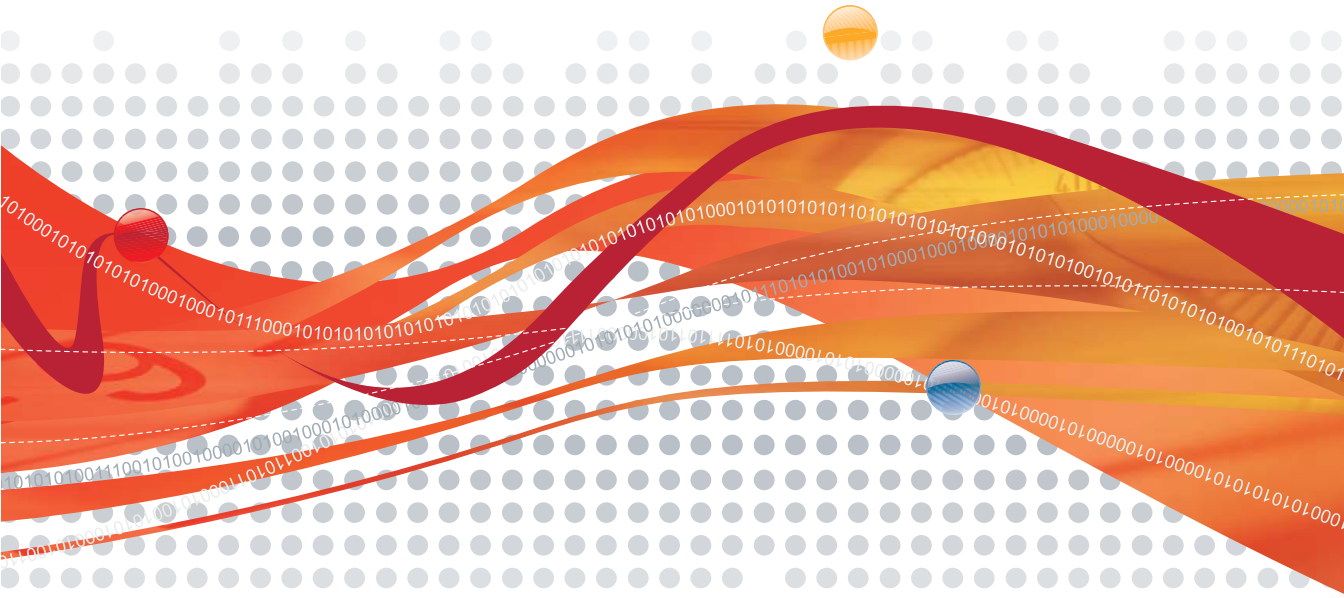
TREND MICRO™

ScanMail™ 3 for Domino™

Proactive Antivirus and Content Security
for the Domino Environment



Administrator's Guide

Document Part No. SDEM33439/71102

Release Date: November 2007

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

The Administrator's Guide for Trend Micro™ ScanMail™ for 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`

Contents

Chapter 7: Updating Components

Chapter 8: Sending ScanMail Notifications

Chapter 9: Using the Log and Quarantine Databases

Chapter 10: Using ScanMail with Trend Micro Control Manager

Chapter 11: Removing ScanMail and the Control Manager Agent for ScanMail

Chapter 12: Troubleshooting

Preface

This Administrator's Guide describes the Trend Micro™ ScanMail™ for Domino 3 product, provides installation and uninstallation instructions, and provides information to help you configure ScanMail functions for your specific needs.

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

- *Introducing Trend Micro ScanMail and ScanMail Suite for Domino 3* provides an overview of the product and description of all new features in this release.
- *Installing ScanMail for Domino* provides step-by-step instructions on installing ScanMail 3.
- *Installing Control Manager Agent for ScanMail* provides step-by-step instructions on installing the Control Manager agent for ScanMail.
- *Getting Started with ScanMail* provides recommended procedures to configure ScanMail after you have installed it.
- *Configuring Scan Tasks* provides procedures to create policies, rules, or expressions that ScanMail 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 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 with Trend Micro Control Manager* provides details on how to use Trend Micro Control Manager™ to manage ScanMail.
- *Removing ScanMail and the Control Manager Agent for ScanMail* provides procedures to remove ScanMail.
- *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 Best Practices* provides the best practices for optimized operations and maximum performance of ScanMail.
- *Control Manager Agent Checklist* provides a checklist, which can be used during the Control Manager agent for ScanMail installation.
- *Program File and Folder Lists* provides a list of the ScanMail and Control Manager files and folder structures that are available upon a successful application installation.
- *SMLN 2.6 and SMD 3 Feature Comparison* provides a comparison of Trend Micro ScanMail for Lotus Notes (SMLN) 2.6 and ScanMail for Domino (SMD) 3 features.

What's New in Version 3

ScanMail for Domino represents a significant advancement in antivirus and content security for Lotus Domino environments. ScanMail Suite for 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 3 make ScanMail more flexible and scalable than ever before.

The following new features are available in ScanMail for Domino 3:

- *Support for automated (silent) install through the command line*
- *Policy-based configuration*
- *Updated and improved user interfaces for ScanMail databases*
- *Customizable anti-spam filtering*
- *New advanced scanning options*
- *Delay or Redirect action for messages that match a scan option setting*
- *Support for trusting servers in a cluster*
- *Support for Lotus Instant Messaging and Web Conferencing notification**
- *Tags to customize notification*
- *Improved statistics*
- *New debug levels for detailed ScanMail task debugging*
- *Support for the Trend Micro Online Registration system*
- *Support for Domino 7.0 (i5/OS platform only)*
- *Discontinued support for Domino 5.x (i5/OS and OS/400 platforms only)*

Support for automated (silent) install through the command line

To enable an easier, automated installation process, use a pre-recorded response file (installation script) to run a silent installation or update on multiple ScanMail servers.

See *Running a silent installation* on page 2-26 for details.

Policy-based configuration

Policy-based configurations apply to real-time mail scanning, real-time and scheduled database scanning, and scheduled updates. A *policy* determines how ScanMail scans unwanted messages and databases, and updates antivirus and content security components based on a schedule. Use policies to apply the same or similar configurations on server groups thereby reducing management effort.

See *Planning for a Policy-based Antivirus and Content Security Protection* on page 5-2 for details.

Updated and improved user interfaces for ScanMail databases

The ScanMail Configuration, Update, Log, and Quarantine databases now have improved user interfaces to allow easy administration and maintenance.

See *Understanding the ScanMail Interface* on page 4-2.

Customizable anti-spam filtering

ScanMail uses the Trend Micro Anti-spam Engine to implement heuristic-based rules when detecting unwanted content, or blocking or automatically allowing a message based on user-defined Approved Senders and Blocked Senders lists.

See *Configure spam filtering* on page 5-25 for instructions on how to configure anti-spam features.

New advanced scanning options

ScanMail implements the following advanced scanning options:

- **ActiveAction** identifies malware types and recommends scan actions based on how each type infects a computer system or environment.

  Viruses and other types of malware are categorized by malicious code, replication, and payload types. When ScanMail detects a virus, the recommended action (clean, quarantine, delete) for the virus category is taken to protect your environment's vulnerable points.
- Script bomb scanning improvement—ScanMail will skip scanning when hot spots in a document are signed by configured trusted users.
- True file type or true file type group scanning and blocking
- Up to 20 layers of compressed file scanning and blocking

See *Introducing ScanMail filters* on page 5-20.

Delay or Redirect action for messages that match a scan option setting

The ScanMail scan and filter actions include two new actions:

- **Redirect** sends a message to an approver (for example, mail administrator or department manager) for approval. The approver decides whether to allow or block a message from delivery.
- **Delay** delivers a message according to the schedule set.

See *Configuring redirect options* on page 5-41 for details on the ScanMail scan actions.

Support for trusting servers in a cluster

Policies enable efficient management of cluster networks. Set up a policy to trust relationships between cluster servers.

See *Managing the trusted cluster servers for a policy* on page 5-7.

Support for Lotus Instant Messaging and Web Conferencing notification*

ScanMail provides Lotus Instant Messaging and Web Conferencing (formerly known as Sametime Connect) notification to inform administrators of scan and filter detections, update information, and policy-related events. When creating a policy, specify the Lotus Instant Messaging IP address, user name, and password. The specified administrator can then receive ScanMail notifications through Lotus Instant Messaging.

See *Defining how ScanMail delivers notifications* on page 8-6.

Note: * This new feature is available in ScanMail for Windows only.

Tags to customize notification

Use tags to include details, such as the threat detected or the virus pattern file and scan engine versions, in a ScanMail notification.

See *Customizing notifications* on page 8-3 and *Setting ScanMail Notifications* on page 8-6.

Improved statistics

ScanMail Log Database provides the following statistics:

- Virus scanning
- Message filtering
- Attachment filtering
- Content filtering
- Script filtering
- Spam filtering
- Outbreak prevention
- Filtering
- Redirected messages

In addition, the Log Database charts are presented in a column layout.

See *Viewing Statistics and Charting* on page 9-7.

New debug levels for detailed ScanMail task debugging

Set up to three levels of debugging for the ScanMail SMDreal, SMDdbs, or SMDmon tasks.

See *Debugging ScanMail Tasks* on page 12-8.

Support for the Trend Micro Online Registration system

Use a Registration Key to register ScanMail to the Trend Micro Online Registration system, and then receive an Activation Code to activate a ScanMail evaluation, full, or suite version.

See *Registering and Activating ScanMail* on page 2-45.

Support for Domino 7.0 (i5/OS platform only)

ScanMail for Domino provides support for Domino 7.0 for i5/OS environments.

Discontinued support for Domino 5.x (i5/OS and OS/400 platforms only)

Domino 5.x versions are not supported on i5/OS and OS/400 platforms.

Audience

The ScanMail 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.

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

TABLE 1. Conventions used in the ScanMail documentation

Chapter 1

Introducing Trend Micro ScanMail and ScanMail Suite for Domino 3

Trend Micro™ ScanMail™ for Domino™ 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 Domino prevents viruses and other malicious code from entering your Domino environment.

ScanMail Suite for Domino provides an added layer of protection through revolutionary anti-spam technologies and systematic content filtering. ScanMail Suite for Domino performs spam detection and content filtering before it performs real-time mail scanning.

This chapter discusses the following topics:

Product Overview

Trend Micro™ ScanMail™ for Domino™ 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 R5/R6 Administration Client.

ScanMail for Domino runs on these platforms:

- Microsoft™ Windows™
- Sun™ Solaris™
- Red Hat™ Enterprise Linux and Novell™ SUSE™ Linux on x86 platforms
- IBM™ AIX™
- IBM i5/OS™ and IBM OS/400™

The ScanMail for Domino Standard version provides virus scanning in all modes and component update. The ScanMail for Domino 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 for Domino fits in a comprehensive approach to protecting your environment, see
`http://www.trendmicro.com/en/products/global/enterprise.htm`

ScanMail for Domino 3 Standard features

ScanMail for Domino 3 Standard version features for Windows, Linux on x86, Solaris, AIX, i5/OS and OS/400 include:

- Multi-threaded in-memory scanning process for fast performance
- Support for true file formats for both malware scanning and attachment blocking
- Support for installing multiple instances of ScanMail on a Domino partitioned server
- 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 (Windows platform only)
- Proactive outbreak prevention through Control Manager
- 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 Domino 3 Suite features

ScanMail for Domino 3 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 .txt, .html, and .rtf files
- the ability to enable or disable the stripping of macros from Microsoft Office files

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

FEATURE	STANDARD	SUITE
Antivirus	Yes	Yes
Anti-Spam	No	Yes
Content Filtering		
Subject/Body/.txt, .html, .rtf files	No	Yes
Microsoft Office files	No	Yes*
Active Update	Yes	Yes
Control Manager Agent	Yes	Yes

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

*. Not available on AIX, i5/OS and OS/400

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 shutdown of 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.

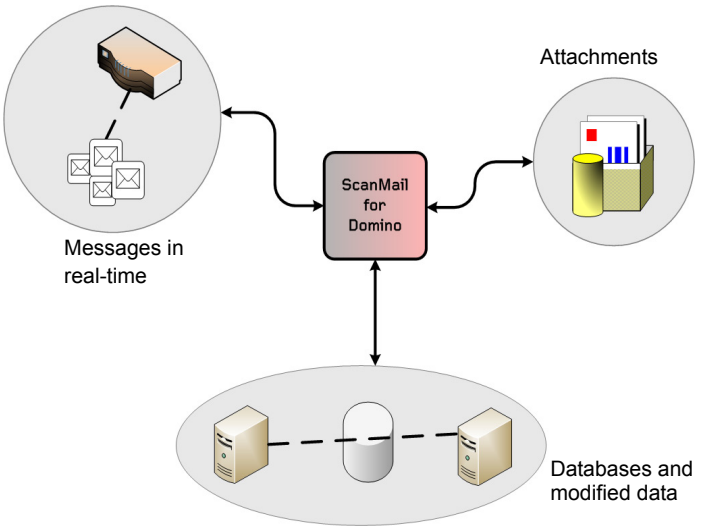


FIGURE 1-1. ScanMail for Domino detects and removes threats before infections can spread to the desktop.

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, and 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 5-2.

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 outdated. 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 *Appendix A*, *Understanding Threats in a Domino Environment* for descriptions of threats in a Domino environment.

Understanding Policies, Rules, and Filters

ScanMail for Domino provides the ability to create ***policies*** that define how ScanMail 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 that ScanMail has the ability to share policies across applicable platforms (for example, Domino servers hosted on Windows and Solaris servers 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 non-real-time 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 on messages and attachments

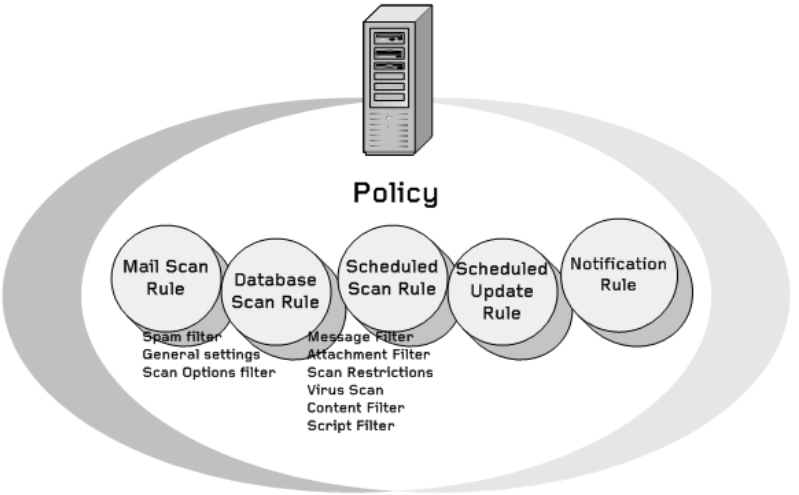


FIGURE 1-2. Policy-filter-rule relationship

ScanMail rules

ScanMail for Domino provides five types of **rules** (Table 1-2) that define how ScanMail scans messages and databases.

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 5-9*.
Database scan rule	scans databases in real time. To create a real-time database scan rule, see *page 5-14*.
Scheduled scan rule	scans databases according to a schedule. To create a scheduled database scan rule, see *page 5-16*.
Scheduled update rule	updates antivirus and content security components. To create a scheduled update rule, see *page 7-4*.
Notification rule	delivers a notification. To create a notification rule, see *page 8-2*.

TABLE 1-2. Types of ScanMail rules

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:

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.

TABLE 1-3. ScanMail filtering options

ScanMail Protection Strategy

An organization must design a protection strategy that provides optimal protection for the enterprise. The key decision factors for selecting an appropriate ScanMail protection strategy 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 ScanMail 3. 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 1-10), 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 5-1, "Recommended file extensions to block," on page 5-37* 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 Domino Suite to implement protection against unwanted spam messages.

- Enable anti-spam protection and specify which actions to take.
- Set filter level in accordance with IT security policies.
- Enable and specify approved senders and blocked senders.

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

Chapter 2

Installing ScanMail for Domino

This chapter guides you through installing ScanMail for Domino on all supported platforms. If you are planning to install Control Manager agent for ScanMail for Domino, install ScanMail for Domino first.

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 for 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 to the ScanMail Log database replicas from 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 7-8).
- If your operating system is AIX version 5.1, verify that you have installed the fix for the problem identified in authorized program analysis report (APAR) IY29345. To check whether the fix is installed, type `instfix -ik IY29345`. If the fix is not installed, download it from `http://www-1.ibm.com/support/docview.wss?uid=isg1IY29345` and install it, or add the line `AIXTHREAD_MNRATIO=1:1` to the Domino server's startup script.

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 3.0, 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 2.5x or 2.6x

To upgrade from ScanMail 2.x to 3, 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.
4. To activate a ScanMail 3 evaluation, standard, or suite version, you must obtain an Activation Code (see *page 2-45*), even if the ScanMail 2.x serial number has not yet expired.
5. During installation, specify all partitioned servers on the target server with ScanMail 2.x installed.

Setup will convert ScanMail 2.x components to ScanMail 3 to avoid program conflicts.

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 system requirements for a ScanMail for Domino server.

The table below lists the system requirements for ScanMail.

Hardware/Software Specifications	Requirements
Operating system (OS)	**ScanMail for Windows™:** Microsoft Windows Server 2003 Standard/Enterprise; Microsoft Windows™ 2000 Server/Advanced Server with Service Pack 3; Microsoft™ Windows NT™ 4.0 with Service Pack 6a **ScanMail for Linux™:** Red Hat™ Linux 7.2, Advanced Server 2.1 or 3.0 Red Hat Enterprise Linux 4 or 5 SUSE Linux 7.2 or 8.0 SUSE Linux Enterprise Server 8, 9, or 10 UnitedLinux 1.0, powered by UnitedLinux 1.0 **Note:** You need ScanMail 3.1 to install on Red Hat Enterprise Linux 4 or 5, or SUSE Linux Enterprise Server 9 or 10. **ScanMail for Solaris™:** Solaris 7.0, 8.0, or 9.0 **ScanMail for AIX™:** AIX 5.3, 5.2, 5.1 **Note:** AIX version 5.1 requires that you install the fix or workaround for the problem identified in APAR IY29345. **ScanMail for i5/OS™** and **OS/400™:** i5/OS V5R3, OS/400 V5R2 **Note:** Before installing ScanMail for Domino 3 for i5/OS and OS/400 on a Lotus Domino 6.x server, you must install IBM PTF(s). Please refer to the Trend Micro Knowledge Base (http://kb.trendmicro.com/search/default.asp) for solution ID 27067, IBM PTFs required on a Lotus Domino 6.x server for ScanMail for Domino 3 for i5/OS and OS/400. **Note:** To manage ScanMail from a Control Manager console, you must have Control Manager 3.0, Service Pack 3, applied on the Control Manager server.

TABLE 2-1. System requirements

Hardware/Software Specifications	Requirements				
Lotus™ Domino™	**Version Supported:**	**8.x**	**7.0.2 or higher**	**6.x**	**R5.0.11-.12-.13a**
	Windows	No	Yes	Yes	Yes
	Linux on x86	Requires version 3.1	Requires version 3.1	Yes	Yes
	Solaris	No	Yes	Yes	Yes
	AIX	No	Yes	Yes	Yes
	i5/OS™, OS/400	No	Yes	Yes	No
CPU	**ScanMail for Windows/Linux:** Intel™ Pentium™ IV Processor 1.3GHz (32-bit machine) **ScanMail for Solaris:** Sun SPARC 7 (32- and 64-bit machine) **ScanMail for AIX:** POWER 3™ RS64, POWER 2™, POWER™, PowerPC **ScanMail for i5/OS™ and OS/400:** PowerPC (RISC) in an IBM @server, iSeries server, or IBM AS/400 server				
Memory	**ScanMail for Windows, Linux, or Solaris:** 256MB RAM **ScanMail for AIX and i5/OS™ and OS/400:** 512MB RAM				

TABLE 2-1. System requirements, continued

Hardware/Software Specifications	Requirements
Disk space	**ScanMail for Windows:** 200MB available disk space for program files 100MB for temporary files 55MB available disk space on each Domino server partition **ScanMail for Linux:** 125MB available disk space for program files 285MB for temporary files 50MB available disk space on each Domino server partition **ScanMail for Solaris:** 155MB available disk space for program files 280MB for temporary files 60MB available disk space on each Domino server partition **ScanMail for AIX:** 150MB available disk space for program files 300MB for temporary files 50MB available disk space on each Domino server partition **ScanMail for i5/OS™** and **OS/400:** 250MB available disk space for program files 600MB for temporary files 65MB available disk space on each Domino server partition
File system	**ScanMail for Windows:** NT File System (NTFS) partition
Monitor	**All Platforms:** VGA monitor capable of 1024 x 768 resolution, with at least 256 colors
Component updates	**All Platforms:** Internet access for component download
Other	**ScanMail for AIX 5:** **xlC C++ Runtime 6.0 or later** You must install VisualAge C++ for AIX v5. **ScanMail for i5/OS™** and **OS/400:** **Java Developer Kit (licensed program 5722JV1), version 1.2 with the Host Servers option (licensed program 5722SS1 option 12) installed and running**

TABLE 2-1. System requirements, continued

Installing ScanMail

Read the following sections before installing ScanMail for Domino.

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

- You cannot automatically roll back to ScanMail for Lotus Notes 2.x after installing version 3.

  To roll back to ScanMail for Lotus Notes 2.6x, remove ScanMail 3 (see *page 11-2*), and then perform a fresh installation of ScanMail 2.6x. Refer to the ScanMail 2.6x documentation for details on how to install this version.
- You cannot install both ScanMail 2.6x and 3 on partitions running on the same Domino server.
- You must shut down the Domino server before installing or removing ScanMail for Domino.
- For partitioned servers, install a copy of ScanMail on each partition.

Pre-installation tasks

Before installing ScanMail for Domino, perform the following tasks:

1. Log on as the Administrator (Windows platform), root user (Linux, Solaris, and AIX platforms), or security officer (i5/OS and OS/400 platforms).

   For i5/OS and OS/400 platforms, ensure that the system value "QALWOBJRST" is set to *ALL.

   a. Type "CHGSYSVAL SYSVAL(QALWOBJRST)" in the CL command entry.

   b. Type *ALL in the "New value" option.

   If installing in a non-English environment, perform the tasks listed in *Installing ScanMail in a non-English environment (i5/OS and OS/400 platforms only)* on page 2-12 before proceeding with the remaining pre-installation tasks.
2. Before installing ScanMail for Domino 3 for i5/OS and OS/400 on a Lotus Domino 6.x server, you must install IBM PTF(s). Refer to the Trend Micro Knowledge Base (http://kb.trendmicro.com/search/default.asp) for solution ID 27067, IBM PTFs required on a Lotus Domino 6.x server for ScanMail for Domino 3 for i5/OS and OS/400.

3. For AIX version 5 and later, install x1C C++ Runtime 6.0 or later. You can download x1C C++ Runtime 6.0 from the IBM site: http://www-1.ibm.com/support/docview.wss?rs=2030&context=SSJT9L&dc=D400&uid=swg24008374&locc-en_US&cs=utf-8&lang=en
4. Determine the `notes.ini` location(s) (including its location on partitioned servers, if applicable).
5. Determine the Domino Data and Domino Binary paths.
6. Ensure that the user/group that has the administrator authority used to manage the ScanMail databases exists. The default group is Administrators.
7. Run one of the following commands to check the available disk space:
   - **For Linux, Solaris, and AIX**, run the `df -k` command.
   - **For i5/OS and OS/400**, use the CL command `dspsyssts` to verify that there is at least 900 MB of free space.
8. Verify that the / mount point has the minimum required disk space.
9. Close any open Notes Clients.
10. Close any open Notes account sessions.

Note: Run the `who` command to determine which sessions are running. If more than one Notes account session is running, close them before upgrading from ScanMail 2.x or installing ScanMail 3 for the first time.

To terminate a Linux, Solaris, or AIX user session remotely:

```
# who
# ps -t {terminal session}
# kill -HUP {pid}
```

To terminate an i5/OS or OS/400 user session remotely:

```
Type the following CL commands:
wrkusrjob user(*all) status(*active)
jobtype(*interact) astlvl(*basic)
Type "4" then press Enter to sign off the user
session remotely.
```

---

11. Shut down all Domino servers installed on this machine completely before:
    - Installing ScanMail 3 for the first time
    - Upgrading from ScanMail 2.6
    - Removing ScanMail 3.x

12. Prepare the ScanMail Activation Code.

    See *page 2-46* for details on the Activation Code.

13. Check the ScanMail Setup file permission (*NIX-based target servers only).

To check the ScanMail Setup file permission:

a. From the command line, run:

```
# ls -l {path/file name}
```

where:

- `path` is the directory where the ScanMail Setup file is located
- `file name` is the full file name of the ScanMail Setup

Examples:

Linux: `# ls -l /temp/installers/SMD3SetupLinux.bin`

AIX: `# ls -l /domino/installers/SMD3SetupAix.bin`

i5/OS and **OS/400:** `$ ls -l /domino/installers/setup.jar(use qsh)`

The above command will produce a result similar to *Figure 2-1*.

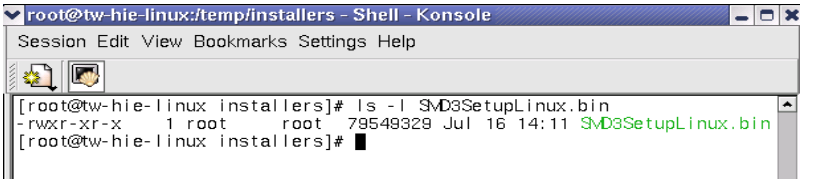


FIGURE 2-1. Checking the ScanMail Setup file permission

The `ls-l` command gives the long listing format of the specified file. In addition to the name of each file, it prints the file type, permissions, number of hard links, owner name, group name, size in bytes, and time stamp (or the modification time).

In this example, the first character of the 10-character code denotes the type of file. The next nine characters describe the permissions on the file. The permissions **`-rwxr-xr-x root root`** mean read, write, and execute rights for the user `root`, execute and read rights for anyone who is a member of the group `root`, and execute rights for any other user on the system.

Refer to your platform documentation for more information on long file names and file permissions.

Tip: On an *NIX system, ordinary users have only write access to their $HOME directory (also known as ~) and the `/tmp` directory, whereas Microsoft Windows NT systems users have access to all the disks except where access has been specifically denied. Since the Domino server runs as an ordinary user, ensure that ownership of files and directories is set correctly.

b. If the account used to install ScanMail does not have sufficient file permission, run `# chmod {###} {file name}` to correct the file access

where:

- `{###}` indicates the read, write, and execute file permissions (see *Table 2-2* for the list of codes and their equivalent permissions)
- `file name` is the ScanMail Setup file name

CODE	PERMISSION
7	Full
6	Read and Write
5	Read and Execute
4	Read only
3	Write and Execute
2	Write only
1	Execute only
0	None

TABLE 2-2. `chmod` codes and permissions

Examples:

Linux: `# chmod 755 SMD3SetupLinux.bin`

AIX: `# chmod 755 /domino/installers/SMD3SetupAix.bin`

i5/OS and **OS/400:** `$ chmod 755 /domino/installers/setup.jar(use qsh)`

This example will grant the account full rights, execute and read rights to the group, and execute right to all others accounts.

Tip: Run the above command in the directory where the ScanMail Setup file is located. Otherwise, include the file path when running the command. For example:

```
# chmod 755 /temp/installers/SMD3SetupLinux.bin
```

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

Installing ScanMail in a non-English environment (i5/OS and OS/400 platforms only)

To successfully install ScanMail in non-English environments on i5/OS and OS/400 platforms:

Before starting the installation, ensure that:

- the user profile setting for CCSID is set to 37
- the user profile setting for locale is /QSYS.LIB/en_US.LOCALE
- the notes.ini CCSID is 819.

Perform the following actions:

1. Type "`CHGUSRPRF USRPRF(USERNAME)`" in CL command entry, then press F4. Example: `chgusrprf usrprf(qsecofr)`
2. Press F10 for additional parameters.
3. Find the "Coded character set ID…" option and change the value to 37.
4. Find the "Locale" option and change the value to /QSYS.LIB/en_US.LOCALE.
5. Press Enter to save the changes.
6. Log off, then log on again.
7. Run the CL command `QSH`.
8. Change the directory to the Domino data path.
9. Back up the notes.ini file. Type "`cp notes.ini notes1.ini`".
10. Change the CCSID for notes.ini; type "`setccsid 819 notes.ini`".

Once the ScanMail installation is complete, you may restore the setting to their original values.

Setup modes

You can use the following methods to install ScanMail:

- **Wizard-based installation** requires user input when installing ScanMail for Domino on a server that supports a graphical user interface.

  The wizard-based installation provides a series of interfaces that help simplify the ScanMail installation. See *page 2-13*.

- **Silent installation** requires no user intervention when installing ScanMail for Domino.

  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 *page 2-26*.

- **Console-based installation** requires user intervention when installing ScanMail for Domino on a server that does not support a graphical user interface.

  ScanMail for Domino Setup on Linux, Solaris, AIX, i5/OS, and OS/400 platforms uses this method. See *page 2-30*.

Setup options

There are four Setup options:

- **Fresh install** installs ScanMail for Domino for the first time.
- **Install** installs the same ScanMail for Domino 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.

The Existing Setup Options screen provides the last three options (**Upgrade**, **Install**, and **Install and Upgrade**) when Setup detects an existing ScanMail 3 installation on the target server. For a first-time ScanMail 3 installation, this screen is skipped.

Running a wizard-based installation

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

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 **ScanMail for Domino** 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 one of the following to launch the Setup program:

PLATFORM	SETUP PROGRAM
Windows	`setupwin32.exe`
Linux	`SMD3SetupLinux.bin`
Solaris	`SMD3SetupSolaris.bin`
AIX	`SMD3SetupAix.bin`

The InstallShield Welcome screen appears, followed by the Welcome screen.

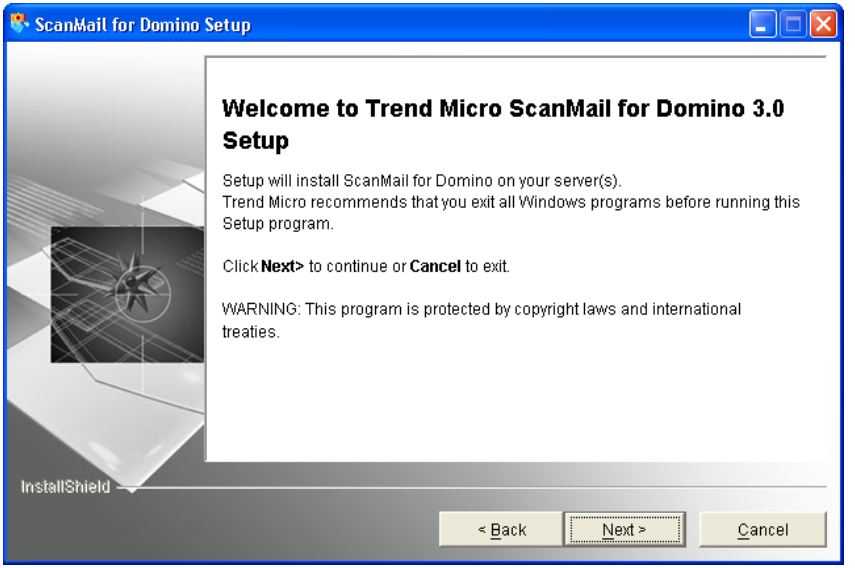


FIGURE 2-2. ScanMail Setup Welcome screen

Note: Domino R6 on Windows 2000 was used to capture screen shots presented in the wizard-based ScanMail Setup.

3. Click **Next >**. The Software License Agreement screen appears.

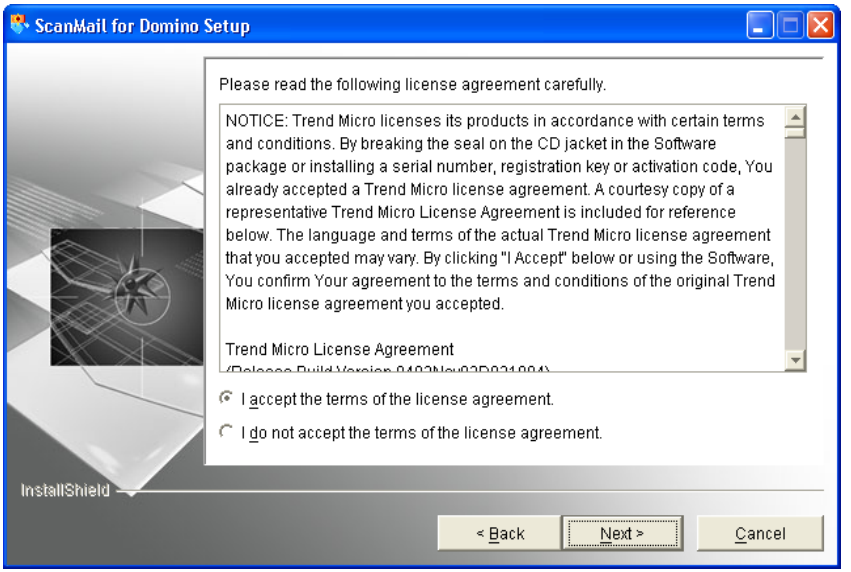


FIGURE 2-3. ScanMail for Domino License Agreement Screen

Select *I accept the terms of the license agreement* to continue with the ScanMail 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 discontinues.

4. Click **Next >**. Setup checks the target server's configuration.

   If the server does not have ScanMail 2.x or 3 already installed, Setup will skip the Existing Setup Options screen and proceed directly to the Product Activation screen.

   If the Existing Setup Options screen appears, select which setup type to run:

   - **Upgrade** upgrades an existing ScanMail installation.

- **Install and Upgrade** upgrades existing ScanMail 3 installations and installs ScanMail 3 on additional Domino servers.
- **Install** installs ScanMail 3 on additional Domino servers.

The screen shown in *Figure 2-4* allows you to have a consistent ScanMail setup on all partitioned servers.

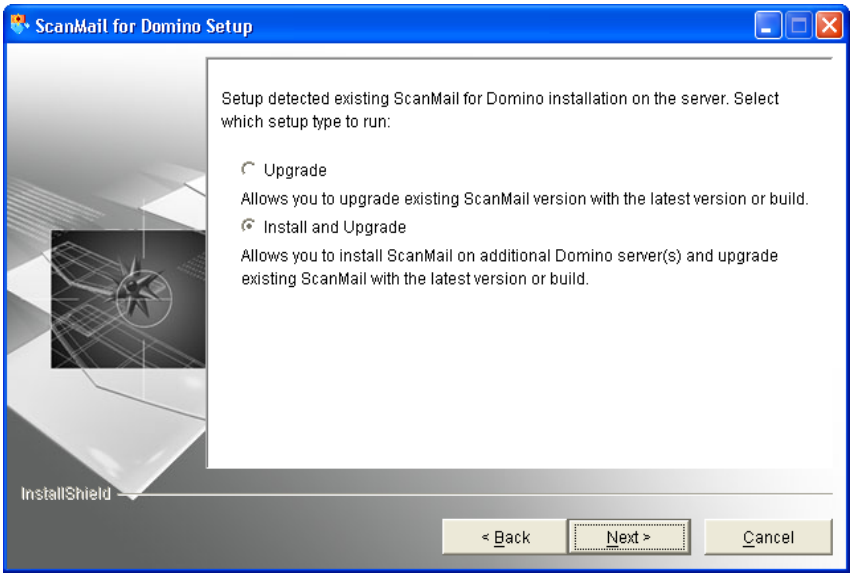


FIGURE 2-4. ScanMail Install and Upgrade screen

The screen shown in *Figure 2-5* allows you to install the same ScanMail version on additional Domino server(s).

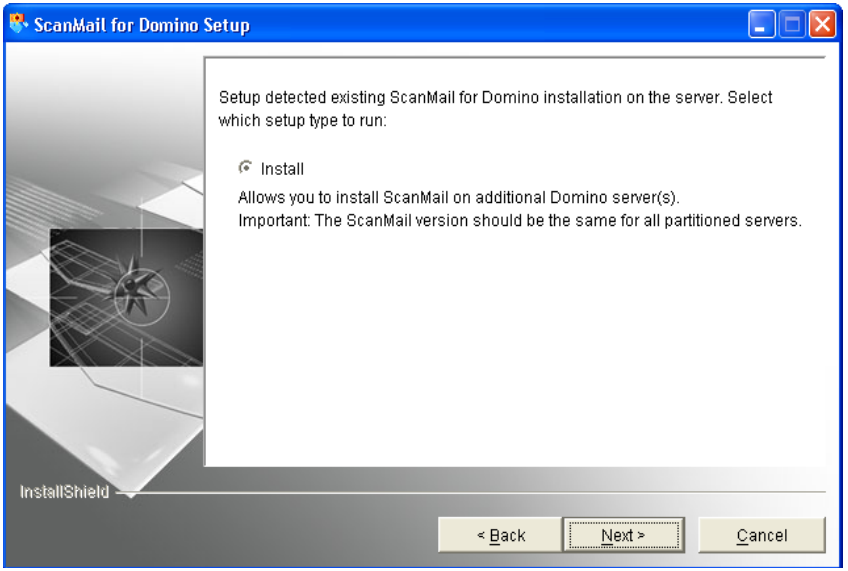


FIGURE 2-5. ScanMail Install Setup screen

See *Setup options* on page 2-13 for details.

5. On the Product Activation screen shown in *Figure 2-6*, you may opt to enter a *ScanMail Activation Code* to activate ScanMail or skip this screen and use the Configuration database to activate later.

Note: Obtain an Activation Code to activate a ScanMail evaluation, standard, or suite version when migrating from ScanMail 2.x, even if the ScanMail 2.x serial number has not yet expired.

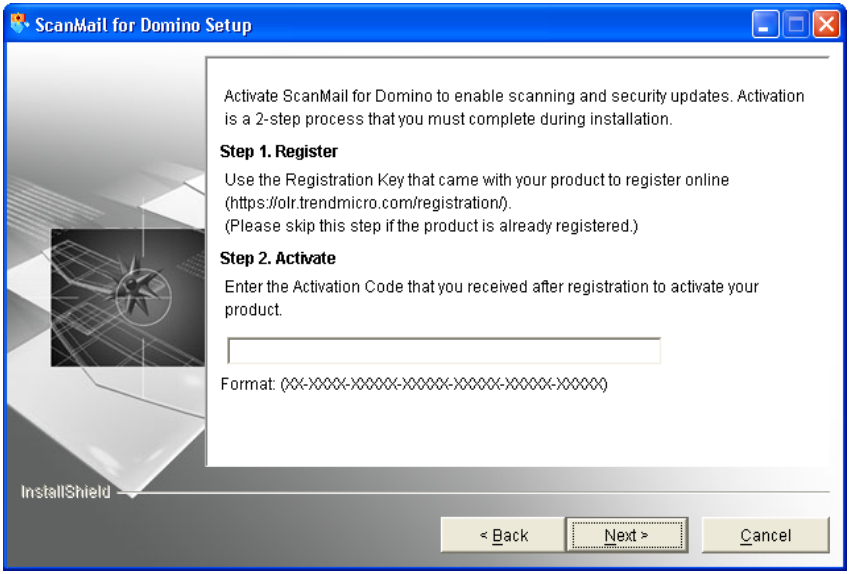


FIGURE 2-6. Product Activation screen

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:

  Go the Trend Micro Product Registration Web site (`https://olr.trendmicro.com/registration`) and follow the on-screen instructions to register your product. Register your product to ensure you are eligible to receive the latest security updates and other product and maintenance services. After registration is complete, Trend Micro sends a *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 3, 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 ScanMail scan or update task will not load. Activate ScanMail immediately after installation to protect your Domino environment (see *page 2-46*).

6. Click **Next >**. Setup extracts installation files to the local temporary directory and then proceeds to the Domino Server screen.
7. On the Domino Server screen, click:
   - **Add** to specify the `notes.ini` file for the target server, including that of the partitioned servers, where ScanMail should be installed.
   - **Remove** to delete a server from the list.

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

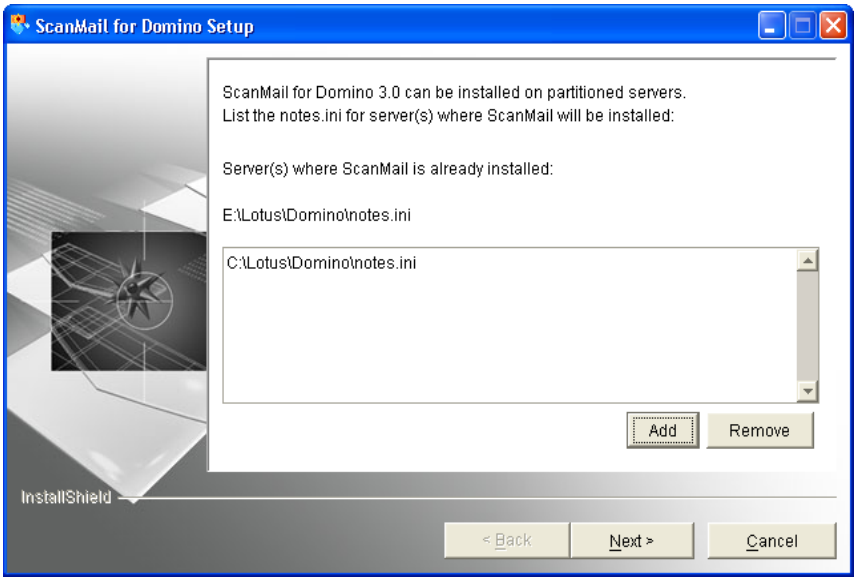


FIGURE 2-7. Setup lists existing ScanMail installations.

8. Click **Next >**. The Domino Server Binary and Data Directories screen, similar to the one shown in *Figure 2-8*, appears.

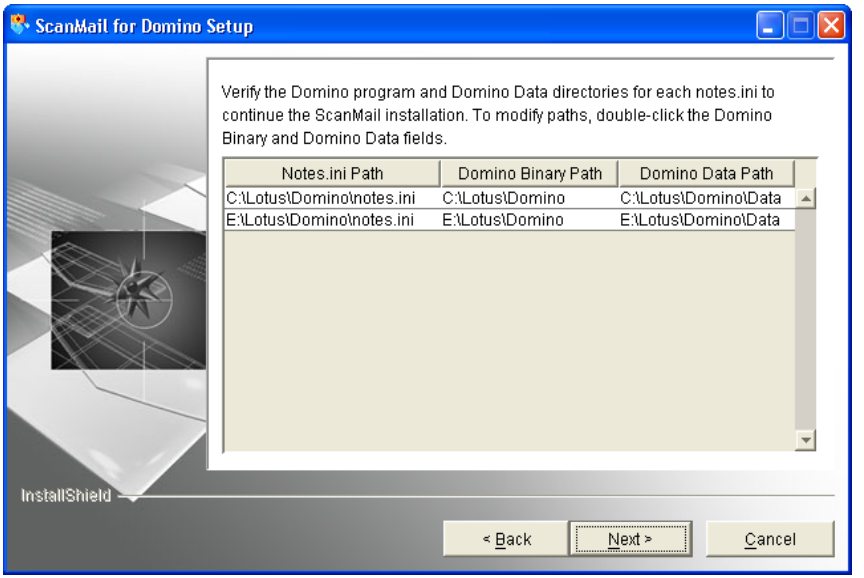


FIGURE 2-8. Verify the Domino program and Data directories screen

Setup detects the Domino Binary and Data paths.

If any of the paths are missing in the `notes.ini` specified, double-click the empty item to specify the correct directory.

Note: Setup checks whether the specified Domino Binary path contains Domino binaries. When Setup detects an invalid Domino Binary path, it displays the message *Invalid Domino Binary or Data directory path. Check the path and try again.*

---

9. Click **Next >**. The Database Replication Selection screen appears.

By default, Setup will enable the replication of 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.

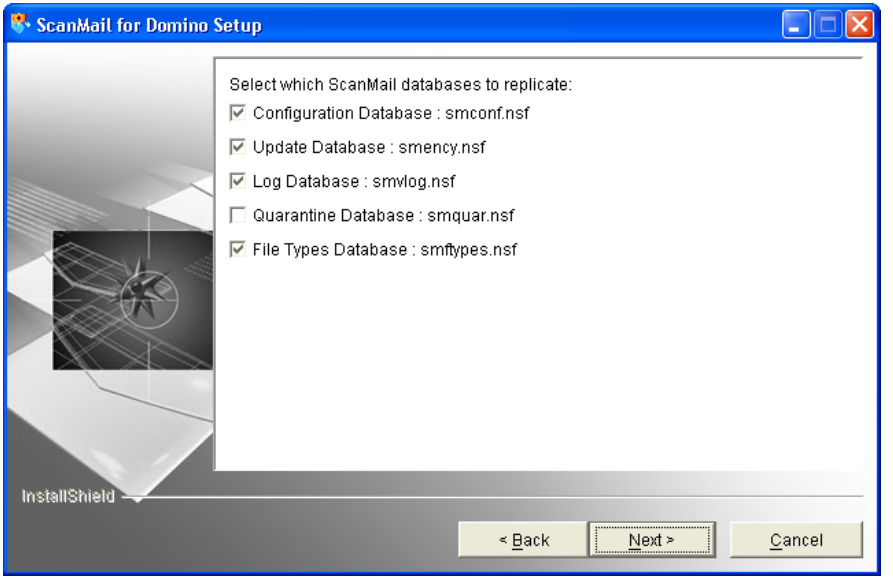


FIGURE 2-9. ScanMail database replication settings

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.

10. 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.

---

11. 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

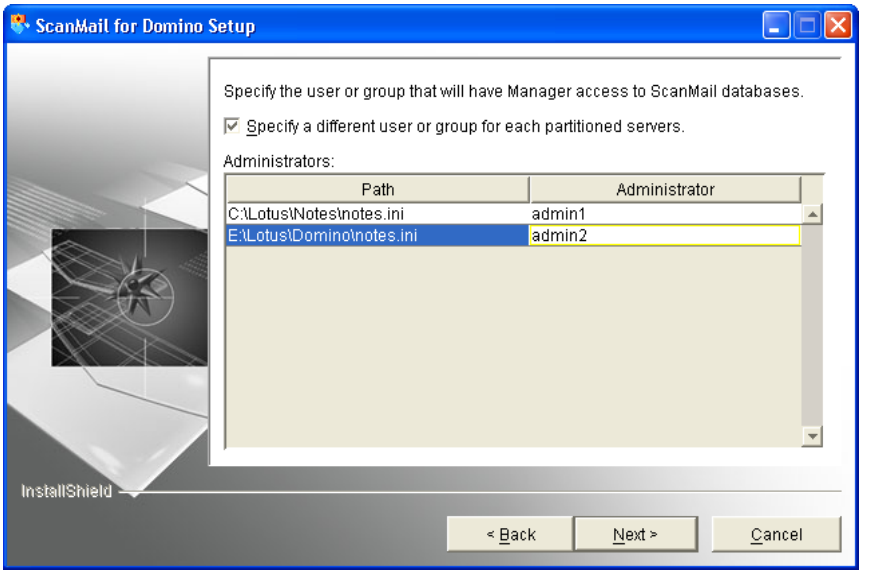


FIGURE 2-10. Specify Manager access screen

12. Click **Next >**. The ScanMail Database Signing screen, shown in *Figure 2-11*, appears.

    Do one of the following:

    - Select **Skip database signing** to prevent Setup from signing ScanMail databases.

      Sign ScanMail databases manually after the installation.

    - 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 target server/partition** to sign ScanMail databases on each partition with a different ID.

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

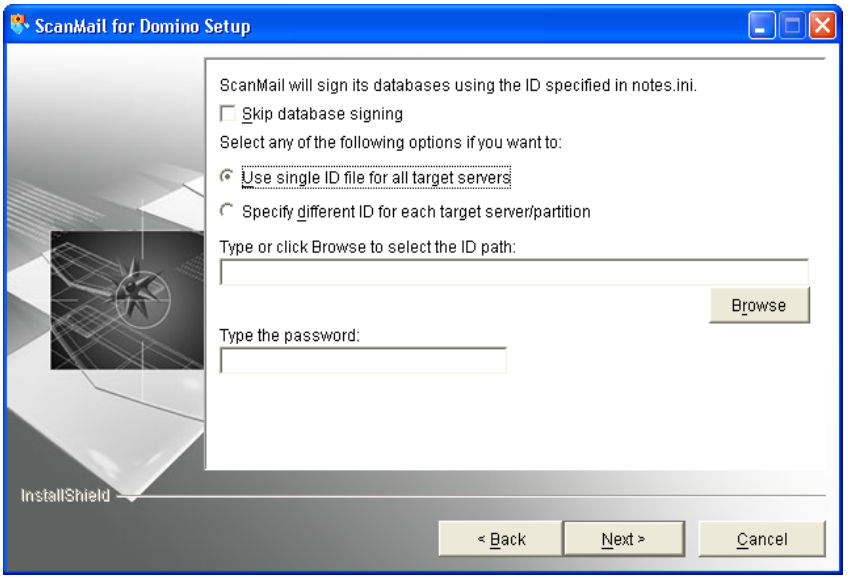


FIGURE 2-11. ScanMail database signing screen

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

13. Click **Next >**. The installation begins.

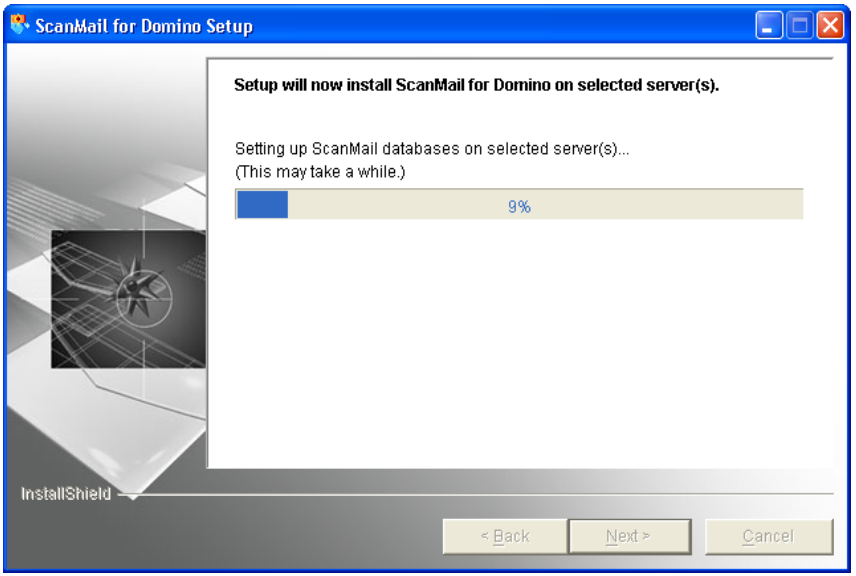


FIGURE 2-12. Setup installs ScanMail on selected server(s).

14. Click **Finish** to close the Setup window.

See *Testing Installation with EICAR* on page 2-49 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 *ScanMail for Domino and other antivirus products* on page 2-45.

Running a silent installation

Silent ScanMail installation minimizes the number of installation windows, 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.
- Read the *Recommended System Requirements* on page 2-5 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.

To install ScanMail in silent mode:

1. From the command console, type the appropriate information below to record the silent installation script file while installing ScanMail to a single or partitioned Domino server:
   - ScanMail for Domino for Windows

     ```
     setupwin32 -options {script path and file name} -silent
     ```

     For example:

     ```
     setupwin32 -options-record c:\smd silent.txt -silent
     ```

     Note: Run this command from a command line prompt opened in a graphical desktop environment (for example, KDE) when recording a script file for a silent ScanMail installation.

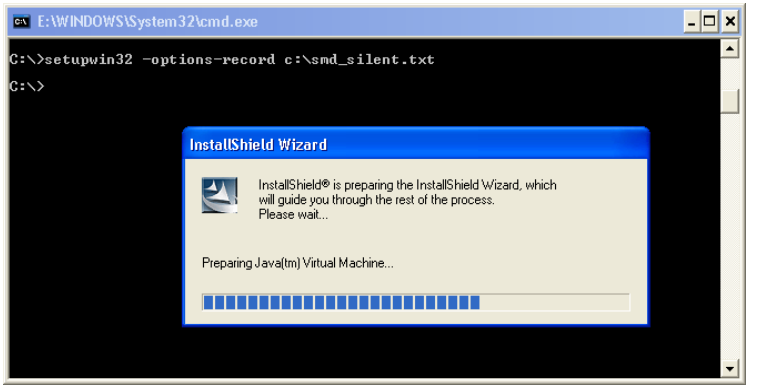


FIGURE 2-13. Recording a ScanMail installation on a Windows server

- ScanMail for Domino for Linux/Solaris/AIX (console-based installation)

  `./SMD3Setup{platform}.bin -console -options-record {path and script file name}`

  Replace `{platform}` with `Linux`, `Solaris`, or `AIX`.

  Example:

  `./SMD3SetupSolaris.bin -console -options-record /tmp/silent.txt`

- ScanMail for Domino for i5/OS and OS/400

  `java -cp ./setup.jar`

  `run -console -options-record ./smd_silent.txt`

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

   - ScanMail for Domino for Windows

     `setupwin32 -options-record "{path and script file name}" -silent`

     For example:

```
setupwin32 -options "c:\smd_silent.txt" -silent
```

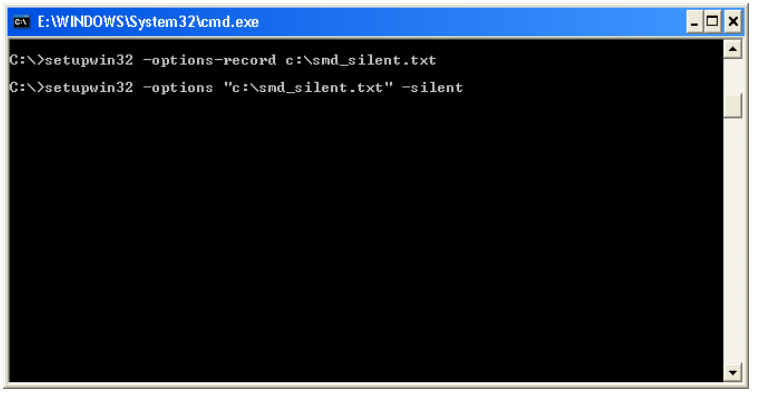


FIGURE 2-14. Running a silent ScanMail installation on a Windows server

- ScanMail for Domino for Linux/Solaris/AIX

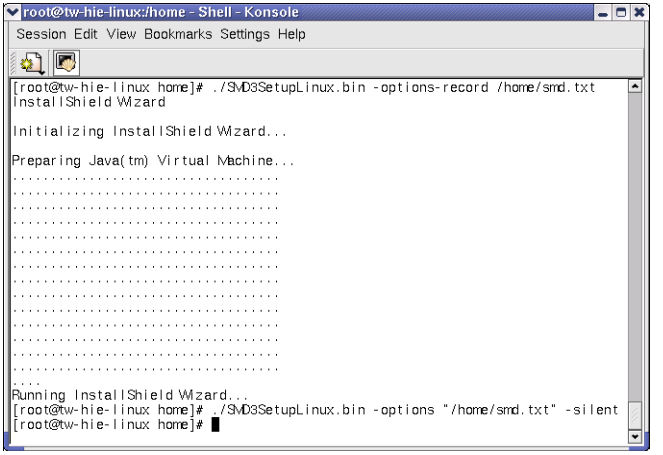


FIGURE 2-15. Running a silent ScanMail installation on a Linux server

- ScanMail for Domino for i5/OS and OS/400

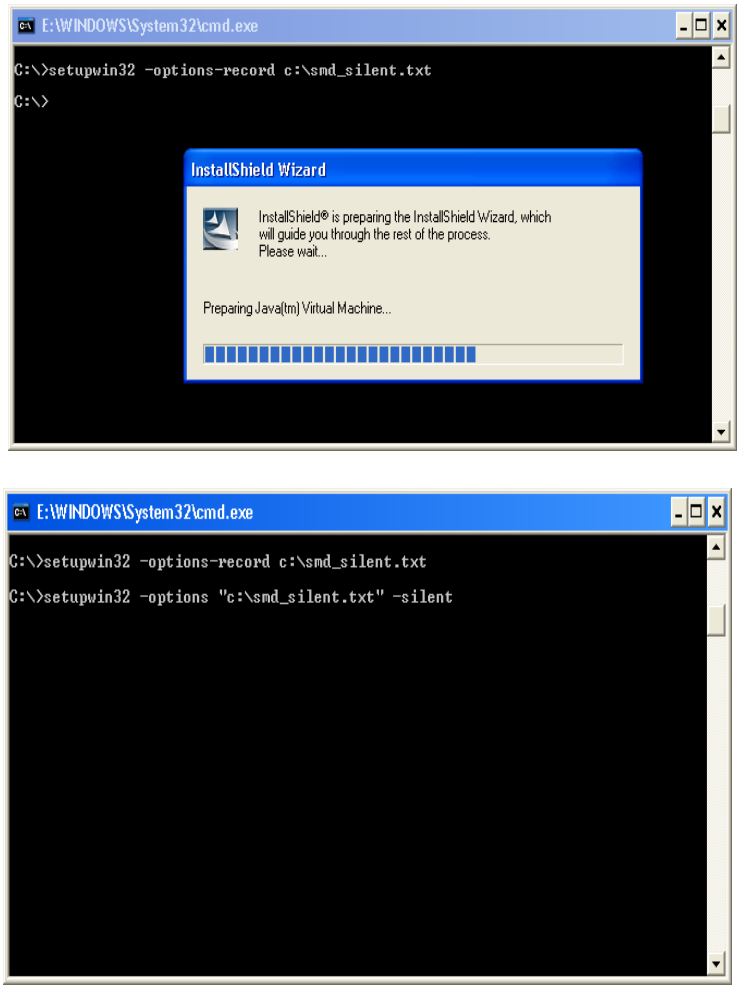


FIGURE 2-16. Running a silent ScanMail installation on an i5/OS or OS/400 server

Open the silent installation log file for the Setup result, `setuplog.txt`, which is created in the same directory as the Setup program. A successful installation records "*Setup successfully installed ScanMail on the following server(s):...*" in the log file. In addition, the following popup message appears:

"*Setup has finished the ScanMail for Domino silent installation. To review...*"

Follow the steps in *Testing Installation with EICAR* to check whether the ScanMail installation is successful.

Running a console-based installation

ScanMail for Domino console-based installation can be run on the following non-Windows platforms:

Platform	Home Page
Solaris 9, 8, and 7	http://wwws.sun.com
Red Hat Enterprise Linux 5, 4 and 3	http://www.redhat.com
SUSE 7.2 SUSE Linux Enterprise Server 10, 9, 8	http://www.suse.com
AIX 5.3, 5.2, 5.1	http://www-900.ibm.com/cn/products/servers/pseries/index.shtml
i5/OS V5R3 OS/400 V5R2	http://www-900.ibm.com/cn/servers/eser/product/iseries.shtml

See *Table 2-1* for detailed system requirements.

Tip: You can use the wizard-based installation to install ScanMail on a Linux, Solaris, or AIX platform. See *page 2-13*.

See *Pre-installation tasks* on page 2-8 for tasks you need to perform before running Setup.

To install ScanMail from the command line:

Note: The console-based ScanMail installation screens shown are i5/OS and OS/400 platform.

1. Do one of the following to navigate to the Setup binary:
   - If you have the Trend Micro Enterprise Solutions CD set, mount the first CD and then navigate to the ScanMail for Domino folder.
   - If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your server.
2. Type the following to launch the console-based installation:

PLATFORM	SETUP PROGRAM
Linux	`./SMD3SetupLinux.bin -console`
Solaris	`./SMD3SetupSolaris.bin -console`
AIX	`./SMD3SetupAix.bin -console`
i5/OS and OS/400	`java -cp ./setup.jar run -console`

Setup launches and ScanMail Welcome appears.

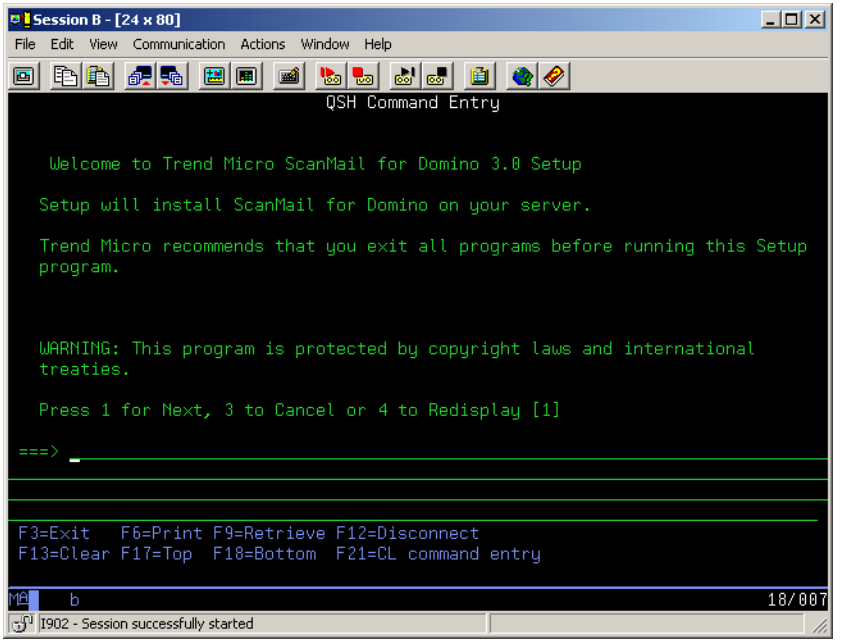


FIGURE 2-17. ScanMail Setup Welcome

Tip: Throughout the console-based Setup, press **ENTER** to accept an existing setting or type **1** to proceed to the next step. Type **3** to cancel Setup.

For most of the screens, the following instructions apply:

- Type 0 to accept the existing setting.
- Type 1 to continue to the next screen.
- Type 2 to return to the previous screen.
- Type 3 to exit Setup.
- Type 4 to redisplay the current screen.

3. Type 1 to start the ScanMail Setup.

4. On the License Agreement screen, press **ENTER** or type `q` to skip reading the ScanMail for Domino License Agreement.

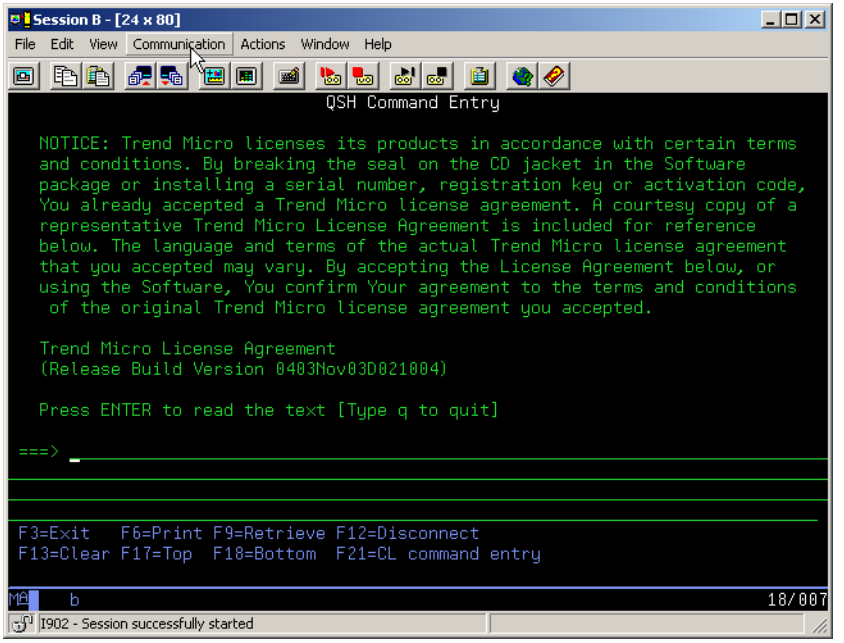


FIGURE 2-18. ScanMail license agreement

5. On the License Agreement prompt, type `1` to select *I accept the terms of the license agreement* and install ScanMail. If you not agree to the terms of the license agreement, type `2` and then type `3` to cancel the ScanMail setup.

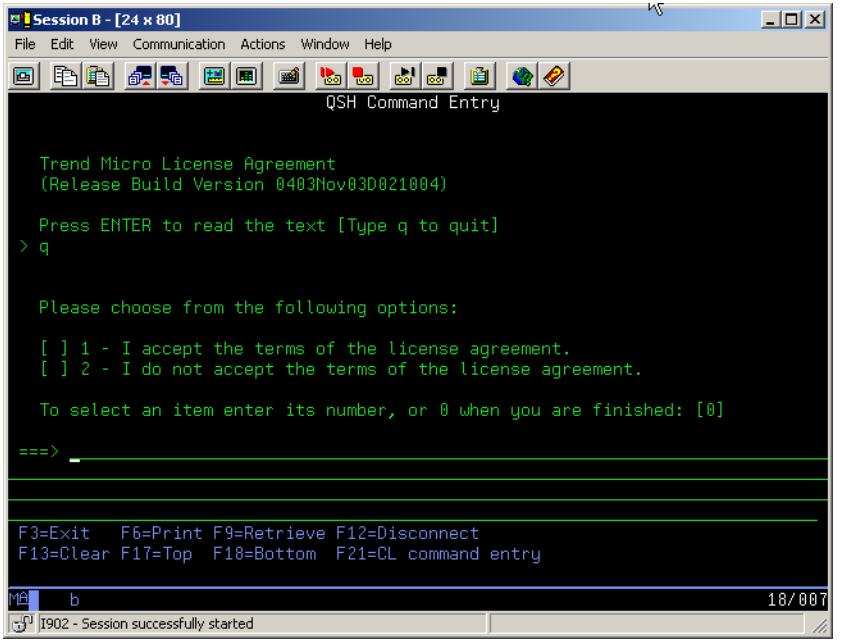


FIGURE 2-19. ScanMail license agreement acceptance screen

6. On Product Activation, you may enter an Activation Code to activate ScanMail or skip this screen and use the Configuration database to activate later.

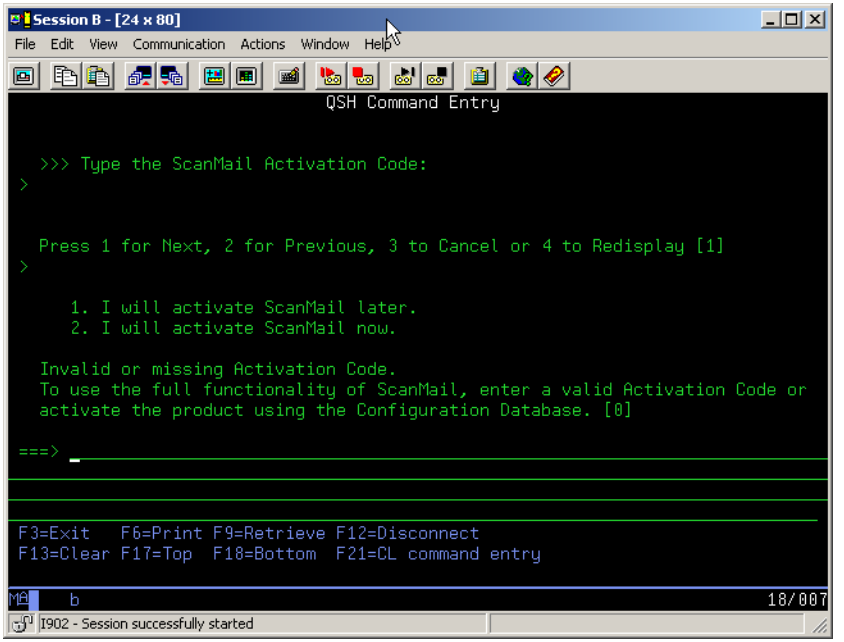


FIGURE 2-20. Product Activation

Do one of the following:

- If you have not registered ScanMail:

  Go the Trend Micro Product Registration Website (https://olr.trendmicro.com/registration) and follow the on-screen instructions to register your product. Register your product to ensure eligibility to receive the latest security updates and other product and maintenance services.

  After completing the registration, Trend Micro sends a ScanMail Activation Code (AC) to the email address specified in the Registration Profile. 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 3, obtain a ScanMail Full or Suite Activation Code, and then activate the software.

- If you do not have a Registration Key nor an Activation Code, or you want to activate later, skip this screen.

  Setup will install ScanMail. However, the ScanMail scan or update task will not load. Activate ScanMail immediately after installation to start the Domino environment protection.

7. On Domino Server, Setup lists the existing ScanMail installation.

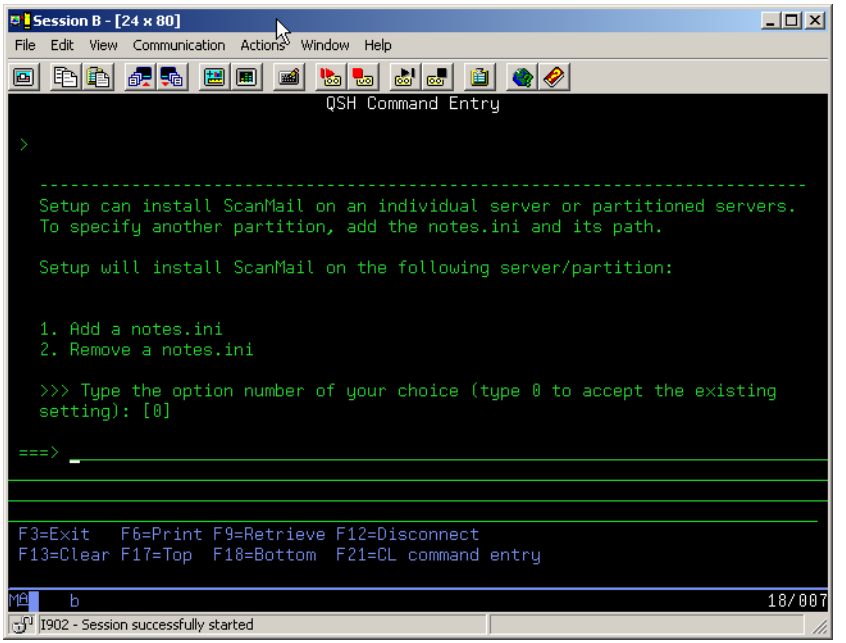


FIGURE 2-21. Domino server list of existing installations

Do one of the following:

- Type **1** to add a `notes.ini` and specify the target Domino server

  For example, `/lotus/notesdata/notes.ini`

  (Linux, Solaris, AIX, and i5/OS and OS/400 platforms)

- Type **2** to remove a `notes.ini` and prevent Setup from installing ScanMail to a Domino server or partition

Setup checks whether the specified Domino Binary path contains Domino binaries. When Setup detects an invalid Domino Binary path, the following message displays:

Invalid Domino Binary or Data directory path. Check the path and try again.

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

8. On the Domino Server Binary and Data Directories screen, select the desired option number to modify the Domino binary or Domino Data path.

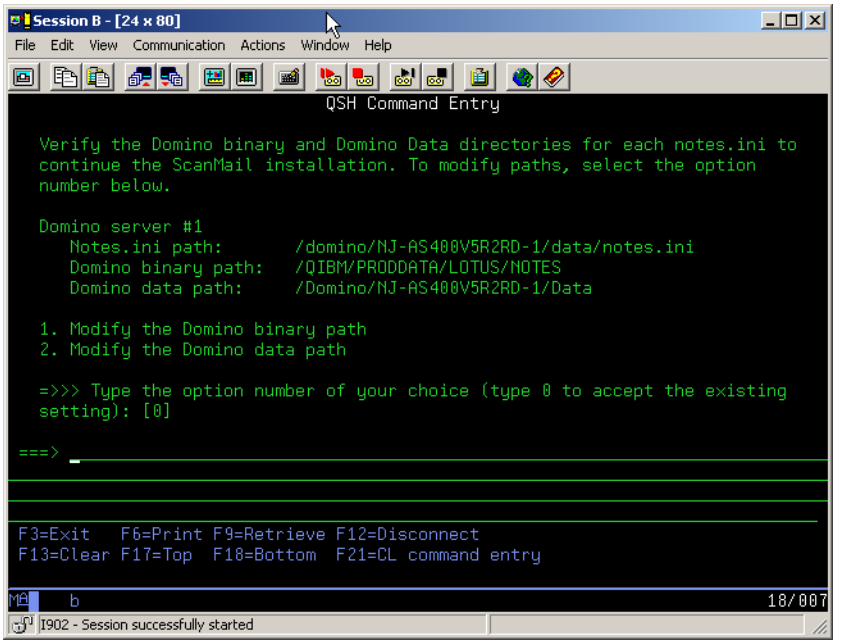


FIGURE 2-22. Domino Server Binary and Data Directories

Setup analyzes the target server(s). It checks for installed ScanMail information and displays the result.

Setup performs an upgrade on target server(s) with an existing ScanMail 3 installation and a fresh ScanMail installation on target server(s) without ScanMail installed.

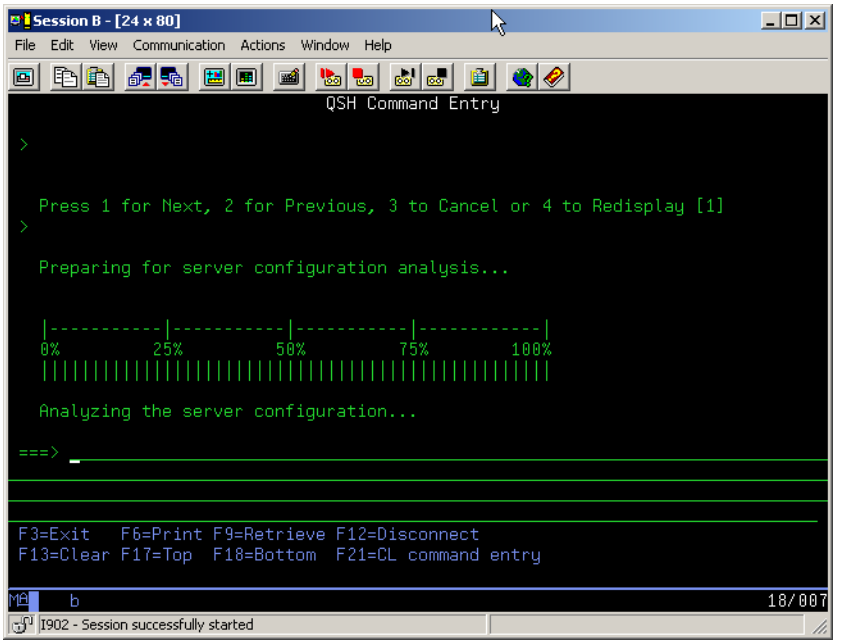


FIGURE 2-23. Configuration Analysis—installing ScanMail for the first time

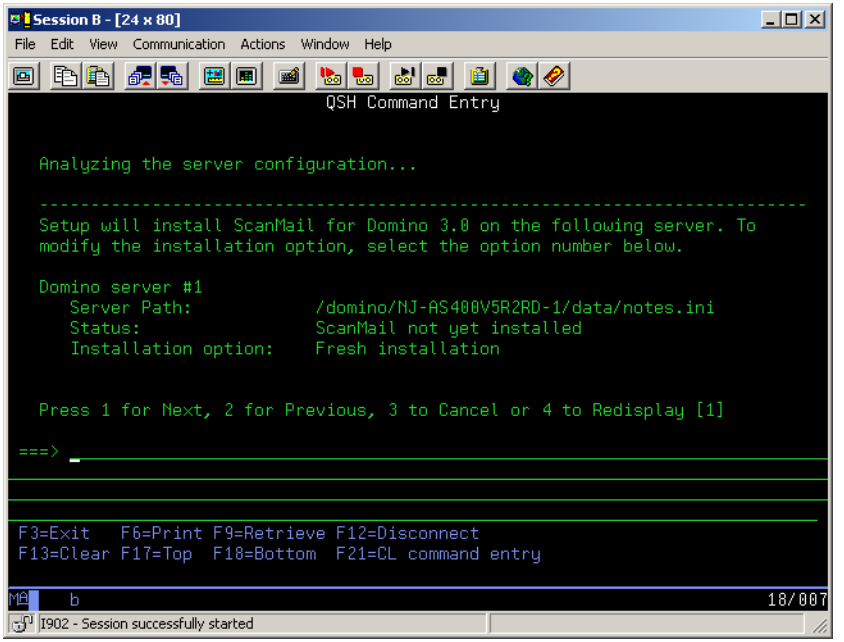


FIGURE 2-24. Configuration Analysis results

9. On the Database Replication Settings, select the ScanMail databases that Setup will enable for replication.

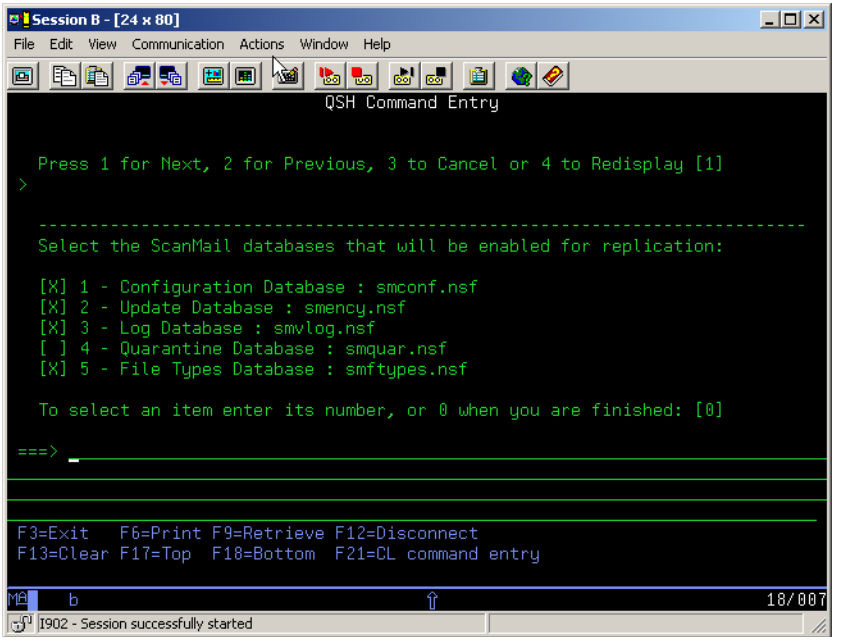


FIGURE 2-25. Database Replication Settings

By default, Setup will enable the replication of 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.

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 to receive the default policy.

---

10. Select whether to accept the default policy.

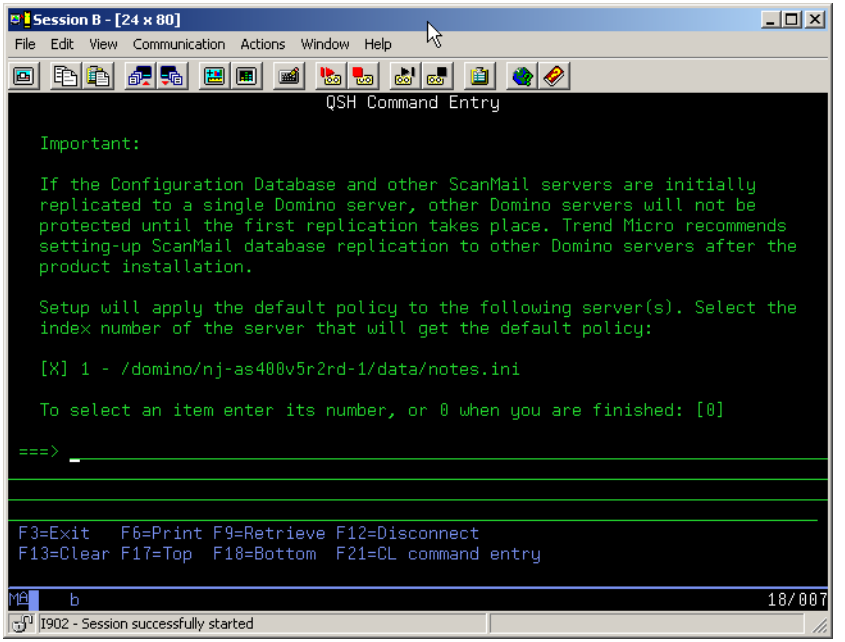


FIGURE 2-26. Accepting the Default Policy

11. On ScanMail Administrator Settings, do one of the following:

- Type the name of the user that will have Manager access to all ScanMail databases (for example, `notes_admin`)
- Otherwise, if the target server(s) are partitioned server(s) and you have different administrator groups for each partition, specify a different user or

user group for each partitioned server and then type the administrator account for each server.

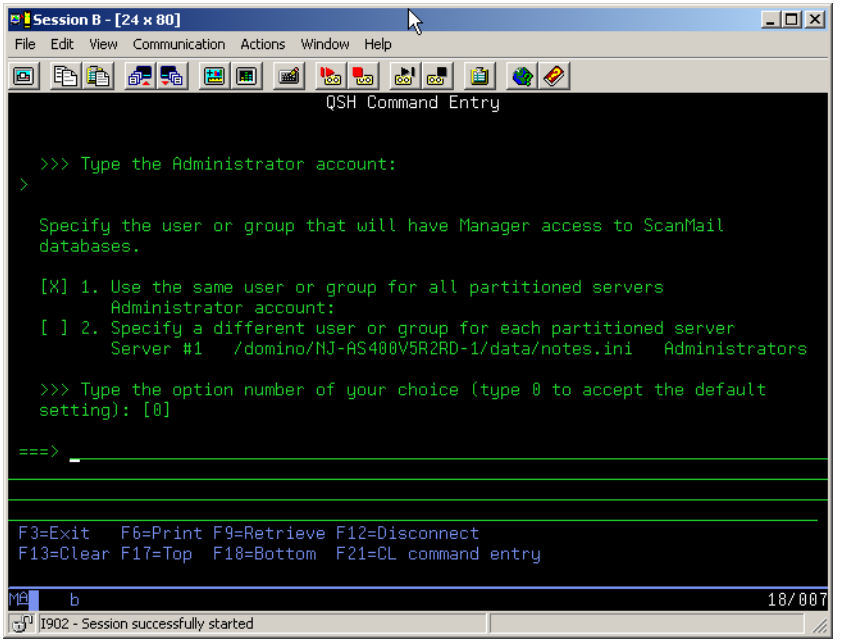


FIGURE 2-27. Administrator account settings

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

12. On ScanMail Database Signing, do one of the following:

- Type **2** to select **Skip database signing** and postpone the ScanMail database signing

  Sign ScanMail databases manually after the installation. Refer to *Signing ScanMail Databases with a Different ID* on page 4-4 for instructions.

- Type **3** to select **Use single ID file for all target servers** and sign the ScanMail databases with a single ID

Type the ID (including its full path) and password.

- Type **4** to select **Specify different ID for each target server/partition** and sign the ScanMail databases on each partition with a different ID

  Type the ID (including its full path) and password.

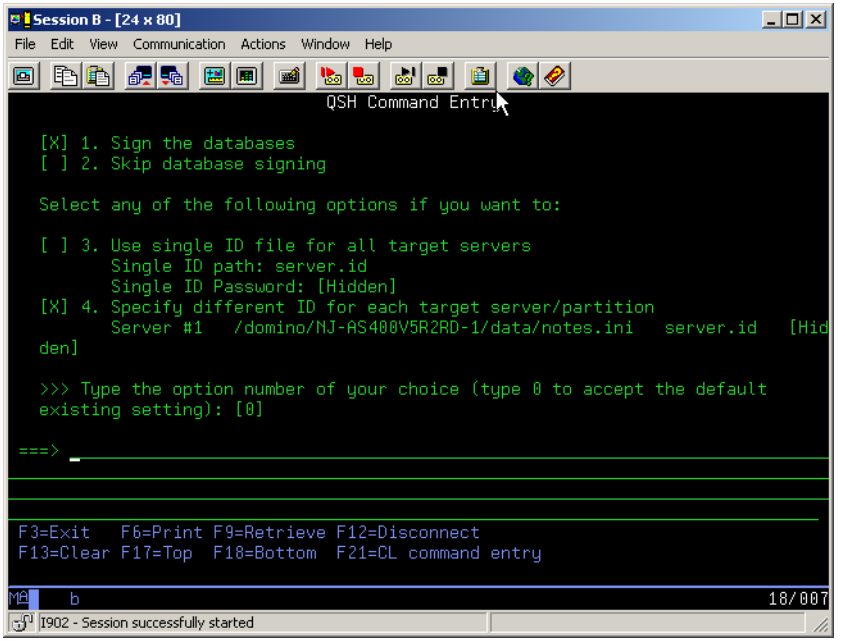


FIGURE 2-28. Database signing screen

Setup copies the ScanMail components to the target server(s).

13. After completing the installation, press ENTER to exit Setup.

ScanMail is now installed.

Starting the Domino Server

After installing ScanMail, start the Domino server to launch the ScanMail tasks and test the installation with EICAR (*page 2-49*) to confirm whether ScanMail is

successfully installed. In addition, refer to *Getting Started with ScanMail* 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 a Linux/Solaris/AIX platform:

1. On a Linux platform using LinuxThread, execute the following command to set the environment variable that will prevent Domino and other applications from hanging:

   ```
   export LD_ASSUME_KERNEL=2.2.5
   ```

2. Make certain you are logged in with the Domino user account and not as root. Check this by issuing the command whoami or id.
3. Change to your Domino data directory (for example, `local/notesdata`), and then type the following command at the command prompt to start the Domino server:

   ```
   server
   ```

   - or -

   ```
   server -jc &
   ```

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

   ```
   /opt/lotus/bin/server
   ```

To start the Domino server on i5/OS and OS/400 platforms:

Run the CL command "`strdomsvr`".

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

ScanMail for Domino 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 an *ScanMail Activation Code*, which you can then use to activate ScanMail.

ScanMail Activation Code

ScanMail for Domino 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 and spam filtering.

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 for Domino 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-hand menu, click **Administration** > **Product License**.
3. *Creating a license profile* (see *page 6-12*).
4. Delete the license profile created during installation (see *page 6-12*).

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 6-12*).
5. Delete the corresponding license profile for the evaluation version (see *page 6-12*).

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-hand 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**.

Note: Do not delete the Control Manager account used to install the Control Manager agent; deleting the account prevents the agent from re-registering with the Control Manager server

---

- Obtain and check the location of the public encryption key of the Control Manager server to which you want to register the agent; only Control Manager agents use this key.

Note: It is still necessary to install an agent for ScanMail even if you have installed a Control Manager agent for other Trend Micro products. However, you do not need to obtain the public encryption key if you will register ScanMail to the same Control Manager server as the other products.
Consequently, Setup will no longer install the Control Manager Communicator if another product agent is available on the same Domino server.

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 the ScanMail Files and Folders

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

- *ScanMail and Control Manager Agent (Windows)* on page D-2
- *ScanMail and Control Manager Agent (Linux/Solaris/AIX)* on page D-4
- *ScanMail and Control Manager Agent (i5/OS and OS/400)* on page D-6

Chapter 3

Installing Control Manager Agent for ScanMail

Trend Micro Control Manager™ is a centralized management console that provides a way to consolidate antivirus and content security protection when you are running multiple instances of ScanMail or using multiple Trend Micro products. When you install Control Manager agent for ScanMail, you can analyze virus logs and make simultaneous virus pattern and scan engine updates from the Control Manager console.

Note: Control Manager agent is not available for i5/OS.

This chapter guides you through installing the Control Manager agent for ScanMail and contains the following topics:

Installing the Control Manager Agent for ScanMail

When installing the Control Manager agent, consider the following points:

- If the Control Manager agent for ScanMail for Lotus Notes is installed, you will need to install the Control Manager agent for ScanMail for Domino.
- If there is a Control Manager agent on a Domino server (for example, because another antivirus product is installed on the same server), you must install the Control Manager agent for ScanMail, too.
- Install one agent on each server running ScanMail.
- For Domino partitioned servers, install a separate instance of the agent on each partition.
- Since the agent Setup requires the Domino server to be running, but the ScanMail Setup requires the Domino server to be stopped, install ScanMail on all your partitions first, start the server, and then install all the agents.
- Control Manager can simultaneously update managed products on various platforms.

Upgrading from ScanMail 2.5x or 2.6x

If you are using Control Manager, remove the existing Control Manager agent before installing Control Manager agent 3.0. Trend Micro recommends that you remove the existing Control Manager agent before installing ScanMail for Domino. Install ScanMail for Domino and then install the latest version of Control Manager agent.

Pre-installation tasks

Perform the following tasks before installing the Control Manager agent for ScanMail:

- Determine the administrator or equivalent credentials on the ScanMail servers where agents are to be installed.
- Obtain the Control Manager User ID with an Administrator, Power User, or Operator account type.

Note: Do not delete the Control Manager account used to install the Control Manager agent or you will not be able to re-register the agent with the Control Manager server.

- Verify that the Control Manager server and the network environment are interacting properly when using the telnet command to communicate between the Domino server and the Control Manager server. Test the following ports:
  - TELNET <control_manager_ip>
  - HTTP
  - 10198
  - 10319
  - SSL
- Obtain the public encryption key for the Control Manager server to which you want to register the agent and verify its location 9 (unnecessary for ScanMail for Domino for i5/OS and OS/400).

Note: You must install an agent for ScanMail even if you have installed a Control Manager agent for other Trend Micro products. However, you do not need to obtain the public encryption key if you will register ScanMail to the same Control Manager server as the other products. Setup will not install the Control Manager Communicator if another product agent is available on the same Domino server.

- Print and fill out the *Control Manager Agent Checklist* on page C-1 to help you gather specific information about your product servers.

Note: On AIX and i5/OS and OS/400 platforms, the Control Manager Agent installation does not support an upgrade from Control Manager Agent for ScanMail for Lotus Notes 2.6 to Control Manager Agent for ScanMail for Domino 3. You must uninstall Control Manager Agent for ScanMail for Lotus Notes 2.6 first and then install Control Manager Agent for ScanMail for Domino 3.

Obtaining the public encryption key (`E2EPublic.dat`)

Control Manager agents use a public encryption key, `E2EPublic.dat`, to identify the Control Manager server with which it will be registered. The key is required during agent installation.

To obtain `E2EPublic.dat`:

1. Access the Control Manager management console (see *page 10-5*).
2. Click **Products** on the menu.
3. Click **Add/Remove Product Agents** on the left-hand menu.

Right-click **Public encryption key**, and then click **Save Target As**. Save the `E2EPublic.dat` file to a location that the agent installation program can access.

Setup modes

Similar to ScanMail for Domino, the following setup modes apply to the Control Manager agent for ScanMail:

- **Wizard-based installation** requires user input when installing the Control Manager agent for ScanMail on a server supporting a graphical user interface.

  The wizard-based installation provides a series of interfaces that help simplify the agent installation. See *page 3-5*.

- **Console-based installation** requires user input when installing the Control Manager agent on a server that does not support a graphical user interface.

  The Control Manager agent for ScanMail Setup on all platforms except Windows use this method. See *page 3-14*.

Running a Wizard-based Installation

Run the corresponding Setup program for the platform where Control Manager will be installed to initialize the wizard-based installation. The i5/OS and OS/400 platforms do not support a graphical interface wizard-based installation.

To install the Control Manager agent for ScanMail from a graphical user interface:

Note: The Control Manager agent for ScanMail for Windows Setup was used to capture screenshots presented in the wizard-based installation.

1. Do one of the following to navigate to the Setup program:
   - If you are installing from the Trend Micro Enterprise Protection CD, go to the `\products\smd\cmagent` folder on the CD.
   - If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your computer, typically the `\cmagent` sub-directory of the ScanMail installation directory.
2. Double-click one of the following to launch the Setup program:

PLATFORM	SETUP PROGRAM
Windows	`smd3-windows-cmagent.exe`
Linux	`CMAgent3SetupLinux.bin`
Solaris	`CMAgent3SetupSolaris.bin`
AIX	`CMAgent3SetupAix.bin`

3. When the program launches, the InstallShield Welcome screen and then a Welcome screen, similar to the one shown in *Figure 3-1*, appears.

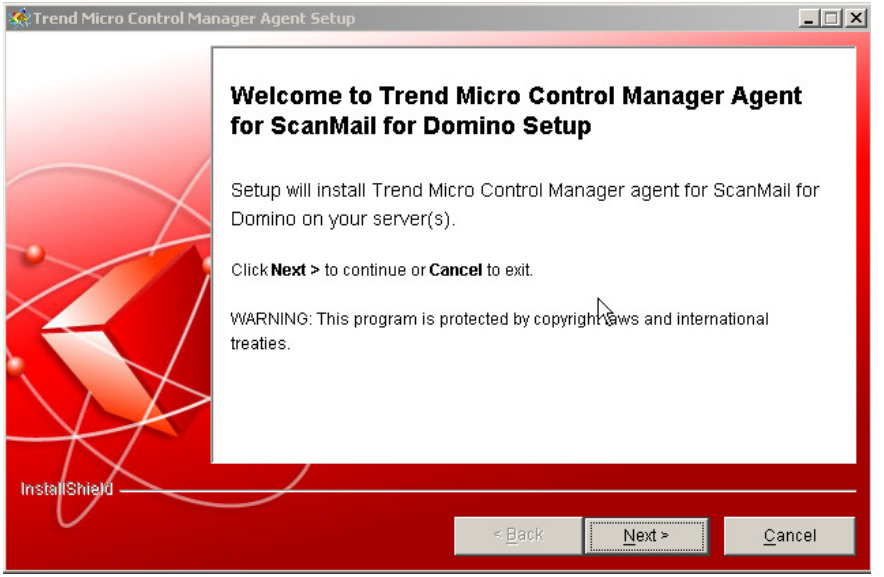


FIGURE 3-1. Trend Micro Control Manager Agent Setup Welcome screen

4. Click **Next >**. The Software License Agreement screen, similar to *Figure 3-2*, appears.

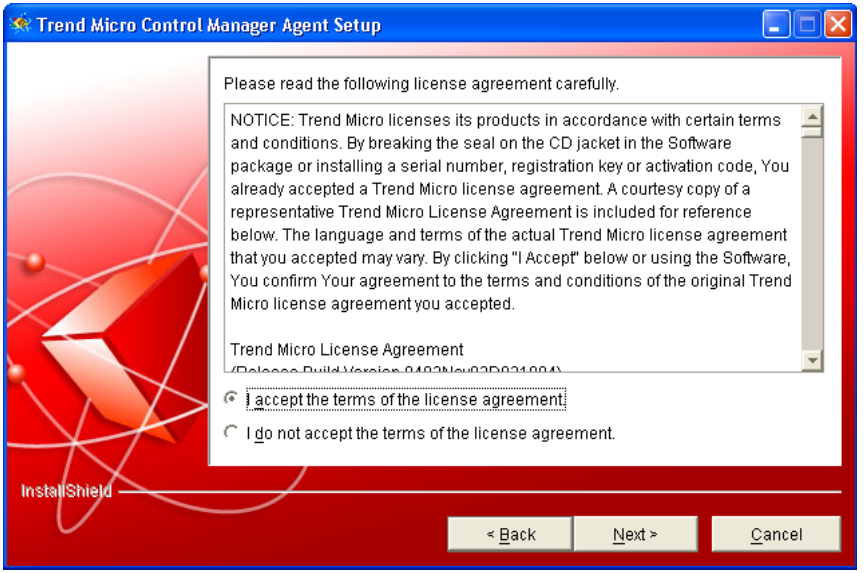


FIGURE 3-2. Trend Micro Control Manager Agent Setup license agreement screen

After you have read the entire license agreement, select **I accept the terms of the license agreement** to continue with the ScanMail 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 process stops.

5. Click **Next >**. Setup extracts installation files to the local temporary directory and then proceeds to the Domino Server Analysis screen (*Figure 3-3*).

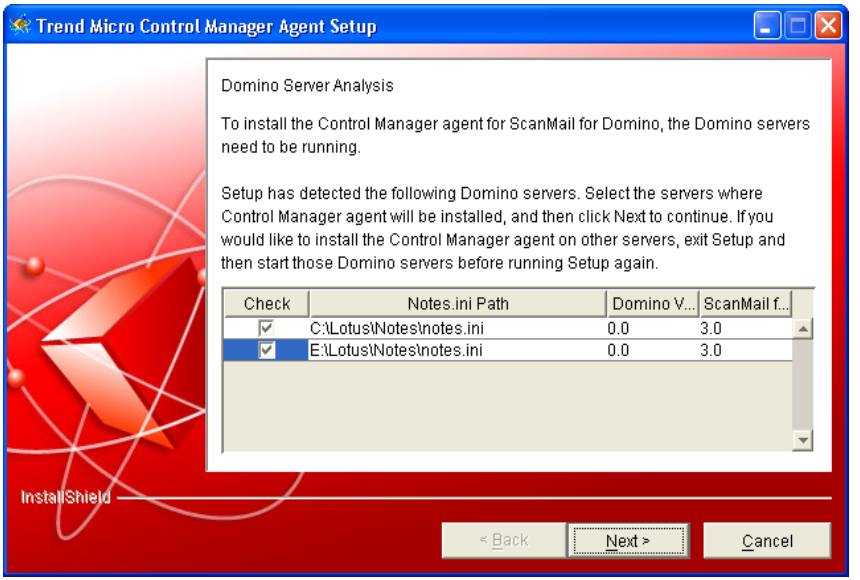


FIGURE 3-3. Trend Micro Control Manager Agent Setup Domino Server Analysis screen

To select the server(s) where you want to install the Control Manager agent, click the corresponding check box and then click **Next >**.

If the server(s) you have selected have the same version of Control Manager agent already installed and you are ***not*** performing a fresh installation, the installation program will ask whether you want to continue the installation.

- Click **Yes** to install Control Manager agent for a new Domino Server.
- Click **No** to finish the installation process without any changes to the servers.

Note: If a Trend Micro Infrastructure (TMI) is already installed on your server, the agent will use the existing Trend Micro Infrastructure, and steps 5 and 6 will be skipped. See *Introducing the Control Manager Agent for ScanMail and Trend Micro Infrastructure* on page 10-3 for more information on TMI.

---

6. (*Windows platform only*) When you click **Next >,** the Message Routing Path Configuration screen, similar to *Figure 3-4*, appears. Specify the routing for

incoming and outgoing messages between the Control Manager server and the ScanMail for Domino server.

To set the path for incoming messages:

Under **Source of incoming message**, select one of the following options:

- **Any host** to accept messages from any source
- **IP Port Forwarding**; type the **firewall's IP address** and **port number** that has been opened for Control Manager communication in the fields provided
- **Proxy server** to use a proxy server

  Click **Proxy Server Configuration** to set proxy server settings.

To set the path for outgoing messages:

Under **Route for outgoing messages**, select one of the following options:

- Direct to server
- Proxy server

Click **Proxy Server Configuration** to set proxy server settings.

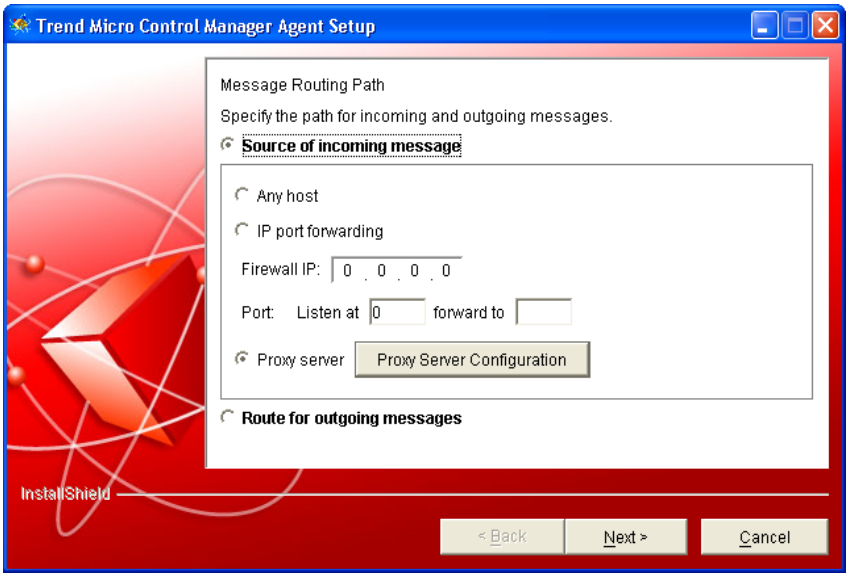


FIGURE 3-4. Trend Micro Control Manager Agent Setup Message Routing Path screen

Click **Next >**.

7. When you click **Next >,** the Public Encryption Key Selection screen shown in *Figure 3-5* appears. Click **Import**. Locate the public encryption key

(`E2EPublic.dat`) of the Control Manager server with which you are registering the agent, and click **Open**.

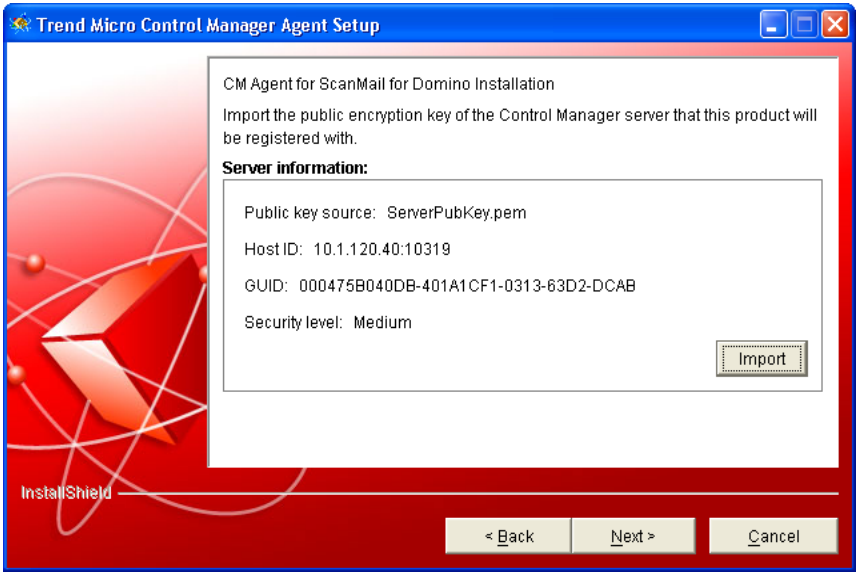


FIGURE 3-5. Import Public Encryption Key Selection screen

- For Windows platform, the Control Manager agent will import the Public Encryption Key file and then display some information that is contained in the Public Encryption Key file on the Server Information view screen.
- For Linux and AIX platforms, the installation program will import the Public Encryption Key file without displaying a Server Information view screen.

8. Click **Next >**. The Control Manager Server Registration screen, similar to *Figure 3-6*, appears.

Type a **root-level Control Manager account** in the **User ID** field.

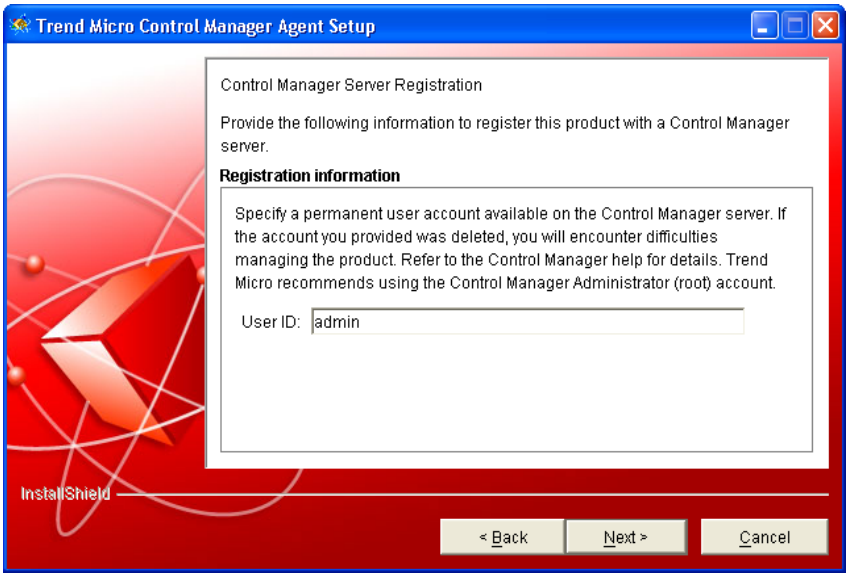


FIGURE 3-6. Trend Micro Control Manager Agent Setup Control Manager Server Registration screen

9. Click **Next >**. Double-click the **Managed Product Name** field to specify name(s) that will appear in the Control Manager Product Directory.

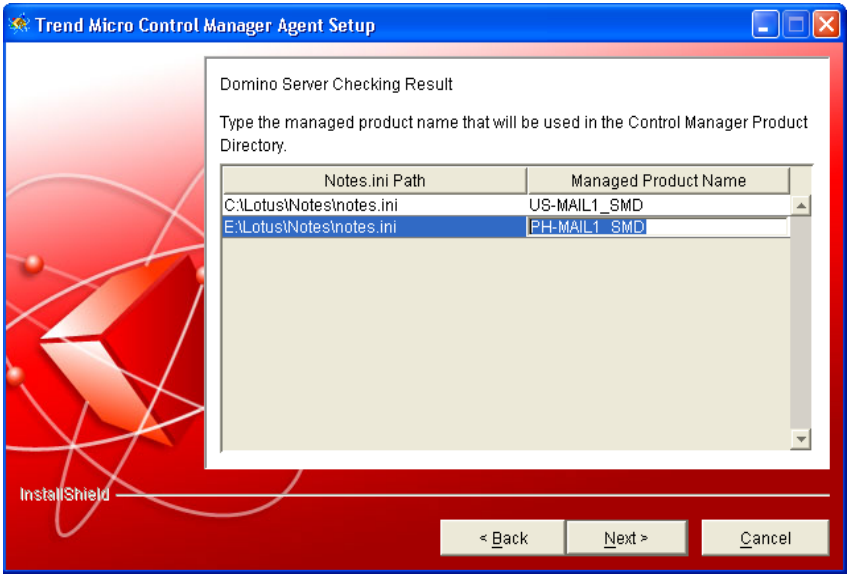


FIGURE 3-7. Trend Micro Control Manager Agent Setup Domino Server Checking Result screen

WARNING! *If you delete the User ID that you specify above from the Control Manager server, you will have difficulty managing the product.*

10. Click **Next >**. At the Installing Agents screen, monitor the status of the installation.
11. Click **Finish** at the final screen.

The Control Manager agent installs. See *page 3-23* to verify a successful Control Manager agent installation.

Running a Console-based Installation

The console-based Control Manager agent installation is available for ScanMail for Domino running on Linux, Solaris, AIX, and i5/OS and OS/400 platforms. The installation flow is almost the same as the wizard-based setup, except for Step 5, which applies to Windows platforms only.

To install Control Manager agent from the command line:

Note: The KDE Shell Konsole was used to capture screenshots presented in the console-based ScanMail installation.

1. Do one of the following to navigate to the Setup binary:
   - If you have the Trend Micro Enterprise Protection CD, mount the CD and then change to the \cmagent subfolder of the ScanMail for Domino folder.
   - If you downloaded the software from the Trend Micro Web site, navigate to the \cmagent subfolder on your server.
2. Type the following to launch the console-based installation:

PLATFORM	SETUP PROGRAM
Linux	`./CMAgent3SetupLinuxbin -console`
Solaris	`./CMAgent3SetupSolaris.bin -console`
AIX	`./CMAgent3SetupAix.bin -console`
i5/OS and OS/400	`java -cp /QIBM/Prod/Data/Java400/jt400ntv.jar:./setup.jar run -console`

Setup launches and Control Manager Agent Welcome prompt appears.

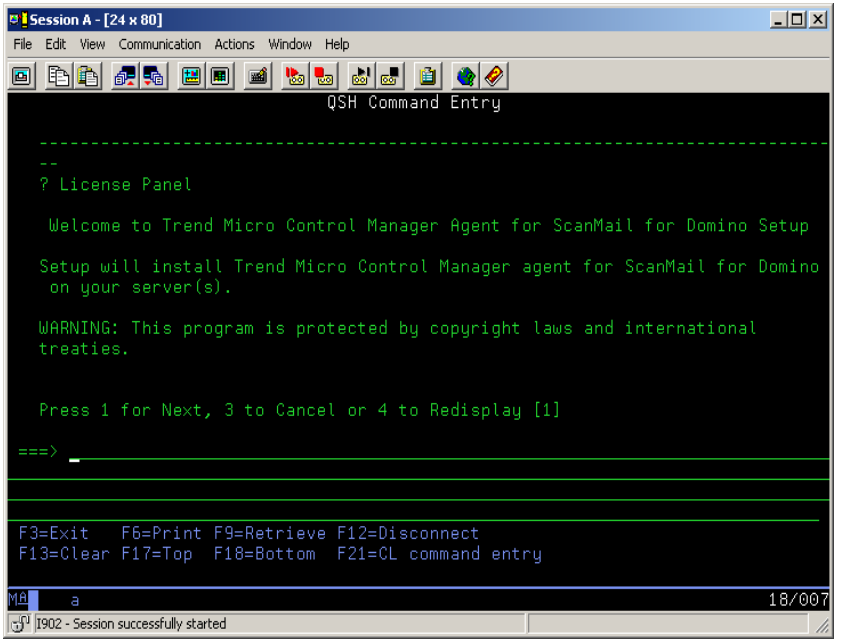


FIGURE 3-8. Control Manager Agent Setup Welcome

Tip: Throughout the console-based setup, press **ENTER** to accept an existing setting or type **1** to proceed to the next step. Type **3** to cancel Setup.

For most of the screens, the following instructions apply:

- Type `0` to accept the existing setting.
- Type `1` to continue to the next screen.
- Type `2` to return to the previous screen.
- Type `3` to exit Setup.
- Type `4` to redisplay the current screen.

3. Type `1` to start the Control Manager agent Setup.

4. On the License Agreement screen, press **ENTER** or type **q** to skip reading the text of the Control Manager agent License Agreement.

   On the License Agreement prompt, type `1` to select *I accept the terms of the license agreement* and install the Control Manager agent. If you disagree with the terms of the license agreement, type `2`.

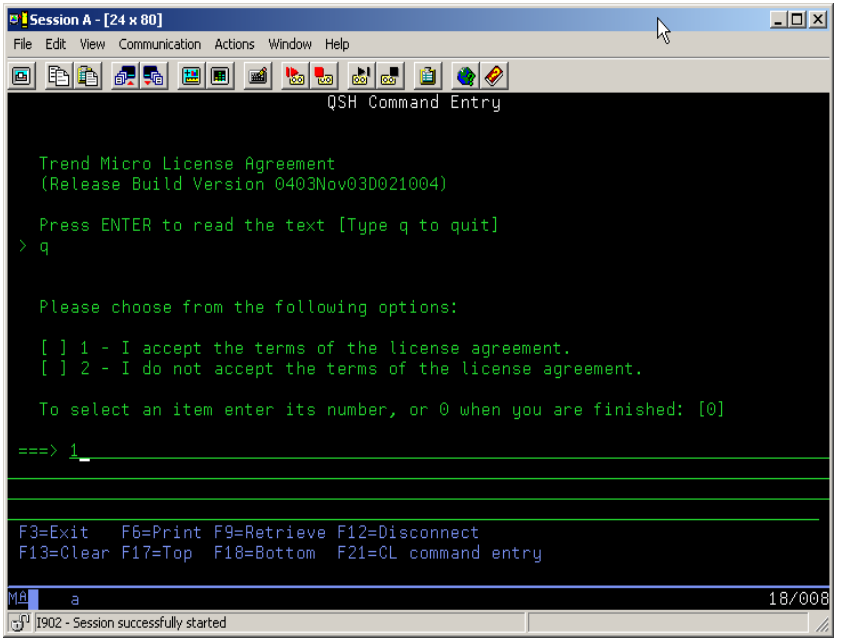


FIGURE 3-9. Control Manager Agent License Agreement

Setup extracts installation files to the local temporary directory.

5. (For i5/OS and OS/400 platforms, skip this step.) On the Public Encryption Key prompt, type the **directory and public encryption key file name**.

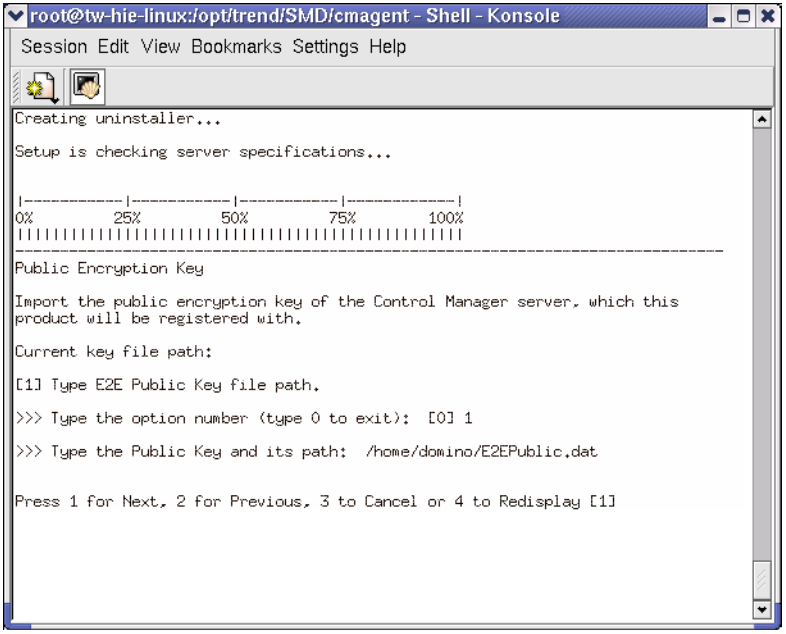


FIGURE 3-10. Public Encryption Key

Note: If a Communicator is already installed on your server, the agent will use the existing Communicator, and step 5 will be skipped.

6. If you are installing the Control Manager agent on i5/OS or OS/400, type the IP address of the control manager server when prompted. If the Control Manager server uses an HTTP port other than the default (80), then include the port

number as part of the IP address. Use the format <CM server IP address>:<port number>.

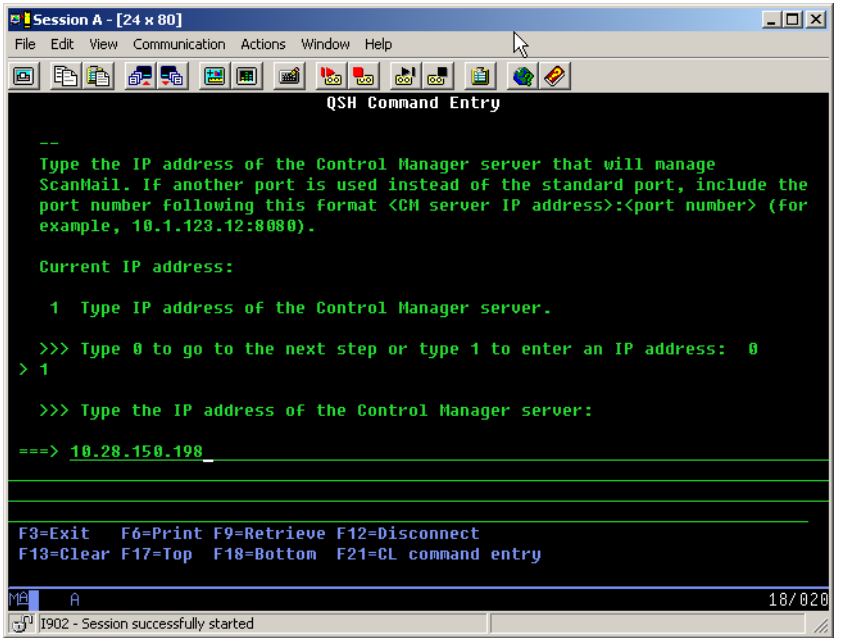


FIGURE 3-11. IP address screen

After you type the IP address, enter "0" to accept the setting. If you want to change the IP address, type "1".

7. On the Domino Server Analysis prompt, type the **index number** of the target server where the Control Manager agent will be installed. For example, type `1` to set server 1.

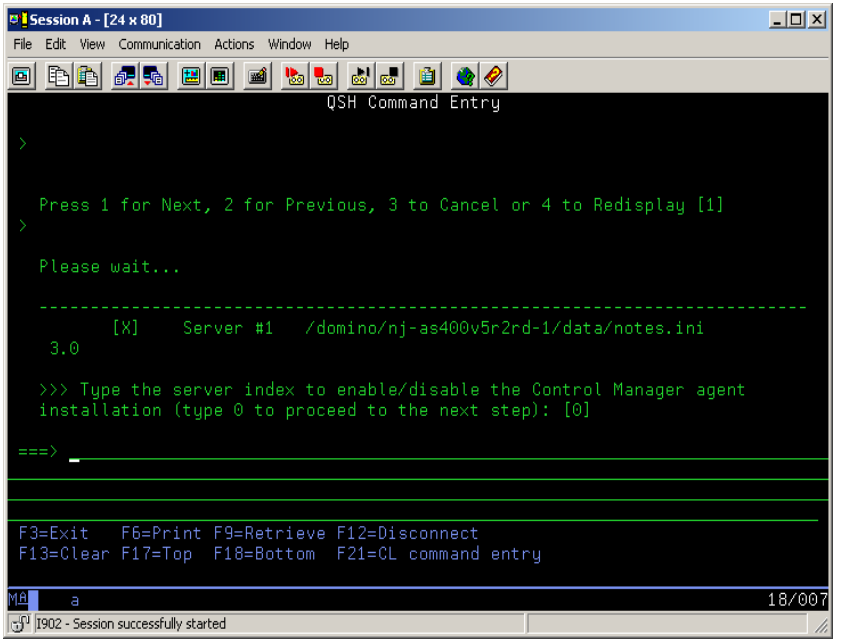


FIGURE 3-12. Domino Server Analysis

8. On the Registration Information prompt, type a **root**-level Control Manager account that will be used to register the ScanMail managed product to the Control Manager server.

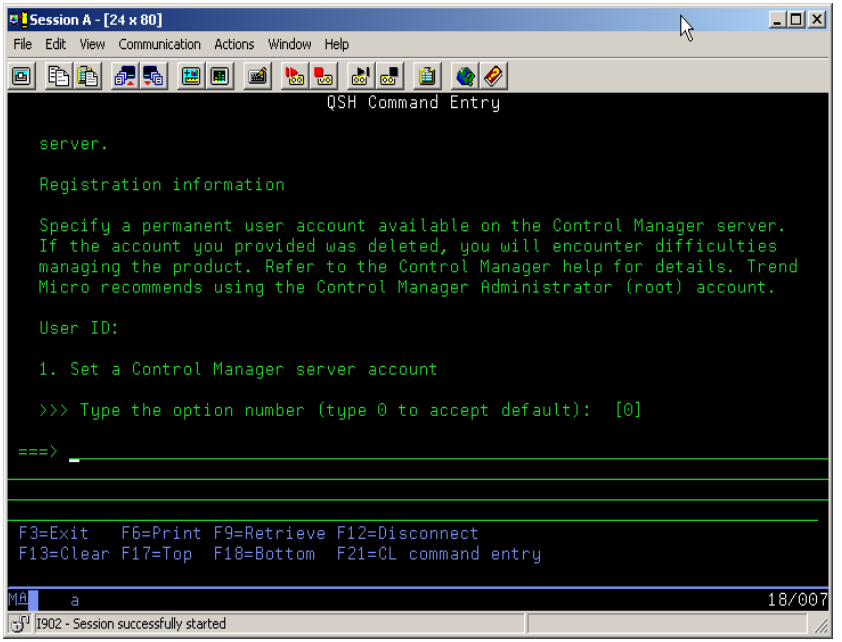


FIGURE 3-13. Control Manager Server Registration information

Note: If you delete the Control Manager User ID that you specify above from the Control Manager server, you will have difficulty managing the product in Control Manager.

9. On the Managed Product Naming prompt, type the **ScanMail managed product name** that will appear in the Control Manager Product Directory.

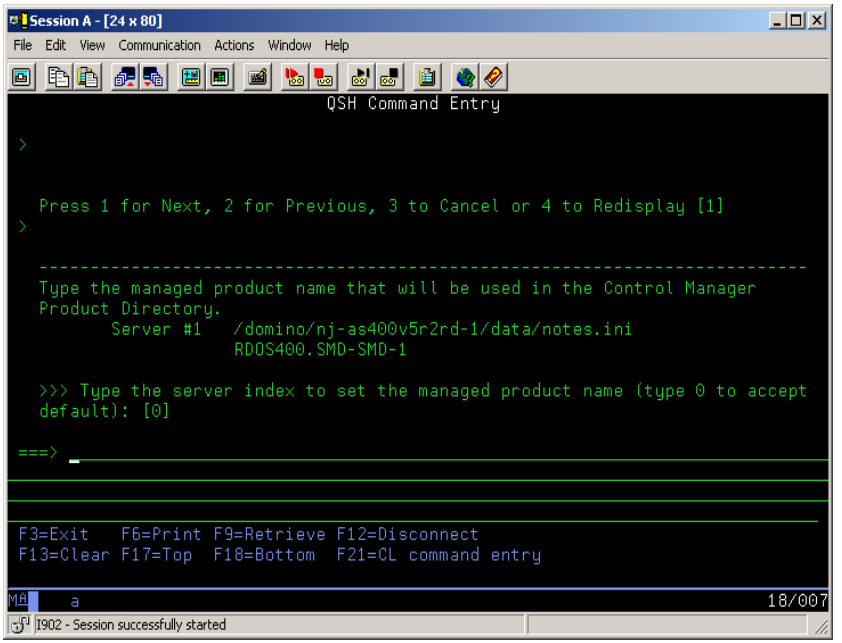


FIGURE 3-14. Managed product name

Tip: Trend Micro recommends assigning a managed product name that appropriately describes the ScanMail server; for example, `SMD_NYmail1`. Check the generated name(s) by installation program (the name follows notes.ini). If the system environment set hostname is null, type a meaningful entity name. The name cannot contain a space.

10. Type **1** to begin the Control Manager agent setup.

11. Press **ENTER** to finish Setup.

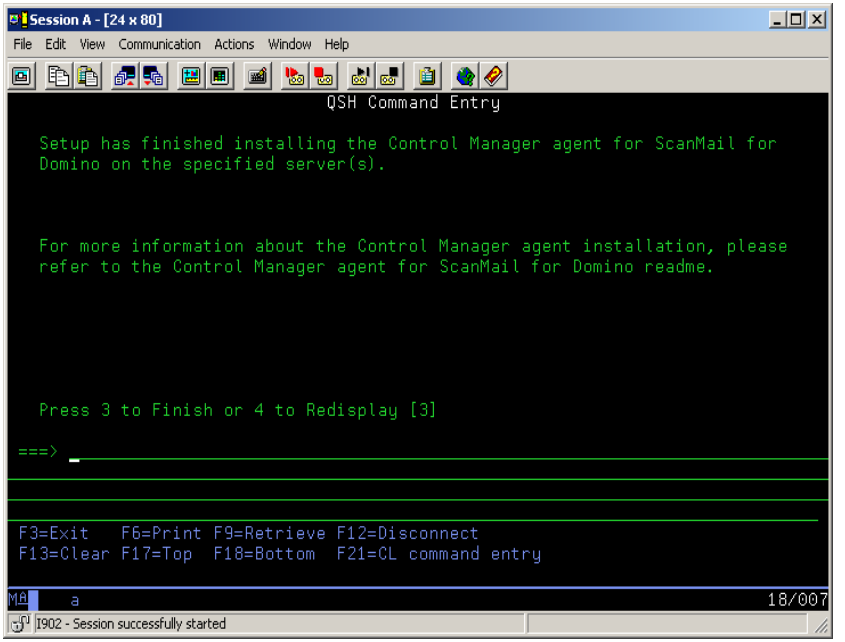


FIGURE 3-15. Installation Complete

See *page 3-23* to verify a successful Control Manager agent installation.

Verifying a Successful Control Manager Agent Installation

To verify a successful agent installation, access the Control Manager management console to see that the product has successfully registered with Control Manager and the Product Directory lists it as a managed product.

To verify a successful Control Manager agent installation:

1. Access the Control Manager management console (see *page 10-5*).
2. Click **Products** on the main menu.
3. On the left-hand menu select **Managed Products** from the list, and then click **Go**.

Under the **New entity** folder in the Product Directory, the ScanMail managed product icon appears.

If you do not see the ScanMail managed product, try the following:

1. Refresh the Product Directory. Click the **Refresh** icon on the upper right corner of the left-hand menu.
2. From the ScanMail server, ping the Control Manager server to confirm that connection is functioning correctly.
3. Restart the Trend Micro Management Infrastructure service on the ScanMail server.
4. Reinstall the Control Manager agent for ScanMail (*Installing the Control Manager Agent for ScanMail* on page 3-2).

Note: If your Domino server ID file is protected by a password, Control Manager agent will not run after it has been installed. Please contact the Trend Micro support team for help in resolving this issue.

Checking the Control Manager Agent for ScanMail Files and Folders

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

- *ScanMail and Control Manager Agent (Windows)* on page D-2
- *ScanMail and Control Manager Agent (Linux/Solaris/AIX)* on page D-4
- *ScanMail and Control Manager Agent (i5/OS and OS/400)* on page D-6

Chapter 4

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

The ScanMail interface layout is as follows:

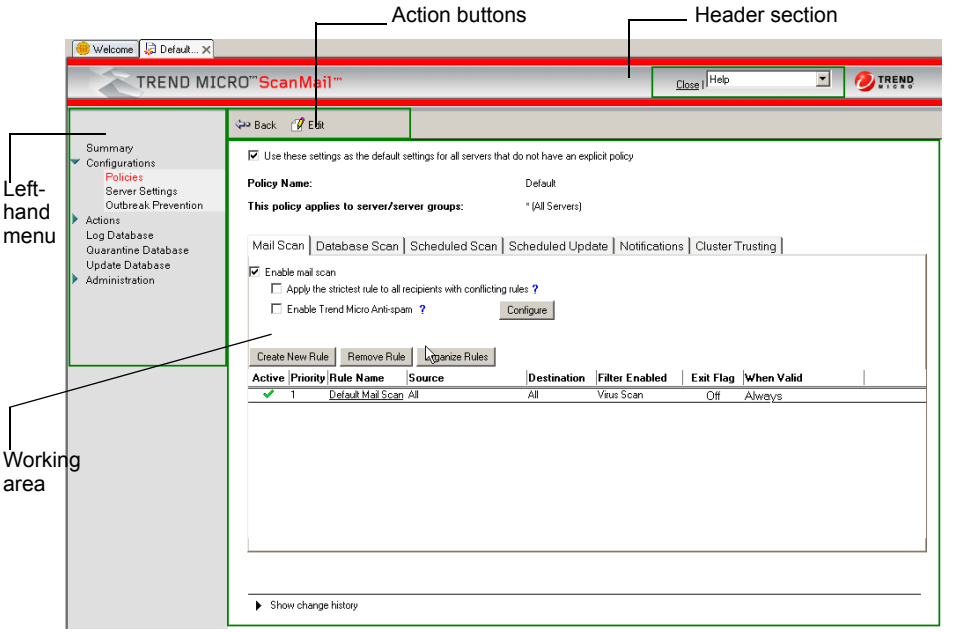


FIGURE 4-1. ScanMail interface

The interface has the following areas:

AREA	PURPOSE
Action buttons	allows you to perform specific actions, such as **Edit** the settings or Go **Back** to the previous displayed document
Header section	includes links to the ScanMail Help Database, Trend Micro Web site, and other support tools
Left-hand 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. In addition, 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 for Domino, 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 tooltip description of the options

Note: Tooltips 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 5-43) 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 5-16) to periodically scan the Notes databases on the local or remote hard drive.

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** > **Database** > **Open**.
2. Enter the **path** and **file name** in the **Filename** field.
3. Click **Open**.

Note: If you are using Domino R5, add the ScanMail Administrator database to the `smadmR5.nsf` workspace.

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, and 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 **Sign every design note** or **All design documents** (Domino R7 and R6.x).
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** > **Database** > **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 below.

PERSON, SERVER, OR GROUP	RECOMMENDED ACCESS LEVEL	DELETE DOCUMENTS OPTION
-Default-	No Access	Not selected
Anonymous	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

TABLE 4-1. Access Control List for ScanMail Databases

   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 9-4*). No check boxes should be selected 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. From the **File** menu, select **Database** and then click **Open**.
3. In the **Server** text box, specify the Domino server where you installed ScanMail for Domino.
4. In the **Database** list, locate the **ScanMail Configuration Database** (`smconf.nsf`).

5. Click **Open**.

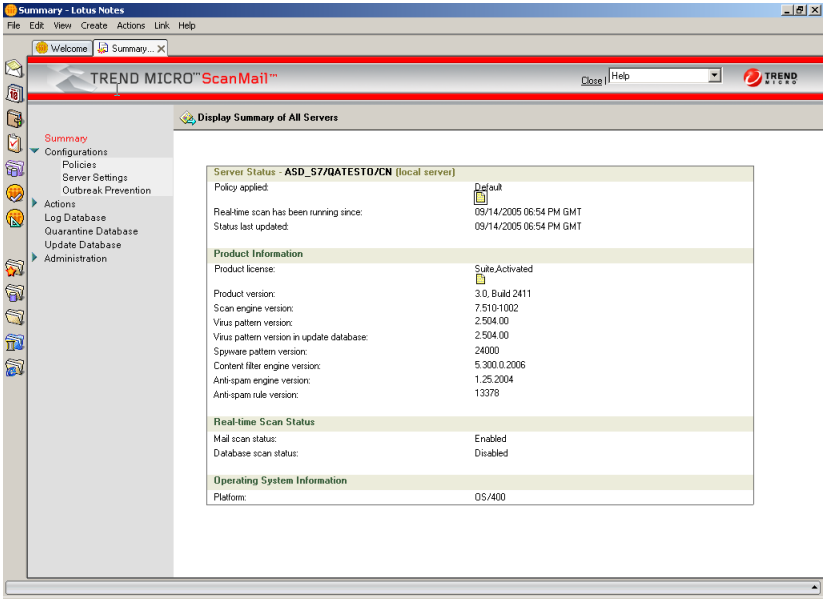


FIGURE 4-2. The Configuration Database displays *Server Summary* as the default first page.

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 R6 or later 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 4-10) for each person under the HTTP password in the Address Book. The Access Control List, as set from the Notes Workspace, can further control access.

To access a ScanMail database using a Web browser:

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

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

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

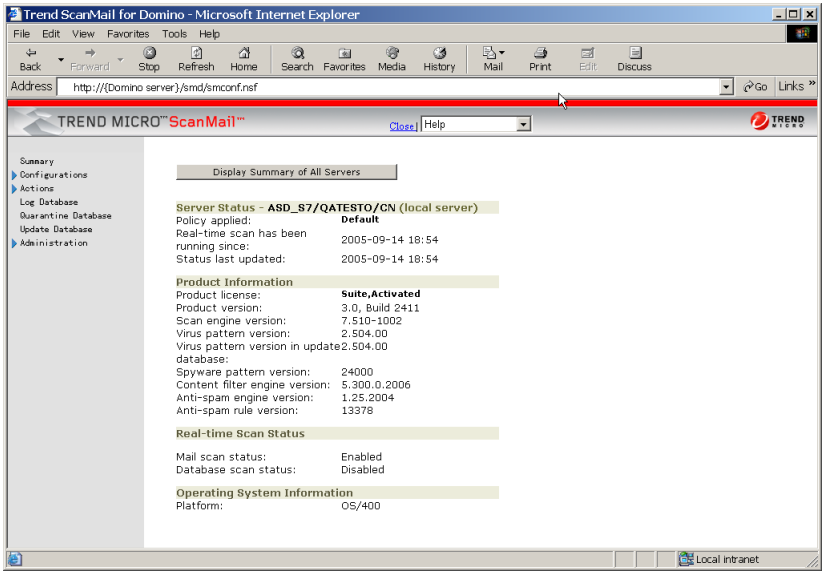


FIGURE 4-3. Access ScanMail databases using a Web browser

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:
  - Log Statistics
  - Database scan history
  - 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 scheme 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 5

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 3 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 1-10). You can easily and quickly create a common set of mail and database 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 1-10.
2. Create server settings for each server in your environment. See *Configuring the Server Settings Menu Options* on page 6-3.
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 6-11.

Managing Policies

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 *page 4-7*).
2. On the left-hand menu, click **Configurations** > **Policies**.

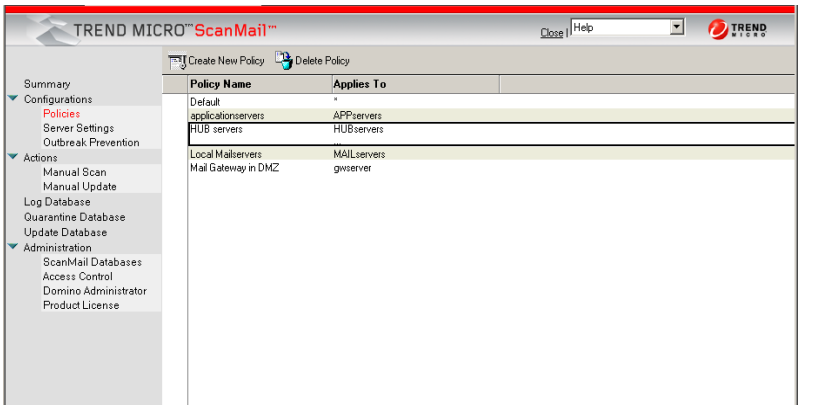


FIGURE 5-1. Policy list

3. On the working area, click **Create New Policy**.

4. Type the **policy name**.

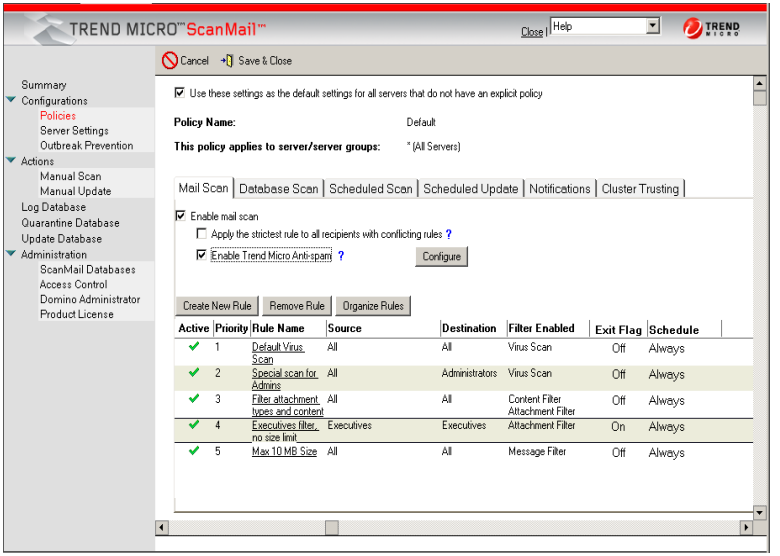


FIGURE 5-2. Creating a policy

5. Select from the list or type 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 R5.

---

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 *page 5-9*).
8. Create a real-time database scan rule (see *page 5-14*).

9. Create a scheduled database scan rule (see *page 5-16*).
10. Define how ScanMail delivers notifications (see *page 8-6*).
11. Define cluster trusting (see *page 5-7*).
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 4-7*).
2. On the left-hand menu, click **Configurations** > **Policies**.
3. On the working area, double-click a **policy**.
4. Modify the **Mail Scan** (*page 5-9*), **Database Scan** (*page 5-14*), **Scheduled Scan** (*page 5-16*), **Scheduled Update** (*page 7-4*), **Notifications** (*page 8-6*), or **Cluster Trusting** (*page 5-7*) 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 *page 4-7*).
2. On the left-hand 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.

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 certain cluster group. Therefore, it cannot be used in the **Cluster Trusting** tab.

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

1. Create (*page 5-9*) or modify (*page 5-6*) a policy.
2. Click the **Cluster Trusting** tab.

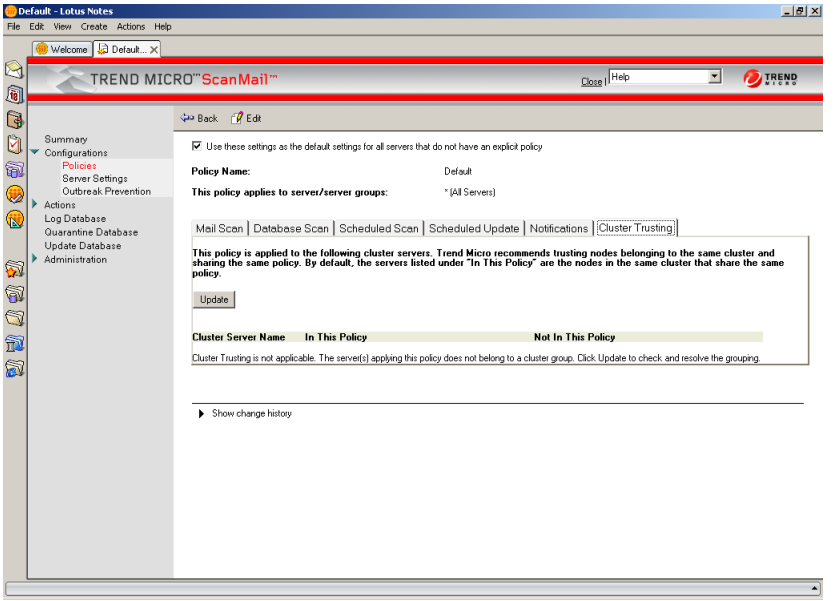


FIGURE 5-3. The Cluster Trusting table lists the servers available in a cluster group.

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 5-4.*.

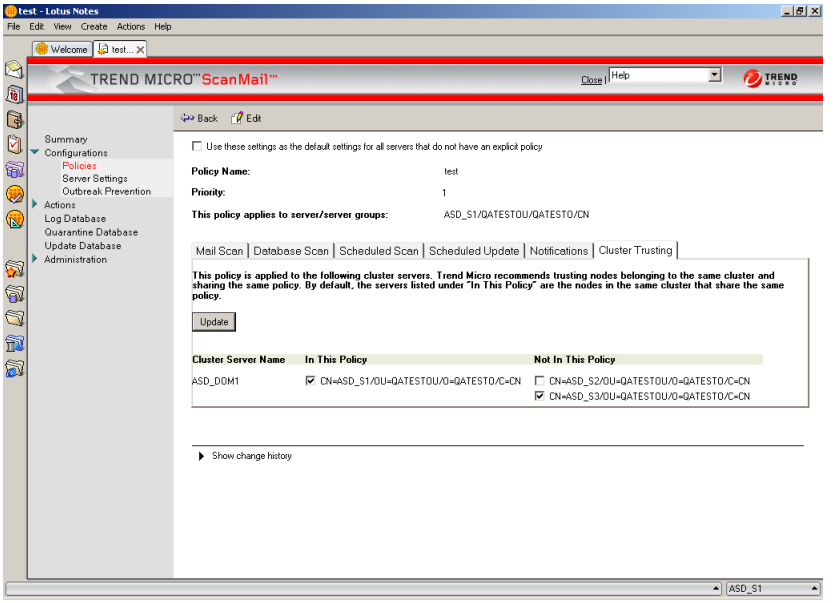


FIGURE 5-4. The cluster named *ASD_DOM1* has three servers: *CN=ASD_S1*, *CN=ASD_S2*, and *CN=ASD_S3*. The policy named *test* is applied only to *CN=ASD_S1*. In the Cluster Trusting table, the servers *CN=ASD_S1* and *CN=ASD_S3* are selected. Therefore, *CN=ASD_S1* will trust *CN=ASD_S3* and *CN=ASD_S2* 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 (see *page 5-9*) or modify (see *page 5-6*) a policy.

2. On the working area, click the **Mail Scan** tab.

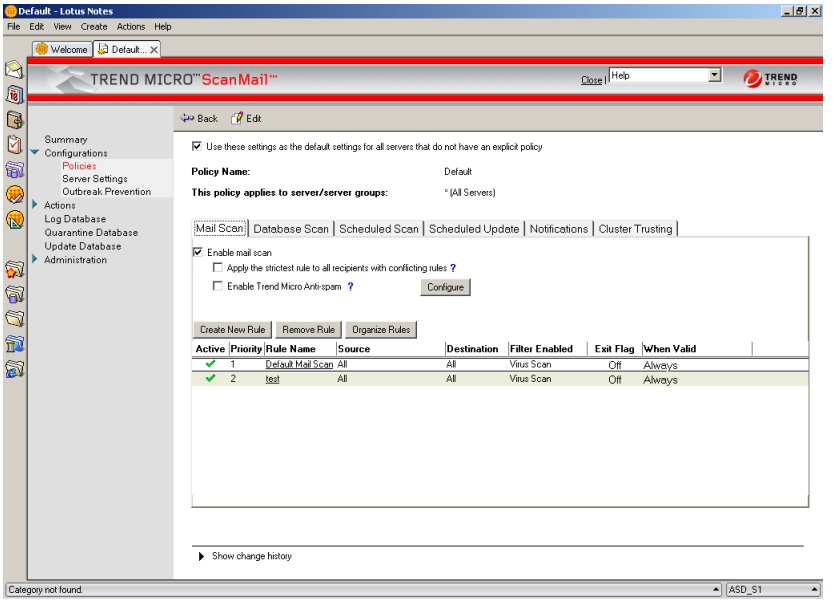


FIGURE 5-5. The *Mail Scan* tab defines ScanMail real-time message scanning.

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 *page 5-11* for details.
4. If you have the Suite edition, select **Enable Trend Micro Anti-spam** and click **Configure** to specify anti-spam settings (see *page 5-25*).
5. Click **Create New Rule**.
6. On the New Mail Rule document, 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**.

---

7. On the **General** tab, specify the **rule name**.

8. Set **general settings** (see *page 5-12*).
9. Click the **Scan Options** tab to set how ScanMail scans and filters messages:
   - **Virus Scan** (see *page 5-28*)
   - **Scan Restrictions** (see *page 5-30*)
   - **Message Filter** (see *page 5-31*)
   - **Attachment Filter** (see *page 5-37*)
   - **Content Filter** (see *page 5-32*)
   - **Script Filter** (see *page 5-40*)

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.

---

10. Set the scan notification (see *page 8-7*).
11. Configure **Redirect Options** (see *page 5-41*).
12. Insert disclaimers (see *page 5-42*).
13. Set the rule schedule (see *page 5-42*).
14. 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 7MB 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. On the mail scan document, 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:
     a. 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`).

     b. Specify the senders to **exclude**.
   - Under the **Recipients** group, choose the target recipients:
     a. 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)

     b. Specify the recipients to **exclude**.

Note: If you specified both sender(s) and recipient(s), select the operator (see *page 5-20*) that ScanMail will use when processing this rule.

---

4. Set the action when the sender and/or recipient match: **Block** or **Deliver**.

   If you select **Deliver**, decide if you want to deliver the message as a **low priority** or deliver it at a **specific time**.

Note: By default, Domino R5 servers route low priority messages between 12 AM and 6 AM.

---

5. Select **Notify sender** to send notification to the message sender.
   a. Type the **subject**.
   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 (see *page 5-9*) or modify (see *page 5-6*) a policy.
2. On the working area, click the **Database Scan** tab.

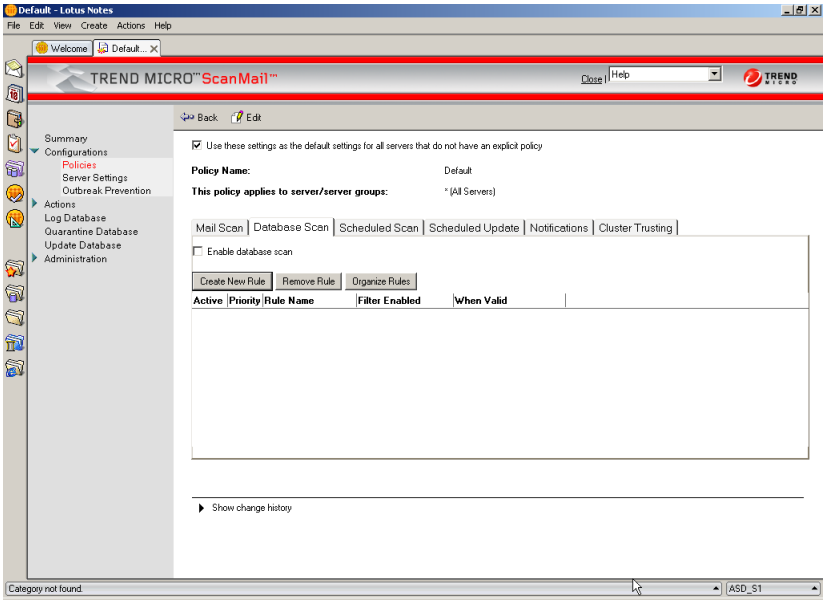


FIGURE 5-6. Use the Database Scan tab to create database scan rules that define how ScanMail filters databases in real-time.

3. Click **Create New Rule**.
4. On the New Database Scan Rule document, specify the **rule name**.
5. 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.

Note: For ScanMail running on Linux, Solaris, AIX, or i5/OS and OS/400, ensure the path name and database name is correct and follows the platform's case-sensitive naming. Otherwise, ScanMail will skip scanning directories or databases with wrong spelling.

---

6. Click the **Scan Options** tab to set how ScanMail scans databases:
   - **Virus Scan** (see *page 5-28*)
   - **Scan Restrictions** (see *page 5-30*)
   - **Script Filter** (see *page 5-40*)
7. Set the scan notification (see *page 8-7*).
8. Set the rule schedule (see *page 5-42*).
9. 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 (see *page 5-9*) or modify (see *page 5-6*) a policy.
2. On the working area, click the **Scheduled Scan** tab.

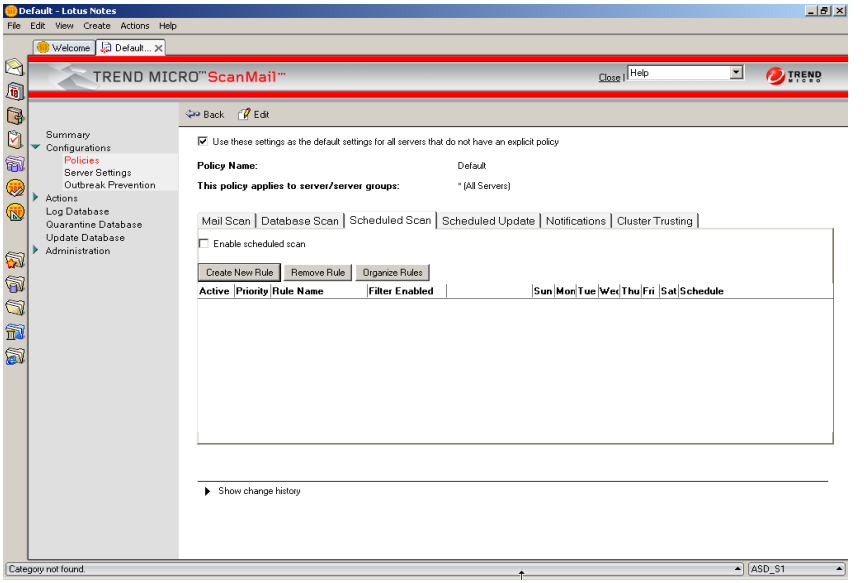


FIGURE 5-7. Scheduled Scan tab

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. Set the **number of times per day**, **duration**, and **days of the week** when the scan should occur.
   c. 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.

---

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.

Note: For ScanMail running on Linux, Solaris, AIX, or i5/OS and OS/400, ensure the path name and database name is correct and follows the platform's case-sensitive naming. Otherwise, ScanMail will skip scanning directories or databases with wrong spelling.

---

6. Click the **Scan Options** tab to set the following scan options:
   - **Virus Scan** (see *page 5-28*)

- **Scan Restrictions** (see *page 5-30*)
- **Script Filter** (see *page 5-40*)

7. Set the scan notification (see *page 8-7*).
8. Set the schedule.
   a. Type the time in the **Run at time** field that corresponds to the time (in 12-hour format) when the schedule scan rule will be run. For example, `06:00 AM, 04:00 AM - 05:00 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.

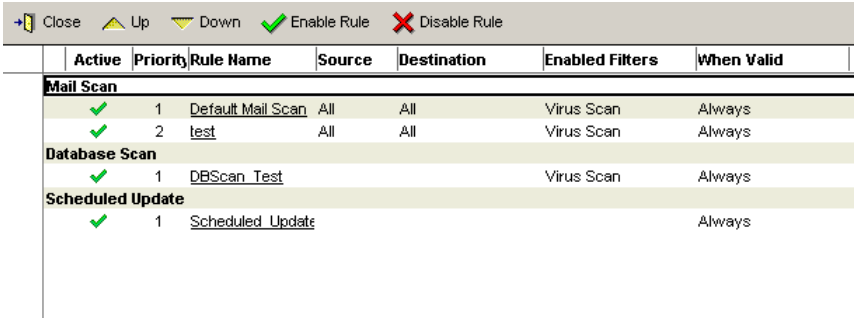


FIGURE 5-8. Click Up or Down to modify a rule's priority. Use the Activate Rule or Deactivate Rule button to enable or disable a rule.

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 5-9. 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 (*page 5-25*) of incoming messages based on Approved Senders and Blocked Senders (when enabled) or the Trend Micro Anti-Spam engine
2. General settings (*page 5-12*)
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 users that do not

belong to the **LocalDomainServers** of the Notes Address Book. 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 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 5-20*).

For example:

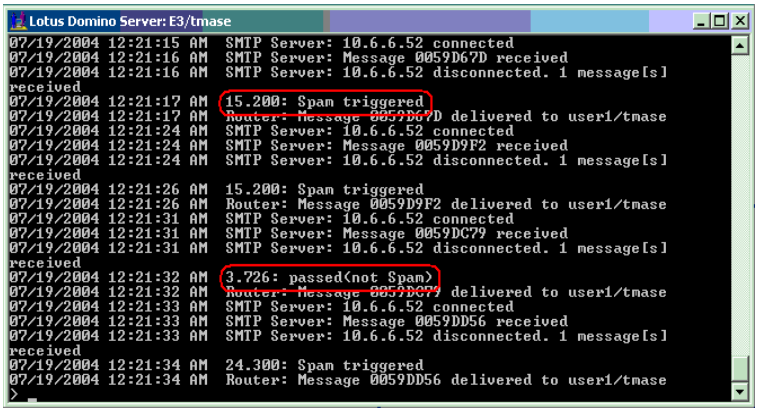


FIGURE 5-10. Sample spam scores

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 5-25*.

Content filtering

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 5-35*.

Note: The .WILD. operator is not valid under Windows, AIX, or i5/OS and OS/400 when using double-byte character sets.

Configure spam filtering

Use the **Anti-spam Configuration** screen to configure how the Trend Micro Anti-Spam engine filters unsolicited or unwanted messages (see *page 5-21*). 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** 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.

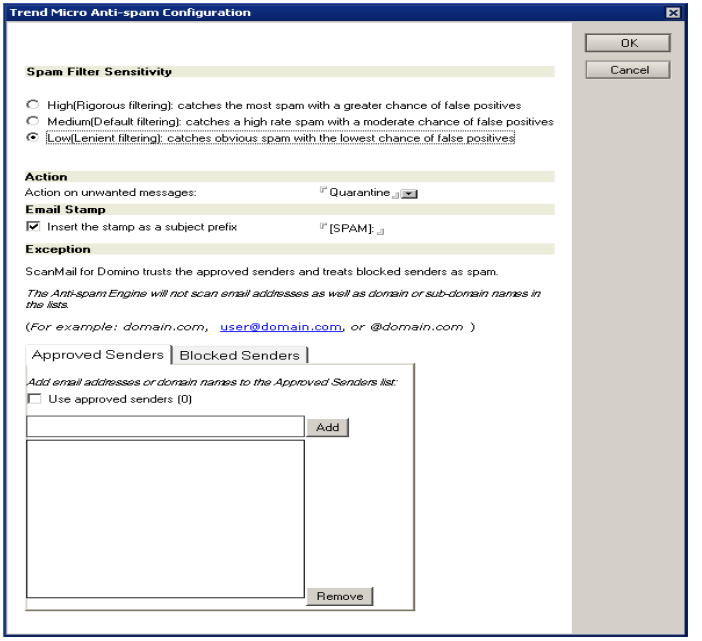


FIGURE 5-11. Trend Micro Anti-spam Configuration screen

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

     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**.
   - Select the **Blocked Senders** check box

     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**.

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 5-21 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)

Configuring the Scan and Filter Settings

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

Configuring virus scan

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

To configure virus scan options:

1. Under **Scan Options**, click the **Virus Scan** tab.
2. Under the **Actions** group of the **Virus Scan** tab, configure the virus scan options.
   a. Specify which **file type** to scan. Select from the following options:
      - **All files** 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.

   b. Select from the available advanced options:
      - **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 binary attachments encoded using MIME, UUencode, or BINHEX formats.

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

  Select the scan action for macros.

c. Set the **scan action** on infected files.

- **Use ActiveAction** 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.

---

d. Set the **notification** when malware was detected, uncleanable, or a scan action was applied on infected file(s).

e. Define the **safe stamp**.

3. 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).

     Note: The default value is 20,000KB (20MB).

   - **Exceed maximum compression level**– restricts ScanMail to scan compressed files that matches 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: By default, 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. Set the **notification** when a file matches the scan restrictions settings.
4. Define the **safe stamp**.
5. Click **Save & Close**.

Configuring 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 mail scan rule** check box.
3. Under the **Actions** 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. Set the **notification** when a file matches the message filters.
5. Define the **email stamp**, which is valid only for encrypted messages.
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 (PDF) files is not available on AIX, i5/OS, and OS/400 platforms.

The **Content Filter** tab allows you to define general and advanced rules (see *page 5-23* for details).

To configure content filter options:

1. Under **Scan Options**, click the **Content Filter** tab.
2. Select the **Enable content filter** check box.
3. Create a **new content filter** (*page 5-32*) or **add an existing one** (*page 5-34*) in the content filter table.
4. Click  to specify the **scan action** on messages with unwanted content.
5. Set the **notification** when a message matches the content filtering settings.

   Insert a filter description in the notification to include additional instructions or descriptions.

   For example: *Contact the Domino Administrator for more details.*
6. 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. Under the **Content Filter** tab, click the **Create New Content Filter** button.
2. On the New Content Filter workspace, type a **name** for the content filter.

3. Under **Select the message part(s) that will be compared against the available expressions**, select the message part (for example, **Subject**, **From**, **To**, **Body**) that ScanMail will filter and compare against the expressions (see *Expressions* starting on page 5-24 for details) specified.

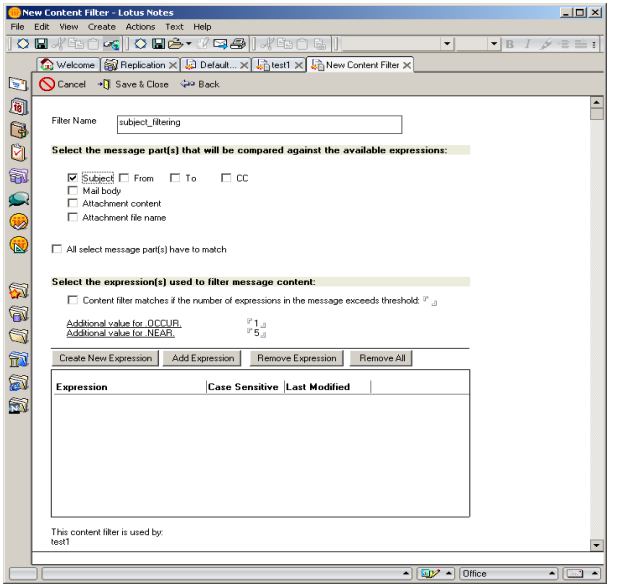


FIGURE 5-12. Creating a new content filter

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

4. Under **Select the expression(s) used to filter message content**, create (see *page 5-35*) or add **expressions** (see *page 5-36*) that ScanMail will use for content filtering.
   - 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.

5. Click **Save & Close**.

Remove content filter

Use the **Content Filter** tab to remove all or a specific content filter.

To remove a content filter:

1. Click the filter to be removed.
2. Click **Remove Content Filter**.

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 a series of base content filters that define what portions of the message to scan, and use these repeatedly as elements of your content filters. For example, create one content filter for scanning the Subject header, another for Attachments, and another to include all parts of the mail and then use these as building blocks for your content filter.

To add a new content filter:

1. From the content filter workspace, click the **Add Expression** button.
2. In the Add Expressions window, click the **expressions** you want to use. 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 the **Create New Expression** button.
2. In the New Expression worksheet, type the **expression** (that is, word or phrase) you want to filter, connected by logical operators. Refer to the help section at the bottom of the New Expression workspace for details on how to use logical operators.
3. **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. Under the **Content Filter** tab, click the **Add Existing Content Filter** button.
2. In the Add Content Filter window, click 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 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:

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

TABLE 5-1. Recommended file extensions to block

EXTENSION	DESCRIPTION
.INF	Information or Setup File
.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

TABLE 5-1. Recommended file extensions to block

To configure attachment filter options:

1. Under **Scan Options**, click the **Attachment Filter** tab.
2. Select the **Enable attachment filter** check box.
3. Set the attachment filtering criteria:
   - To filter attachments according to **file size**, select **Enable attachment filtering by size**.

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).

- To filter attachments according to **file type**, select **Enable attachment filtering by file type**.

  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 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.

4. Specify the **attachment file name** that will be exempted from filtering in the **Allowed attachments** field. Use the wildcard character * 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 overwrite the attachment filtering criteria.

5. Set the **notification** when a file matches the attachment filters.
6. Define the **email stamp**.
7. 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. Under **Scan Options**, click the **Script Filter** tab.
2. Select the **Enable script filter** check box.
3. Type the **stored form** and **rich text hotspot scripts** to filter:
   - **@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`
   - **URLs called by URLOPEN** can open any valid URLOPEN command in Lotus Formula language. For example: `offensivesite.com` or `www.offensivesite.com`
4. Click  to set the **filter action** on **Stored form hotspots and events** and the action on **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.

The **Auto-clean** action for stored form is not operational at this time. Trend Micro recommends using the **Delete: Delete the stored form** action for stored form hotspots and events.

---

5. Set the **notification** when a file matches the scan restrictions settings.
6. Define the **email stamp**.
7. 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. 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 *page 4-5* to know 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. 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** to enable a 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 the **disclaimer name**.

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

5. Type the **subject** and **message body** disclaimer **content**.
6. Click **Save & Close**.

Setting the rule schedule

Use the **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 next sections for details on how to invoke 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 relative 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/databas
e4.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. On the left-hand menu, click **Actions** > **Manual Scan**.
3. On the working area, click **Edit**.
4. Click the **General** tab to **enable incremental scanning** and specify the **number of minutes** that corresponds to the duration of the scan.

Note: If the scan duration is set to 0, the manual scan task will stop once it has finished scanning all databases.

---

5. Click the **Databases to scan** tab to set which database(s) to scan:
   - **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.

Note: For ScanMail running on Linux, Solaris, AIX, or i5/OS and OS/400, ensure the path name and database name is correct and follows the platform's case-sensitive naming. Otherwise, ScanMail will skip scanning directories or databases with wrong spelling.

---

6. Click the **Scan Options** tab to set the following scan options:
   - **Virus Scan** (see *page 5-28*)
   - **Scan Restrictions** (see *page 5-30*)
   - **Script Filter** (see *page 5-40*)

7. Define the **notification template**.
8. Click **Scan Now**.

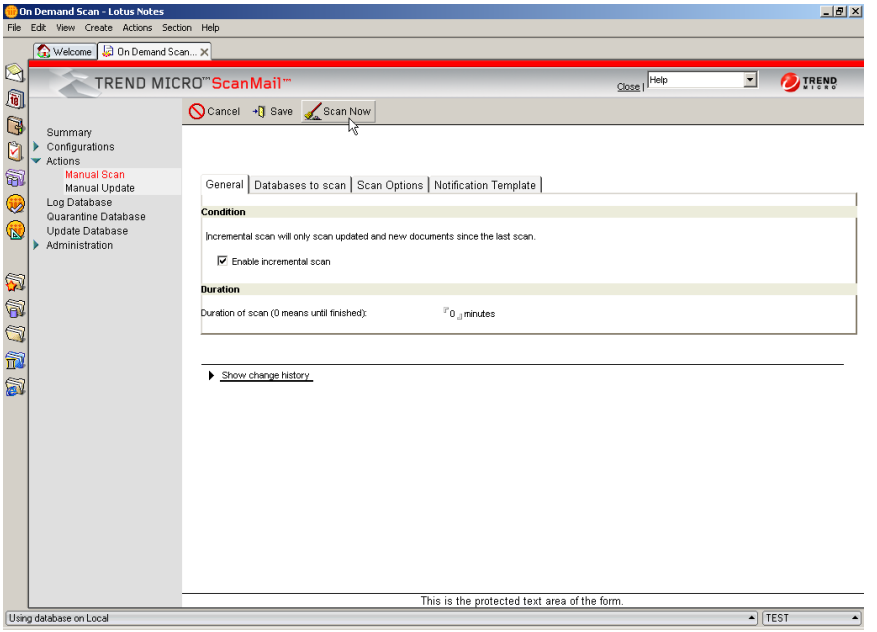


FIGURE 5-13. The ID used to run *Scan Now* must have the appropriate access right to submit server console command.

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

Ending 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 6

Performing Administrative Tasks

The **Summary**, **Server Settings**, and **Administration** options are some of the new menu options 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

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 *page 4-7*).
2. On the left-hand menu, click **Summary**.

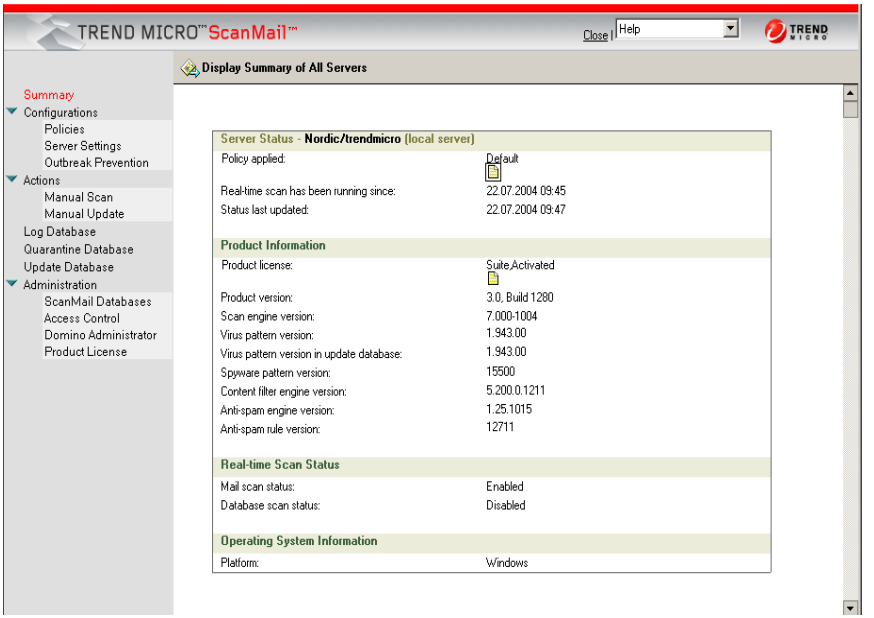


FIGURE 6-1. The Status view displays the status of the current server

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 *page 4-7*).
2. On the left-hand menu, click **Configurations** > **Server Settings**.
3. On 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 *page 6-4*).
6. Set the memory size used for scanning (see *page 6-5*).
7. Configure the proxy server settings that ScanMail will use for component download and product activation (see *page 6-6*).
8. Select the event that will trigger ScanMail to display notification via the Domino server console (see *page 6-7*).

9. Enable server task monitoring (see *page 6-6*).
10. Specify the default character set that ScanMail should use when it cannot detect the character set of a message (see *page 6-7*).
11. Configure miscellaneous settings (see *page 6-8*).
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 *page 4-7*).
2. On the left-hand menu, click **Configurations** > **Server Settings**.
3. On the working area, double-click a server settings rule document or click the **Edit** button.
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 (see *page 6-3*) or modify (see *page 6-4*) a server settings rule.
2. On the working area, click the **Temporary Directory** tab.
3. For each scan type, type the directories relative 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 2MB, you can allocate only 2MB 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 5MB 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 5MB for each ScanMail task is suitable.

To set scan memory size:

1. Create (see *page 6-3*) or modify (see *page 6-4*) a server settings rule.
2. On 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 component download and product activation.

Note: You can specify another proxy server for component download in the scheduled update or manual update document. See *Defining the proxy server settings for component download* on page 7-9.

To configure the proxy server settings:

1. Create (see *page 6-3*) or modify (see *page 6-4*) a server settings rule.
2. On the working area, click the **Proxy Settings** tab.
3. Select **Use a proxy server**.
4. Select the proxy server **protocol**.
5. Specify the proxy server **address** or **host name**, and the **port number**.
6. Type the **user name** and **password** used for proxy authentication.
7. 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 (see *page 6-3*) or modify (see *page 6-4*) a server settings rule.
2. On the working area, click the **Task Monitoring** tab.
3. Select **Send a notification message to the administrator if a task ended abnormally.**

4. Type or click  to set which **administrator(s)** should receive the notification.
5. Type the **subject** and **message body** for the notification message.
6. Click **Save & Close**.

Monitor server events

Use the **Event Log** tab to monitor the following events and display or write them to the Domino server console:

- **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 (see *page 6-3*) or modify (see *page 6-4*) a server settings rule.
2. On 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**.

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 *page 5-42*.

To specify the default character set:

1. Create (see *page 6-3*) or modify (see *page 6-4*) a server settings rule.
2. On the working area, click the **Regional Option** tab.
3. Select which **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 (see *page 6-3*) or modify (see *page 6-4*) a server settings rule.
2. On the working area, click the **Misc** tab.
3. Type the integer that corresponds to the **number of threads** used for mail and 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 5 threads per scanner.

4. Type or click  to select the **trusted SMTP** and **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.

5. Attach the warning image (for example, `*.gif`, `*.jpg`, or `*.bmp`) that ScanMail should insert in its notification when a virus or other malware type is detected or an attachment is blocked because of other reasons not covered in the **Attachment Filter** tab (see *page 5-37*).

   Specify images saved in the `smd` folder belonging to the `Domino Data` directory.

6. Under Warning Bitmap, select whether to **Insert the warning bitmap behind the existing icon** or **Remove/hide icon when attachment is removed**.

   Note: ScanMail is unable to delete the icon from Notes messages. If **Remove/hide icon when attachment is removed** is selected, ScanMail replaces the attachment with a 2-byte file.

7. 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 Warning and Note information below.

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: Depending on the server's hardware specification, the SMDreal task for ScanMail for Domino Suite may take time to load when installed on a Linux, Solaris, AIX, i5/OS, or OS/400 server. ScanMail initially loads the Trend Micro Anti-Spam engine, followed by the rest of the ScanMail tasks. 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.

8. Under **Exclude tasks**, 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.

This feature is available on all platforms except Windows.

9. Click **Save & Close**.

Configuring the Administrator Menu Options

Use the Configuration Database **Administrator** 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 **Administrator** > **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 R5 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 *page 4-7*).
2. On the left-hand menu, click **Administration** > **ScanMail Databases**.
3. On the working area, type or click  to select **Domino server(s)**.
4. Select whether to **enable**, **disable**, or **retain (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.

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 *page 4-7*).
2. On the left-hand menu, click **Administration** > **Domino Administrator**.
3. On the working area, click **Copy to domadmin.nsf**.

Including ScanMail in the Domino R6 Web Administrator page

Use the Configuration database to include ScanMail in the Domino R6 Web Administrator page.

To include ScanMail in the Domino R6 Web Administrator page:

1. Open the ScanMail Configuration Database (see *page 4-7*).
2. On the left-hand menu, click **Administration** > **Domino Administrator**.
3. On the working area, click **Copy to webadmin.nsf**.

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 *page 4-7*).
2. On the left-hand menu, click **Administration** > **Access Control**.
3. On 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**.
9. Click **Apply Settings to ACL**.

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 *page 4-7*).
2. Click **Administration** > **Product License**.
3. On the working area, click **Create License Profile**.
4. Type or copy the **ScanMail Activation Code** 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 *page 2-47*.

To delete a license profile:

1. Open the ScanMail Configuration database (see *page 4-7*).
2. Click **Administration** > **Product License**.
3. On 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 7

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** 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.
- **Anti-spam rule** detects unwanted content based on an updatable file containing spam definitions.
- **Scan engine** detects all virus and malware known to be "in the wild", or actively circulating.

  The 32-bit, multi-threaded scan engine checks files in real-time using the process called pattern matching. VSAPI 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.

  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.
- **Anti-spam engine** detects unsolicited commercial or bulk email messages (UCEs, UBEs).
- **ScanMail for Domino 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* starting on page 2-45.

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 *page 4-7*).
2. On the left-hand menu, click **Actions** > **Manual Update**.
3. On the working area, click **Edit**.
4. Select which **component(s)** to update.
5. Set the **update source**.
6. Configure the **proxy server settings** for component download.
7. Define the **update notification**.
8. Click **Save** to save the manual update settings.

9. Click **Update Now**.

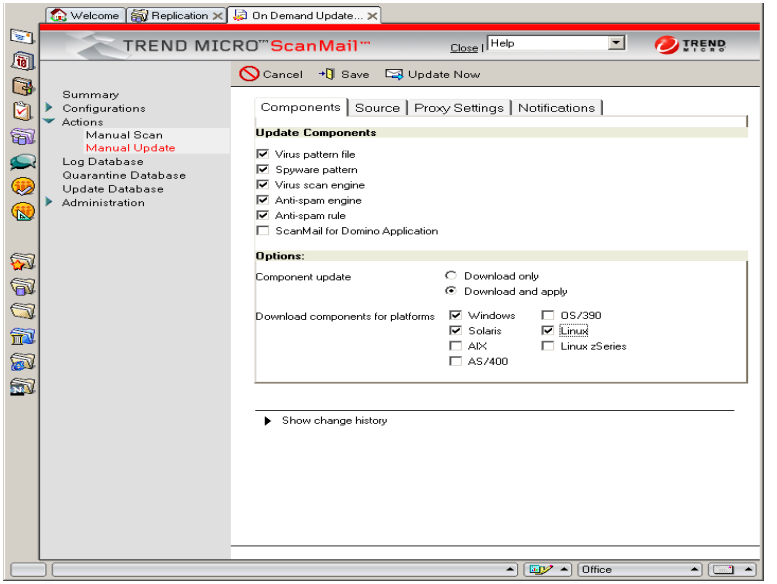


FIGURE 7-1. Click *Update Now* to download the latest antivirus and content security components.

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 (see *page 5-4*) or modify (see *page 5-6*) a policy.
2. On the working area, click the **Scheduled Update** tab.
3. Select **Enable scheduled update**.
4. Set which components to deploy automatically (see *page 7-6*).
5. Click **Create New Rule**.

6. On the New Scheduled Update Rule document, specify the **general settings** in the **General** tab:
   - Specify the scheduled update **rule name**.
   - Select **All server(s) of the parent policy** or **Specified server**, and then click to choose server(s) from the list.
7. Select which **components** to download.

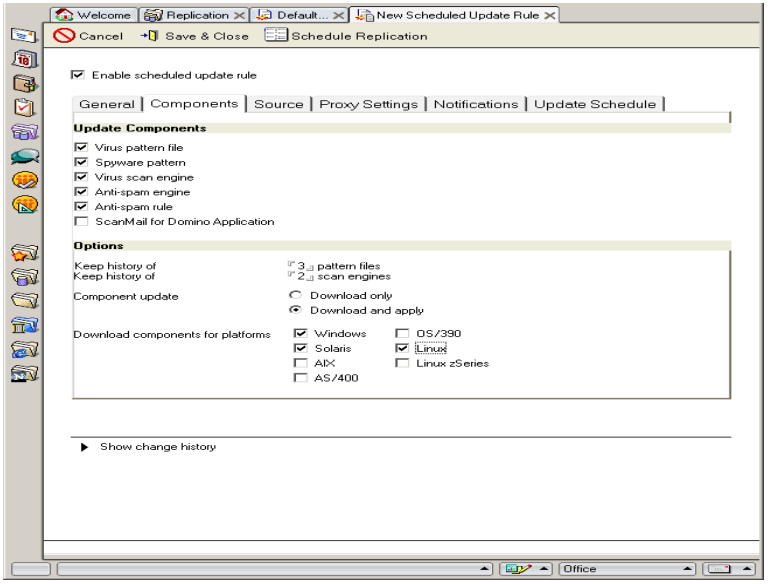


FIGURE 7-2. Creating a scheduled update rule > defining the components to update

8. Set the **update source** (see *page 7-8*).
9. Configure the **proxy server settings** for component download (see *page 7-9*).
10. Define the **update notification** (see *page 8-7*).

Note: ScanMail sends scheduled update rule notifications to the email address(es) set in the policy **Notifications** tab.

11. Click the **Update Schedule** tab to set the number of times per day, duration, and days of the week when the scheduled update should occur.
12. Click the **Schedule Replication** button to launch the Notes Address Book and configure the schedule replication (refer to the *Setting options on the Replicator* topic in the Notes Help).
13. 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 (see *page 5-4*) or modify (see *page 5-6*) a policy.
2. On the working area, click the **Scheduled Update** tab.
3. Select **Enable component deployment**, and then click **Configure**.
4. On the Component Deployment Configuration window, select which component(s) you want to deploy automatically.
5. Type the **number** of pattern file and scan engine versions that ScanMail will save in the **Keep history** field.

Note: Because virus pattern and scan engine files can take up disk space, Trend Micro recommends keeping 3 previous pattern file and 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 (see *page 7-3*) or manual update (see *page 7-3*) document, click the **Components** tab to set which components to download.
2. Under **Update Components**, select the components to download.
3. Set the **download options**:
   a. Type the **number of virus pattern** and **scan engine** that ScanMail will save in the **Keep history** field.

Note: Because pattern files and scan engine can take up disk space, Trend Micro recommends keeping 3 previous pattern file and 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.

---

   b. 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.

---

c. Select which **platforms** should apply the component(s) downloaded.

4. 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 (see *page 7-3*) or manual update (see *page 7-3*) document, click the **Source** tab to select one of the following **update sources**:

   - **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: 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://smln-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: Refer to *Update Issues* starting on page 12-4 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 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 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 (see *page 7-3*) or manual update (see *page 7-3*) document, click the **Proxy Settings** tab.
2. Select **Use Proxy** if connecting to the Internet requires a proxy server.
3. Select whether to use the proxy server found in **Server Settings** or **another proxy server**.
4. Select the proxy server **protocol**.
5. Specify the proxy server **address** or **host name** and **port** used.
6. Type the **user name** and **password** used for proxy authentication.
7. 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. Download the latest pattern file from `www.trendmicro.com`.
2. Delete old versions of the pattern files using from the pattern directory.
3. Open the ScanMail Update Database (see *page 4-7* or *page 4-10*).
4. On the left-hand menu, click **Virus Pattern File**.
5. On the working area, click **Edit**.
6. Modify the **Pattern version**.
7. Attach the latest version pattern file to the **Pattern file** field.
8. Click **Save & Close**.
9. Load `SMDupd` using the Domino server console:
10. load SMDupd

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. Download the spyware pattern from `www.trendmicro.com`.
2. Open the ScanMail Update Database (see *page 4-7* or *page 4-10*).
3. On the left-hand menu, click **Spyware Pattern**.
4. On the working area, click **Edit**.
5. Modify the **Spyware Pattern version**.
6. Attach the latest spyware pattern file to the **Spyware pattern** field.
7. Click **Save & Close**.
8. Load `SMDupd` at the Domino server console:

```
load SMDupd
```

To load the latest anti-spam rule:

1. Download the latest anti-spam component (spam.zip) by going to the ActiveUpdate Web site-`http://smln-t.activeupdate.trendmicro.com/activeupdate/pattern/spam.zip`.
2. Save and extract the content(s) of `spam.zip` to a temporary directory.
3. Open the ScanMail Update Database (see *page 4-7* or *page 4-10*).
4. On the left-hand menu, click **Anti-spam Rule**.
5. On the working area, click **Edit**.
6. Attach the latest version to the **Anti-spam rule** field.
7. Update the **Anti-spam rule version**.
8. Click **Save & Close**.
9. Load **`SMDupd`** at the Domino server console:

```
load SMDupd
```

Note: For i5/OS and OS/400 platforms, Trend Micro recommends that you define a separate anti-spam update rule that schedules the update during light system traffic hours (for example, midnight), when your Domino server(s) or i5/OS or OS/400 machine has relatively low mail throughputs.

To load the latest anti-spam engine:

1. Download the latest anti-spam component (spam.zip) by going to the ActiveUpdate Web site-`http://smln-t.activeupdate.trendmicro.com/activeupdate/pattern/spam.zip`.
2. Save and extract the content(s) of `spam.zip` to a temporary directory.
3. Open the ScanMail Update Database (see *page 4-7* or *page 4-10*).
4. On the left-hand menu, click **Anti-spam Engine**.
5. On the working area, double-click the corresponding platform for the anti-spam engine.
6. On the Spam Engine Database document, click **Edit**.
7. Attach the latest version to the **Anti-spam engine** field.
8. Update the **Anti-spam engine version**.
9. Click **Save & Close**.
10. Load **`SMDupd`** at the Domino server console:

```
load SMDupd
```

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 *page 4-7* or *page 4-10*).
5. On the left-hand 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
```

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 for some reason 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 8

Sending ScanMail 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
	%CAUSE%	Matching script filter option
	%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
%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 (see *page 8-6*) to deliver notification. 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 5-27*
- **Virus Scan** stamp, see *page 5-29*
- **Scan Restrictions** stamp, see *page 5-30*
- **Message Filter** stamp, see *page 5-31*
- **Attachment Filter** stamp, see *page 5-39*
- **Script Filter** stamp, see *page 5-40*

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 (see *page 5-4*) or modify a policy (see *page 5-6*).
2. On the working area, click the **Notifications** tab.
3. Double-click the document or click the **Edit** button to configure the following settings:
   a. Click  or type the address in the **Return address** field to assign a **From:** address to the notification.
   b. Type the **Sametime server DNS/IP address** and **password** to instruct ScanMail to send notification to a Lotus Instant Messaging and Web Conferencing account.
   c. 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).

   Note: The Instant Messaging notifications do not apply to ScanMail for Linux and Solaris releases.
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. On a mail, database, or scheduled scan rule, click the **Notification Template** tab.
2. Click the **Add >>** button 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 8-6).

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** does not use 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 (see *page 7-4*) or manual update (see *page 7-3*) document, click the Notification tab.
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 *page 7-2*)
- 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** of the update notification.
5. Click **Save & Close**.

Chapter 9

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 ScanMail logs according to the following priorities:

- Group by Action, Date, User, Detection Name (malware name), or Rule

  View records for any of the groups for a single day, week, month, or all dates.
- Grouped by service– mail scan or database scan

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.

To view ScanMail logs:

1. Do one of the following to open the Log Database:
   - Click the **Log Database** option from the Configuration Database left-hand menu.
   - Open `smvlog.nsf`.

2. Select and organize the logs you want to view according to the following criteria:
   - **Action** displays logs according to ScanMail actions.
   - **Date** displays logs according to dates when ScanMail detects a virus or other malware types.
   - **User** displays logs according to recipients of unsafe or unwanted messages.
   - **Detection Name** displays logs according to the name of the virus or other malware types detected.
   - **Rule** displays logs according to the name of the rule that detected the malware or other unwanted content.
   - **Database Scan** displays logs generated by the ScanMail database scan.
   - **Mail Scan** displays logs generated by the ScanMail mail scan.
3. Do one of the following:
   - Organize the search results by time period.

     View all dates, today's date, the past 7 days, and the past 30 days.
   - Click  to sort fields in ascending or descending order.

Enabling/disabling log deletion

Use the Log database to enable or disable log deletion. When a log is enabled for deletion, ScanMail can delete it automatically. You can manually delete a log anytime, even if it is not enabled for deletion.

Note: When you delete a quarantine log from the Quarantine database, ScanMail automatically deletes the same record from the Log database.

To delete quarantine logs automatically:

1. Do one of the following to open the Quarantine database:
   - Click the **Log Database** option from the Configuration database menu.
   - Open `smvlog.nsf`.
2. Select which **logs** you want to enable or disable for deletion.

3. Click **Enable Log Deletion** or **Disable Log Deletion**.

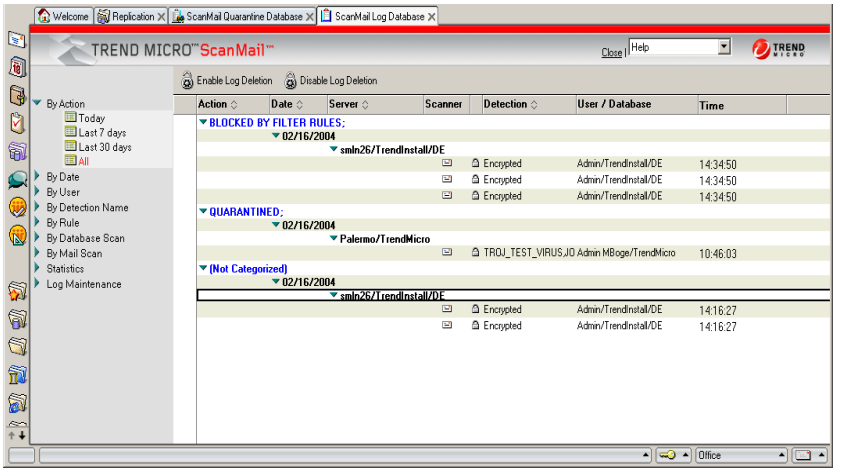


FIGURE 9-1. Enabling/disabling log deletion from the Log database

---

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:
   - Click the **Log Database** option from the Configuration Database left-hand menu
   - Open `smvlog.nsf`

2. On the left-hand menu of the Log database, click **Log Maintenance** > **Scheduled Deletion**. The Scheduled Deletion screen appears.

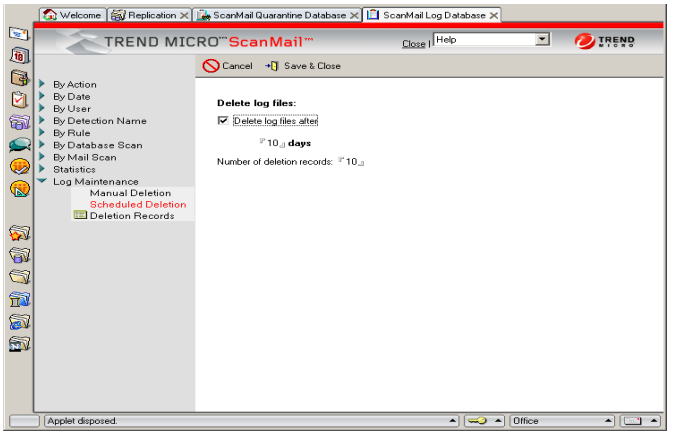


FIGURE 9-2. Deleting logs automatically

3. On the working area, 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**.

Note: For ScanMail running on SUSE LINUX Enterprise Server 8 with Service Pack 3 servers, virus logs may not be deleted automatically. The following error message displays on the Domino console:

AMgr: Agent 'Delete log files (Auto)' in 'smd/smvlog.nsf' does not have proper execution access, cannot be run

As a workaround, use Domino Administrator to manually sign the ScanMail Log database with server.id.

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:
   - Click the **Log Database** option from the Configuration database left-hand menu.
   - Open `smvlog.nsf`.
2. On the left-hand menu of the Log Database, click **Log Maintenance** > **Manual Deletion**. The Manual Deletion screen appears.

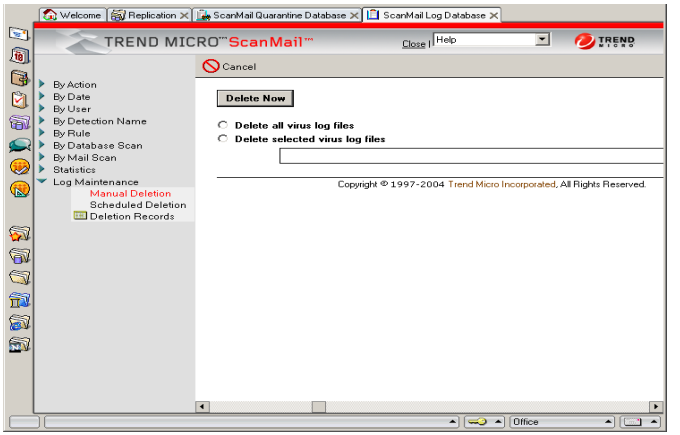


FIGURE 9-3. Deleting logs manually

3. On the working area, 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.
     a. Click **Browse** to launch the Log Files window.
     b. Select which **logs** to delete.
     c. Click **OK**.
4. Click **Delete Now**.

ScanMail will only delete the virus logs enabled for deletion.

Viewing Statistics and Charting

The **Statistics** option provides the ability 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, 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:
   - Click the **Log Database** option from the Configuration Database left-hand menu.
   - Open `smvlog.nsf`.
2. On the left-hand menu of the Log database, click **Statistics** > **Log Statistics**.
3. On the working area, select all statistics or a specific statistic to view.
4. Select the **server(s)** where the logs you want are located.
5. Select the **time range**.
6. Click **Calculate** to begin compiling a summary report for the logs you selected.
7. Click **Export** to export the raw data to a `*.csv` file.

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.
    i. Select **Delimited** and then click **Next**.
    ii. Deselect the **Tab checkbox** (if marked). Choose **Comma**, and then for the **Text Qualifier**, choose **None**.
    iii. Click **Finish**, without making any changes, in the last Wizard screen.
5. Save the document as an Excel file (`*.xls`) so you do not need to import and reformat again.

Generating and viewing charts

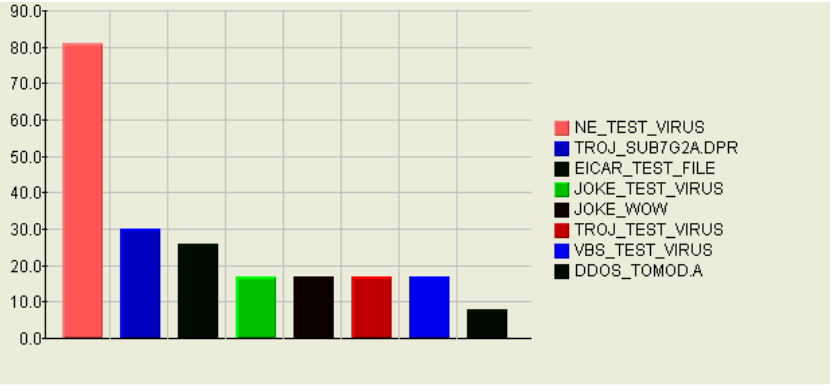
The **Statistics** option allows you to generate any of the following charts in a column layout:

- **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:
    - Click the **Log Database** option from the Configuration Database left-hand menu
    - Open `smvlog.nsf`
2. On the left-hand menu of the Log Database, click **Statistics** > **Top 10 Charts**.
3. On the working area, select the **chart type** to generate and view.
4. Select the **date range**.
5. Click **Generate Chart**.

The screen displays a column-type chart with the top 10 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 9-4. A sample Detection Chart

Using the Quarantine Database

The ScanMail Quarantine database (`smquar.nsf`) stores copies of messages quarantined for content, malware, or spam violations.

Depending on the volume of traffic a server handles and the amount of malware ScanMail encounters, the Quarantine database may grow quite large. ScanMail generates a log, which it stores as new document in the smvlog.nsf database, every time it quarantines malware.

Configure ScanMail to delete quarantine logs every x days automatically (see *Deleting virus logs automatically* starting on page 9-4). Alternatively, you can delete logs manually from the Log database (see *Deleting virus logs manually* starting on page 9-6).

Viewing quarantined messages or attachments

Use the ScanMail Quarantine database to access and view quarantined items.

To view quarantined messages or attachments:

1. Do one of the following to open the Quarantine database:
   - Click the **Quarantine Database** option from the Configuration database left-hand menu.
   - Open `smquar.nsf`.
2. Select and organize the quarantined items you want to view according to the following criteria:
   - **Infected Attachments** displays messages that ScanMail quarantined because of a virus or other malware infection.
   - **Blocked Messages** displays messages that ScanMail quarantined according to content filters, script filters, and scan restriction matches.
   - **Blocked Attachments** displays attachments that ScanMail quarantined according to attachment filter matches.
   - **Encrypted messages** displays messages that ScanMail quarantined according to message filter matches.
   - **Other sorting**

- **Recipient** displays quarantined attachments according to message recipients.
- **Sender** displays quarantined attachments according to message senders.

3. Do one of the following:
   - Organize the search results by time period by viewing all dates, today's date, the past week, and the past month.
   - Click  to sort fields in ascending or descending order.

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:
   - Click the **Quarantine Database** option from the Configuration database left-hand menu.
   - Open `smquar.nsf`.
2. On the left-hand menu, select and organize the quarantined message you want to resend.
3. On the working area, click **Enable Resend**.
4. The icon  represents a message enabled for resending. A missing  signifies that an item has been disabled for resending.
5. 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:
   - Click the **Quarantine Database** option from the Configuration database left-hand menu.
   - Open `smquar.nsf`.
2. On the left-hand menu, select and organize the quarantined document you want to restore.
3. On the working area, select a quarantined document, right-click, and then select **Copy**.
4. Open the database where the quarantined document was supposed 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. You can manually delete quarantined items anytime, even if it is not enabled for deletion.

To delete quarantined items automatically:

1. Do one of the following to open the Quarantine Database:
   - Click the **Quarantine Database** option from the Configuration Database menu
   - Open `smquar.nsf`
2. Select which **quarantined item** you want to enable or disable for deletion.

3. Click **Enable Deletion** or **Disable Deletion**.

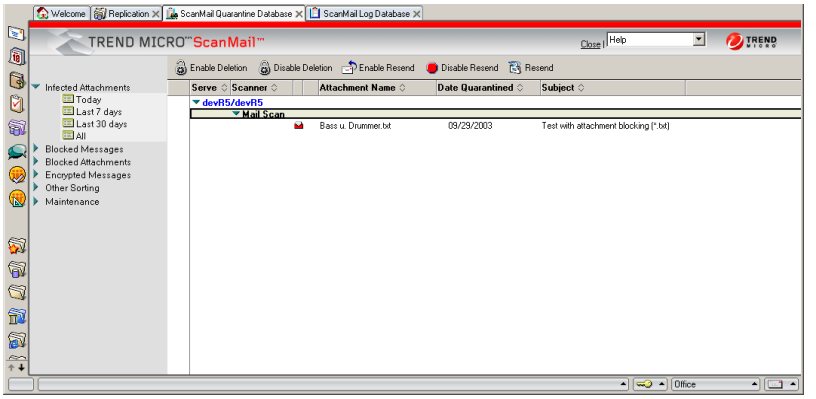


FIGURE 9-5. Enabling/Disabling quarantined item for deletion

Note: Before enabling deletion, Trend Micro recommends reviewing them to be sure that they are indeed expendable.

Deleting quarantine logs automatically

Use the Quarantine database to schedule ScanMail to delete quarantine logs older than the specified number of days automatically. This feature is especially useful if a Domino server handles a large amount of traffic.

Note: ScanMail automatically deletes quarantine logs enabled for deletion.

To enable automatic quarantine log deletion:

1. Do one of the following to open the Quarantine database:
   - Click the **Quarantine Database** option from the Configuration database menu.
   - Open `smquar.nsf`.

2. On the left-hand menu of the Quarantine Database, click **Maintenance** > **Scheduled Deletion**.
3. On the working area, select **Enable automatic deletion**.
4. Select the **quarantine log type**, and type the **number of days** that corresponds to the age of the logs that ScanMail will save.
5. Type the **number of records** that corresponds to the number of deletion records that ScanMail will keep.
6. Click **Save & Clos**e.

Deleting quarantine logs manually

Use the Quarantine Database to delete quarantine logs manually.

To delete quarantined items manually:

1. Do one of the following to open the Quarantine database:
   - Click the **Quarantine Database** option from the Configuration database menu.
   - Open `smquar.nsf`.
2. On the left-hand menu of the Quarantine database, click **Maintenance** > **Manual Deletion**.
3. On 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.
     a. Click **Browse** to launch the Log Files window.
     b. Select which quarantine logs ScanMail will delete.
     c. Click **OK**.
4. Click **Delete Now**.

ScanMail will only delete quarantine logs enabled for deletion.

Chapter 10

Using ScanMail 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

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 configuration console
- Centralized distribution of components

Introducing the Control Manager Agent for ScanMail and Trend Micro Infrastructure

A ScanMail managed product has its own agent, which is responsible for the following actions:

- Receiving commands from the Control Manager server through the Communicator
- Collecting managed product status and logs, and sending them to the Control Manager server through the Communicator

The Communicator, or the Message Routing Framework, is the communication backbone of the Control Manager system. It is a component of the Trend Micro Infrastructure (TMI). Communicators handle all communication between the Control Manager server and managed products. They interact with Control Manager agents to communicate to managed products.

The Control Manager agent is an application installed on a ScanMail server that allows Control Manager to manage the product. Agents interact with the managed product and the Communicator. An agent serves as the bridge between managed products and the Communicator. Hence, you must install the Control Manager agent for ScanMail for Domino on the same server as ScanMail.

After installing, Control Manager agent and TMI files can be found in the following locations:

On a Window-based server:

- `<root>:\Program Files\<Trend Micro or Trend>\Common\TMI`
- `<root>:\Program Files\Trend Micro\ScanMail for Domino\CMAgent`

On Linux, Solaris, and AIX servers:

- `/opt/Trend/TMI`
- `/opt/Trend/SMD/CMAgent`

On i5/OS and OS/400 servers:

- `/qibm/UserData/Trend/TMI`
- `/qibm/UserData/Trend/SMD/CMAgent`

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 **user name** and **password** in the field provided.
3. Click **Enter**.

To access the console remotely:

1. Type the following at your browser's address field to open the Log on page:

   `http://{host name}/ControlManager`

   where `{host name}` is the Control Manager server's fully qualified domain name (FQDN), IP address, or server name.
2. Type the **user name** and **password** in the field 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 Domino to deploy the latest scan engine.

To manage ScanMail from the management console:

1. Access the Control Manager management console (see page 10-5).
2. Click **Products** on the main menu.
3. On the left-hand menu select **Managed Products** from the list, and then click **Go**.
4. Under Product Directory, select the ScanMail for Domino (SMD) managed product to manage.

   Perform one of the following:

   - Check ScanMail status

     To check ScanMail status:

     On the working area, click the **Product Status** tab.

     The Product Status screen displays the **Product Information**, **Component Status**, **Operating System Information**, and **Agent Environment Information**.

   - Configure ScanMail

     To configure ScanMail:

     a. On the working area, click the **Configuration** tab.

     b. Choose **ScanMail (ver)** from the product list that appears, and then click **Next>>**.

        The ScanMail Configuration Database Web console appears.

c. If necessary, type the **user name** and **password** used to access the Configuration database. Contact your administrator for the password set for ScanMail

d. Configure ScanMail as you would from a Notes Client interface.

- Deploy pattern file, scan engine, or anti-spam rule

  To deploy pattern file, scan engine, or anti-spam rule:

  a. On the working area, click the **Tasks** tab.

  b. Pick a task from the **Select a task** list, make sure that **ScanMail (ver)** is listed in the **Supported products**, and then click **Next>>**.

  c. Click **Next>>** to begin updating the Domino server with the latest pattern file, scan engine, or anti-spam rule.

- View security and event logs

  To view security and event logs:

  a. On the working area, click the **Logs** tab.

  b. Click the type of logs you want to view:

  - **Security logs** include all virus log incidents, content security violations, viruses found in download traffic (HTTP, FTP), email, files, and Web security violations.
  - **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.

  c. Provide the search parameters (for example, Severity, Incident) after selecting the type of logs you want to view.

  d. Click **Display Logs** to begin query.

  e. 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. On Export Logs into CSV, right-click **Retrieve the File** and then select **Save Target As...**.
2. On the Save As screen, specify the **location** where you want to keep the file.
3. 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-hand 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 10-5).
  b. Click **Services** on the main menu.
  c. On the left-hand menu under Services, click **Outbreak Prevention**.

  This page automatically refreshes to ensure that the top threat and status information is current.

Deleting an expired Outbreak Prevention Policy

Note: ScanMail does not apply Outbreak Prevention Services if the real-time scan is not enabled.

Use the Configuration database to delete an inactive or expired Outbreak Prevention Policy (OPP).

To delete an expired OPP:

1. Open the ScanMail Configuration database.
2. On the left-hand menu, click **Configurations** > **Outbreak Prevention**.
3. On the working area, click **Enable Expired OPP Automatic Deletion**.
4. Click **OK** to confirm.

An expired OPP can be deleted if the ID used to sign the Configuration database has:

- At least **Editor** privileges
- Delete documents ACL option enabled

The Control Manager agent will check OPP duration and delete the expired OPP once every 30 minutes.

Chapter 11

Removing ScanMail and the Control Manager Agent for ScanMail

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.

- For Windows, Linux, Solaris, and AIX, you can use a wizard to uninstall ScanMail.
- For Linux, Solaris, AIX, and i5/OS and OS/400, you can use console-based commands to uninstall ScanMail.
- Although an automatic uninstall is recommended, you can remove ScanMail manually on all platforms.

Before removing ScanMail, perform the following:

- Confirm that the Domino server and client are not running; if they are, shut down the Domino server and client.
- For i5/OS and OS/400 platforms, ensure that the target server is ended and that all jobs in the trendmicro library are not locked.
- If you installed the Control Manager agent for ScanMail, uninstall it first before removing ScanMail.

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 graphical interfaces that guide you with the uninstallation process.

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

1. Do one of the following to navigate to the uninstall program:
   - If you are removing ScanMail for Windows, perform any of the following tasks to launch the uninstall program:
     a. Click the **Start** button and then select **Programs** > **Trend Micro ScanMail for Domino** > **Uninstall ScanMail for Domino 3.x**.
     b. Go to `<root>:\Program Files\Trend Micro\ScanMail for Domino\Uninstall`.

c. If you are removing ScanMail for Linux/Solaris/AIX, go to `/opt/trend/SMD/Uninstall`.

2. Double-click one of the following to launch the Uninstall program:

PLATFORM	UNINSTALL PROGRAM
Windows	`uninstaller32.exe`
Linux	`SMD3UninstallerLinux.bin`
Solaris	`SMD3UninstallerSolaris.bin`
AIX	`SMD3UninstallerAix.bin`

TABLE 11-1. ScanMail for Domino Uninstall programs

3. Click **Yes** to begin the ScanMail uninstallation.

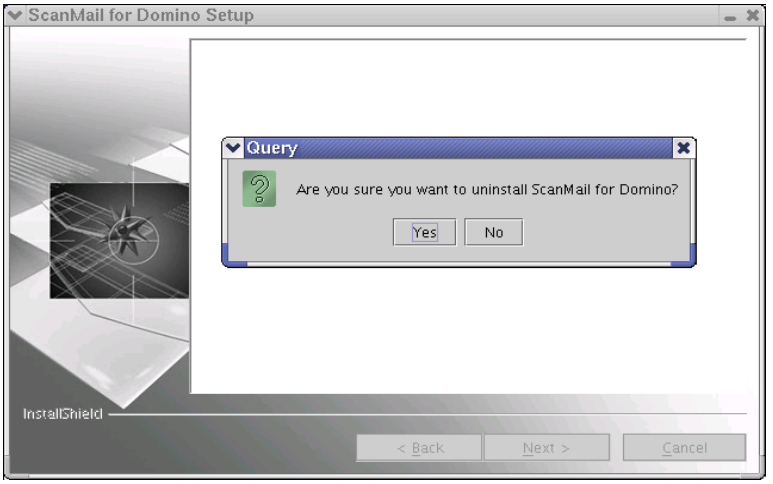


FIGURE 11-1. Click *Yes* to uninstall ScanMail from a single server or partitioned servers

4. On the Domino Server Selection screen, select the server(s) from which to remove ScanMail.

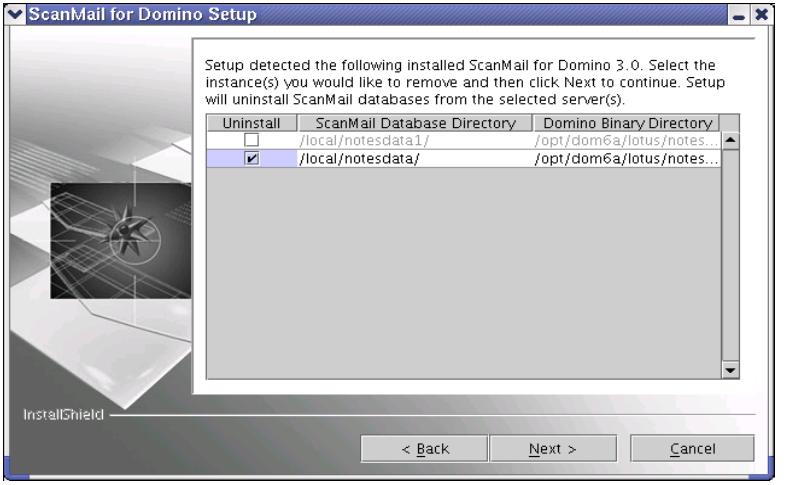


FIGURE 11-2. Select the ScanMail instance to be removed

5. Click **Next >**.

   Setup will remove shared and standard program files installed under the `Domino Data` directory, as well as program folders, items, directories, and entries made to the Windows registry, and entries added to `notes.ini`.

6. Click **Finish** to complete the uninstallation.

7. If you are running ScanMail on an AIX server, run the following commands to manually delete the install/uninstall log file and empty product folder:

```
cd /opt/trend
rm smdins.log (smduins.log,cmains.log,cmauins.log)
rm -fr SMD
```

Note: On the Windows platform, you may also remove ScanMail by selecting **ScanMail for Domino** from the Windows **Start** > **Control Panel** > **Add/Remove Programs**.

Running a ScanMail console-based uninstallation

Running a console-based uninstallation applies to ScanMail for Domino installed on all platforms except Windows.

To run an automatic ScanMail uninstallation from a command console for Linux, Solaris, or AIX:

1. From the directory containing the ScanMail uninstall binary (typically, `/opt/trend/SMD/Uninstall`), issue the following command:

   ```
   ./SMD3Uninstaller{platform}.bin -console
   ```

   where `{platform}` refers to Linux, Solaris, or AIX. For example, issue the following command to uninstall ScanMail for Linux.

   ```
   ./SMD3UninstallerLinux.bin -console
   ```

2. Type `1` to uninstall ScanMail.
3. If there are multiple ScanMail installations present, type the index number to select the server where ScanMail will be removed.
4. Type `3` to exit Setup.
5. Run the following commands to manually delete the install/uninstall log file and empty product folder:

   ```
   cd /opt/trend
   rm smdins.log (smduins.log,cmains.log,cmauins.log)
   rm -fr SMD
   ```

Note: If the ScanMail Icons on the Notes Workspace still appear after uninstallation, right-click each icon and then select **Remove From Workspace** from the menu that appears. In addition, you can remove the ScanMail entries (for example, `ScanMailInstallPath`) in the `notes.ini` file manually.

To run a ScanMail uninstallation from a command console for i5/OS and OS/400:

1. From the directory containing the ScanMail uninstall binary (typically, `/QIBM/UserData/trend/SMD/Uninstall`), issue one of the following commands:
   - **QSHell:**

     ```
     java -cp /QIBM/ProdData/Java400/jt400ntv.jar:
     /QIBM/UserData/trend/SMD/Uninstall/setup.jar run
     -console
     ```

   - **CL command:**

     ```
     RUNJVA CLASS(run) PARM('-console') CLASSPATH
     ('/QIBM/ProdData/Java400/jt400ntv.jar:/QIBM/UserData
     /trend/SMD/Uninstall/setup.jar')
     ```

2. Type `1` to uninstall ScanMail.
3. If there are multiple ScanMail installations present, type the index number to select the server where ScanMail will be removed.
4. Type `3` to exit Setup.

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 (shared) installations of ScanMail and you want to manually uninstall all these instances, the procedure is similar to manually removing ScanMail on a single (not shared) installation.

The installation information and file paths for each instance are all recorded in smdsys.ini, which will also have multiple instances of `[DomSvrX]`.

To manually remove a single or shared ScanMail installation:

Tip: Refer to *Program File and Folder Lists* on page D-1 for the list of ScanMail and Control Manager 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`
   - `ProductID`

   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]
DomSvrISMDCount=5 \\indicates the number of ScanMail installations
ProductID=1faa7e494dca845ffe3515a3b077fa29
ProductVersion=V3.0.0.1183
ProductPath=C:\Program Files\Trend Micro\ScanMail for Domino\
[DomSvr0] \\indicates the first instance of a ScanMail installation
DomSvr0NotesIniPath=D:\Lotus\R6.5\Data2\notes.ini
DomSvr0DominoBinPath=d:\lotus\r6.5\Prog\
DomSvr0DataPath=d:\lotus\r6.5\data2\
DomSvr0DominoVersion=0
DomSvr0SMDVersion=3.0
[DomSvr1] \\indicates the second instance of a ScanMail installation
DomSvr1NotesIniPath=D:\Lotus\R6\Data1\notes.ini
DomSvr1DominoBinPath=d:\lotus\r6\
DomSvr1DataPath=d:\lotus\r6\data1\
DomSvr1DominoVersion=0
DomSvr1SMDVersion=3.0
[DomSvr2] \\indicates the third instance of a ScanMail installation
DomSvr2NotesIniPath=D:\Lotus\R6\data2\notes.ini
DomSvr2DominoBinPath=d:\lotus\r6\
DomSvr2DataPath=d:\lotus\r6\data2\
DomSvr2DominoVersion=0
DomSvr2SMDVersion=3.0
```

2. 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 D-1.* on page D-2).
   - `DominoBinPath` ScanMail files on a Linux/Solaris/AIX server (see *Table D-3.* on page D-4).
   - `DominoBinPath` ScanMail files on an i5/OS or OS/400 server (*Table D-5.* on page D-6).
3. Navigate to the directory specified in `DomSvr{X}DataPath`, and then delete the ScanMail installation and temporary folders:

- ScanMail installation and temporary folders on a Windows server (see *Table D-2.* on page D-3).
- ScanMail installation and temporary folders on a Linux/Solaris/AIX server (see *Table D-4.* on page D-5).
- ScanMail installation and temporary folders on an i5/OS or OS/400 server (see *Table D-6.* on page D-7).

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`
   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. 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 *page 12-2*).
9. For ScanMail installed on a Windows server, complete the following tasks:
   a. Open the Registry, and then delete the uninstall key:

      ```
      HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion
      \Uninstall\${ProductID}
      ```

      where `{ProductID}` is the value of `ProductID` in `smdsys.ini`.
   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
```

10. Close and then delete `smdsys.ini`.
11. For i5/OS and OS/400 platforms only, use CL command `go licpgm`, then type `12` to delete the SMD license.
12. Restart the Domino server.

Removing the Control Manager Agent for ScanMail

If you want to remove ScanMail, the Control Manager agent, or both, always start by stopping Domino. Remove the agent first, then the product, and finally, the TMI (Trend Micro Infrastructure). To remove the agent only, you do not have to remove the TMI.

To remove the Control Manager agent for ScanMail, run one of the following:

- A wizard-based Control Manager agent uninstallation
- A console-based Control Manager agent uninstallation

Tip: The console-based uninstallation applies to all platforms except Windows.

Running a Wizard-based Control Manager Agent uninstallation

The Wizard-based Control Manager agent uninstallation uses graphical interfaces that guide you with the uninstallation process.

To run a wizard-based Control Manager agent uninstallation:

1. Do one of the following to navigate to the uninstall program:

- If you are removing ScanMail for Windows, go to `<root>:\Program Files\Trend Micro\ScanMail for Domino\CMAgent\Uninstall\.`

  Tip: Alternatively, you can remove the Control Manager agent from the Windows taskbar, click **Start**, then **Settings** > **Control Panel** > **Add/Remove Programs**.

- If you are removing ScanMail for Linux/Solaris/AIX, go to `/opt/trend/SMD/CMAgent/Uninstall/.`

2. Double-click one of the following to launch the Uninstall program:

PLATFORM	UNINSTALL PROGRAM
Windows	`cmaunins32.exe`
Linux	`CMAgent3UninstallerLinux.bin`
Solaris	`CMAgent3UninstallerSolaris.bin`
AIX	`CMAgent3UninstallerAix.bin`

TABLE 11-2. Control Manager Uninstall Programs

3. Click **Yes** to confirm.
4. After uninstall is complete, click **Close**.

Setup removes the Control Manager agent. To verify, access the Control Manager management console and check whether the ScanMail for Domino managed product is no longer in the Product Directory.

Running a console-based Control Manager Agent uninstallation

Running a console-based uninstallation only applies to the Control Manager agent for ScanMail installed on a Linux, Solaris, AIX, i5/OS, or OS/400 server.

To run a console-based Control Manager agent uninstallation for i5/OS and OS/400:

1. From the directory containing the Control Manager agent uninstall binary (typically, `/QIBM/UserData/trend/SMD/CMAgent/Uninstall/`), issue the following command:

   ```
   java -cp
   /QIBM/ProdData/Java400/jt400ntv.jar:/QIBM/UserData/trend/SMD/
   CMAgent/Uninstall/setup.jar run -console
   ```

2. Type `1` to uninstall the Control Manager agent.
3. Type `3` to exit Setup.

Setup removes the Control Manager agent. To verify, access the Control Manager management console and check whether the ScanMail for Domino managed product is no longer in the Product Directory.

To run a console-based Control Manager agent uninstallation for Linux, Solaris, or AIX:

1. From the directory containing the Control Manager agent uninstall binary (typically, `/opt/trend/SMD/CMAgent/Uninstall/`), issue the following command:

   ```
   ./CMAgent3Uninstaller{platform}.bin -console
   ```

   where `{platform}` refers to Linux, Solaris, or AIX. For example, issue the following command to uninstall the Control Manager agent for ScanMail for Solaris

   ```
   ./CMAgent3UninstallerSolaris.bin -console
   ```

2. Type `1` to uninstall the Control Manager agent.
3. Type `3` to exit Setup.

Setup removes the Control Manager agent. To verify, access the Control Manager management console and check whether the ScanMail for Domino managed product is no longer in the Product Directory.

Removing the Trend Micro Management Infrastructure

For ScanMail for Windows, remove the Trend Micro Management Infrastructure (TMI) component if there are no other Control Manager agents running on the Domino server.

For i5/OS and OS/400 platforms, the Control Manager agent uninstaller will remove the TMI if an agent is no longer on the server.

To remove TMI:

1. From the Windows taskbar, click **Start**, then **Settings** > **Control Panel** > **Add/Remove Programs**.
2. Scroll down the list to select **Trend Micro Management Infrastructure**, then click **Remove** and **Yes** to begin removing the Control Manager agent.
3. After uninstall is complete, click **Close**.

Chapter 12

Troubleshooting

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

This chapter discusses the following topics:

Locating Installation and Uninstallation Logs

The following are the ScanMail and Control Manager agent for ScanMail installation and uninstallation logs:

PLATFORM	LOCATION AND FILE NAME	DESCRIPTION
Windows	<root>\smdins.log	ScanMail installation log
	<root>\smdunins.log	ScanMail uninstallation log
	<Setup program path>\Setuplog.txt	ScanMail silent installation log
	<root>\cmains.log	Control Manager agent for ScanMail installation log
	<root>\cmaunins.log	Control Manager agent for ScanMail uninstallation log
Linux/Solaris/AIX	/opt/trend/smdins.log	ScanMail installation log
	/opt/trend/smdunins.log	ScanMail uninstallation log
	/opt/trend/cmains.log	Control Manager agent for ScanMail installation log
	/opt/trend/cmauins.log	Control Manager agent for ScanMail uninstallation log
i5/OS and OS/400	/QIBM/UserData/trend/smdins.log	ScanMail installation log
	/QIBM/UserData/trend/smdunins.log	ScanMail uninstallation log
	/QIBM/UserData/trend/cmains.log	Control Manager agent for ScanMail installation log
	/QIBM/UserData/trend/cmauins.log	Control Manager agent for ScanMail uninstallation log

TABLE 12-1. Installation and uninstallation logs

Resolving CMAgent Registration Failure on AIX

If the ScanMail for Domino CMAgent fails to register with Control Manager after CMAgent is installed or upgraded, restart the Trend Micro Infrastructure (TMI).

To restart TMI, type the following:

1. `cd /opt/trend/TMI`
2. `./tmi stop`
3. `slibclean`
4. `./tmi start`

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 mail box and release the held messages.

To scan the system mail box 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 (see page *7-8*) to download antivirus and content security components (see page *7-2*) from the update source, and updated components cannot be downloaded, 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 `http://smln-p.activeupdate.trendmicro.com/activeupdate` from the Domino server.

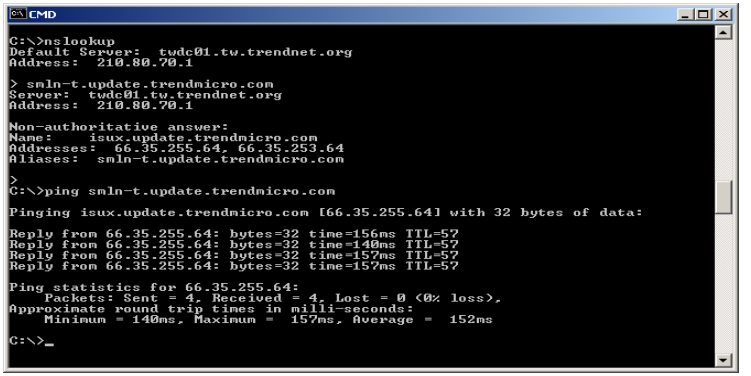


FIGURE 12-1. Use ping and nslookup to test connection between Domino server and ActiveUpdate server

  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%3
2%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&LastN=%41%50%54%47%2
d%39%39%39%32%2d%31%32%32%31%2d%32%39%32%39%2d%32%32%31%30&E
Mail=%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%32%31%2d%32%39%32%39%2d%32%32%31%30&OPhone=%41%50%54%47%2
d%39%39%39%32%2d%31%32%32%31%2d%32%39%32%39%2d%32%32%31%30&F
ax=%41%50%54%47%2d%39%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%2d%31%32%32%31%2d%32%39%32%39%2d%32%32%31%30&State=%4
1%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%31%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.

FIGURE 12-2. 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 (see *Debugging ScanMail Tasks*) and then contact Trend Micro Support.

Scheduled Scan/Update Issue

A ScanMail for Domino 3 scheduled scan/update cannot be re-run if the scheduler didn't start up during schedule time. A workaround method 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, attempt 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
```

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 page *12-7*). However, note that recreating a database does not restore its original contents.

Using the Database Templates to Recreate ScanMail Databases

If for some reason, a 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 an `*.NTF` copy of the database you would like to replace and place it in the following directory:
   - For Domino R4: `Notes\Data`
   - For Domino R5/R6: `Lotus\Domino\Data`
2. Launch a Notes Client, and then open the **Workspace** tab containing the ScanMail databases (see *Defining Access and Roles to ScanMail Databases* on page 4-5 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** > **Database** > **Replace Design**. The Replace Database Design window appears.
5. Click the **Template Server** button.
6. Click the corresponding **server** from the list, and 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`, or `SMDmon` 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 3 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
- **Linux/Solaris/AIX:** smdreal_20040211.dbg
- **i5/OS and OS/400:** SMDREAL_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
- `<Domino Data>\SMDTemp\dbmigrate.log` for ScanMail database migration debug logs

ScanMail saves all debug files to the `\SMD\SMDtemp\` folder under the `Domino Data` directory.

Debugging the Control Manager Agent for ScanMail

Modify `entity.cfg` to debug the Control Manager agent for ScanMail.

Tip: Use care when modifying Control Manager `*.xml` or `*.cfg` files. To ensure that you can roll back to the original settings, back up `entity.cfg`.

To debug the Control Manager agent for ScanMail:

1. Using a text editor, open `entity.cfg` found in the `Domino Data` directory.
2. Search the parameter `LOG_level` and modify its value. The possible values are:

LEVEL	DESCRIPTION
0	Shows detailed debug information
2	Shows error messages only

3. Search the parameter `LOG_filename` and modify its value to set the debug log file name.
4. Save, and then close `entity.cfg`.

The Control Manager agent debug log will be created in the `{TMI installation path}\dbglog\` folder using the file name specified in `LOG_filename`.

Collecting ScanMail and Domino Debug Logs

In the unlikely event that ScanMail is not functioning, collect logs for Trend Micro Support analysis.

To collect Domino debug logs:

Check `NOTES.RIP` generated under the `Domino Data` directory.

To collect ScanMail debug logs:

Launch the ScanMail Support tool. Do one of the following:

- Using the Domino server console, issue:

  ```
  load SMDSupp
  ```

- Using Microsoft Windows Explorer (Windows platforms), double-click `<root>:\Program Files\Trend Micro\ScanMail for Domino\program\V3.1.0.####\nSMDSupp.exe`
- Using a bash terminal (in Solaris) or Shell console (in Linux), perform the following:

Note: Log on using the account used to install the Domino server application when running the following commands. Otherwise, the error *Do not run Domino as root* or similar message appears. This prevents you from running the ScanMail Support tool.

---

a. Run the following commands consecutively:

```
# export LD_LIBRARY_PATH={Notes path}:{ScanMail
  path}/program/latest

# export Notes_ExecDirectory={Notes directory}
```

where:

- `{Notes path}` is the full path of the Domino Binary directory

  For examples, `/opt/lotus/notes/latest/linux` in Linux and `/opt/lotus/notes/latest/sunspa` in Solaris.

- `{ScanMail path}` is the full path of the ScanMail Binary directory

  For example, `/opt/trend/SMD`.

b. Navigate to the directory where notes.ini is located (for example, `/local/notesdata`)

c. To invoke the ScanMail Support tool, run:

```
# {ScanMail path}/program/latest/smdsupp
```

See *Figure 12-3* for sample command execution.

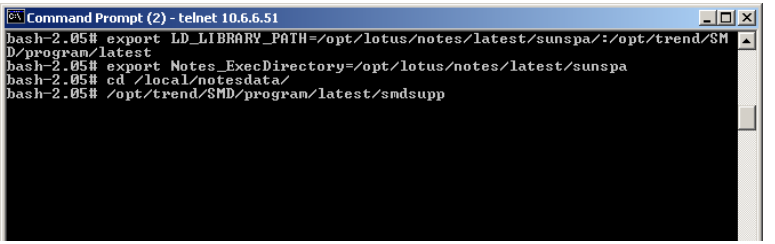


FIGURE 12-3. Running SMDsupp from a Solaris bash terminal

- From the i5/OS or OS/400 main menu (i5/OS and OS/400 platforms), run the following CL commands:

  a. `chgcurdir` to navigate to the directory where notes.ini is located (for example, /local/notesdata)

  b. `ADDLIBLE LIB(QNOTES)`

  c. `ADDLIBLE LIB(QDOMINOxxx)`

  where ### is the Domino version for releases after 6.0.3.

  d. `call trendmicro/smdsupp`

The tool collects the server task debug log, `notes.ini`, server mail.box, `log.nsf`, and `smconf.nsf` logs and saves them to a zip file with the following convention:

```
SMDSuppyyyy-mm-dd.zip
```

You can find this file under the `\SMD\SMDtemp\` folder in the `Domino Data` directory.

Note: The ScanMail Support tool compresses and password-protects the collected logs. Use the password `trendsmd` to decompress and check the collected logs.

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.
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. Refer to *Activating ScanMail*.
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.	*Renew ScanMail maintenance*
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.	

MESSAGE	CAUSE	WHAT TO DO
SMDdbs: Invalid database list settings. Check the database list in the Manual or Scheduled scan rule setting.	The format of the database list in the Configuration Database is incorrect.	Check **Databases to Scan** list in the **Real-time Database Scan**, **Scheduled Scan**, or **Manual Scan** documents. Use semicolons to separate multiple entries.
SMDreal: Unable to read Domino directory. Check server status.	The fully qualified name (FQDN) of the Domino server is empty. Alternatively, other Domino configuration is wrong.	Correct the Domino settings.
SMDreal: Cannot open database {database name}. Check the database name in the Configuration Database.	ScanMail cannot open the database when trying to scan the special document in that database. Probably, the database was deleted before ScanMail was able to scan it.	No action needed.
SMDdbs: Cannot read Database Scan settings. Check Configuration Database.	Database Scan setting is incorrect.	Check database scan rule (see *Creating real-time database scan rules*).
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.

MESSAGE	CAUSE	WHAT TO DO
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 (see *Running Manual Scan*) or scheduled update rule (see *Updating Components*).
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.	*Renew ScanMail maintenance*
SMDupd: Unable to update to the latest version. Refer to ScanMail Help > Troubleshooting for details.	Connection to the ActiveUpdate server cannot be established or unable to perform integrity checking for the downloaded component.	Check the network connection and the proxy server connection and configuration. Refer to `<ScanMail Installation Path>\AU_Log\TmuDump.txt` for details.
SMD Loader: The executable file exceeds the allowable maximum size {maximum size}	The path name of executable file is too long. This could be caused by multiple cascading subdirectories or long file names.	Reinstall ScanMail on a directory with a short path name.

MESSAGE	CAUSE	WHAT TO DO
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 13

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

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://kb.trendmicro.com/solutions/solutionSearch.asp`

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://kb.trendmicro.com/solutions/solutionSearch.asp`

- 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:

```
www.trendmicro.com/en/security/trendlabs/overview.htm
```

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

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.

How Malware Spreads in a Notes Environment

ScanMail provides constant detection and protection of the three points of entry where the Notes Client environment is most vulnerable:

- Email transmissions– ScanMail performs real-time scanning on all incoming and outgoing email messages and their attachments to stop malware from entering your system, or infecting someone else's (for example, a customer)
- Client database accesses– ScanMail monitors database files that are modified in real time to prevent viruses from being archived among your stored database documents
- Replications– ScanMail checks all files modified through the Notes database replicator in real time to keep viruses from being replicated from other Notes servers

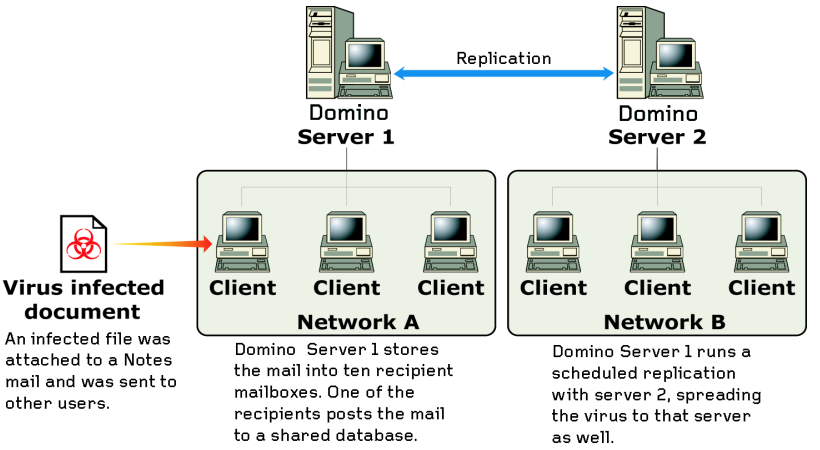


FIGURE B-1. A virus infected document spreading in a Notes environment.

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 Best Practices

This appendix provides the best practices for optimized operations and maximum performance of ScanMail. This includes:

Tuning the Domino Server

Trend Micro recommends the following settings for servers running ScanMail for 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) Modify the `ServerTasks` line in Notes.ini to relocate the SMDreal and SMDdbs entries in front of the `Router` entry
- (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 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.

Upgrading ScanMail for Domino from 3

If you are upgrading from ScanMail for Domino 3 to a later version and want to keep the original configuration, you do not need to perform a complete new installation of ScanMail.

To upgrade from ScanMail for Domino 3 without reinstalling:

1. Back up the original databases from the older version to a folder (for example, backup1):
   - smconf.nsf
   - smency.nsf
   - smquar.nsf
   - smvlog.nsf
2. Uninstall the older version and do a fresh install for the newer version.
3. Move the new databases and templates from <domino data\smd\>to notes data folder.
4. Copy the original databases (smconf.nsf/smency.nsf/smquar.nsf/smvlog.nsf, from backup1) to the <domino data\smd\> folder.
5. One by one, replace the design of the original version databases with the new database template (in notes data folder).
6. One by one, manually sign all the databases with server.id or user.id.

Appendix C

Control Manager Agent Checklist

Use the Control Manager agent checklist in this appendix to record relevant system information that will be needed from time to time.

INFORMATION REQUIRED	SAMPLE	YOUR VALUE
Control Manager server Administrator account User ID	root	
Encryption key location	<Domino Data>\E2EPulic.dat	

Note: You can use any user ID instead of the root account user ID. However, Trend Micro recommends using the Root account because if you delete the User ID specified during agent installation, you will have difficulty managing the agent.

PRODUCT NAME	ADMINISTRATOR-LEVEL ACCOUNT	IP ADDRESS	HOST NAME
Sample	Admin	10.225.225.225	PH-antivirus

Appendix D

Program File and Folder Lists

This appendix provides a list of the ScanMail and Control Manager 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 12-2.

ScanMail and Control Manager Agent (Windows)

Refer to table *D-1* and *D-2* for the list of files created by a successful ScanMail and Control Manager agent installation 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 ndbmigrate25.exe ndbmigrate26.exe smd.ini	The ScanMail loader, filter, Extension Manager, dbsetup, and ScanMail configuration files
...WINNT\smdsys.ini	The main ScanMail for Domino configuration file
...\Program Files\Trend Micro\ScanMail for Domino	The ScanMail for Domino installation folder
...\engine	Contains the TMASE and virus scan engine folders
...\engine\tmase	Contains the Trend Micro Anti-spam Engine (TMASE)
...\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
...\program	Contains the ScanMail readme file and the binary and configuration file folders
...\program\V3.#.#.####	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 D-1. ScanMail files and folders available on a Windows server

FILE/FOLDER	DESCRIPTION
`...WINNT\cmasys.ini`	The main Control Manager agent configuration file
`...\Program Files\Trend Micro\ScanMail for Domino\cmagent`	The Control Manager agent installation folder, which contains the Control Manager agent program and configuration files
`…\Program Files\Trend Micro\ScanMail for Domino\CMAgent\Uninstall`	Contains the Control Manager agent uninstall program

TABLE D-2. Control Manager agent files and folders available on a Windows server

ScanMail and Control Manager Agent (Linux/Solaris/AIX)

Refer to table *D-3* and *D-4* for the list of files created by a successful ScanMail and Control Manager agent installation on a Linux, Solaris, or AIX server.

FILE/FOLDER	DESCRIPTION
`/etc/smdsys.ini`	The ScanMail for Domino main configuration file
`/opt/trend/SMD/`	The ScanMail for Domino installation 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 pattern file
`.../program`	Contains the ScanMail readme file and the binary and configuration file folders
`./program/V3.#.#.####`	Contains the ScanMail binary and configuration files where: `.#.#` (the first two) indicate the minor version `.####` (the last four #) indicate the build number

`/opt/lotus/notes/latest/<OS name>`
`...smddbs`
`...smddbsy`
`...smdemf`
`...smd.ini`
`...smdmon`
`...smdreal`
`...smdsch`
`...smdsupp`
`...smdupd`
`...libsmdext.so`
`...libsmlnredid.so`
	Contains the ScanMail configuration, binary, and database files under the Domino Program directory where `<OS name>` is one of the following:
	
	Linux: `linux`
	Solaris: `sunspa`
	AIX: `ibmpow`

`/local/notesdata/smd`	Contains the ScanMail databases and templates
`/local/notesdata/smdtemp`	Contains the Setup dbsetup.log and the temporary files used by the ScanMail scan tasks

TABLE D-3. ScanMail files and folders on a Linux/Solaris/AIX server

FILE/FOLDER	DESCRIPTION
/etc/cmasys.ini	The Control Manager agent main configuration file
/opt/trend/SMD/CMAgent	The Control Manager agent installation folder, which contains the Control Manager agent binary and configuration files
…/CMAgent/Uninstall	Contains the Control Manager agent uninstall program
.../CMAgent/temp	Contains temporary files
Entity.cfg	Located in the target Domino server data folder, this file contains configuration information for the Control Manager agent.
Entity.ini	Temporary file that contains parameters that are used when CMAgent is running.
Entity.tmp	Temporary file that contains parameters that are used when CMAgent is running.
/opt/trend/TMI	The Trend Micro Infrastructure (TMI) installation folder, which contains the TMI binary and configuration files

TABLE D-4. Control Manager agent files and folders available on a Linux/Solaris/AIX server

ScanMail and Control Manager Agent (i5/OS and OS/400)

Refer to Table *D-5* for the list of files created by a successful ScanMail and Control Manager agent installation on an i5/OS or OS/400 server.

FILE/FOLDER	DESCRIPTION
/etc/smdsys.ini	The ScanMail for Domino main configuration file
/qibm/userdata/trend/smd/	The ScanMail for Domino installation 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 pattern file
.../program	Contains the ScanMail readme file and the binary and configuration file folders
./V3.#.#.####	Contains the ScanMail binary and configuration files where: .#.# (the first two) indicate the minor version .#### (the last four #) indicate the build number
/QIBM/ProdData/LOTUS/NOTES —or— /QIBM/ProdData/LOTUS/Domino### ...smd.ini ...smdemf.pgm ...smdreal.pgm ...smdsupp.pgm ...smddbs.pgm ...smdmon.pgm ...smdsch.pgm ...smdupd.pgm ...dbmigrate26.pgm ...dbsetup.pgm	Use for Domino versions lower than 6.0.3. where ### is the Domino version for releases after 6.0.3. Contains the ScanMail configuration, binary, and database files under the Domino Program directory
/local/notesdata/smd	Contains the ScanMail databases and templates
/local/notesdata/smdtemp	Contains the Setup dbsetup.log and the temporary files used by the ScanMail scan tasks

TABLE D-5. ScanMail files and folders on an i5/OS or OS/400 server

FILE/FOLDER	DESCRIPTION
/etc/cmasys.ini	The Control Manager agent main configuration file
/qibm/userdata/trend/smd/cmagent	The Control Manager agent installation folder, which contains the Control Manager agent binary and configuration files
../cmagent/uninstall	Contains the Control Manager agent uninstall program
../cmagent/temp	Contains temporary files
$DominoData/Entity.cfg	Located in the target Domino server data folder, this file contains configuration information for the Control Manager agent.
$DominoData/Entity.ini	Temporary file that contains parameters that are used when CMAgent is running.
$DominoData/Entity.tmp	Temporary file that contains parameters that are used when CMAgent is running.
/qibm/userdata/trend/tmi	The Trend Micro Infrastructure (TMI) installation folder, which contains the TMI binary and configuration files
/etc/tmicfgdir	A file that contains the TMI configuration path in ASCII.

TABLE D-6. Control Manager agent files and folders available on an i5/OS or OS/400 server

SMLN 2.6 and SMD 3 Feature Comparison

The following table presents a comparison of Trend Micro ScanMail for Lotus Notes (SMLN) 2.6 and ScanMail for Domino (SMD) 3.

FEATURE	SCANMAIL FOR LOTUS NOTES 2.6	SCANMAIL FOR DOMINO 3
INSTALLATION/PLATFORM SUPPORT		
Supports Domino 7.0 (i5/OS only)	Yes	Yes
Supports Domino 6.5.x	Yes	Yes
Supports Domino 6.0.x	Yes	Yes
Supports Domino 5.0.13a, 5.0.12, 5.0.11	Yes	Yes[A]
Supports cluster server (full support with task on each server and trusting)	No	Yes
Supports partitioned servers	Yes	Yes
Simultaneous installation on multiple partitions	No	Yes
Scripted/silent installation on all platforms	No	Yes
Preparation for replication during installation	No	Yes
Configuration of ACL during installation	No	Yes
Database signing during installation	Yes	Yes
Database signing with alternate ID/password or skip signing	No	Yes
Replicates Configuration database across platforms	No	Yes
SUPPORTED DOMINO APPLICATIONS		
Lotus Domino Database (.nsf)	Yes	Yes
Lotus Domino Web Access (formerly iNotes Web Access)	No	Yes

TABLE APPENDIX E-1. ScanMail 2.6 and 3 feature comparison

FEATURE	SCANMAIL FOR LOTUS NOTES 2.6	SCANMAIL FOR DOMINO 3
PRODUCT ACTIVATION		
Uses serial numbers	Yes	No
Two serial numbers (one for ScanMail, optional for eManager)	Yes	No
Trend Micro Online Registration system	No	Yes
One Activation Code (either for ScanMail for Domino or ScanMail for Domino Suite)	No	Yes
SCANNING (GENERAL)		
Multi-threaded scanning	No	Yes
Multi-threaded scan tasks	No	Yes
Separate actions for Adware/Spyware	No	Yes
MAIL SCANNING		
Real-time scan	Yes	Yes
Mail scan rule based on mail sender/recipient	No	Yes
Different scan settings for users/groups with exceptions	No	Yes
Scheduled scanning with different settings at different times	No	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
Selectively scans embedded OLE objects	Yes	Yes

TABLE APPENDIX E-1. ScanMail 2.6 and 3 feature comparison, continued

Feature	ScanMail for Lotus Notes 2.6	ScanMail for Domino 3
Adware Detection		
Configurable action upon detection	No	Yes
Spyware Detection		
Configurable action upon detection	No	Yes
Mail/Bandwidth Management		
Redirects email for approval	No	Yes
Supports selectable grouping of file types	No	Yes
Configurable attachment blocking by true file type (individual file types)	No	Yes
Configurable action for Microsoft Office macros	No	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
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
SPAM filtering (requires ScanMail for Lotus Domino Suite/eManager)		
Uses heuristics technology	No	Yes

Table Appendix E-1. ScanMail 2.6 and 3 feature comparison, continued

FEATURE	SCANMAIL FOR LOTUS NOTES 2.6	SCANMAIL FOR DOMINO 3
Supports Approved/Blocked Senders lists	No	Yes
Configurable filter sensitivity	No	Yes
Uses rule file	Yes	Yes
DATABASE SCANNING		
Real-time scanning	Yes	Yes
Scheduled scanning	Yes	Yes
Manual scanning	Yes	Yes
Configurable time period for multiple real-time scanning configurations	No	Yes
Script scanning support in real-time scanning	Yes	Yes
Scheduled scanning within defined time periods (maximum duration)	No	Yes
Support for several scheduled scans with different settings	No	Yes
Resume a scan that did not finish	No	Yes
Script scanning support in scheduled scanning	Yes	Yes
Configurable scan schedule through Configuration database	No	Yes
ADMINISTRATION		
Full integration with R6/5 Administrator Client and Notes Client	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	No	Yes
Server status monitoring available through user interface	No	Yes
Server task watch dog	No	Yes

TABLE APPENDIX E-1. ScanMail 2.6 and 3 feature comparison, continued

Feature	ScanMail for Lotus Notes 2.6	ScanMail for Domino 3
Task status monitoring	No	Yes
Share server settings and antivirus policies between servers and groups of servers	No	Yes
User-defined and controlled rules to define actions	No	Yes
Ability to define rules based on users and groups	No	Yes
Configurable server settings that are policy-independent	No	Yes
Role-based access configurable through the Notes interface	No	Yes
One-button information collector (Support Tool)	No	Yes
Antivirus and Content Security Component Updates		
Manual update	Yes	Yes
Select components and set recurring scheduled updates	No	Yes
Automated pattern update through ActiveUpdate	Yes	Yes
Automated scan engine update through ActiveUpdate	Yes	Yes
Automated program updates through ActiveUpdate	No	Yes
Pattern/Engine integrity check after update	Yes	Yes
Product integrity check after update	No	Yes
Notification Options		
Customized notifications	No	Yes
Notifications via Lotus Instant Messaging (ScanMail for Domino for Windows only)	No	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	No	Yes

Table Appendix E-1. ScanMail 2.6 and 3 feature comparison, continued

FEATURE	SCANMAIL FOR LOTUS NOTES 2.6	SCANMAIL FOR DOMINO 3
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	No	Yes
Multiple disclaimer support	No	Yes
Single disclaimer inserted when an email passes multiple servers	Yes	Yes
Supports disclaimer positioning	No	Yes
QUARANTINE		
Automatically deletes quarantined logs based on type, age, and records to retain	Yes	Yes
Supports resend/restore of quarantined items	Yes	Yes
LOGGING/STATISTICS		
Exports statistics to a Microsoft Excel spreadsheet	No	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

TABLE APPENDIX E-1. ScanMail 2.6 and 3 feature comparison, continued

A. There is no support for Domino 5.x on OS/400 platforms.

Index

A

C

D

E

F

H

I

J

L

M

N

T

U

V

W