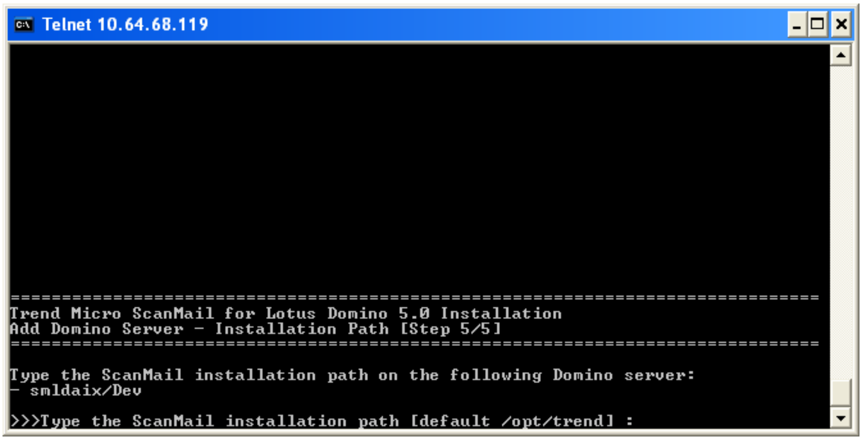
```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Add Domino Server - Signing Database[Step 4/5]
================================================================================

ScanMail will sign its databases using the ID specified in notes.ini.

--------------------------------------------------------------------------------
1.  Sign the databases.
2.  Skip database signing.
--------------------------------------------------------------------------------

>>>Type the option number [default 1] :
```

FIGURE 2-28. Database Signing screen

On the **Add Domino Server - Signing Database[Step 4/5]** screen shown in Figure 2-28, do one of the following:

- To sign all ScanMail databases with a single ID, type 1 and press **Enter**. The setup will prompt for the ID and password.
  - Type the ID (including full path) and press **Enter**.
  - Type the desired **password** and press **Enter**.
- To skip signing the ScanMail databases, type 2 and press **Enter**. You can sign ScanMail databases manually after the installation.

e. After the **Database Signing** screen, the **Add Domino Server - Install Path [Step 5/5]** screen appears.



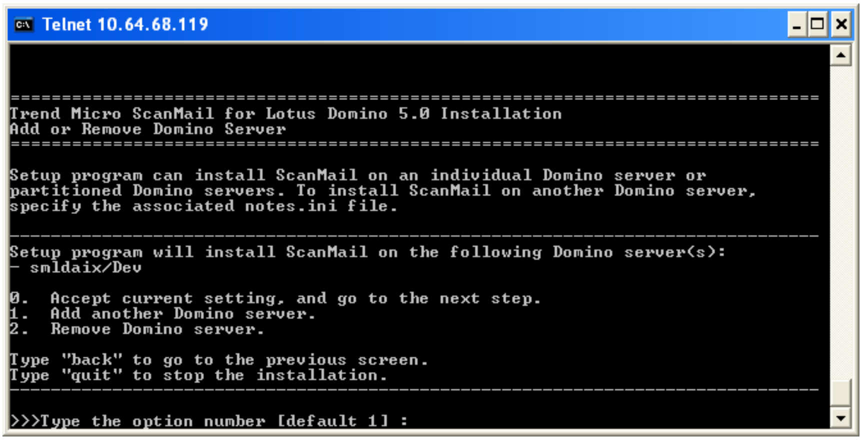
```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Add Domino Server - Installation Path [Step 5/5]
================================================================================

Type the ScanMail installation path on the following Domino server:
- smldaix/Dev

>>>Type the ScanMail installation path [default /opt/trend] :
```

FIGURE 2-29. Installation Path selection screen

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

Note: If SMLD 5.0 for AIX has already been installed on one partition servers, the default installation path for the subsequent installation(s) will remain same and cannot be changed.

f. 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 serve(s).



Telnet 10.64.68.119

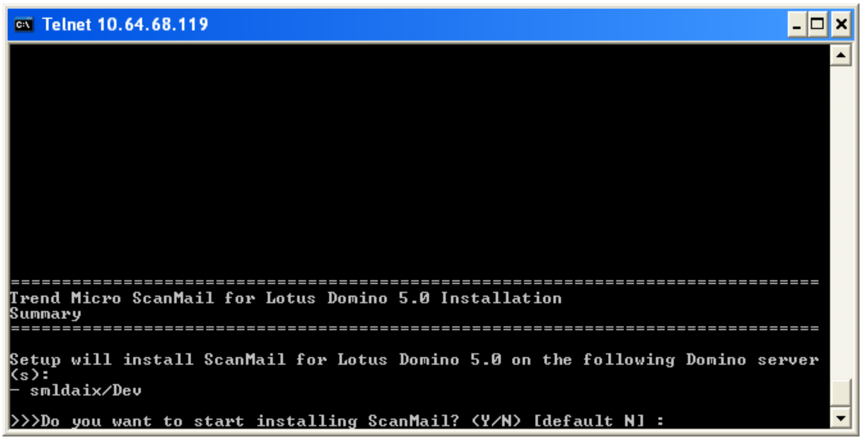
```
===============================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Add or Remove Domino Server
===============================================================================

Setup program can install ScanMail on an individual Domino server or
partitioned Domino servers. To install ScanMail on another Domino server,
specify the associated notes.ini file.

-------------------------------------------------------------------------------
Setup program will install ScanMail on the following Domino server(s):
- smldaix/Dev

0.  Accept current setting, and go to the next step.
1.  Add another Domino server.
2.  Remove Domino server.

Type "back" to go to the previous screen.
Type "quit" to stop the installation.
-------------------------------------------------------------------------------

>>>Type the option number [default 1] :
```

FIGURE 2-30. Add or Remove Domino Server screen

On the **Add or Remove Domino Server** screen shown in Figure 2-30, 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 e of Step 8 on page 2-33.
- Type `2` to remove Domino server(s) previously selected.

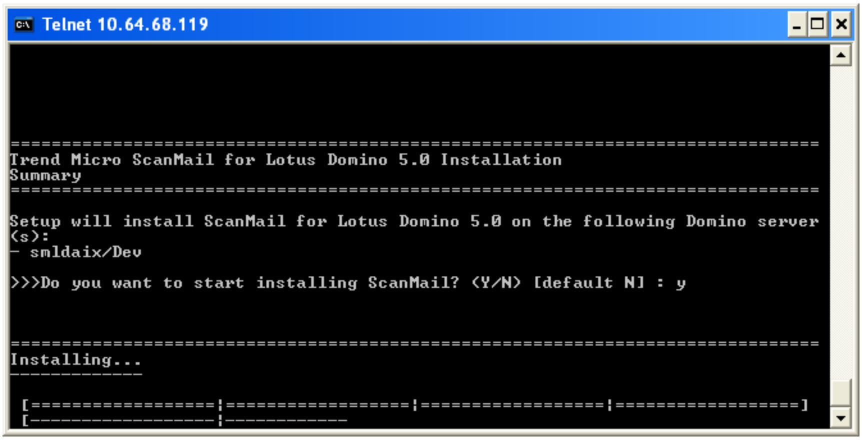
9. Press **Enter**. The **Summary** screen appears. Type *Y* or *y* to start installing the selected Domino server(s).



```
===============================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Summary
===============================================================================

Setup will install ScanMail for Lotus Domino 5.0 on the following Domino server
(s):
- smldaix/Dev

>>>Do you want to start installing ScanMail? (Y/N) [default N] :
```

FIGURE 2-31. Installation Summary screen

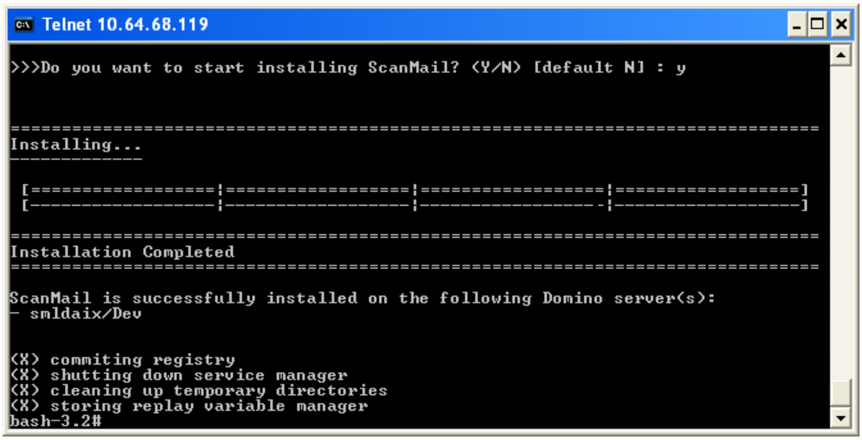
10. Press **Enter**. The installation begins.



```
===============================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Installation
Summary
===============================================================================

Setup will install ScanMail for Lotus Domino 5.0 on the following Domino server
(s):
- smldaix/Dev

>>>Do you want to start installing ScanMail? (Y/N) [default N] : y


===============================================================================
Installing...
-------------

 [==================¦==================¦==================¦==================]
 [------------------¦------------
```

FIGURE 2-32. Setup installs ScanMail on selected server(s)

After the installation shown in Figure 2-32 completes, the **`Installation Complete`** message displays on the screen.



```
>>>Do you want to start installing ScanMail? (Y/N) [default N] : y


===============================================================================
Installing...
-------------

 [==================|==================|==================|==================]
 [------------------|------------------|----------------- -|------------------]

===============================================================================
Installation Completed
===============================================================================

ScanMail is successfully installed on the following Domino server(s):
- smldaix/Dev


(X) commiting registry
(X) shutting down service manager
(X) cleaning up temporary directories
(X) storing replay variable manager
bash-3.2#
```

FIGURE 2-33. ScanMail Installation Complete screen

Running a Silent Installation

Silent ScanMail 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 a ScanMail 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 Table 2-4, "ScanMail for Windows Hardware and Software Requirements," on page 2-5 for the hardware and software requirements, if installing ScanMail on Windows platform. If installing ScanMail on IBM AIX platform, see Table 2-5, "ScanMail for IBM AIX Hardware and Software Requirements," on page 2-7 for the hardware and software requirements.
- 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 ScanMail installation and automate ScanMail installation on multiple servers. Alternatively, use an installation script to customize the type of ScanMail setup or to specify options to install on the Domino server.

Installing ScanMail for Windows

To install ScanMail in the silent mode:

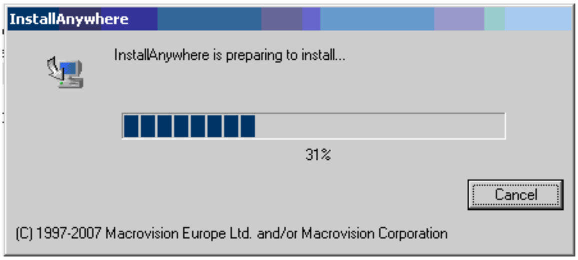
1. From the command console, type information as follows to record the silent installation script file while installing ScanMail to a single or multiple Domino server(s):

   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 ScanMail installation.



InstallAnywhere
InstallAnywhere is preparing to install...
31%
Cancel
(C) 1997-2007 Macrovision Europe Ltd. and/or Macrovision Corporation

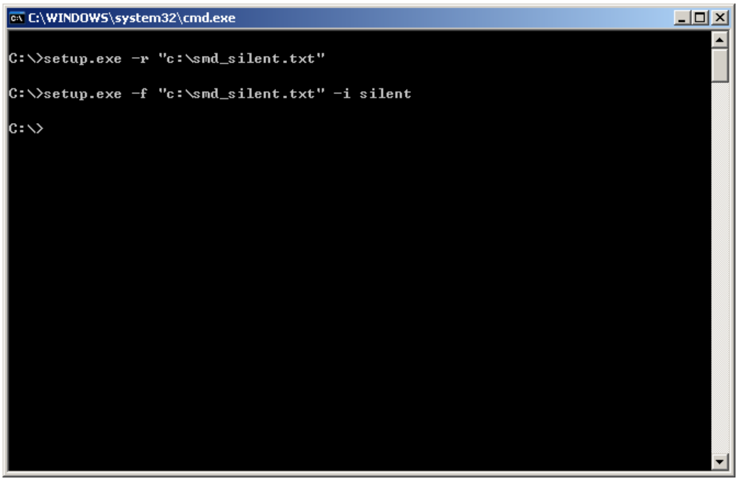
FIGURE 2-34. Recording ScanMail installation on a Windows server

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

   setup.exe -f "{absolute path and script file name}" -i silent

   For example:

   setup.exe -f "c:\smd_silent.txt" -i silent



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

C:\>setup.exe -f "c:\smd_silent.txt" -i silent

C:\>
```

FIGURE 2-35. Running a silent ScanMail installation on a Windows server

3. Open the silent installation log file for the Setup result, ***smdins.log***, which is created in the Windows system root directory. Follow the steps in *Testing Installation with EICAR* on page 2-47 to check whether the ScanMail installation is successful.

Installing ScanMail for AIX

To install ScanMail in the silent mode:

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

   ./SMLD5SetupAIX.bin –i console –r {path and script file name}

   Example:

   ./SMLD5SetupAIX.bin –i console –r /tmp/silent.txt

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

   ./SMLD5SetupAIX.bin –i silent –f {path and script file name}

   For example:

   ./SMLD5SetupAIX.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 2-47 to check whether the ScanMail installation is successful.

Starting the Domino Server

After installing ScanMail, start the Domino server to launch the ScanMail tasks and test the installation with EICAR (page 2-47) to confirm whether ScanMail is successfully installed. Additionally, refer to *Getting Started with ScanMail* 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** > **Lotus Applications** > **Domino Server**.

To start the Domino server on IBM AIX platform:

1. Make certain you are logged in with the Domino user account and not as root. Check this by issuing the command **whoami** or **id**.
2. Change to your Domino data directory (for example, `local/notesdata`), and then type the following command at the Terminal to start the Domino server:
   $ /opt/ibm/lotus/bin/server –jc &

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

/opt/ibm/lotus/bin/server

Refer to your Domino documentation for more information on how to start a Domino server.

SMLD and Other Antivirus Products

If you are running ServerProtect or another antivirus product on the Domino server where you will install ScanMail, exclude the ScanMail `smd` and temporary directories on each partition from scanning (refer to your temporary directory settings found in *Set Directories Used for Scanning*) to prevent a scanning conflict.

If you are using ServerProtect, refer to the ServerProtect documentation for instructions to exclude Domino folders and directories from scanning.

Registering and Activating ScanMail

Use your Registration Key to register your product on the Trend Micro Online Registration Web site. 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 *ScanMail Activation Code*, which you can then use to activate ScanMail.

ScanMail Activation Code

ScanMail has three types of Activation Codes:

- An Evaluation AC allows you to implement the full functionality of ScanMail. During the evaluation period, ScanMail performs malware and unwanted content filtering and scanning, as well as component update. When an Evaluation AC expires, all ScanMail functions are disabled, leaving your Domino environment unprotected.
- A Standard AC allows you to implement limited ScanMail functionalities. ScanMail Standard edition provides virus scanning in all modes and component update. However, content and spam filtering are unavailable.
- A Suite AC allows you to implement ScanMail's full functionalities, including content, spam filtering, and Web Reputation.

ScanMail displays the remaining number of days before an evaluation version, Standard edition, or Suite edition expires via the Domino server console. Trend Micro recommends registering and obtaining a Suite AC before the expiration date to allow uninterrupted Domino environment protection.

Obtaining a ScanMail Activation Code

Activate the ScanMail server to keep your antivirus and content security updates current. To activate your product, register online and obtain a ScanMail 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.
- Are using an evaluation version, the evaluation version is fully functional for 30 days, after which ScanMail tasks will continue to load, but no virus scanning, message filtering, nor component update will occur.

  Obtain a full version Registration Key from your reseller and then follow the instructions to activate the product.

Activating ScanMail

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

To activate ScanMail:

1. Open the ScanMail Configuration Database.
2. On the left menu, click **Administration** > **Product License**.
3. *Creating a License Profile* (see page 5-13).
4. Delete the license profile created during installation (see page 5-14).

Convert to a Full Version

Upgrade and activate the full version of ScanMail to continue using it beyond the evaluation period. Activate ScanMail 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 5-13).
5. Delete the corresponding license profile for the evaluation version (see page 5-14).

Renew ScanMail 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 ScanMail 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 ScanMail 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 ScanMail installation with EICAR:

1. Open an ASCII text file and copy the following 68-character string to it.

   X5O!P%@AP[4\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 ScanMail Log Database or check the notification sent to the administrator (if Notification is set).

Checking ScanMail Files and Folders

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

- *ScanMail for Windows* on page C-2
- *ScanMail for AIX* on page C-3

Chapter 3

Getting Started with ScanMail

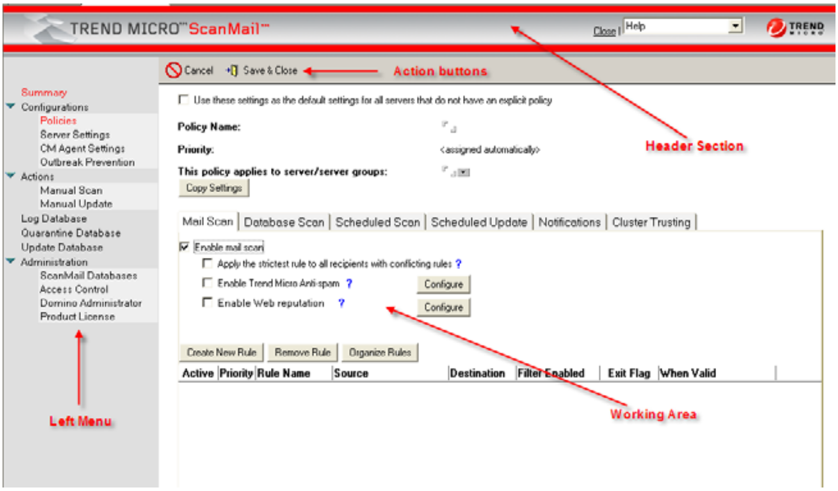
This chapter presents post-installation and post-activation tasks that you need to perform to configure ScanMail.

This chapter includes the following topics:

- *Understanding the ScanMail 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 3-4
- *Defining Access and Roles to ScanMail Databases* on page 3-5
- *Signing ScanMail Databases with a Different ID* on page 3-4
- *Defining Access and Roles to ScanMail Databases* on page 3-5
- *Accessing ScanMail Databases* on page 3-7

Understanding the ScanMail Interface

The ScanMail interface layout is as follows:



□ Use these settings as the default settings for all servers that do not have an explicit policy

Policy Name:

Priority: <assigned automatically>

This policy applies to server/server groups:

☑ Enable mail scan

□ Apply the strictest rule to all recipients with conflicting rules ?

□ Enable Trend Micro Anti-spam ?

□ Enable Web reputation ?

FIGURE 3-1. ScanMail interface

The interface contains the following areas:

TABLE 3-6. ScanMail interface layout description

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

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 4-49) 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 4-17) 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 > Application > Open**.
2. Enter the **path** and **file name** in the **Filename** field.
3. Click **Open**.

Refer to the *Notes Workspace* topic in the Lotus 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:

- Sign databases for the first time because the database signing was skipped during installation
- 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 Lotus Notes Client, click **Files** > **Security** > **Switch ID** to switch to the ID that will be used to sign ScanMail databases.
2. Start the Lotus 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 from **Manager** 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*

   TABLE 3-7. Access Control List for ScanMail Databases

PERSON, SERVER, OR GROUP	RECOMMENDED ACCESS LEVEL	DELETE DOCUMENTS OPTION
-Default-	No Access	Not selected
ID used to sign ScanMail databases	Manager	Selected
ScanMail Administrator(s)	Editor (or higher)	Selected
Domino server	Manager	Selected
LocalDomainServers (if you are using replication)	Editor (or higher)	Selected
OtherDomainServers	No access	Not selected

   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 8-4). 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

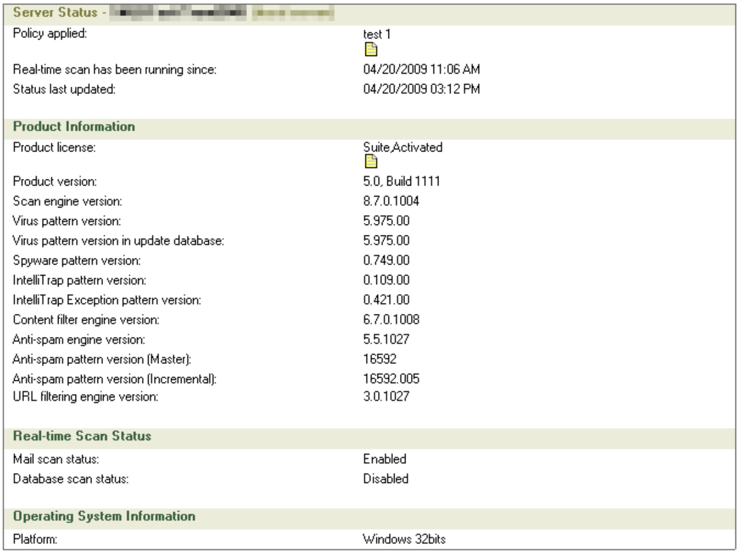
Accessing ScanMail Databases Using a Notes Client

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 > Application > Open**.
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**.



Server Status - [redacted]	
Policy applied:	test 1
Real-time scan has been running since:	04/20/2009 11:06 AM
Status last updated:	04/20/2009 03:12 PM
Product Information	
Product license:	Suite,Activated
Product version:	5.0, Build 1111
Scan engine version:	8.7.0.1004
Virus pattern version:	5.975.00
Virus pattern version in update database:	5.975.00
Spyware pattern version:	0.749.00
IntelliTrap pattern version:	0.109.00
IntelliTrap Exception pattern version:	0.421.00
Content filter engine version:	6.7.0.1008
Anti-spam engine version:	5.5.1027
Anti-spam pattern version (Master):	16592
Anti-spam pattern version (Incremental):	16592.005
URL filtering engine version:	3.0.1027
Real-time Scan Status	
Mail scan status:	Enabled
Database scan status:	Disabled
Operating System Information	
Platform:	Windows 32bits

FIGURE 3-2. The Configuration Database displays *Server Summary* as the default first page

Lotus 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.

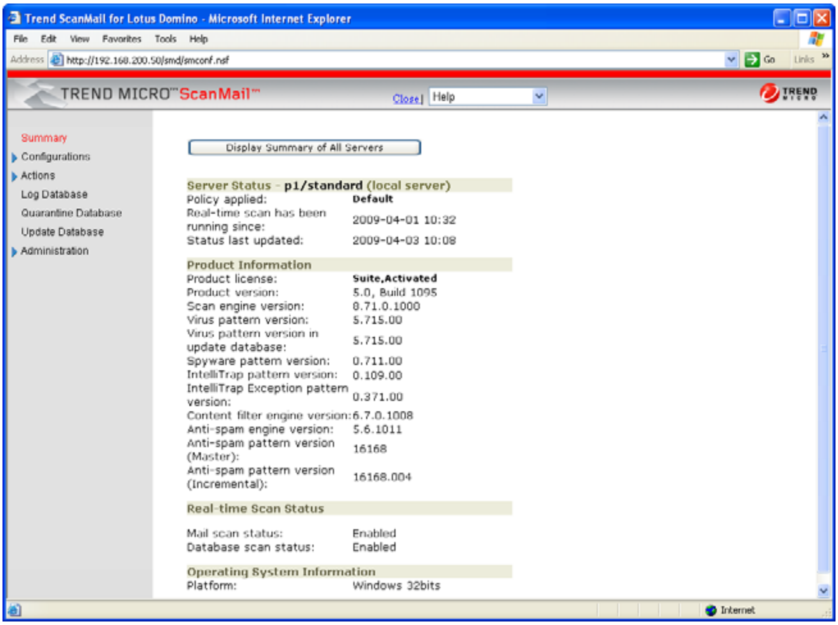
Domino provides password security for ScanMail. System administrators can configure the password (see *Set the Internet Password for ScanMail Database Access through a Web Browser* on page 3-11) for each person under the HTTP password in the Address Book. The Access Control List, as set from the Notes 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.


Trend ScanMail for Lotus Domino - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Address http://192.168.200.50/smd/smconf.nsf
Go
Links
TREND MICRO™ ScanMail™
Close |
Help
TREND MICRO
Summary
Configurations
Actions
Log Database
Quarantine Database
Update Database
Administration
Display Summary of All Servers
Internet

Server Status - p1/standard (local server)	
Policy applied:	**Default**
Real-time scan has been running since:	2009-04-01 10:32
Status last updated:	2009-04-03 10:08
Product Information	
Product license:	**Suite,Activated**
Product version:	5.0, Build 1095
Scan engine version:	8.71.0.1000
Virus pattern version:	5.715.00
Virus pattern version in update database:	5.715.00
Spyware pattern version:	0.711.00
IntelliTrap pattern version:	0.109.00
IntelliTrap Exception pattern version:	0.371.00
Content filter engine version:	6.7.0.1008
Anti-spam engine version:	5.6.1011
Anti-spam pattern version (Master):	16168
Anti-spam pattern version (Incremental):	16168.004
Real-time Scan Status	
Mail scan status:	Enabled
Database scan status:	Enabled
Operating System Information	
Platform:	Windows 32bits

FIGURE 3-3. Access ScanMail databases using a Web browser

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

- 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 Lotus 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

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

Trend Micro recommends that you use the policy-based features in ScanMail 5.0 to establish and maintain a standard antivirus 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 5-12.

Managing Policies

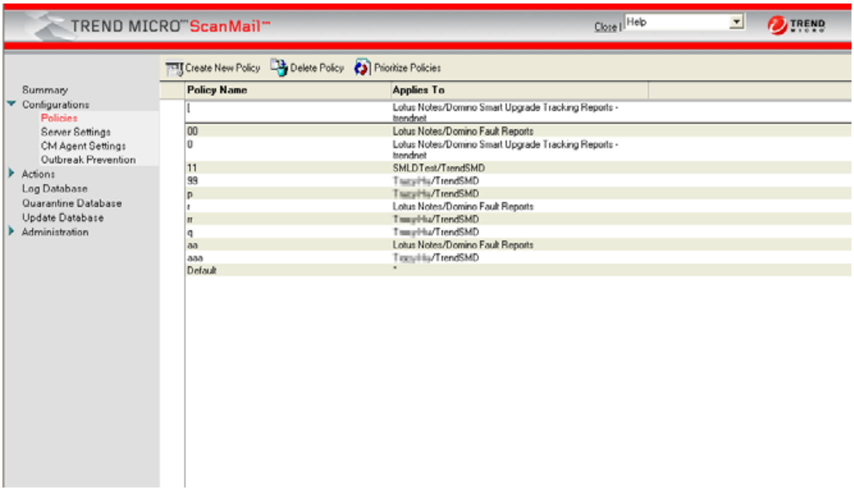
This section describes how to use the ScanMail Configuration database to manage policies.

Creating Policies

Use the ScanMail Configuration database to create policies.

To create policies:

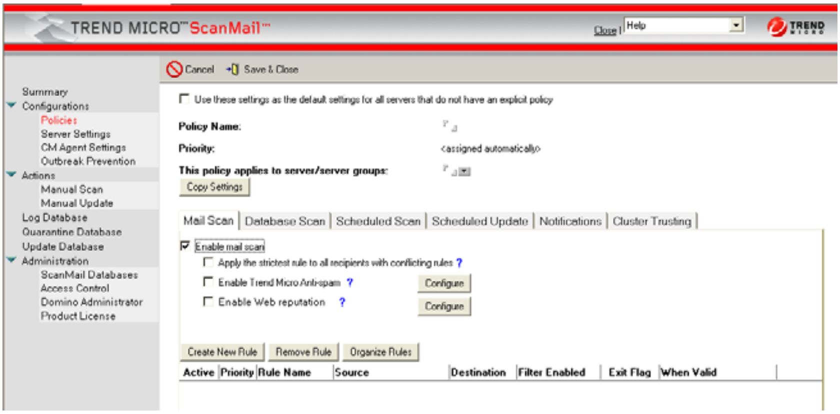
1. Open the ScanMail Configuration Database (See *Accessing ScanMail Databases* on page 3-7).
2. From the left menu, click **Configurations** > **Policies**.



Policy Name	Applies To
[	Lotus Notes/Domino Smart Upgrade Tracking Reports - trendnet
00	Lotus Notes/Domino Fault Reports
0	Lotus Notes/Domino Smart Upgrade Tracking Reports - trendnet
11	SMLDTest/TrendSMD
99	[redacted]/TrendSMD
p	[redacted]/TrendSMD
r	Lotus Notes/Domino Fault Reports
rr	[redacted]/TrendSMD
q	[redacted]/TrendSMD
aa	Lotus Notes/Domino Fault Reports
aaa	[redacted]/TrendSMD
Default	*

FIGURE 4-1. Policy list

3. From the working area, click **Create New Policy**.
4. Type the **Policy Name**.



□ Use these settings as the default settings for all servers that do not have an explicit policy

Policy Name:

Priority: <assigned automatically>

This policy applies to server/server groups:

☑ Enable mail scan

□ Apply the strictest rule to all recipients with conflicting rules ?

□ Enable Trend Micro Anti-spam ?

□ Enable Web reputation ?

Active	Priority	Rule Name	Source	Destination	Filter Enabled	Exit Flag	When Valid

FIGURE 4-2. Creating a policy

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

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 4-10).
8. Create a real-time database scan rule (See *Creating Real-time Database Scan Rules* on page 4-15).
9. Create a scheduled database scan rule (See *Creating Scheduled Database Scan Rules* on page 4-17).

10. Define how ScanMail delivers notifications (See *Defining How ScanMail Delivers Notifications* on page 7-6).
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 3-7).
2. On the left menu, click **Configurations** > **Policies**.
3. On the working area, double-click a **policy**.
4. Modify the **Mail Scan** (page 4-10), **Database Scan** (page 4-15), **Scheduled Scan** (page 4-17), **Scheduled Update** (page 6-4), **Notifications** (page 7-6), 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 3-7).
2. On the left menu, click **Configuration** > **Policies**. The Policies view appears.
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 3-7).
2. From the left menu, click **Configuration** > **Policies**. The Policies view appears.
3. From the working area, click **Prioritize Polices**. 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.

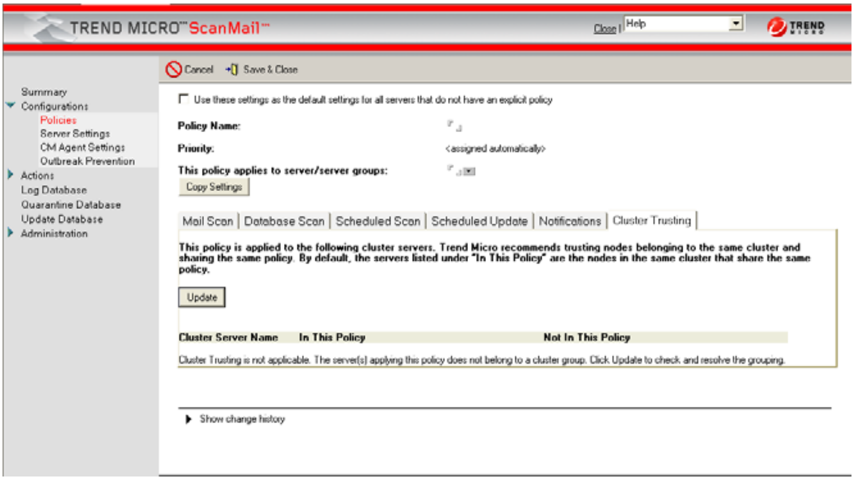
Managing the Trusted Cluster Servers for a Policy

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 4-10) or (See *Modifying Policies* on page 4-6) for more information.
2. Click the **Cluster Trusting** tab.



□ Use these settings as the default settings for all servers that do not have an explicit policy

Policy Name:

Priority: <assigned automatically>

This policy applies to server/server groups:

This policy is applied to the following cluster servers. Trend Micro recommends trusting nodes belonging to the same cluster and sharing the same policy. By default, the servers listed under "In This Policy" are the nodes in the same cluster that share the same policy.

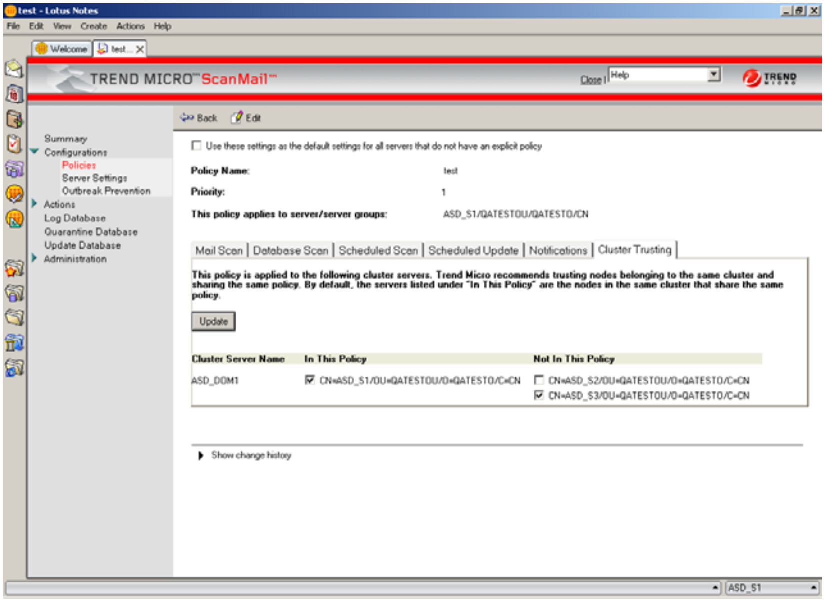
Cluster Server Name	In This Policy	Not In This Policy

Cluster Trusting is not applicable. The server(s) applying this policy does not belong to a cluster group. Click Update to check and resolve the grouping.

FIGURE 4-3. The Cluster Trusting table lists the servers available in a cluster group.

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*.



☐ Use these settings as the default settings for all servers that do not have an explicit policy

Policy Name: test

Priority: 1

This policy applies to server/server groups: ASD_S1/QATESTOU/QATESTO/CN

This policy is applied to the following cluster servers. Trend Micro recommends trusting nodes belonging to the same cluster and sharing the same policy. By default, the servers listed under "In This Policy" are the nodes in the same cluster that share the same policy.

Cluster Server Name	In This Policy	Not In This Policy
ASD_DOM1	☑ CN=ASD_S1/OU=QATESTOU/O=QATESTO/C=CN	☐ CN=ASD_S2/OU=QATESTOU/O=QATESTO/C=CN ☑ CN=ASD_S3/OU=QATESTOU/O=QATESTO/C=CN

FIGURE 4-4. Selecting server to include in the trusted cluster group

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.

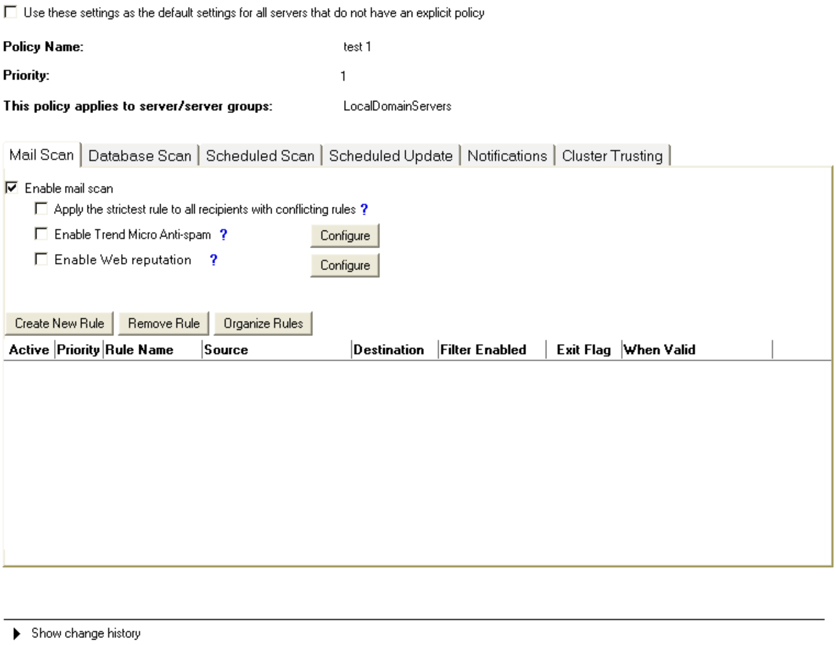
Tip: If a rule has too many conditions, it can become unpredictably complex. Trend Micro recommends creating multiple simple rules rather than one or two complex rules per policy.

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 4-10) or (See *Modifying Policies* on page 4-6) for more information.
2. From the working area, click the **Mail Scan** tab.



□ Use these settings as the default settings for all servers that do not have an explicit policy

Policy Name: test 1

Priority: 1

This policy applies to server/server groups: LocalDomainServers

☑ Enable mail scan

□ Apply the strictest rule to all recipients with conflicting rules ?

□ Enable Trend Micro Anti-spam ?

□ Enable Web reputation ?

Active	Priority	Rule Name	Source	Destination	Filter Enabled	Exit Flag	When Valid

FIGURE 4-5. The *Mail Scan* tab defines ScanMail real-time message scanning.

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 4-13 for details.

4. If you have the Suite edition, select **Enable Trend Micro Anti-spam** and click **Configure** to specify anti-spam settings (See *Configure Anti-Spam Filtering* on page 4-27).

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

Note: You must have Trend Micro Anti-spam functionality enabled to use Web reputation functionality.

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 4-14).
10. Click the **Scan Options** tab to set how ScanMail scans and filters messages:
    - Virus Scan (See *Configuring Virus Scan* on page 4-33)
    - Scan Restrictions (See *Configuring Scan Restrictions* on page 4-36)
    - Message Filter (See *Configuring the Message Filter* on page 4-36)
    - Attachment Filter (See *Configuring the Attachment Filter* on page 4-43)
    - Content Filter (See *Create a New Content Filter* on page 4-38)
    - Script Filter (See *Configuring Script Filter* on page 4-46)

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 7-7).
12. Configure **Redirect Options** (See *Configuring Redirect Options* on page 4-47).
13. Insert disclaimers (See *Inserting Disclaimers* on page 4-48).
14. Set the rule schedule (See *Setting the Rule Schedule* on page 4-49).
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:

General:	**Include specified recipients** = `All of Accounting`
Scan Options > **Attachment Filter:**	**Enable attachment filtering by size** = 10MB **Action** = Block mail

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

General:	**Include specified recipients** = `user@domain.com` `user@domain.com` is a member of the All of Accounting group.
Scan Options > **Attachment Filter:**	**Enable attachment filtering by size** = 5MB **Action** = Block mail

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** group, 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** group, choose the target recipients:
     - **i.** Select which senders 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)

- 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 4-21) that ScanMail will use when processing this rule.

4. From the **Action when Sender and Recipients Match** group, 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 group, 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**.

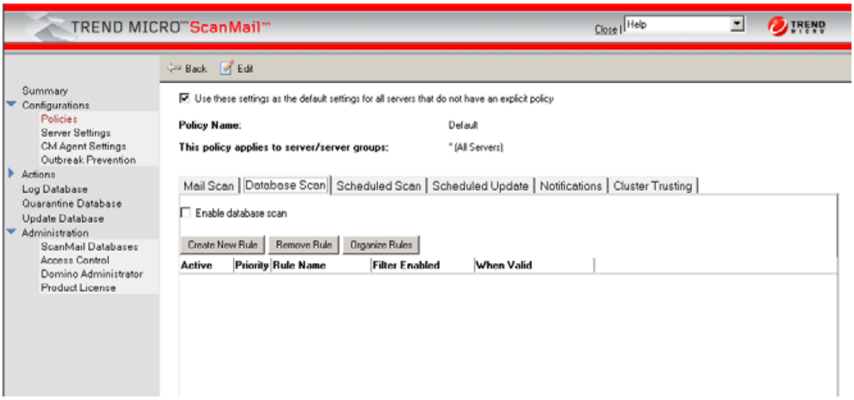
Settings such as a rule name, priority, sender and recipient inclusion/exclusion, schedule, and Exit Flag settings, and the **Scan Options** enabled are available in the **Mail Scan** tab view.

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 create or modify a policy (See *Creating Rules* on page 4-10) or (See *Modifying Policies* on page 4-6) for more information.
2. On the working area, click the **Database Scan** tab.



☑ Use these settings as the default settings for all servers that do not have an explicit policy

Policy Name: Default

This policy applies to server/server groups: * (All Servers)

□ Enable database scan

Active	Priority	Rule Name	Filter Enabled	When Valid

FIGURE 4-6. 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** group, 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 4-21 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:
   - Virus Scan (See *Configuring Virus Scan* on page 4-33)

- Scan Restrictions (See *Configuring Scan Restrictions* on page 4-36)
- Script Filter (See *Configuring Script Filter* on page 4-46)

8. Set the scan **Notification** (See *Setting the Scan Notifications* on page 7-7).
9. Set the rule schedule (See *Setting the Rule Schedule* on page 4-49).
10. Click **Save & Close**.

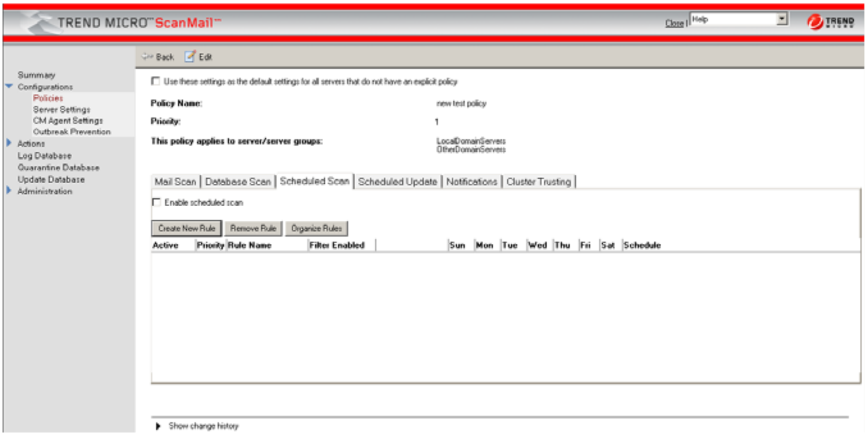
Tip: To configure ScanMail to perform a real-time scan whenever a database file is opened, instead of only when it is modified, set `SMDEnableOpenEvent=1` in ***`notes.ini`***.

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 create or modify a policy (See *Creating Rules* on page 4-10) or (See *Modifying Policies* on page 4-6) for more information.
2. On the working area, click the **Scheduled Scan** tab.



☐ Use these settings as the default settings for all servers that do not have an explicit policy

Policy Name: new test policy

Priority: 1

This policy applies to server/server groups: LocalDomainServers
OtherDomainServers

☐ Enable scheduled scan

Active	Priority	Rule Name	Filter Enabled		Sun	Mon	Tue	Wed	Thu	Fri	Sat	Schedule

FIGURE 4-7. 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:
   - Virus Scan (See *Configuring Virus Scan* on page 4-33)
   - Scan Restrictions (See *Configuring Scan Restrictions* on page 4-36)
   - Script Filter (See *Configuring Script Filter* on page 4-46)
7. Set the scan notification (See *Setting the Scan Notifications* on page 7-7).
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.

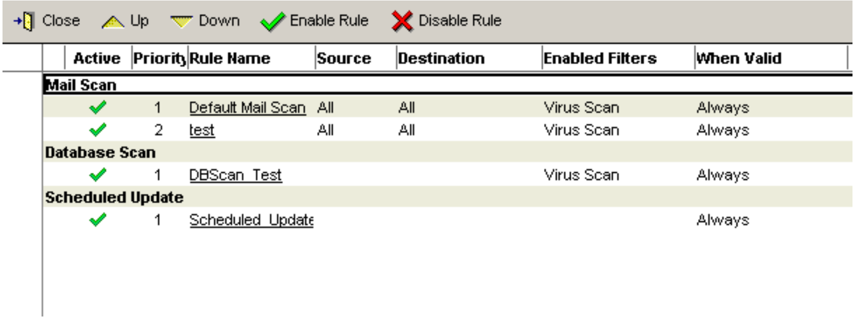
   b. Type how long the scan will run in the **Duration of scan** field. `0` (zero) will instruct ScanMail to stop only when scanning is finished completely.

   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.



Active	Priority	Rule Name	Source	Destination	Enabled Filters	When Valid
Mail Scan						
✓	1	Default Mail Scan	All	All	Virus Scan	Always
✓	2	test	All	All	Virus Scan	Always
Database Scan						
✓	1	DBScan Test			Virus Scan	Always
Scheduled Update						
✓	1	Scheduled Update				Always

FIGURE 4-8. Click Up or Down 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 to promote a rule
   - Click ▼ Down 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.

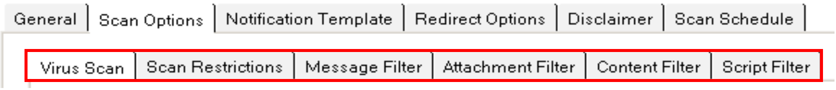


FIGURE 4-9. The Scan Options tabs

Use the following tabs to define how ScanMail scans or filters messages, attachments, and content (in the following order):

ORDER	FILTER	PROVIDES OPTIONS TO SET SPECIFIC SCANNING ACTION ON...
1	**Message Filter**	Various message types
2	**Attachment Filter**	Unwanted attachments
3a	**Scan Restrictions**	Compressed, encrypted, and other attachment types **Note:** ScanMail applies the **Scan Restrictions** settings when **Virus Scan** is enabled.
3b	**Virus Scan**	Virus and other malware types
4	**Content Filter**	Messages with unwanted content based on administrator-defined explicit rules
5	**Script Filter**	Messages with stored form or rich text hot spot content

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

1. Spam filtering (*Configure Anti-Spam Filtering* on page 4-27) of incoming messages based on Approved Senders and Blocked Senders (when enabled) or the Trend Micro Anti-Spam engine
2. General settings (*Configure General Mail Scan Rule Settings* on page 4-14)
3. **Scan Options** filter enabled

Spam Filtering (Suite Edition 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:

ORDER	COMPONENT	SOURCE	DESCRIPTION
1	Approved Senders	User-defined	A list of people and/or organizations from whom messages will be accepted. Other messages take the **Action on unwanted messages**.
2	Blocked Senders	User-defined	A list of people and/or organizations from whom messages will be blocked. Other messages will be accepted.
3	Rule files	Trend Micro	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.

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:

FILTER LEVEL/SENSITIVITY	THRESHOLD LEVEL
High (Rigorous filtering)	4.5
Medium (Default filtering)	5
Low (Lenient filtering)	7

where:

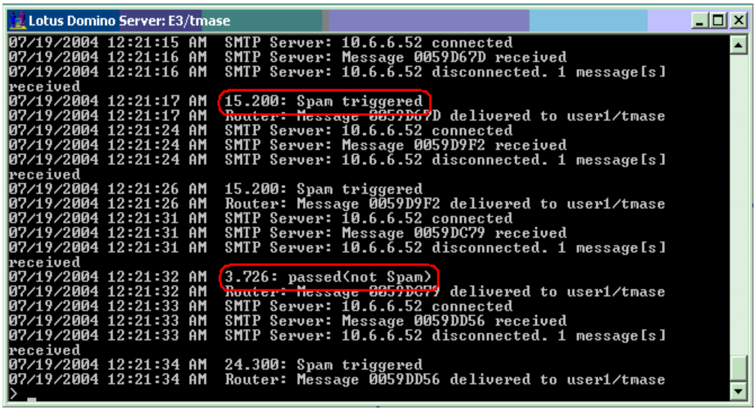
- **Filter level** defines the TMASE sensitivity when filtering for spam

- **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 4-22).

Note: SMLD5.0 has a dynamic threshold level, which changes according to different spam rules.

For example:



```
07/19/2004 12:21:15 AM  SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:16 AM  SMTP Server: Message 0059D67D received
07/19/2004 12:21:16 AM  SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:17 AM  15.200: Spam triggered
07/19/2004 12:21:17 AM  Router: Message 0059D67D delivered to user1/tmase
07/19/2004 12:21:24 AM  SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:24 AM  SMTP Server: Message 0059D9F2 received
07/19/2004 12:21:24 AM  SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:26 AM  15.200: Spam triggered
07/19/2004 12:21:26 AM  Router: Message 0059D9F2 delivered to user1/tmase
07/19/2004 12:21:31 AM  SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:31 AM  SMTP Server: Message 0059DC79 received
07/19/2004 12:21:31 AM  SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:32 AM  3.726: passed(not Spam)
07/19/2004 12:21:32 AM  Router: Message 0059DC79 delivered to user1/tmase
07/19/2004 12:21:33 AM  SMTP Server: 10.6.6.52 connected
07/19/2004 12:21:33 AM  SMTP Server: Message 0059DD56 received
07/19/2004 12:21:33 AM  SMTP Server: 10.6.6.52 disconnected. 1 message[s]
received
07/19/2004 12:21:34 AM  24.300: Spam triggered
07/19/2004 12:21:34 AM  Router: Message 0059DD56 delivered to user1/tmase
> _
```

FIGURE 4-10. Sample spam scores

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 4-27.

Content Filtering (Suite Edition 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:

```
.(. .OCCUR. apple .). .AND. .(. apple .NEAR. computer .). .OR.
.(. apple .NEAR. macintosh .). .AND. .(. .NOT. .(. .OCCUR. eat
.). .).
```

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 4-41.

Configuring the Scan and Filter Settings

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

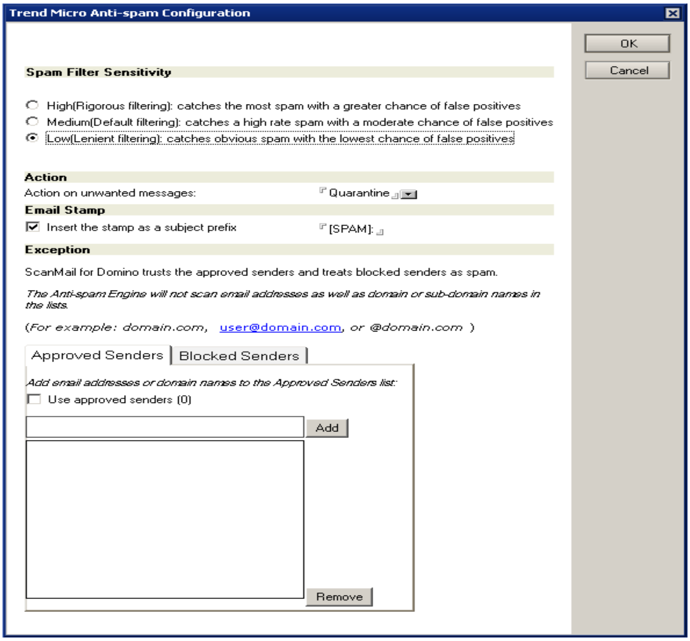
Configure Anti-Spam Filtering

Use the **Anti-spam Configuration** screen to configure how the Trend Micro Anti-Spam engine filters unsolicited or unwanted messages (see page 4-23). 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.

Note: The **Anti-spam Filter**, **Web Reputation Filter** and **Content Filter** features are available only in the ScanMail for Domino Suite. See *ScanMail Activation Code* on page 2-45 for details. In addition, the ScanMail spam filtering only applies to mail scan rules.

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

Spam Filter Sensitivity

○ High(Rigorous filtering): catches the most spam with a greater chance of false positives
○ Medium(Default filtering): catches a high rate spam with a moderate chance of false positives
● Low(Lenient filtering): catches obvious spam with the lowest chance of false positives

Action

Action on unwanted messages: Quarantine

Email Stamp

☑ Insert the stamp as a subject prefix [SPAM]:

Exception

ScanMail for Domino trusts the approved senders and treats blocked senders as spam.

The Anti-spam Engine will not scan email addresses as well as domain or sub-domain names in the lists.

(For example: domain.com, user@domain.com, or @domain.com)

Approved Senders | Blocked Senders

Add email addresses or domain names to the Approved Senders list:

☐ Use approved senders (0)

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/domain**s 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 only)* on page 4-23 for details on how ScanMail applies the Trend Micro rules and user-defined 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** (Lotus Notes console interface)

     - or -
   - **Save** (Web interface)

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.

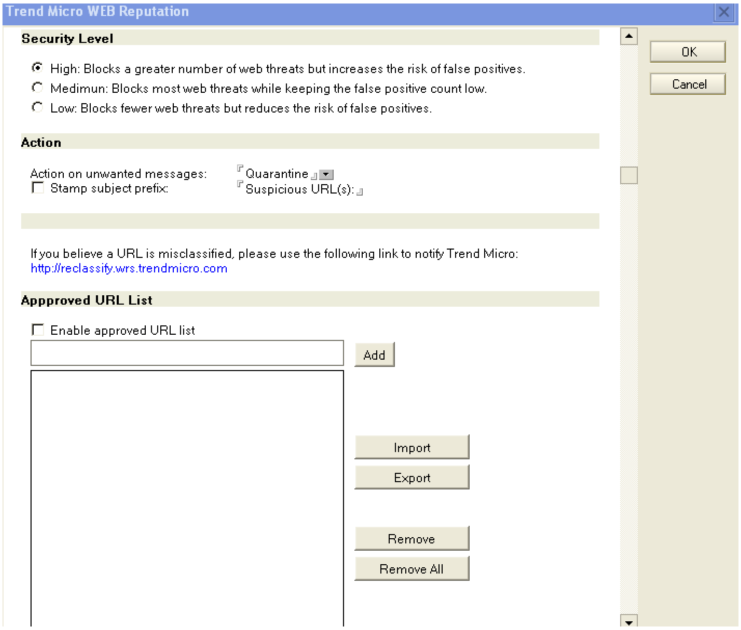
To configure Web reputation:

Note: Anti-spam functionality must be enabled to use Web Reputation. See *Configure Anti-Spam Filtering* on page 4-27.

The proxy setting used for Web Reputation is the same proxy setting as that configured in Server Settings. For more information see *Configure the Proxy Server Settings* on page 5-6.

WARNING! **When Web Reputation is enabled, Internet access is required to query the reputation of URLs contained in email.**

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

Security Level

● High: Blocks a greater number of web threats but increases the risk of false positives.
○ Medimun: Blocks most web threats while keeping the false positive count low.
○ Low: Blocks fewer web threats but reduces the risk of false positives.

Action

Action on unwanted messages: Quarantine
□ Stamp subject prefix: Suspicious URL(s):

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

Appproved URL List

□ Enable approved URL list

FIGURE 4-12. Trend Micro Anti-spam Configuration screen

2. On the Trend Micro Web Reputation configuration window, select the Security Level:

   - **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.

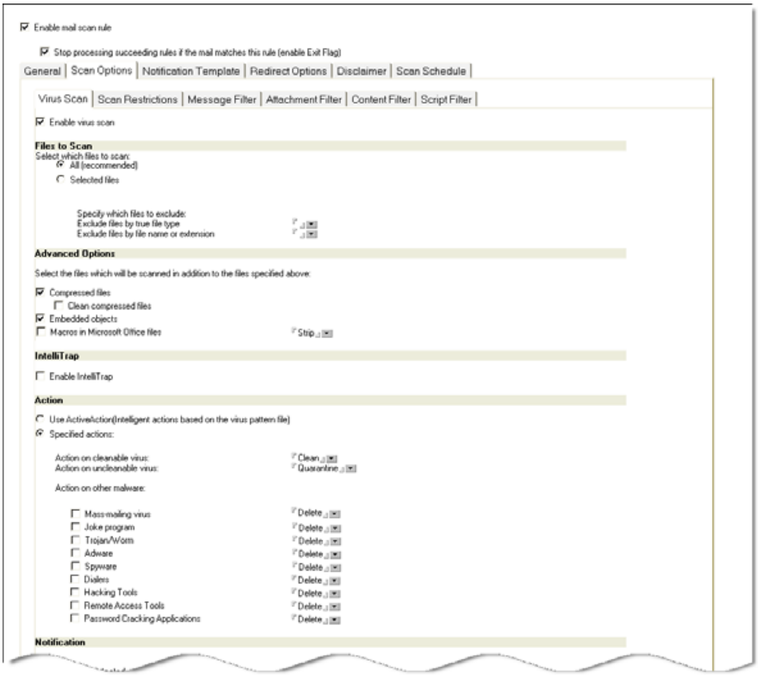
3. In the **Action** section, select the **Action on unwanted messages**: **Pass**, **Quarantine**, or **Block**.
4. Select **Stamp subject prefix**, and then type a **stamp** label to add eye-catching notices or keywords in the subject header.

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

5. 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**.
6. After you complete all settings, click **OK** to save and exit.

Configuring Virus Scan

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



☑ Enable mail scan rule

☑ Stop processing succeeding rules if the mail matches this rule (enable Exit Flag)

☑ Enable virus scan

Files to Scan

Select which files to scan:
● All (recommended)
○ Selected files

Specify which files to exclude:
Exclude files by true file type
Exclude files by file name or extension

Advanced Options

Select the files which will be scanned in addition to the files specified above:

☑ Compressed files
□ Clean compressed files
☑ Embedded objects
□ Macros in Microsoft Office files — Strip

IntelliTrap

□ Enable IntelliTrap

Action

○ Use ActiveAction(Intelligent actions based on the virus pattern file)
● Specified actions:

Action on cleanable virus: Clean
Action on uncleanable virus: Quarantine

Action on other malware:

□ Mass-mailing virus — Delete
□ Joke program — Delete
□ Trojan/Worm — Delete
□ Adware — Delete
□ Spyware — Delete
□ Dialers — Delete
□ Hacking Tools — Delete
□ Remote Access Tools — Delete
□ Password Cracking Applications — Delete

Notification

FIGURE 4-13. Scan Options > Virus Scan screen

To configure virus scan options:

1. Under **Scan Options** click the **Virus Scan** tab.
2. Under the **Files to Scan** group of the **Virus Scan** tab, configure the virus 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.

3. Under the **Advanced Options** group, 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 Lotus Notes mail.

   - **Macros in Microsoft Office files** scans files for macros found in Microsoft Office files (for example, `*.doc`, `*.xls`).

     Select the scan action for macros.

4. Under the **IntelliTrap** group, 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.

5. Under the **Action** group, 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.

For example, when **Mass-mailing virus** is enabled and the **Delete** action is selected, ScanMail will automatically delete a detected mass-mailing virus.

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

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

Configuring the Message Filter

Use the **Message Filter** tab to define how ScanMail treats encrypted or partial 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** group, 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 encrypted 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.
4. In the N**otification** group, select the notification options for when a file matches the notification filters.
5. In the **Email Stamp** group, define the safe email stamp settings.
6. 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** group, select **Create New Content Filter** (page 4-38) or **Add Existing Content Filter** (page 4-40).
5. In the **Action** group, select the **Action on mails with unwanted content** to specify the scan action.
6. In **Notification** group, 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**.

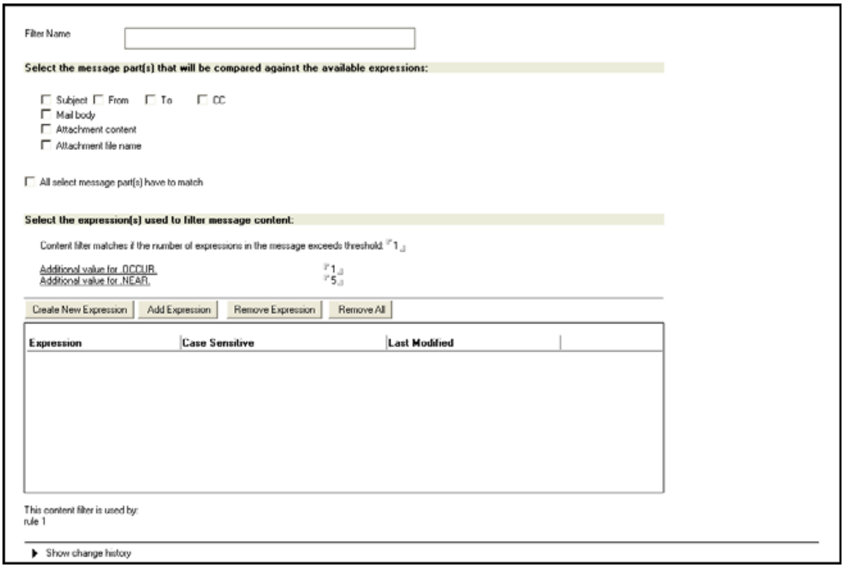
Create a New Content Filter

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 4-25 for details).



Filter Name

Select the message part(s) that will be compared against the available expressions:

□ Subject □ From □ To □ CC
□ Mail body
□ Attachment content
□ Attachment file name

□ All select message part(s) have to match

Select the expression(s) used to filter message content:

Content filter matches if the number of expressions in the message exceeds threshold: 1

Additional value for .OCCUR. 1
Additional value for .NEAR. 5

Expression	Case Sensitive	Last Modified

This content filter is used by:
rule 1

FIGURE 4-14. Creating a new content filter

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 4-41 or *Add New Expressions Based on Existing Expressions* on page 4-42 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 SMLD 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.(00[1-9]|0[1-9][0-9]|[1-6][0-9][0-9]|7[0-3][0-3]|7[56][0-9]|77[0
-2])[[:space:]|\.|\\|\||-]?\d{2}[[:space:]|\.|\\|\||-]?\d{4}
```

For Visa, MC, Discover, Switch/Solo, and JCB

```
.REG.(6011|5[1-5]\d{2}|4\d{3}|67\d{2})[[:space:]|\.|\\|\||-]?\d{4}[[:
space:]|\.|\\|\||-]?\d{4}[[:space:]|\.|\\|\||-]?\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 causes it to become unpredictably complex. Trend Micro recommends including one or two content filters per mail scan rule.

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 4-8. Recommended file extensions to block

EXTENSION	DESCRIPTION
`.386`	Windows Enhanced Mode Driver or Swap File
`.ACM`	Audio Compression Manager Driver (Windows) and Windows System File
`.ASP`	Active Server Page
`.AVB`	Inoculan Anti-Virus virus infected file
`.BAT`	Batch Processing
`.BIN`	Binary File
`.CLA`	Java Class File (usually `*.CLASS` but can be shortened)
`.CLASS`	Java Class File
`.CMD`	OS/2, Windows NT Command File, DOS CP/M Command File, dBase II Program File
`.CNV`	MS Word Data Conversion File
`.COM`	Executable File
`.CS*`	Corel Script
`.DLL`	Dynamic Link Library
`.DRV`	Device Driver
`.EXE`	Executable File
`.GMS`	Corel Global Macro Storage
`.HLP`	Windows Help File
`.HTA`	Hypertext Application (runs applications from HTML files)

`.HTM`
`.HTML`
	Hypertext Markup Language

`.HTT`	Hypertext Template
`.INF`	Information or Setup File

TABLE 4-8. Recommended file extensions to block

EXTENSION	DESCRIPTION
`.INI`	Initialization/Configuration file

`.JS*`
`.JS`
`.JSE`
	JavaScript Source Code

`.LNK`	Linker File, Windows Shortcut File
`.MHT*`	Microsoft MHTML Document (Archived Web Page)
`.MPD`	Mini Port Driver
`.OCX`	Object Linking and Embedding (OLE) Control Extension
`.OV*`	Program Overlay File (.OVL)
`.PIF`	Windows Program Information File
`.SCR`	Screen Saver Script
`.SHS`	Shell Scrap Object File
`.SYS`	System Device Driver
`.TLB`	Remote Automation Truelib Files
`.TSP`	Windows Telephony Service Provider
`.VBS`	Visual Basic Script
`.VBE`	Visual Basic Script Encrypted
`.VXD`	Virtual Device Driver
`.WBT`	WinBatch Script
`.WIZ`	Wizard File
`.WSH`	Windows Script Host Settings File

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** group, 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** group, 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**.

      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** group **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 N**otification** group, select the notification options for when a file matches the attachment filters.
8. In the **Email Stamp** group, define the safe email stamp settings.
9. Click **Save & Close**.

Configuring Script Filter

Use the **Script Filter** tab to define how ScanMail filters Lotus 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** group, type the stored form and rich text hotspot scripts to filter as follows:
   - **@Function strings** may contain any valid Lotus Notes function in Lotus Formula language. For example: `prompt`
   - **@Command strings** may contain any valid Lotus Notes formatted command in Lotus Formula language. For example: `[Execute]` or `[FileDatabaseDelete]`
   - **Script strings** may contain any valid LotusScript command from your operating system. For example: `shell`, `getobject`, `kill`, `rmdir`, or `activate`
   - **@URLOPEN URLs** can open any valid URLOPEN command in Lotus Formula language.
4. From the **Action** group, select the **Action on** items as appropriate.
5. Click ▼ to set the filter action for **Stored form hotspots and events** and the action for **Rich text hotspots**.

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 N**otification** group, select the notification options for when a file matches the notification filters.
7. In the **Email Stamp** group, 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. User the Administrator group, 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 3-5 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 group, 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:

```
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:

```
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 group, select **Enable incremental scan.**
6. Under the Duration group, specify the number of minutes that corresponds to the duration of the scan.

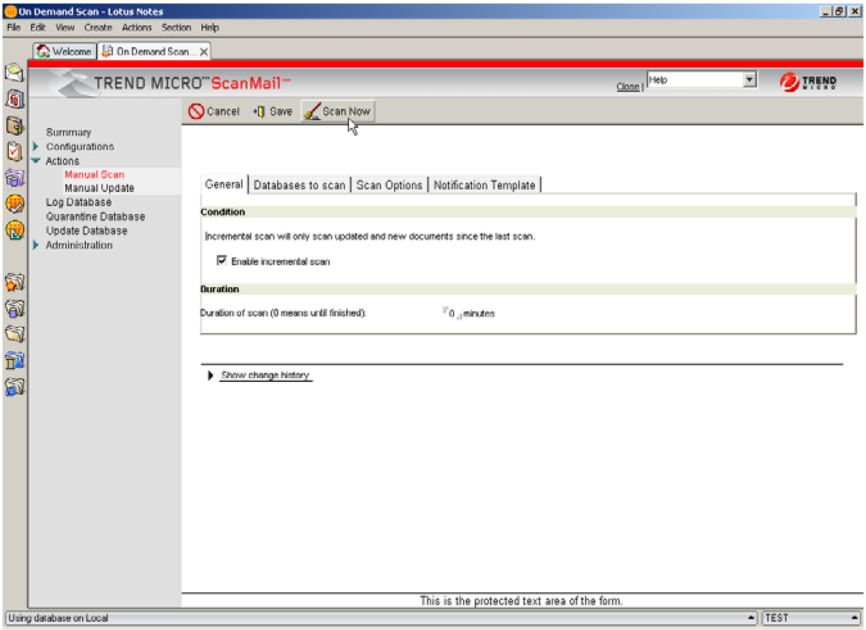
Note: If the scan duration is set to zero (0), the manual scan task will stop once it finishes scanning all databases.

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 set the following scan options:
   - Virus Scan (See *Configuring Virus Scan* on page 4-33)
   - Scan Restrictions (See *Configuring Scan Restrictions* on page 4-36)
   - Script Filter (See *Configuring Script Filter* on page 4-46)
9. Define the **notification template**.

10. Click **Scan Now**.



Condition

Incremental scan will only scan updated and new documents since the last scan.

☑ Enable incremental scan

Duration

Duration of scan (0 means until finished): 0 minutes

This is the protected text area of the form.

FIGURE 4-15. 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.

Chapter 5

Performing Administrative Tasks

The **Summary**, **Server Settings**, **CMAgent 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:

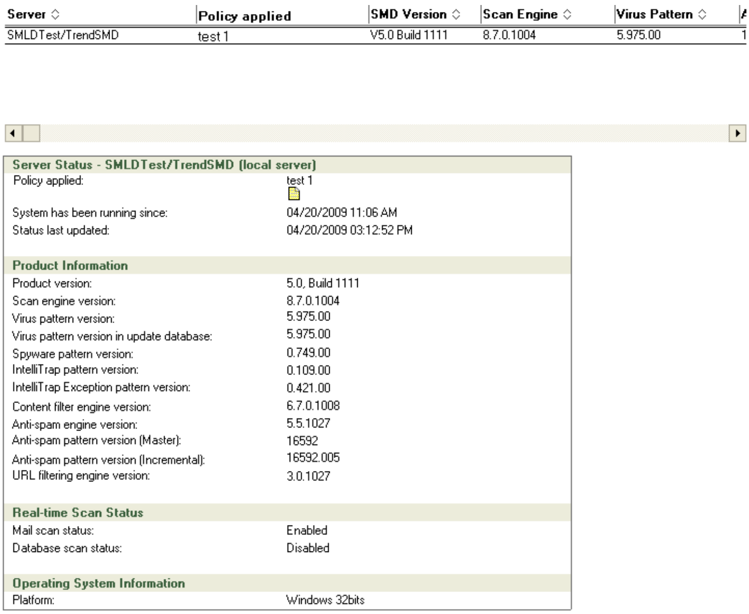
- *Viewing the Summary of All Servers* on page 5-2
- *Configuring the Server Settings Menu Options* on page 5-3
- *Configuring CMAgent Settings* on page 5-10
- *Configuring the Administration Menu Options* on page 5-11

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 3-7).
2. From the left menu, click **Summary**.



Server ◇	Policy applied	SMD Version ◇	Scan Engine ◇	Virus Pattern ◇	A
SMLDTest/TrendSMD	test 1	V5.0 Build 1111	8.7.0.1004	5.975.00	1

Server Status - SMLDTest/TrendSMD (local server)	
Policy applied:	test 1
System has been running since:	04/20/2009 11:06 AM
Status last updated:	04/20/2009 03:12:52 PM
Product Information	
Product version:	5.0, Build 1111
Scan engine version:	8.7.0.1004
Virus pattern version:	5.975.00
Virus pattern version in update database:	5.975.00
Spyware pattern version:	0.749.00
IntelliTrap pattern version:	0.109.00
IntelliTrap Exception pattern version:	0.421.00
Content filter engine version:	6.7.0.1008
Anti-spam engine version:	5.5.1027
Anti-spam pattern version (Master):	16592
Anti-spam pattern version (Incremental):	16592.005
URL filtering engine version:	3.0.1027
Real-time Scan Status	
Mail scan status:	Enabled
Database scan status:	Disabled
Operating System Information	
Platform:	Windows 32bits

FIGURE 5-1. The Status view displays the status of the current server

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.

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
- 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 3-7).
2. On the left menu, click **Configurations** > **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 Directories Used for Scanning* 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. Select the event that will trigger ScanMail to display notification via the Domino server console (see *Monitor Server Events* on page 5-7).
9. Enable server task monitoring (see *Enable Server Task Monitoring* on page 5-7).
10. 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 5-8).
11. Configure miscellaneous settings (see *Configure Miscellaneous Settings* on page 5-8).
12. 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 3-7).
2. From the left menu, click **Configurations** > **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**, **Event Log**, **Task Monitoring**, **Regional Option**, and **Misc** tabs to set the properties of a Server Setting rule.

Set Directories Used for Scanning

Use the **Temporary Directory** tab to set the directories that ScanMail should use when detaching temporary files for scanning.

To set temporary directories:

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. For each scan type, 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 3 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 6-10.

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**.

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 4-48.

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 real-time on-demand database scanning

Tip: Set the value per thread 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, type the number that corresponds to the number of trusted SMTP server(s) and type or click ▼ to select the trusted Domino server(s).

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 CMAgent Settings

The communication between SMLD and Control Manager uses a new protocol as SMLD no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of SMLD and Control Manager. The Control Manager Agent can be registered after completing the SMLD installation. The following describes how to configure the CMAgent settings:

Note: CMAgent is automatically installed during the SMLD 5.0 installation process.

To create or modify CMAgent Settings:

1. From the left menu, select **Configurations > CMAgent Settings**.
2. From the working area, click **Create CMAgent Settings**.

   Note: To modify and existing setting, double-click the setting and click **Edit** on the Control Manager settings screen.

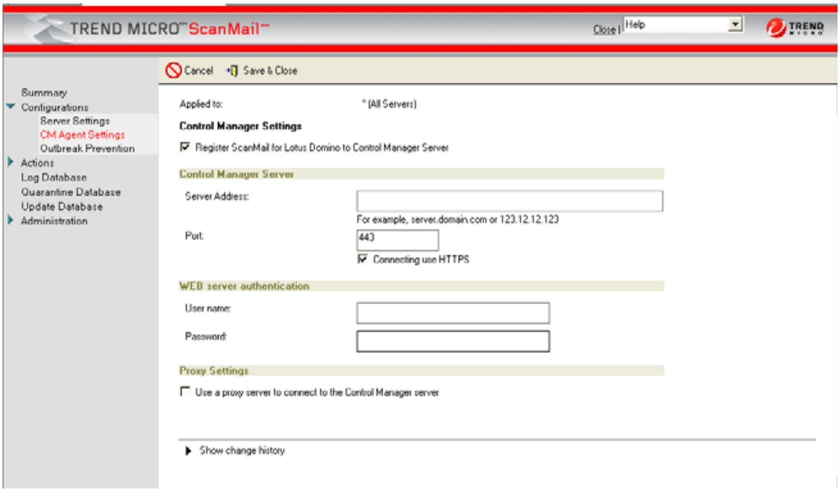
3. Type the server name in the Applied to field, or click ▼ to choose.
4. Under the **Control Manager Settings** group, select **Register ScanMail for Lotus Domino to Control Manager Server**.
5. Under the **Control Manager Server** group, type the **Server Address** and **Port** number in the appropriate 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:

- 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**.



Applied to: * (All Servers)

Control Manager Settings

☑ Register ScanMail for Lotus Domino to Control Manager Server

Control Manager Server

Server Address:

For example, server.domain.com or 123.12.12.123

Port: 443

☑ Connecting use HTTPS

WEB server authentication

User name:

Password:

Proxy Settings

☐ Use a proxy server to connect to the Control Manager server

FIGURE 5-2. Control Manager settings screen

Configuring the Administration Menu Options

Use the Configuration Database **Administration** menu to define additional ScanMail database properties such as creating the license profile or applying a new ACL entry.

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.

To set and apply Notes database properties to ScanMail databases:

1. Open the ScanMail Configuration Database (see *Accessing ScanMail Databases* on page 3-7).
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 3-7).
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 3-7).
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 3-7).
2. Click **Administration** > **Product License**.

3. From the working area, click **Create License Profile**.
4. Type or copy the *ScanMail Activation Code* on page 2-45 in the field provided.
5. Click **Save & Close**.

Deleting a License Profile

Use the Configuration database to create a license profile to delete the license profile of an old or expired ScanMail version.

Note: To convert an evaluation version to a full version, create a new license profile first before deleting the old profile. See *Convert to a Full Version* on page 2-46.

To delete a license profile:

1. Open the ScanMail Configuration database (see *Accessing ScanMail Databases* on page 3-7).
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

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 rule** 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 **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 ScanMail* on page 2-44.

Updating Components

There are two ways to update the ScanMail components:

- Manually
- Automatically

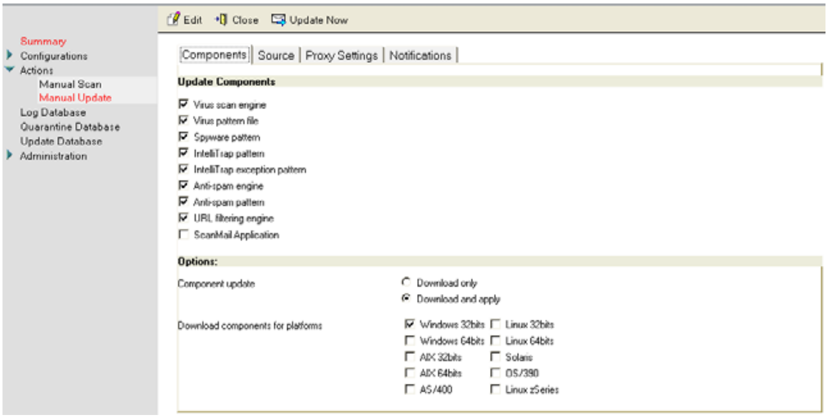
Updating Components Manually

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 3-7).
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 **Update 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**.



Update Components

☑ Virus scan engine
☑ Virus pattern file
☑ Spyware pattern
☑ IntelliTrap pattern
☑ IntelliTrap exception pattern
☑ Anti-spam engine
☑ Anti-spam pattern
☑ URL filtering engine
☐ ScanMail Application

Options:

Component update: ○ Download only ● Download and apply

Download components for platforms:

☑ Windows 32bits	☐ Linux 32bits
☐ Windows 64bits	☐ Linux 64bits
☐ AIX 32bits	☐ Solaris
☐ AIX 64bits	☐ OS/390
☐ AS/400	☐ Linux zSeries

FIGURE 6-1. **Click *Update Now* to download the latest antivirus and content security components.**

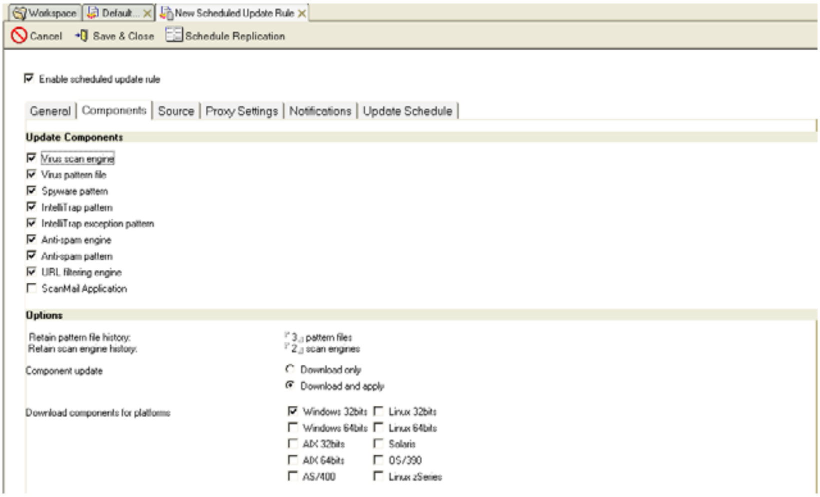
Updating Components Automatically Using Scheduled Update Rules

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 4-6).
2. Click **Configurations > Policies > Edit/Create New Policy > Scheduled Update** tab.
3. Select **Enable scheduled update**.

4. Set which components to deploy automatically (see *Deploy Specific Components Automatically* on page 6-6).
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.



☑ Enable scheduled update rule

Update Components

☑ Virus scan engine
☑ Virus pattern file
☑ Spyware pattern
☑ IntelliTrap pattern
☑ IntelliTrap exception pattern
☑ Anti-spam engine
☑ Anti-spam pattern
☑ URL filtering engine
☐ ScanMail Application

Options

Retain pattern file history: 3 pattern files
Retain scan engine history: 2 scan engines

Component update: ○ Download only ● Download and apply

Download components for platforms: ☑ Windows 32bits ☐ Linux 32bits ☐ Windows 64bits ☐ Linux 64bits ☐ AIX 32bits ☐ Solaris ☐ AIX 64bits ☐ OS/390 ☐ AS/400 ☐ Linux zSeries

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 6-8).
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 6-10).
13. Click the **Notifications** tab.
14. Under the **Notify administrator** group, define the notification settings as appropriate (see *Setting the Update Notifications* on page 7-7).

> **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 4-6).
2. Click **Configurations > Policies > Edit/Create New Policy > Scheduled Update** tab.
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: Lotus 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:

  http://smld5-p.activeupdate.trendmicro.com/activeupdate/

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.

Note: The UNC source only applies to ScanMail for Lotus 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.

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 (see *Automatically* on page 6-3) or (*Manually* on page 6-3).
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://smld5-p.activeupdate.trendmicro.com/activeupdate/server.ini

2. Open the file, and locate the latest zip file name for the virus pattern: for example: ***`vsapi952.zip`***.
3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:

   ```
   http://smld5-p.activeupdate.trendmicro.com/activeupdate/patt
   ern/vsapi952.zip
   ```

4. Open the ScanMail Update Database (see *Accessing ScanMail Databases* on page 3-7 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-11).
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` using the Domino server console:
11. Load SMDupd

    ```
    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://smld5-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:

   http://smld5-p.activeupdate.trendmicro.com/activeupdate/pattern/ssaptn.zip
4. Open the ScanMail Update Database (see *Accessing ScanMail Databases* on page 3-7 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-11).
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 rule:

1. Locate the latest anti-spam rule version number from the activeupdate ***`server.ini`*** file at:

   http://smld5-p.activeupdate.trendmicro.com/activeupdate/server.ini
2. Open the file, and locate the latest zip file name for the anti-spam rule: for example: ***`ias6176.zip.`***
3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:

   http://smld5-p.activeupdate.trendmicro.com/activeupdate/antispam/ias6176.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 3-7 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-11).

6. On the left menu, click Anti-spam Rule.
7. On the working area, click Edit.
8. Attach the latest version to the Anti-spam rule field.
9. Update the Anti-spam rule 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://smld5-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:

   http://smld5-p.activeupdate.trendmicro.com/activeupdate/antispam/tmaseng.zip
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 3-7 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-11).
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://smld5-p.activeupdate.trendmicro.com/activeupdate/server.ini

2. Open the file, and locate the latest zip file name for IntelliTrap: for example: ***`tmblack110.zip`***.
3. Combine the appropriate path and filename information to the following URL according to the latest pattern file; for example:

   http://smld5-p.activeupdate.trendmicro.com/activeupdate/pattern/tmblack110.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 3-7 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-11).
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://smld5-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:

   http://smld5-p.activeupdate.trendmicro.com/activeupdate/pattern/tmwhite.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 3-7 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-11).
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`.
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:\Lotus\Domino`).
4. Open the ScanMail Update Database (see *Accessing ScanMail Databases* on page 3-7 or *Accessing other ScanMail Databases through the Configuration Database* on page 3-11).
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 Lotus Domino Notifications

When ScanMail detects a virus or other threat infection in a mail, attachment, or document, ScanMail can automatically alert, by email or Lotus 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

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.

There are two ScanMail 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.

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:

SCAN OPTIONS	TAGS	RETURNS WHAT
Virus Scan	%FILE%	File name of the infected file
	%DETECTION%	Name of the malware detected
	%ACTION%	Scan action
Scan Restrictions	%FILE%	File name of the infected file
	%CAUSE%	Matching scan restriction option
	%ACTION%	Scan action
Message Filter	%CAUSE%	Matching message filter option
	%ACTION%	Filter action
Attachment Filter	%FILE%	File name of the infected attachment
	%CAUSE%	Matching attachment filter option
	%ACTION%	Filter action
Content Filter	%CONTENT_FILTER_NAME%	Matching content filter
	%MAILPART%	Message part that matches the content filter: Header, message body, or attachment
	%ACTION%	Filter action
Script Filter	%FORM_PART%	Message part that matches the script filter
	%KEYWORDS%	Matching keyword(s)

- 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.

TAGS	RETURNS WHAT
%DATABASE%	Database name
%version%	Pattern/Engine version
%SERVER%	Domino/ScanMail server
%SENDER%	Sender of the message that matched a scan rule
%RECIPIENTS%	Recipient(s) of the message that matched a scan rule
%SUBJECT%	Subject header of the message that matched a scan rule
%SEND_TIME%	Time (in hh:mm format) when the message was sent
%FINAL_ACTION%	Final scan/Filter action taken
%MATCHING_FILTER%	Matching filter
%SCAN_TIME%	Time (in hh:mm format) when ScanMail scanned a message
%PRODUCTVERION%	ScanMail for Domino version
%PATTERNVERSION%	Virus pattern file version
%SCANENGINEVERSION%	Scan engine version
%RULENAME%	Rule name
%RULENUMBER%	Rule priority
%ADMIN_FILTER_INFORMATION%	Consolidates selected filter-based tags () for notifications sent to administrators
%OWNER_FILTER_INFORMATION%	Consolidates selected filter-based tags for notifications sent to database owners
%INTERNAL_FILTER_INFORMATION%	Consolidates selected filter-based tags for notifications sent to senders or recipients belonging to the Domino address book
%EXTERNAL_FILTER_INFORMATION%	Consolidates selected filter-based tags for notifications sent to senders or recipients not belonging to the Domino address book
%OS%	Platform (for example, Windows)
%COMPONENT%	Antivirus or content security component

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 7-6). 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:

Scan Options Tab	Available Email Stamp
Virus Scan	You can: • Insert warning to the original mail if a virus is detected • Insert message to the original mail if mail is malware-free Insert email stamps at the end of the subject header or message body.
Scan Restrictions	You can Insert the stamp as a subject prefix.
Message Filter	You can Insert the stamp as a subject suffix.
Attachment Filter	You can Insert the stamp as a subject suffix.
Script Filter	Insert email stamps at the end of the subject header or at the beginning of the message body. You can also replace hotspots with email stamps as hotspots.

Check the following links to define safe stamps for applicable filters:

- **Spam filter** stamp, see page 4-29
- **Web Reputation** stamp, see page 4-30
- **Virus Scan** stamp, see page 4-35
- **Scan Restrictions** stamp, see page 4-36
- **Message Filter** stamp, see page 4-36
- **Attachment Filter** stamp, see page 4-46
- **Script Filter** stamp, see page 4-46

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 Lotus Instant Messaging and Web Conferencing. Use the **Notifications** tab to define the medium that ScanMail uses to deliver notifications.

To define how ScanMail delivers notifications:

1. Create or modify a policy (see *Creating Policies* on page 4-3) or (*Modifying Policies* on page 4-6).
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 a Lotus 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 Lotus 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 Lotus Instant Messaging and Web Conferencing account(s).

4. Click **Save & Close**.

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 7-6).

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 6-4) or (*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:

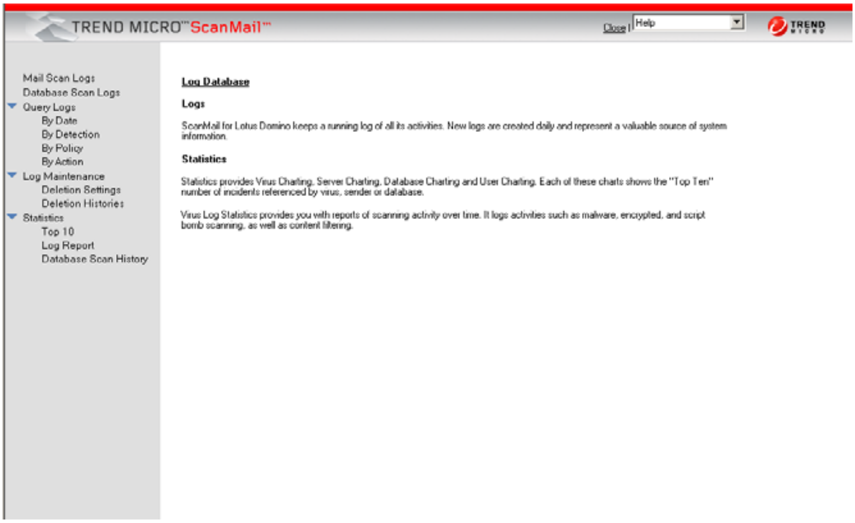
Using the Log Database

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.



Log Database

Logs

ScanMail for Lotus Domino keeps a running log of all its activities. New logs are created daily and represent a valuable source of system information.

Statistics

Statistics provides Virus Charting, Server Charting, Database Charting and User Charting. Each of these charts shows the "Top Ten" number of incidents referenced by virus, sender or database.

Virus Log Statistics provides you with reports of scanning activity over time. It logs activities such as malware, encrypted, and script bomb scanning, as well as content filtering.

FIGURE 8-1. ScanMail Log Database main screen

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.

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.

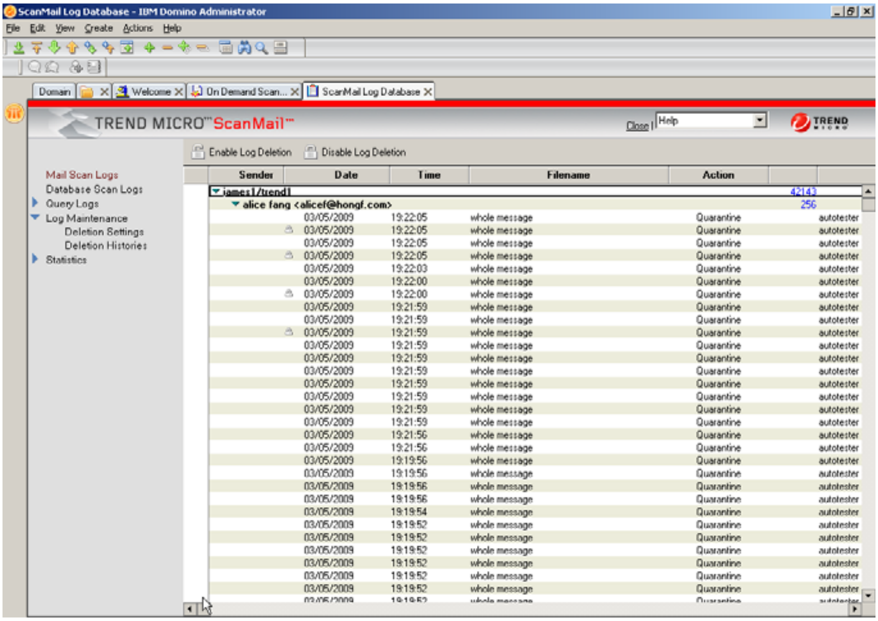
Use the ScanMail Log Database to access and view ScanMail logs.

Enable/Disable 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**.



Sender	Date	Time	Filename	Action		
james1/trend1					42143	
alice fang <alicef@hongf.com>					256	
	03/05/2009	19:22:05	whole message	Quarantine		autotester
🔒	03/05/2009	19:22:05	whole message	Quarantine		autotester
	03/05/2009	19:22:05	whole message	Quarantine		autotester
🔒	03/05/2009	19:22:05	whole message	Quarantine		autotester
	03/05/2009	19:22:03	whole message	Quarantine		autotester
	03/05/2009	19:22:00	whole message	Quarantine		autotester
🔒	03/05/2009	19:22:00	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
🔒	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:59	whole message	Quarantine		autotester
	03/05/2009	19:21:56	whole message	Quarantine		autotester
	03/05/2009	19:21:56	whole message	Quarantine		autotester
	03/05/2009	19:19:56	whole message	Quarantine		autotester
	03/05/2009	19:19:56	whole message	Quarantine		autotester
	03/05/2009	19:19:56	whole message	Quarantine		autotester
	03/05/2009	19:19:56	whole message	Quarantine		autotester
	03/05/2009	19:19:54	whole message	Quarantine		autotester
	03/05/2009	19:19:52	whole message	Quarantine		autotester
	03/05/2009	19:19:52	whole message	Quarantine		autotester
	03/05/2009	19:19:52	whole message	Quarantine		autotester
	03/05/2009	19:19:52	whole message	Quarantine		autotester
	03/05/2009	19:19:52	whole message	Quarantine		autotester
	03/05/2009	19:19:52	whole message	Quarantine		autotester
	03/05/2009	19:19:52	whole message	Quarantine		autotester

FIGURE 8-2. 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.

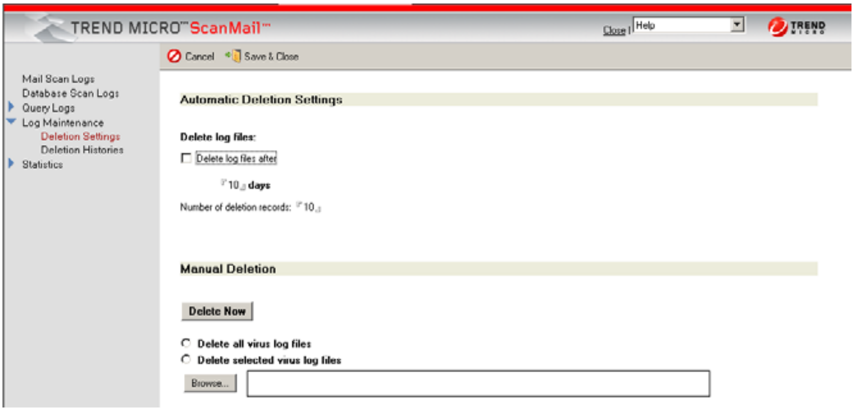
Deleting Virus Logs Automatically

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 8-3).



Automatic Deletion Settings

Delete log files:

□ Delete log files after

10 days

Number of deletion records: 10

Manual Deletion

○ Delete all virus log files

○ Delete selected virus log files

FIGURE 8-3. Automatic / Manual Deletion settings

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 8-3).
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 virus scanning, message filtering, attachment filtering, content filtering, script filtering, spam filtering, URL 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**
   - **Virus Scan**
   - **Message Filter**
   - **Attachment Filter**
   - **Content Filter**
   - **Script Filter**
   - **Spam Filter**
   - **Web Reputation**
   - **Outbreak Prevention Filter**
   - **Redirected Messages**
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.

Note: Use an electronic spreadsheet application (for example, Microsoft Excel™) to open `*.csv` files.

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

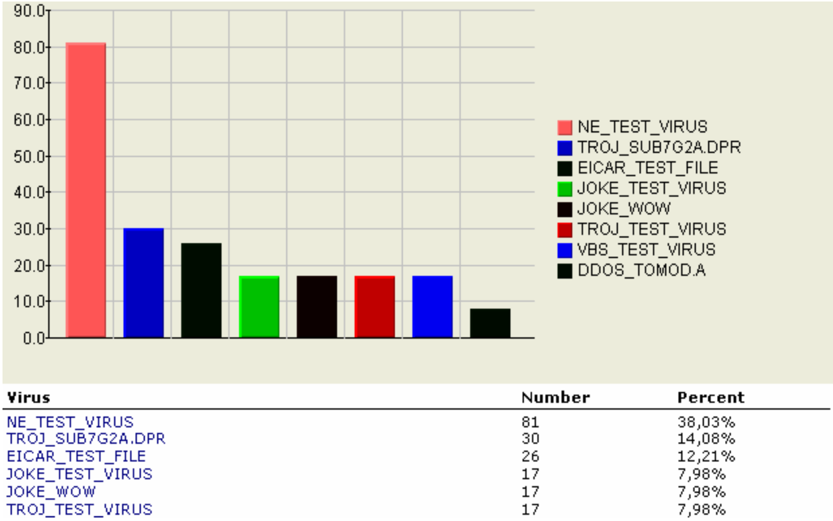
The **Statistics > Top 10** option allows you to generate any of the following charts in a column layout:

- **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**.
   - Open ***`smvlog.nsf`***
2. From the Log Database left menu, click **Statistics** > **Top 10**.
3. From the working area, select the chart type to generate and view.
4. Select a date, either **All** or a **Date Range**.
5. 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.



Virus	Number	Percent
NE_TEST_VIRUS	81	38,03%
TROJ_SUB7G2A.DPR	30	14,08%
EICAR_TEST_FILE	26	12,21%
JOKE_TEST_VIRUS	17	7,98%
JOKE_WOW	17	7,98%
TROJ_TEST_VIRUS	17	7,98%

FIGURE 8-4. A sample Detection Chart

Enabling/Disabling Database Scan History Deletion

Use the Log database to enable or disable Database Scan History deletion.

Deleting Database Scan History Automatically

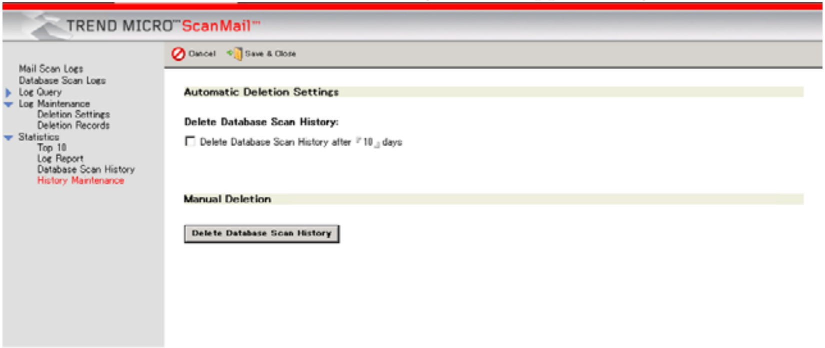
Use the Log database to schedule ScanMail to delete Database Scan History older than the specified number of days automatically. This is especially useful if a Domino server handles a large amount of traffic.

To delete Database Scan History 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 **Statistics** > **History Maintenance**. The Automatic / Manual Deletion Settings screen appears (Figure 8-5).



Automatic Deletion Settings

Delete Database Scan History:

□ Delete Database Scan History after 10 days

Manual Deletion

FIGURE 8-5. Automatic / Manual Deletion settings

3. On the **Automatic Deletion Settings** section, select **Delete Database Scan History after**.

4. Type the **number of days** that corresponds to the age of Database Scan History that ScanMail will save.

5. Click **Save & Close**.

Deleting Database Scan History Manually

Use the Log database to delete Database Scan History manually.

To delete Database Scan History manually:

1. Do one of the following to open the Log database:
   - From the ScanMail Configuration left menu, click **Log Database**.
   - Open ***`smvlog.nsf`***.

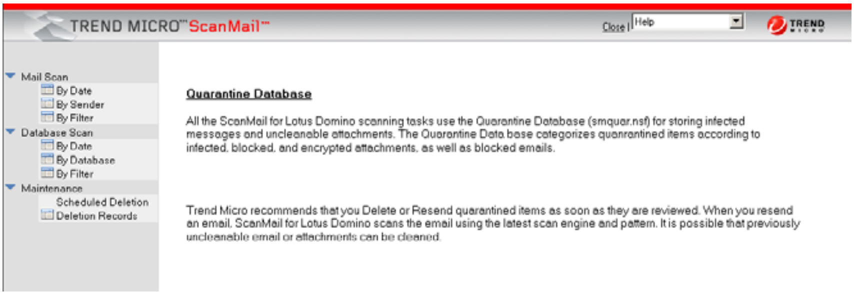
2. From the left menu of the Log database, click **Statistics** > **History Maintenance**. The Automatic / Manual Deletion Settings screen appears (see Figure 8-5).

3. On the **Manual Deletion** section, select **Delete Database Scan History** to delete all existing Database Scan History available on the Log database.

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.



Quarantine Database

All the ScanMail for Lotus Domino scanning tasks use the Quarantine Database (smquar.nsf) for storing infected messages and uncleanable attachments. The Quarantine Data base categorizes quanrantined items according to infected, blocked, and encrypted attachments, as well as blocked emails.

Trend Micro recommends that you Delete or Resend quarantined items as soon as they are reviewed. When you resend an email, ScanMail for Lotus Domino scans the email using the latest scan engine and pattern. It is possible that previously uncleanable email or attachments can be cleaned.

FIGURE 8-6. Quarantine Database main screen

Configure ScanMail to delete quarantined items every "x" days automatically (see *Deleting Quarantined Items Automatically* starting on page 8-14). Alternatively, you can manually delete quarantined items from the Quarantine database (see *Deleting Quarantined Items Manually* starting on page 8-16).

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; then, right-click, and select **Copy**.
4. Open the database where the quarantined document was to be saved, and **Paste** the copied document.

Enabling/Disabling Quarantined Item Deletion

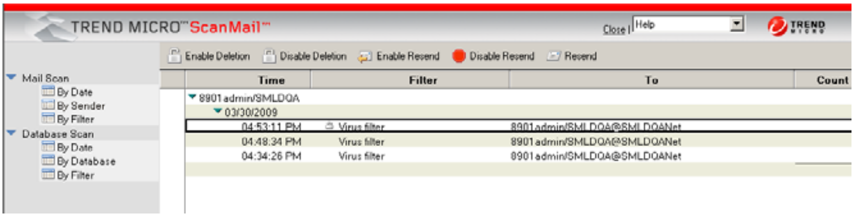
Use the Quarantine database to enable or disable quarantined item deletion. When an item is enabled for deletion, ScanMail can delete it automatically.

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**.



Time	Filter	To	Count
8901 admin/SMLDQA			
03/30/2009			
04:53:11 PM	Virus filter	8901admin/SMLDQA@SMLDQANet	
04:48:34 PM	Virus filter	8901admin/SMLDQA@SMLDQANet	
04:34:26 PM	Virus filter	8901admin/SMLDQA@SMLDQANet	

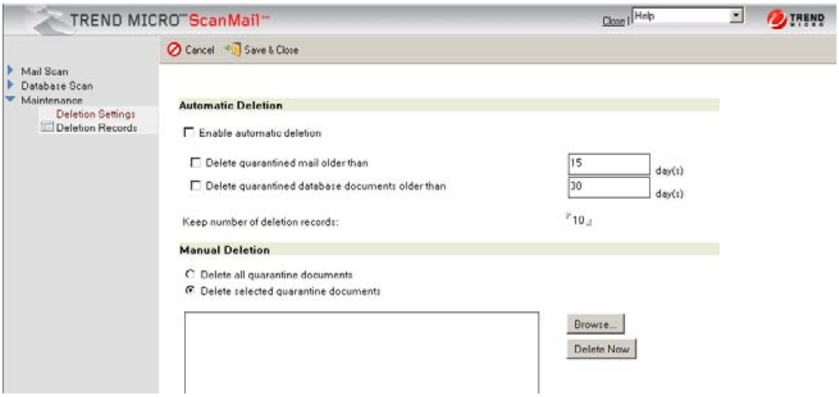
FIGURE 8-7. Enabling/Disabling quarantined item for deletion

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 8-8).

Note: ScanMail automatically deletes quarantine items enabled for deletion.



Automatic Deletion

□ Enable automatic deletion

□ Delete quarantined mail older than 15 day(s)

□ Delete quarantined database documents older than 30 day(s)

Keep number of deletion records: 10

Manual Deletion

○ Delete all quarantine documents

● Delete selected quarantine documents

FIGURE 8-8. Automatic and Manual deletion screen

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.

Note: Deleted Mail Scan and Database Scans are kept in the Deletion Records folder according to the number of deletion records set to keep in **Maintenance > Deletion Settings > Keep number of deletion records**.

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.

Chapter 9

Using ScanMail for Lotus 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 9-4

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 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 SMLD and the Control Manager uses a new protocol called the Trend Micro Control Manager Management Communication Protocol (MCP). SMLD no longer supports the Trend Micro Management Infrastructure (TMI) protocol used by previous versions of SMLD and the Control Manager.

The Control Manager Agent can be registered after installing SMLD. SMLD supports Web console redirection from the Control Manager. Access the SMLD product console directly from the Control Manager product console using a separate user name and password for the SMLD 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 3.5-http://{host name}/ControlManager
   ```

   ```
   For TMCM 5.0-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 scan engine** on the Control Manager management console, the Control Manager agent instructs ScanMail for Lotus 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 SMLD 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 rule, 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 rules
   - 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 event logs:

1. From the working area, click **Logs**.
2. Select the type of logs you want to view:

- **Security logs** include all virus log incidents, content security violations, Spam Violation Log, and viruses found in email and databases.
- **Event logs** include Control Manager server commands sent to its managed products and managed product status change events.

Note: Events specific to ScanMail appear only in the content security violations portion of the Security log.

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. Click **Save**.
3. On the **Save As** screen, specify the location where you want to keep the file.
4. 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 **Configurations** > **Outbreak Prevention**.

Details of the active Outbreak Prevention Policy should display on the working area.

- Through the Control Manager management console > **Services** page

  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 SMLD

This chapter provides information on how to remove ScanMail components from a Domino environment.

This chapter includes the following topics:

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.

Note: Before removing ScanMail, confirm that the Domino server and client are not running; if they are, shut down the Domino server and client.

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 ScanMail for Windows

To run an automatic ScanMail uninstallation using a graphical desktop environment:

1. Click **Start** > **Programs** > **Trend Micro ScanMail for Lotus Domino** > **Uninstall ScanMail for Lotus Domino 5.0**.

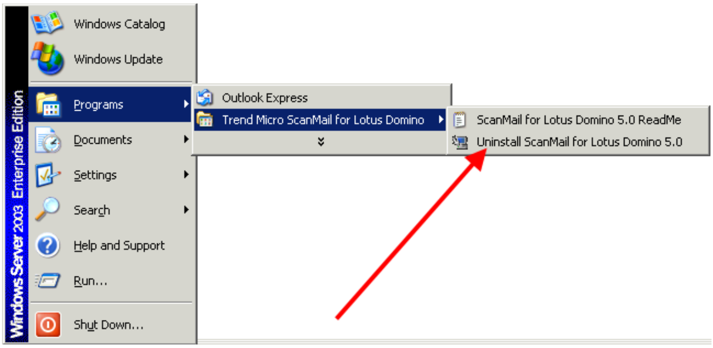
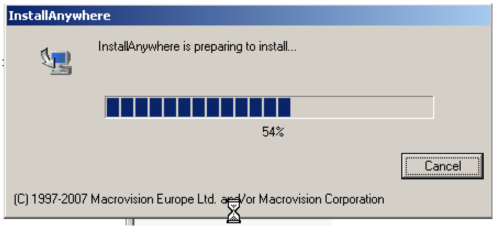

Windows Server 2003 Enterprise Edition
Windows Catalog
Windows Update
Programs
Documents
Settings
Search
Help and Support
Run...
Shut Down...
Outlook Express
Trend Micro ScanMail for Lotus Domino
ScanMail for Lotus Domino 5.0 ReadMe
Uninstall ScanMail for Lotus Domino 5.0

FIGURE 10-1. Select Uninstall ScanMail for Domino 5.0

2. After selecting **Uninstall ScanMail for Lotus Domino 5.0**, the uninstallation progress screen appears.


InstallAnywhere

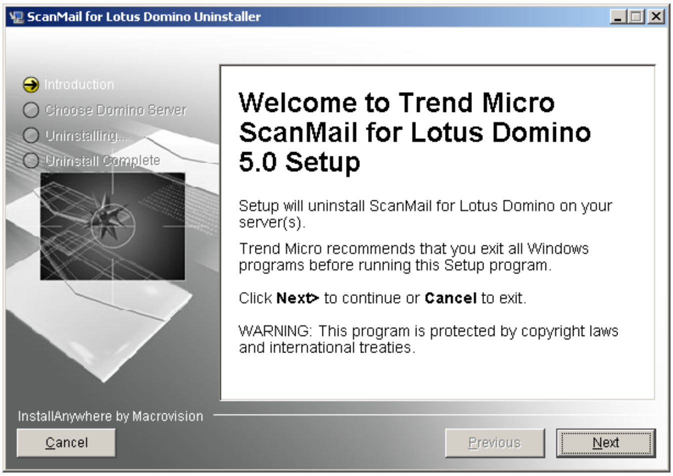
InstallAnywhere is preparing to install...

54%

(C) 1997-2007 Macrovision Europe Ltd. and/or Macrovision Corporation

FIGURE 10-2. Uninstallation progress screen

3. After the uninstallation progress screen completes, the **Welcome to Trend Micro ScanMail for Lotus Domino Uninstaller** screen appears. Click **Next**; the wizard proceed to **Choose Domino Server** step.



Welcome to Trend Micro ScanMail for Lotus Domino 5.0 Setup

Setup will uninstall ScanMail for Lotus Domino on your server(s).

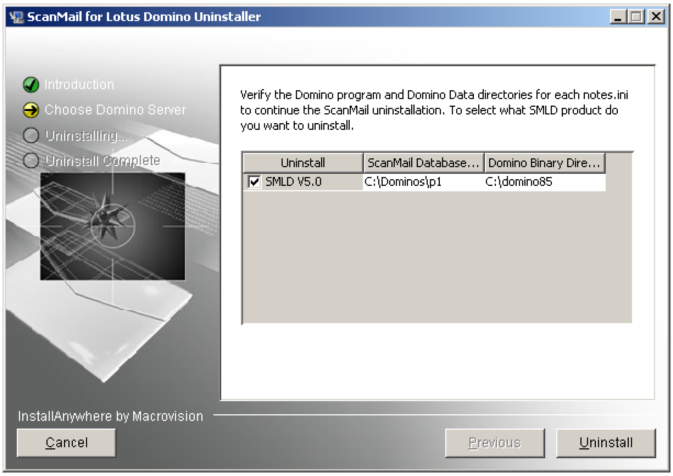
Trend Micro recommends that you exit all Windows programs before running this Setup program.

Click **Next>** to continue or **Cancel** to exit.

WARNING: This program is protected by copyright laws and international treaties.

FIGURE 10-3. Welcome Screen

4. On the **Choose Domino Server** step, select the server(s) from which to remove ScanMail and click **Uninstall**.

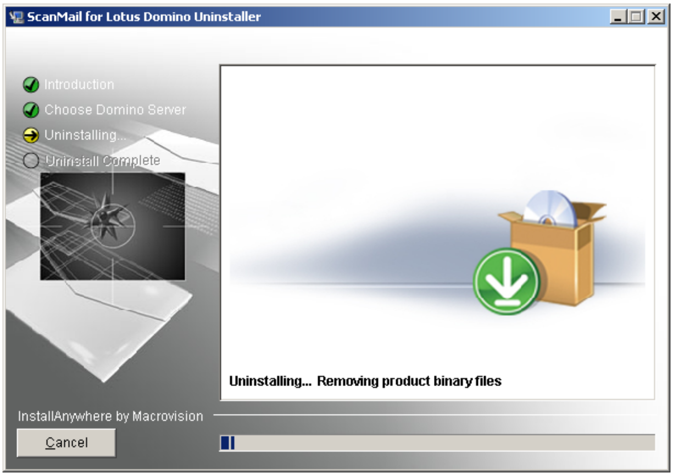


Verify the Domino program and Domino Data directories for each notes.ini to continue the ScanMail uninstallation. To select what SMLD product do you want to uninstall.

Uninstall	ScanMail Database...	Domino Binary Dire...
☑ SMLD V5.0	C:\Dominos\p1	C:\domino85

FIGURE 10-4. Select server from which to uninstall SMLD

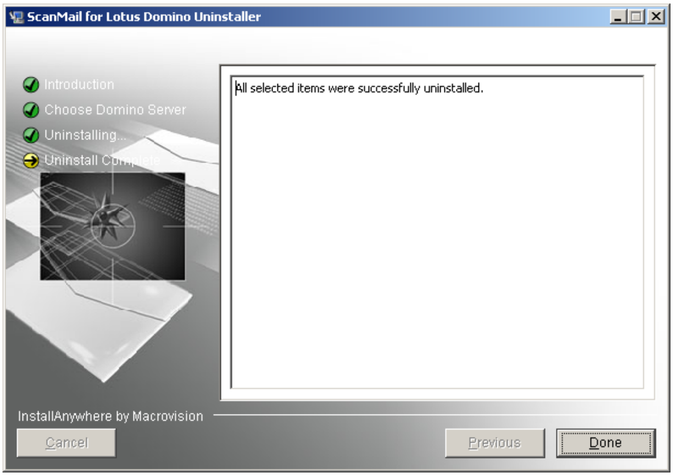
5. After you execute the uninstall process, the **Uninstalling** progress screen displays.



Uninstalling... Removing product binary files

FIGURE 10-5. Uninstalling ScanMail

6. When the **Uninstalling** process finishes, the **Uninstall Complete** screen appears. Click **Done**. See Figure 10-6.



All selected items were successfully uninstalled.

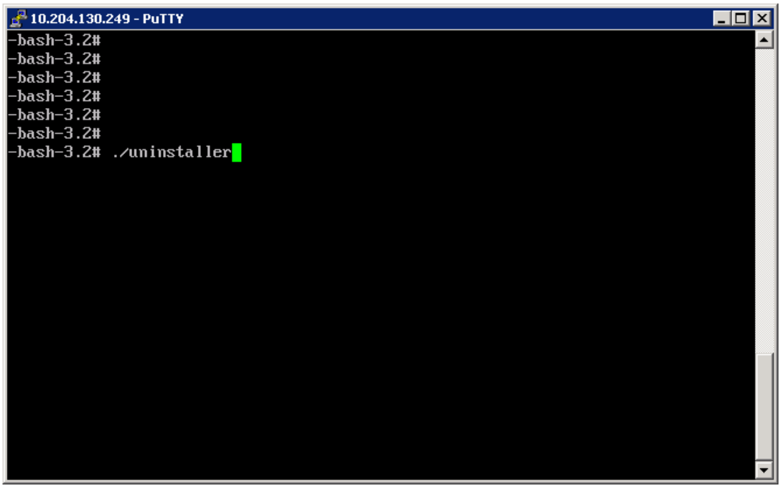
FIGURE 10-6. Uninstallation complete

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 ScanMail for AIX

To remove ScanMail, perform the following steps:

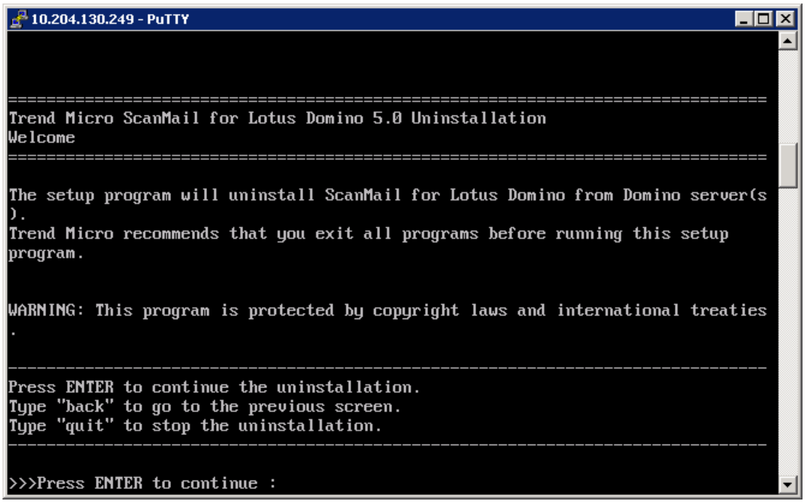
1. Open **Terminal**, and navigate to ***`uninstall`*** folder under SMLD installation path (for example, `/opt/trend/SMLD/uninstall`).
2. Run the uninstallation file (***`uninstaller`***) using command **./uninstaller**.



```
-bash-3.2#
-bash-3.2#
-bash-3.2#
-bash-3.2#
-bash-3.2#
-bash-3.2#
-bash-3.2# ./uninstaller
```

FIGURE 10-7. Running the uninstallation file

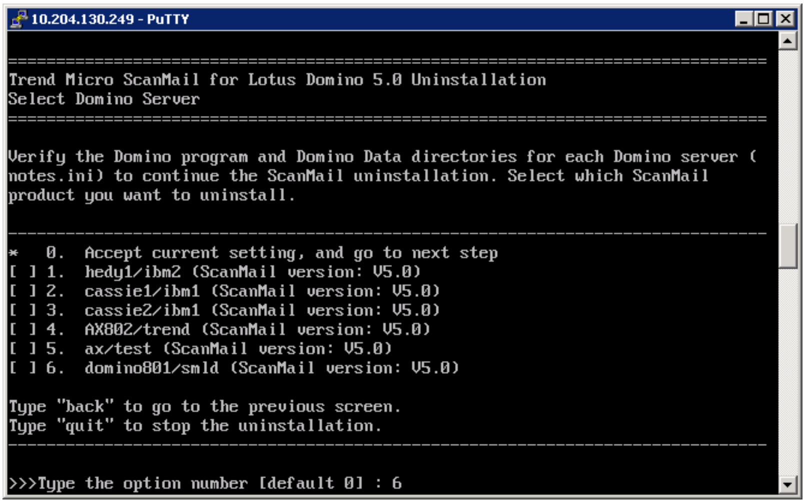
The SMLD uninstall **Welcome** screen appears.



```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Uninstallation
Welcome
================================================================================

The setup program will uninstall ScanMail for Lotus Domino from Domino server(s
).
Trend Micro recommends that you exit all programs before running this setup
program.


WARNING: This program is protected by copyright laws and international treaties
.

--------------------------------------------------------------------------------
Press ENTER to continue the uninstallation.
Type "back" to go to the previous screen.
Type "quit" to stop the uninstallation.
--------------------------------------------------------------------------------

>>>Press ENTER to continue :
```

FIGURE 10-8. Welcome screen

3. Press **Enter**. The **Select Domino Server** screen appears.



```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Uninstallation
Select Domino Server
================================================================================

Verify the Domino program and Domino Data directories for each Domino server (
notes.ini) to continue the ScanMail uninstallation. Select which ScanMail
product you want to uninstall.

--------------------------------------------------------------------------------
*   0.  Accept current setting, and go to next step
[ ] 1.  hedy1/ibm2 (ScanMail version: V5.0)
[ ] 2.  cassie1/ibm1 (ScanMail version: V5.0)
[ ] 3.  cassie2/ibm1 (ScanMail version: V5.0)
[ ] 4.  AX802/trend (ScanMail version: V5.0)
[ ] 5.  ax/test (ScanMail version: V5.0)
[ ] 6.  domino801/smld (ScanMail version: V5.0)

Type "back" to go to the previous screen.
Type "quit" to stop the uninstallation.
--------------------------------------------------------------------------------

>>>Type the option number [default 0] : 6
```

FIGURE 10-9. Select Domino Server screen showing installed Domino server(s)

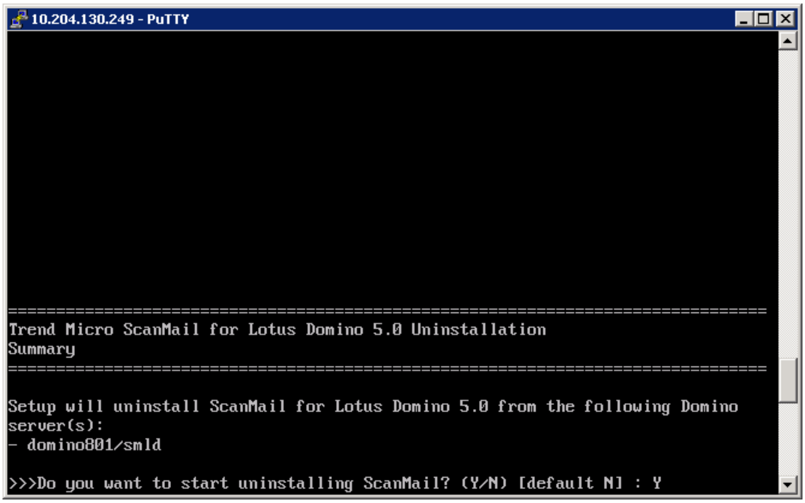
On the screen shown in Figure 10-9, the list of all Domino servers installed is displayed. Select or deselect the domino server(s) you want to remove or keep.

To select or deselect the Domino server:

a. Type the corresponding number. For example, if you want to select the server named as **domino801/smld** from the list shown on the screen in Figure 10-9, type *6*.

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.

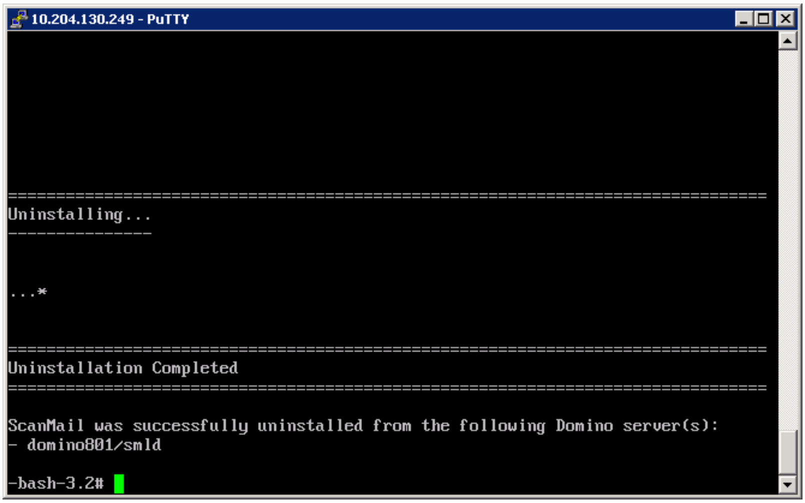


```
================================================================================
Trend Micro ScanMail for Lotus Domino 5.0 Uninstallation
Summary
================================================================================

Setup will uninstall ScanMail for Lotus Domino 5.0 from the following Domino
server(s):
- domino801/smld

>>>Do you want to start uninstalling ScanMail? (Y/N) [default N] : Y
```

FIGURE 10-10. 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.



```
================================================================================
Uninstalling...
---------------


...*


================================================================================
Uninstallation Completed
================================================================================

ScanMail was successfully uninstalled from the following Domino server(s):
- domino801/smld

-bash-3.2#
```

FIGURE 10-11. Uninstallation Complete

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`***, 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 Appendix C, *Program File and Folder Lists* on page C-1 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: `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 ***smdsys.ini*** for a Windows server that has multiple instances of ScanMail:

```
[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=V5.0 \\indicates ScanMail version is 5.0
InstallType=32-bit \\indicates it is a 32-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\Lotus\Domino1\Data1\notes.ini
DomSvr0DominoBinPath=C:\IBM\Lotus\Domino1
DomSvr0DataPath=C:\IBM\Lotus\Domino1\Data1
DomSvr0DominoVersion=0
DomSvr0SMDVersion=5.0
[DomSvr1] \\indicates the second partition server of first
ScanMail instance
w=C:\IBM\Lotus\Domino1\Data2\notes.ini
DomSvr1DominoBinPath=C:\IBM\Lotus\Domino1
DomSvr1DataPath=C:\IBM\Lotus\Domino1\Data2
DomSvr1DominoVersion=0
DomSvr1SMDVersion=5.0
[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=V5.0
DomSvrISMDSecs=DomSvr2 \\indicates partition servers of
second ScanMail instance
[DomSvr2] \\indicates the first partition server of second
ScanMail instance
DomSvr2NotesIniPath=C:\IBM\Lotus\Domino2\Data1\notes.ini
DomSvr2DominoBinPath=C:\IBM\Lotus\Domino2
DomSvr2DataPath=C:\IBM\Lotus\Domino2\Data1
DomSvr2DominoVersion=0
DomSvr2SMDVersion=5.0
```

2. If the SMLD instance is removed from all the partition servers that share the Domino binary, then navigate to the directory specified in

`DomSvr{X}DominoBinPath`, and then search for and delete the corresponding ScanMail files:

- `DominoBinPath` ScanMail files on a Windows server (see *Table C-1* on page C-2).

3. Navigate to the directory specified in `DomSvr{X}DataPath`, and then delete the ScanMail installation and temporary folders.
4. Using a text editor, open the ***`notes.ini`*** specified in `DomSvr{X}NotesIniPath`, 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. Delete ***`smd.ini`***. This file is located in the path specified in `DomSvr{X}DominoBinPath`.
7. If the SMLD instance is removed from all the partition servers that share the SMLD 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\CurrentVer
sion\Uninstall\ScanMail for Domino
```

b. Delete the Trend Micro ScanMail for Domino folder from `C:\Documents and Settings\All Users\Start Menu\Programs`. This action removes the ScanMail program folder from the Start menu.

c. Delete the ScanMail product key from the Registry:

   `HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\ScanMail for Lotus Notes`

d. Close the registry editor

10. Delete and modify the information of partition server which installs the specified SMLD instance in ***`smdsys.ini`***.

    - DomSvrISMDCount
    - DomSvrISMDSecs
    - DomSvrX (delete the related information of the partition server of ScanMail instance)

    If the SMLD instance is removed from all the partition servers that share the SMLD binary, delete the `SMDConfx` instance in ***`smdsys.ini`***.

    If all SMLD instances are removed fromthe target server, delete ***`smdsys.ini`***.

11. Restart the Domino server.

Removing a Single or Shared ScanMail Installation on AIX

Tip: Refer to Appendix C, *Program File and Folder Lists* on page C-1 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}
   - 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 ***smdsys.ini*** for an AIX server that has multiple instances of ScanMail:

```
[SMDConf] \\indicates the first ScanMail instance
ProductPath=/ibm2/aix/trend/SMLD
ProductVersion=V5.0 \\indicates ScanMail version is 5.0
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/aix/notesdata0/notes.ini
[SMDConf0] \\indicates the second ScanMail instance
ProductPath=/ibm1/trend/SMLD
ProductVersion=V5.0
InstallType=64-bit
DomSvrISMDCount=2 \\indicates the partition server number
of second ScanMail instance
DomSvrISMDSecs=DomSvr2,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/SMLD
ProductVersion=V5.0
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 SMLD 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 an AIX server (see *Table C-2* on page C-3).

3. Navigate to the Domino Data directory, and then delete the SMLD 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 SMLD instance is removed from all the partition servers that share the SMLD 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 SMLD instance in ***smdsys.ini***.
   - DomSvrISMDCount
   - DomSvrISMDSecs
   - DomSvrX (delete the related information of the partition server of ScanMail instance)

   If the SMLD instance is removed from all the partition servers that share the SMLD binary, delete the `SMDConfx` instance in ***smdsys.ini***.

   If all SMLD instances are removed fromthe target server, delete ***smdsys.ini***.
9. Restart the Domino server.

Chapter 11

Troubleshooting

This chapter describes how to troubleshoot problems that may occur with ScanMail for Lotus Domino.

This chapter discusses the following topics:

Locating Installation and Uninstallation Logs

The following are the ScanMail installation and uninstallation logs:

TABLE 11-9. Installation and uninstallation logs

PLATFORM	LOCATION AND FILE NAME	DESCRIPTION
Windows	`C:\smdins.log`	ScanMail installation log
	`C:\smdunins.log`	ScanMail uninstallation log
IBM AIX	`/var/log/smdins.log`	ScanMail installation log
	`/var/log/smdunins.log`	ScanMail uninstallation log

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 uses 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 6-8 and *Understanding the Antivirus and Content Security Components* on page 6-2.

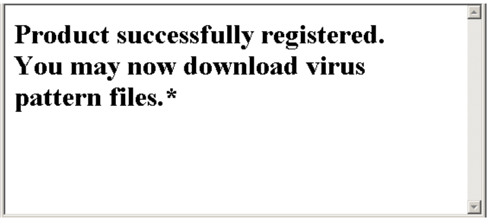
Perform the following steps to help troubleshoot the cause of the issue:

- 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:

    ```
    smld5-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://smln-t.update.trendmicro.com/cgi-bin/patregister.
cgi?Serial=%41%50%54%47%2d%39%39%39%32%2d%31%32%32%31%2d
%32%39%32%39%2d%32%32%31%30&FirstN=%41%50%54%47%2d%39%39
%39%32%2d%31%32%32%31%2d%32%39%32%39%2d%32%32%31%30&Last
N=%41%50%54%47%2d%39%39%39%32%2d%31%32%32%31%2d%32%39%32
%39%2d%32%32%31%30&EMail=%41%50%54%47%2d%39%39%39%32%2d%
31%32%32%31%2d%32%39%32%39%2d%32%32%31%30&Company=%41%50
%54%47%2d%39%39%39%32%2d%31%32%32%31%2d%32%39%32%39%2d%3
2%32%31%30&OPhone=%41%50%54%47%2d%39%39%39%32%2d%31%32%3
2%31%2d%32%39%32%39%2d%32%32%31%30&Fax=%41%50%54%47%2d%3
9%39%39%32%2d%31%32%32%31%2d%32%39%32%39%2d%32%32%31%30&
Addr=%41%50%54%47%2d%39%39%39%32%2d%31%32%32%31%2d%32%39
%32%39%2d%32%32%31%30&City=%41%50%54%47%2d%39%39%39%32%2
d%31%32%32%31%2d%32%39%32%39%2d%32%32%31%30&State=%41%50
%54%47%2d%39%39%39%32%2d%31%32%32%31%2d%32%39%32%39%2d%3
2%32%31%30&ZIP=%41%50%54%47%2d%39%39%39%32%2d%31%32%32%3
1%2d%32%39%32%39%2d%32%32%31%30&country=%41%50%54%47%2d%
39%39%39%32%2d%31%32%32%31%2d%32%39%32%39%2d%32%32%31%30
%20HTTP/1.0
```

A page similar to the following will open in a browser window.



Product successfully registered. You may now download virus pattern files.*

FIGURE 11-1. Test connection to ActiveUpdate server when using an HTTP proxy server.

- 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 11-6).

Scheduled Scan/Update Issue

An SMLD 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***.
2. Use the same settings that are specified in the Scheduled Scan/update settings to configure the Manual Scan/update 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:

```
load fixup {database path and file name}
```

For example, if the administrator wants to recover a corrupted Configuration Database, the following command should be issues from the Domino server console:

```
load fixup smd\smconf.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 11-5).

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 3-4 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.

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:

```
SMDEMDEBUG=1
```

c. Save and close ***notes.ini***.

Debug Levels

The ScanMail scanning tasks uses the following debug levels:

LEVEL	DESCRIPTION
1	Shows fatal errors only
2	Shows abbreviated debug information
3	Shows detailed debug information

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:** nSMDreal_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 `\SMD\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:

MESSAGE	CAUSE	WHAT TO DO
SMDreal: Unable to create message queue. Restart Domino server.	Domino server may not be running properly.	Restart the Domino server.
SMDreal: Unable to initialize common message. Unload and then reload SMDreal.	Message files are missing.	Uninstall, and then re-install ScanMail.
SMDreal: Unable to initialize scan engine. Check the scan engine and pattern file.	The scan engine or pattern file is missing. ***`smconf.nsf`*** does not contain policy document	Uninstall, and then re-install ScanMail. Create a policy in ***`smconf.nsf`***, and then load `smdreal` again
SMDreal: Missing Extension Manager in ***`notes.ini`***. Re-install ScanMail.	ScanMail was installed using a wrong installation package. Alternatively, ScanMail was removed manually.	Uninstall, and then re-install ScanMail.

Message	Cause	What To Do
SMDreal: Invalid Activation Code. Activate ScanMail via the Configuration Database and then reload SMDreal.	Activation Code (AC) was not entered during ScanMail installation. Alternatively, an invalid AC was entered.	Enter a valid AC using the ScanMail Configuration Database > **Administration** > **Product License** document. See *Registering and Activating ScanMail* on page 2-44.
SMDreal: The evaluation period has expired. Obtain a Registration Key and then activate ScanMail.	An AC evaluation version was entered during installation, and the AC already expired.	See *Renew ScanMail Maintenance* on page 2-46
SMDreal: Unable to load policy. Check Configuration Database and then reload SMDreal.	The Configuration Database might be corrupt.	Reinstall ScanMail.
SMDreal: Unable to load Message Database. Check ***smmsg.nsf*** and then reload SMDreal.	***smmsg.nsf*** (ScanMail Message Database) might be corrupt.	
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 4-15).

Message	Cause	What To Do
SMDupd: Unable to run multiple SMDupd 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.
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 4-49 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.	
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 ScanMail Maintenance* on page 2-46
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.

MESSAGE	CAUSE	WHAT TO DO
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.
SMD Loader: Unable to find the latest program directory	Unable to find `ScanMailInstallPath` in ***`notes.ini`***. This is caused by incomplete installation or manual deletion of ScanMail files.	Reinstall ScanMail or add `ScanMailInstallPath` parameter and value in ***`notes.ini`***.
SMD Loader: Unable to browse the latest program directory {path}	The path name specified by `ScanMailInstallPath` is an invalid path or directory.	Reinstall ScanMail or add the correct `ScanMailInstallPath` parameter and value in ***`notes.ini`***.
SMD Loader: Unable to load dynamic library "%s"	Unable to load the dynamic library because a file is missing, corrupted, or has insufficient permission.	Reinstall ScanMail or obtain a valid file and overwrite the corrupted one on the Domino server.
SMDsch: Unable to start the scheduled task "%s"		

Chapter 12

Getting Support

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.

For more information about TrendLabs, please visit:

http://us.trendmicro.com/us/about/company/trendlabs/

Other Useful Resources

Trend Micro offers a host of services via its Web site, www.trendmicro.com.

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 a Lotus 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 Lotus 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 SMLD 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 4-30.

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.

Note: Web Reputation is only available when the Anti-Spam filter is enabled. See *Configure Anti-Spam Filtering* on page 4-27 and *Configure Web Reputation* on page 4-30.

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

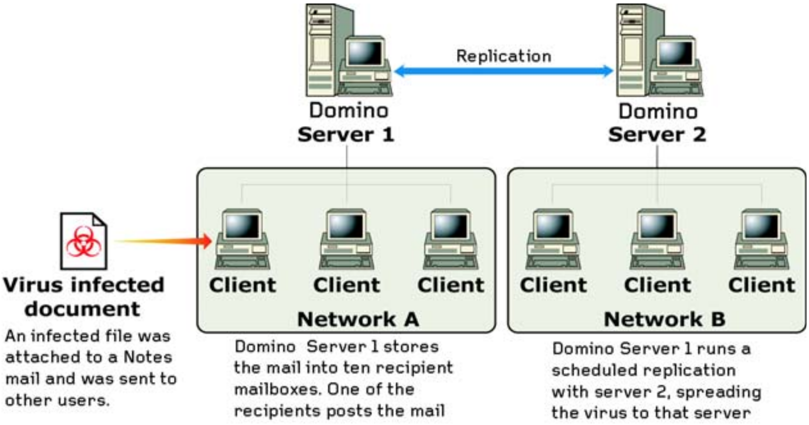

Replication
Domino Server 1
Domino Server 2
Virus infected document
An infected file was attached to a Notes mail and was sent to other users.
Client
Client
Client
Network A
Domino Server 1 stores the mail into ten recipient mailboxes. One of the recipients posts the mail
Client
Client
Client
Network B
Domino Server 1 runs a scheduled replication with server 2, spreading the virus to that server

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 Lotus 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 Lotus Domino:

- (Windows only) Set `HKEY_Local_Machine\System\CurrentControlSet\Control\PriorityControl\Win32PrioritySeparation` to **`0`** rather than the default value of **`24`**, in accordance with Lotus 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 Lotus 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 C-1. ScanMail files and folders available on a Windows server

FILE/FOLDER	DESCRIPTION

`...\Lotus\Domino`
`...nSMDext.dll`
`...nSMDemf.exe`
`...nSMDreal.exe`
`...nSMDsch.exe`
`...nSMDmon.exe`
`...nSMDdbs.exe`
`...nSMDupd.exe`
`...nSMDsupp.exe`
`...ndbsetup.exe`
`...nsmlnredID.dll`
`...nsmdcm.exe`
`...smd.ini`
	The ScanMail loader, filter, Extension Manager, dbsetup, and ScanMail configuration files

`...WINDOWS\smdsys.ini`	The main ScanMail for Lotus Domino configuration file
`...\Program Files\Trend Micro\ScanMail for Domino`	The ScanMail for Lotus Domino default installation folder
`...\engine`	Contains the TMASE and virus scan engine folders
`...\engine\tmase`	Contains the Trend Micro Anti-spam Engine (TMASE)
`...\engine\tmufe`	Contains the Trend Micro tmufe engine
`...\engine\vsapi`	Contains the Trend Micro scan engine
`...\pattern`	Contains the TMASE and virus scan rule/pattern folders
`...\pattern\tmase`	Contains the TMASE rule files
`...\pattern\vsapi`	Contains the virus pattern file, spyware pattern and Intellitrap pattern files
`...\program`	Contains the ScanMail readme file and the binary and configuration file folders
`...\program\V5.#.#.####`	Contains the ScanMail binary and configuration files
`...\Uninstall`	Contains the ScanMail uninstall program
`...\Lotus\Domino\Data\smd\smtemp`	The ScanMail folder used to extract temporary files for scanning

TABLE C-1. ScanMail files and folders available on a Windows server

FILE/FOLDER	DESCRIPTION
`...\Lotus\Domino\Data\smd`	Contains the ScanMail databases and templates

ScanMail for AIX

Refer to *Table C-2* for the list of files created by a successful ScanMail and Control Manager agent installation on an AIX server.

TABLE C-2. ScanMail files and folders available on an AIX server

FILE/FOLDER	DESCRIPTION
`/etc/smdsys.ini`	The ScanMail for Domino main configuration file
`/opt/trend/SMD/`	The ScanMail for Domino default installation folder. The installation can however, be done in any other folder.
`.../engine/tmase`	Contains the Trend Micro Anti-spam Engine (TMASE)
`.../engine/vsapi`	Contains the Trend Micro scan engine
`.../pattern/tmase`	Contains the TMASE rule files
`.../pattern/vsapi`	Contains the virus, spyware, and Intellitrap pattern files
`.../engine/tmufe`	Contains the Trend Micro tmufe engine
`.../program`	Contains the ScanMail readme file and the binary and configuration file folders
`.../program/V5.#.#.####`	Contains the ScanMail binary and configuration files Where: • .#.# (the first two) indicate the minor version • .#### (the last four #) indicate the build number

TABLE C-2. ScanMail files and folders available on an AIX server

FILE/FOLDER	DESCRIPTION

`/opt/lotus/notes/latest/ibm-pow`
`...smddbs`
`...smdemf`
`...smdcm`
`...smdmon`
`...smdreal`
`...smdsch`
`...smdsupp`
`...smdupd`
`...libsmdext.so`
	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/smtemp`	The ScanMail dafault folder used to extract temporary files for scanning which is under the Domino Data directory.

Appendix D

SMD 3.0 and SMLD 5.0 Feature Comparison

The following table presents a comparison of Trend Micro ScanMail for Domino (SMD) 3.0 and ScanMail for Lotus Domino (SMLD) 5.0.

TABLE D-1. ScanMail 3.0 and SMLD 5.0 feature comparison

Feature	ScanMail for Domino 3.0	ScanMail for Lotus Domino 5.0
Installation/Platform Support		
Supports Domino 6.5.x	Yes	No
Supports Domino 6.0.x	Yes	No
Supports Domino 5.0.13a, 5.0.12, 5.0.11	Yes	No
Supports Domino 7.0.2, 7.0.3, 8.0	Yes	No
Supports 32-bit Domino 8.0.1, 8.0.2, and 8.5	Yes	Yes
Supports 64-bit Domino 8.0.1, 8.0.2, 8.5 and 8.5.1	No	Yes
Supports IBM AIX 64-bit 5.3 or later	No	Yes
Supports cluster server (full support with task on each server and trusting)	Yes	Yes
Supports partitioned servers	Yes	Yes
Simultaneous installation on multiple partitions	Yes	Yes
Scripted/silent installation on all platforms	Yes	Yes
Preparation for replication during installation	Yes	Yes
Configuration of ACL during installation	Yes	Yes
Database signing during installation	Yes	Yes
Database signing with alternate ID/password or skip signing	Yes	Yes
Replicates Configuration database across platforms	Yes	Yes
Supports installation parameterization	No	Yes
Multi-instance support	No	Yes
Supports new CM and Management Communication Protocol (MCP) Agents	No	Yes
Supported Domino Applications		
Lotus Domino Database (.nsf)	Yes	Yes

TABLE D-1. ScanMail 3.0 and SMLD 5.0 feature comparison (Continued)

FEATURE	SCANMAIL FOR DOMINO 3.0	SCANMAIL FOR LOTUS DOMINO 5.0
Lotus Domino Web Access (formerly iNotes Web Access)	Yes	Yes
Native 64-bit support	No	Yes
PRODUCT ACTIVATION		
Trend Micro Online Registration system	Yes	Yes
One Activation Code (either for ScanMail for Domino or ScanMail for Domino Suite)	Yes	Yes
SCANNING (GENERAL)		
Multi-threaded scanning	Yes	Yes
Multi-threaded scan tasks	Yes	Yes
Separate actions for Adware/Spyware	Yes	Yes
MAIL SCANNING		
Real-time scan	Yes	Yes
Mail scan rule based on mail sender/recipient	Yes	Yes
Different scan settings for users/groups with exceptions	Yes	Yes
Scheduled scanning with different settings at different times	Yes	Yes
Virus cleaning upon detection	Yes	Yes
Configurable action upon detection	Yes	Yes
Nested compressed file scanning with selectable scanning depth	Yes	Yes
MIME/HTML body scanning for script viruses	Yes	Yes
Malicious notes script, hot spots, and URL scanning	Yes	Yes
Signature-based scanning	Yes	Yes
Supports trusted antivirus server(s) to avoid rescanning	Yes	Yes

TABLE D-1. ScanMail 3.0 and SMLD 5.0 feature comparison (Continued)

FEATURE	SCANMAIL FOR DOMINO 3.0	SCANMAIL FOR LOTUS DOMINO 5.0
Selectively scans embedded OLE objects	Yes	Yes
IntelliTrap support	No	Yes
Microsoft Office 12 support	No	Yes
Decompression algorithm support RAR, SFX, CHM, NSIS, and ZIP SFX files	No	Yes
WEB REPUTATION		
Web reputation support	No	Yes
ADWARE DETECTION		
Configurable action upon detection	Yes	Yes
SPYWARE DETECTION		
Configurable action upon detection	Yes	Yes
MAIL/BANDWIDTH MANAGEMENT		
Redirects email for approval	Yes	Yes
Supports selectable grouping of file types	Yes	Yes
Configurable attachment blocking by true file type (individual file types)	Yes	Yes
Configurable action for Microsoft Office macros	Yes	Yes
Configurable attachment blocking by extension or file-name	Yes	Yes
Configurable attachment blocking by true file type (group)	Yes	Yes
Strips macros from Microsoft Office documents	Yes	Yes
Delays mail according to a specific schedule	Yes	Yes
Blocks mail depending on size	Yes	Yes
Lower priority setting	Yes	Yes
Blocks mail based on the attachment's true file type	Yes	Yes

TABLE D-1. ScanMail 3.0 and SMLD 5.0 feature comparison (Continued)

FEATURE	SCANMAIL FOR DOMINO 3.0	SCANMAIL FOR LOTUS DOMINO 5.0
Blocks mail based on the attachment's file or extension name	Yes	Yes
CONTENT FILTERING (REQUIRES SCANMAIL FOR LOTUS DOMINO SUITE / EMANAGER)		
Message header field scanning	Yes	Yes
Filters for text in message body	Yes	Yes
Filters for text in message attachment	Yes	Yes
Regular expression support	No	Yes
Microsoft Office 2007 file support	No	Yes
Additional OLE layer scanning support for a maximum of 20-layers	No	Yes
Uses heuristics technology	Yes	Yes
Supports Approved/Blocked Senders lists	Yes	Yes
Configurable filter sensitivity	Yes	Yes
Uses rule file	Yes	Yes
Real-time scanning	Yes	Yes
Scheduled scanning	Yes	Yes
Manual scanning	Yes	Yes
Configurable time period for multiple real-time scanning configurations	Yes	Yes
Script scanning support in real-time scanning	Yes	Yes
Scheduled scanning within defined time periods (maximum duration)	Yes	Yes
Support for several scheduled scans with different settings	Yes	Yes
Resume a scan that did not finish	Yes	Yes
Script scanning support in scheduled scanning	Yes	Yes

Table D-1. ScanMail 3.0 and SMLD 5.0 feature comparison (Continued)

Feature	ScanMail for Domino 3.0	ScanMail for Lotus Domino 5.0
Configurable scan schedule through Configuration database	Yes	Yes
Administration		
Full integration with R6/5 Administrator Client and Notes Client	Yes	No
Lotus Notes 7/8 support	Yes	Yes
Remote administration through a Web interface	Yes	Yes
Remote administration through a Notes Client	Yes	Yes
User interface uses frames and follows the latest Trend Micro standard	Yes	Yes
Server status monitoring available through user interface	Yes	Yes
Server task watch dog	Yes	Yes
Task status monitoring	Yes	Yes
Share server settings and antivirus policies between servers and groups of servers	Yes	Yes
User-defined and controlled rules to define actions	Yes	Yes
Ability to define rules based on users and groups	Yes	Yes
Configurable server settings that are policy-independent	Yes	Yes
Role-based access configurable through the Notes interface	Yes	Yes
One-button information collector (Support Tool)	Yes	Yes
Antivirus and Content Security Component Updates		
Manual update	Yes	Yes
Select components and set recurring scheduled updates	Yes	Yes

TABLE D-1. ScanMail 3.0 and SMLD 5.0 feature comparison (Continued)

FEATURE	SCANMAIL FOR DOMINO 3.0	SCANMAIL FOR LOTUS DOMINO 5.0
Automated pattern update through ActiveUpdate	Yes	Yes
Automated scan engine update through ActiveUpdate	Yes	Yes
Automated program updates through ActiveUpdate	Yes	Yes
Pattern/Engine integrity check after update	Yes	Yes
Product integrity check after update	Yes	Yes
Full and Small pattern download support for TMASE.	No	Yes
IntelliTrap pattern update support	No	Yes
NOTIFICATION OPTIONS		
Customized notifications	Yes	Yes
Notifications via Lotus Instant Messaging (ScanMail for Domino for Windows only)	Yes	Yes
Sender, recipient, or administrator notifications	Yes	Yes
Separate notifications to internal/external users	Yes	Yes
Rich text configurable message	Yes	Yes
Supports notification insertion in a MIME email	Yes	Yes
Removes icon when attachment is removed	No	Yes
Safe stamp in the message subject	Yes	Yes
Safe stamp in Notes message body	Yes	Yes
Safe stamp in SMTP message body	Yes	Yes
Multiple disclaimer support	Yes	Yes
Single disclaimer inserted when an email passes multiple servers	Yes	Yes
Supports disclaimer positioning	Yes	Yes
QUARANTINE		
Automatically deletes quarantined logs based on type, age, and records to retain	Yes	Yes

TABLE D-1. ScanMail 3.0 and SMLD 5.0 feature comparison (Continued)

FEATURE	SCANMAIL FOR DOMINO 3.0	SCANMAIL FOR LOTUS DOMINO 5.0
Supports resend/restore of quarantined items	Yes	Yes
LOGGING/STATISTICS		
Exports statistics to a Microsoft Excel spreadsheet	Yes	Yes
Automatically deletes logs	Yes	Yes
Identify the sender of an infected message	Yes	Yes
Identify infected file	Yes	Yes
Records the recipient information	Yes	Yes
Records the action taken on a threat	Yes	Yes
Graphical email statistics/reports	Yes	Yes

Index