Trend Micro™

ScanMail For IBM Domino Deployment

Best Practice Guide

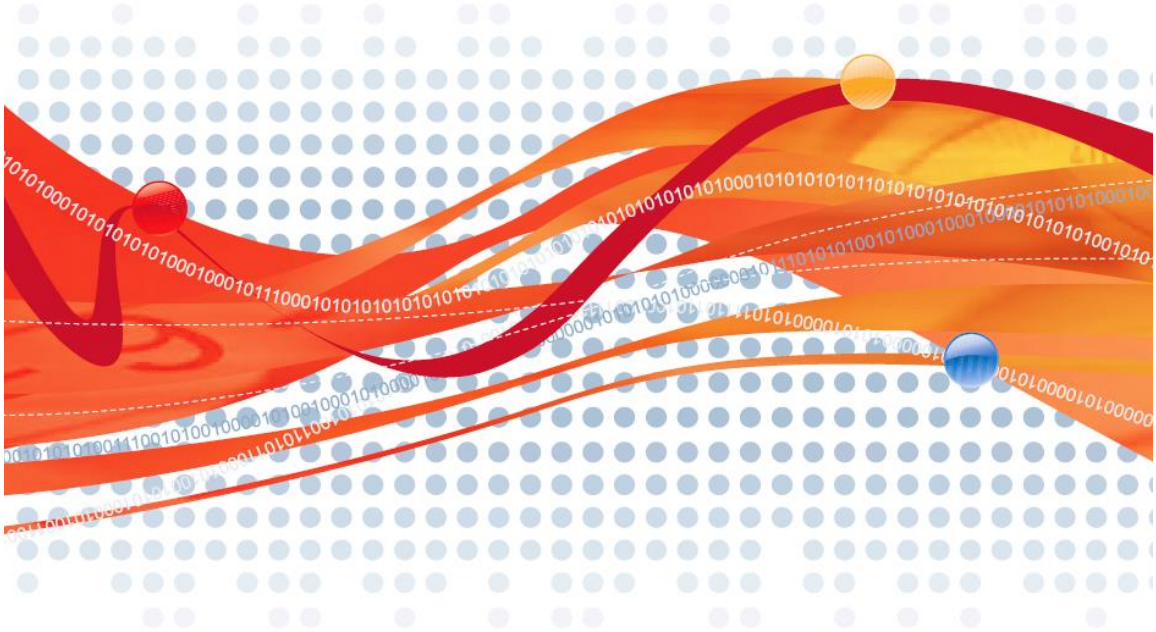


Table Of Contents

Table Of Contents 2

About this Book 4

1.1 Preface 4

1.2 Authors 4

1.3 Prerequisites 4

1.4 Abbreviations and Terms 4

1.5 Conventions 6

1.6 Revision 7

Chapter 1: Product Overview 8

1.1 How SMID Works 9

1.2 How SMID Protects Your Data Privacy 9

1.3 Management 10

1.4 Configuration 10

1.5 ScanMail for IBM Domino Editions 11

Chapter 2: Deploy on Windows Platform 13

2.1 Recommended System Requirements 13

2.2 Pre-installation Tasks 14

2.3 Installing SMID for Windows 14

Chapter 3: Deploy on Linux Platform 22

3.1 Recommended System Requirements 22

3.2 Pre-installation Tasks 23

3.3 Installing SMID for Linux 24

Chapter 4: Deploy on AIX Platform 30

4.1 Recommended System Requirements 30

4.2 Pre-installation Task 31

4.3 Installing SMD for AIX 32

Chapter 5: Troubleshooting 37

5.1 Manually update components 37

5.1.1 How to manually update components for AIX 37

5.1.2 How to manually update components for Linux 38

5.1.3 How to manually update components for Windows 39
5.2 ScanMail For Domino Database 40
5.2.1 Databases 40
5.2.2 Recovering a Corrupt ScanMail Database 42
5.3 Database Replication 43
5.4 Update the SMID License 44
Appendix Ⅰ: How To Collect SMD Logs 45
Appendix Ⅱ Hidden Key 47
Appendix III Auto-Generated Key 49

About this Book

1.1 Preface

Welcome to the **Trend Micro ScanMail for IBM Domino (SMID) Deployment Best Practice Guide**. This document serves as a guideline to help customers how to deploy SMID to Domino server that on the AIX platform.

This document provides in-depth information about SMID architecture, configuration and deployment process as well as troubleshooting.

This document should be read in conjunction with the *Trend Micro ScanMail For Domino Administrator Guide*.

1.2 Authors

This **Best Practice Guide** is written by Nickel Xu. Additional information was provided by the members of SMD Engineering groups, including:

Hedy Xu

Claire Shi

1.3 Prerequisites

This Best Practice Guide covers the basic administration procedures for SMID or common industry technologies. The readers and course participants must have a good working knowledge of the following topics:

- ScanMail for lBM Domino functions and administration
- Domino Server Administration
- Domino Mail Routing
- Domino Database

1.4 Abbreviations and Terms

The following table decodes many abbreviations used throughout this document. The abbreviations listed include acronyms and other linguistic shortenings of names, along with certain code words, file- and folder-name extensions, and other short-form references.

The table also includes abbreviations that may not be used directly in this document but may be encountered within the various log files, configuration files, file names, directory names, registry sub-keys, additional engineering documents, diagrams, and so forth that may be encountered when working with the product.

However, although this list of terms is intended to be comprehensive, due to the large number of abbreviations that appear in registry entries, filenames, configuration files, and so forth, it is not complete.

Abbreviation	Meaning
APT	Advanced Persistent Threat
ATP	Advanced Threat Protection
ATSE	Advanced Threat Scan Engine
CLP	License Portal for Complete User Protection (CUP) Suites
CSV	Comma Separated Values
DDAaaS	Deep Discovery Analyzer as a Service
DLP	Data Loss Prevention
SMID	Trend Micro™ ScanMail for IBM Domino; The all-in-one malware and malicious content protection for IBM Domino messaging environments.
SMID Server	The ScanMail for IBM Domino Server; The target server where both SMID and Lotus Domino are running.
DB	Database: Refers to either an SMID or a Lotus Domino database, unless otherwise specified
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IBM Domino object	Refers to either a mail or database, which SMID is able to scan.
<Domino binary directory>	The path where the Domino Server's program files are installed. By default, this is in \IBM\Domino.
<Domino data directory>	The path where the Domino Server's data files are installed. By default, this is in \IBM\Domino\data.
TMCM	Trend Micro Control Manager
TMUFE	Trend Micro URL Filtering Engine
URL	Uniform Resource Locator
VA	Virtual Analyzer
WTP	Web Threat Protection

1.5 Conventions

The following conventions are used in this Best Practice Guide:

Convention	Description
`monospace`	Registry, logs, configuration file parameters, commands, syntax, file names, and folder names
Tip ✓	Recommended configuration/actions
NOTE	Brief comment or explanation
Refer to	References to other documents or sections of this Support Track
Warning	Critical actions or configurations

1.6 Revision

Date Released	Updates/ Changes
01/04/2018	Nickel Xu (TS-CN)

Chapter 1: Product Overview

This chapter contains an overview of the product to give the audience a bird’s eye view of the product.

1.1 How SMID Works

The Trend Micro scan engine uses both rule-based and pattern recognition technologies, as well as MacroTrap technology that detects and removes macro viruses. Frequently, automatic virus pattern and scan engine updates occur through a Web-based download mechanism, which does not require ScanMail to be turned off.

ScanMail scans and cleans attachments and document content on all entry points, as illustrated in Figure 1-1.

- Email attachments are scanned in real-time at the IBM Domino mail server.
- Database events are monitored and attachments are scanned immediately before a document is closed.
- Databases and modified data are scanned during replication.
- Existing attachments in mailboxes and Domino databases are scanned to root out old infections.

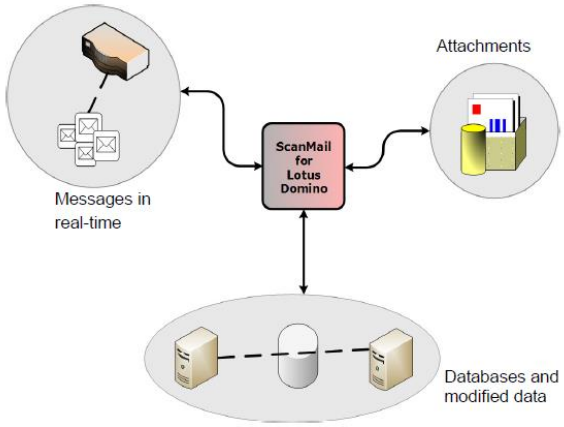


FIGURE 1-1. ScanMail detects and removes threats before infections can spread to the desktop.

1.2 How SMID Protects Your Data Privacy

Trend Micro ScanMail for IBM Domino (SMID) provides an integrated defense against multiple threats, data compromises, and vulnerabilities in IBM Domino systems. It is capable of protecting Domino Server against malware, spyware, spam, phishing, script bomb and other unwanted contents.

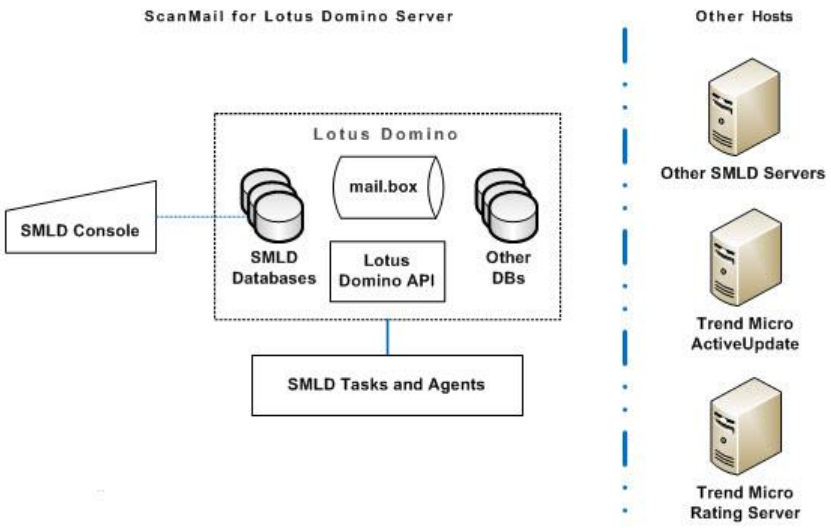


Figure 1-2

An SMID Server may communicate with other SMID Servers for the purpose of replication. It also needs to interface with the ActiveUpdate Server to get the necessary component updates. Lastly, if the web reputation feature is enabled, an SMID Server would need to connect to the Trend Micro's Rating Server as well.

ScanMail forIBM Domino provides real-time, on-demand (manual) and scheduled scanning of emails and databases. It uses a multi-threaded, in-memory mechanism which significantly increases its scanning speed.

1.3 Management

ScanMail for IBM Domino can be administered using several methods:

- Using Domino Administrator or Lotus Notes client
- Using a web browser (if HTTP service is available on the Domino Server)
- Using Trend Micro Control Manager (TMCM)

1.4 Configuration

ScanMail for IBM Domino uses a policy-based configuration with only one main policy active, everytime. As shown in **Error! Reference source not found.**1-3.

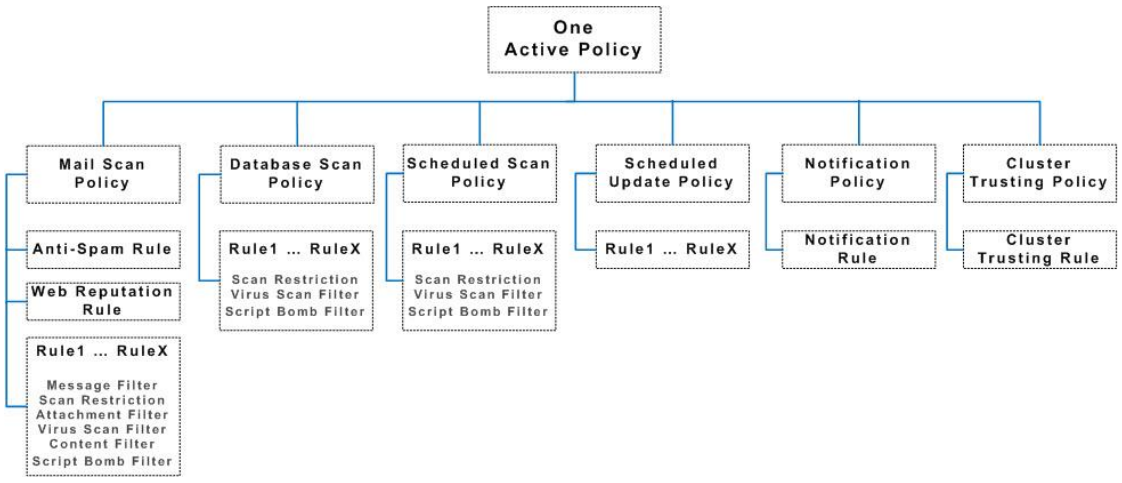


Figure 1-3

Each policy may contain the configuration for the following functions:

Mail Scan	Notification
Database Scan	Scheduled Scan
Scheduled Update	Cluster Trusting

Specific to the scanning related functions, SMID provides the option to define rules for one or more supported filters:

Anti-spam	Attachment Filter
Web reputation	Virus Scan Filter
Message Filter	Content Filter
Scan Restriction	Script Bomb Filter

1.5 ScanMail for IBM Domino Editions

There are two editions of ScanMail for IBM Domino depending on its Activation Code (AC)

- Standard – provides the basic protection for Domino Servers
- Suite – provides the Standard protection plus anti-spam, web reputation and content filtering

Their differences are mainly on the available scanning filters as shown in Table 1-1.

Features	Standard	Suite
Anti-spam		✓
Web reputation		✓
Message Filter	✓	✓

Features	Standard	Suite
Scan Restriction	✓	✓
Attachment Filter	✓	✓
Virus Scan Filter	✓	✓
Content Filter		✓
Script Bomb	✓	✓
Component Update	✓	✓
Logs and Notification	✓	✓
Control Manager integration	✓	✓

Table 1-1 ScanMail for IBM Domino editions feature list

Chapter 2: Deploy on Windows Platform

2.1 Recommended System Requirements

The Figure 2-1 lists the hardware and software requirements for ScanMail for IBM Domino 5.6 SP1 for Windows.

Hardware / Software	***Requirement***
Processor	Intel™ Pentium™ or higher and compatibles (32-bit and 64-bit chips as appropriate), or equivalent
Memory	• 512-MB minimum • 512-MB or more recommended per CPU
Disk Space	1.5-GB minimum per partition
Disk swap space	Twice the physical RAM installed
Protocols	• NetBIOS over IP (32-bit processor only, only Microsoft IP is supported) • NetBIOS over IPX (32-bit processor only) • TCP/IP (includes IPv6)
Domino Server	• Lotus Domino 8.0.1 (32/64-bit) • Lotus Domino 8.0.2 (32/64-bit) • Lotus Domino 8.5 (32/64-bit) • Lotus Domino 8.5.2 (32/64-bit) • Lotus Domino 8.5.3 (32/64-bit) • IBM Domino 9.0 (32/64-bit) • IBM Domino 9.0.1(32/64-bit)
IBM Notes	• Lotus Notes 8.0.1 • Lotus Notes 8.0.2 • Lotus Notes 8.5 • Lotus Notes 8.5.2 • Lotus Notes 8.5.3 • IBM Notes 9.0 • IBM Notes 9.0.1

Hardware / Software	Requirement
Platform	• MS Windows 2003 Server Standard Edition • MS Windows 2003 Server Enterprise Edition Service Pack 2 • MS Windows 2003 Server • MS Windows 2008 Server • MS Windows 2008 R2 Service Pack 1 • MS Windows 2008 R2 Server • MS Windows 2012 Server • MS Windows 2012 R2 Server • MS Windows 2016 Server
Browser	• Microsoft Internet Explorer 6.0 Service Pack 2 • Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0 • Microsoft Internet Explorer 9.0

Figure 2-1

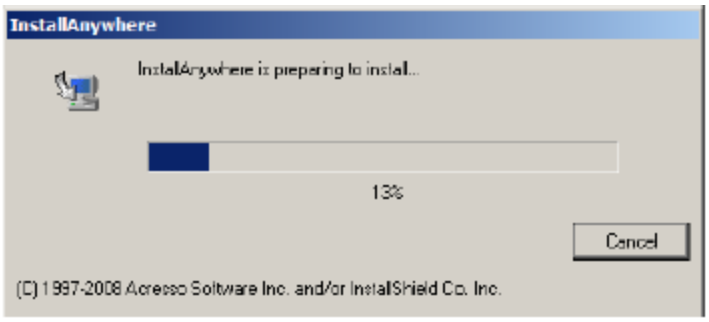
2.2 Pre-installation Tasks

Before installing SMID, perform the following tasks:

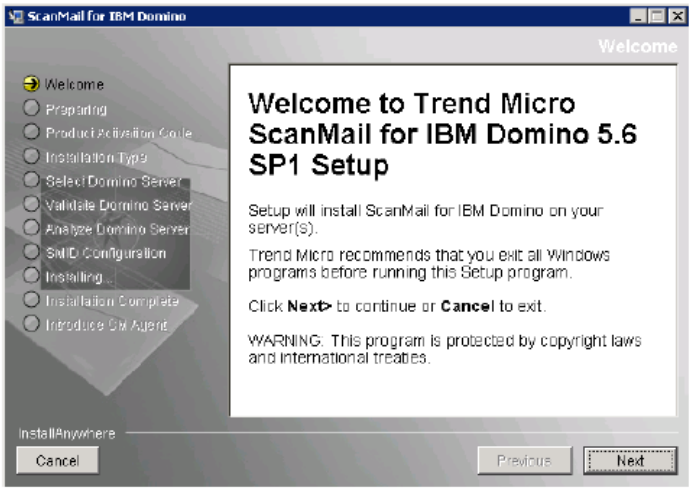
1. Log on to the Windows platform as administrator.
2. Determine the **notes.ini** location(s) (including its location on partitioned servers, if applicable).
3. Determine the Domino Data and Domino Binary paths.
4. Ensure that the user/group that has the administrator authority used to manager the SMID database exists. The default group is **LocalDomainAdmins**.
5. Check the available disk space to verify there is at least 1.5GB of free space.
6. Close any open Notes Clients.
7. Close any open Notes account sessions.
8. Shut down all Domino servers.
9. Prepare the SMID activation Code.
10. Make sure the network connection between domino server and TMCM/Global AU (http://smid56-p.activeupdate.trendmicro.com/activeupdate/) is good.

2.3 Installing SMID for Windows

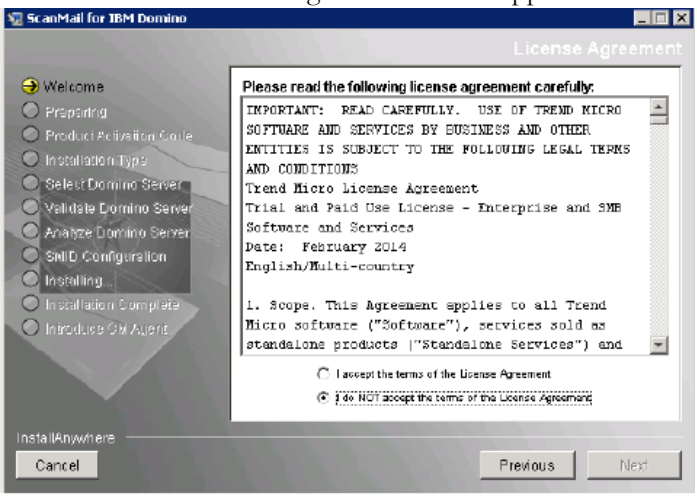
1. To navigate to the Setup program, double-click **setup.exe**
   The InstallAnywhere screen appears followed by the SMID install screen.



2. After the SMID installAnywhere screen completes its progress, the SMID welcome screen appears.

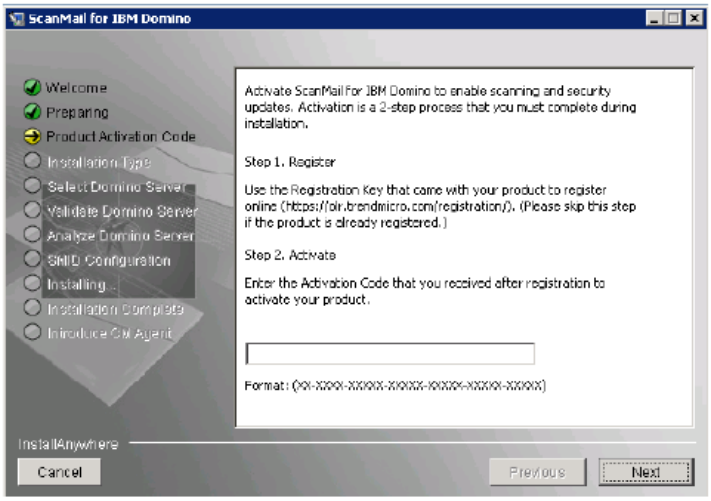


3. Click **Next**. The License Agreement screen appears.



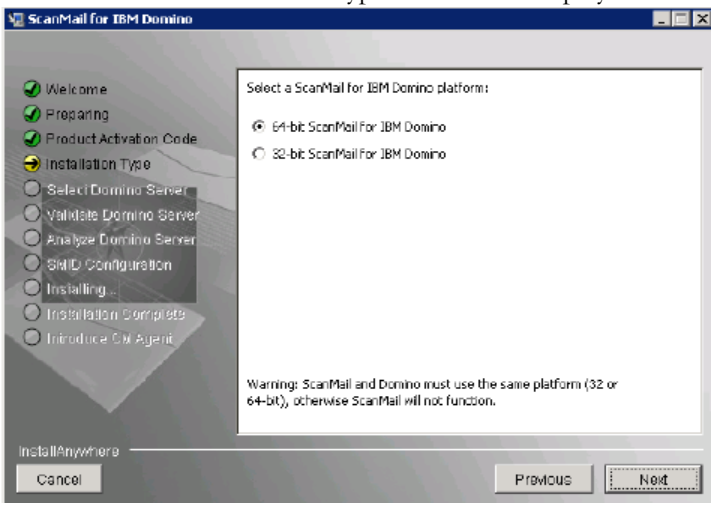
Select **I accept the terms of the license agreement** to continue with the SMID installation. If you do not agree with the terms of the license, click **I do NOT accept the terms of the license agreement,** the installation then stops.

4. Click **Next.** The Product Activation Code screen then displays. Enter the correct SMID activation code to activate SMID.



NOTE Without a correct activation code, the SMID scan or update task will not load. Make sure that the license is correct or activate SMID immediately after installation to protect your Domino environment.

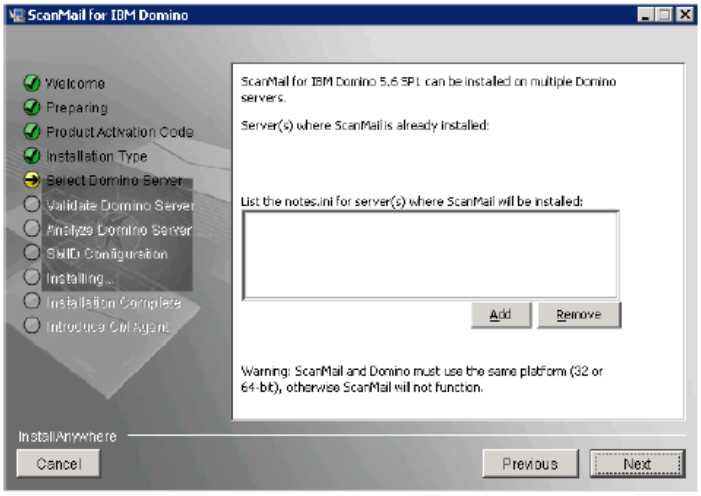
5. Click **Next**. The Installation Type screen then displays.



WARNING! The Domino server platform must match the SMID installation type. Otherwise, SMID will not function.

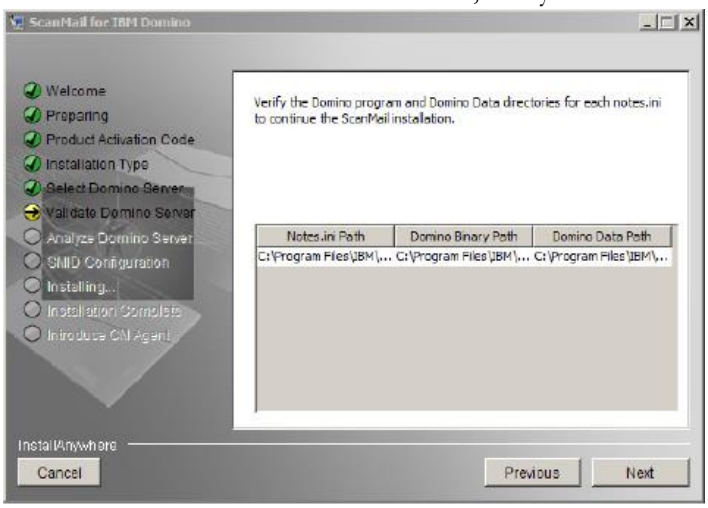
NOTE You can check the Domino sysinfo file to confirm the Domino platform version. The default path is: /domino/data/IBM_TECHNICAL_SUPPORT

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

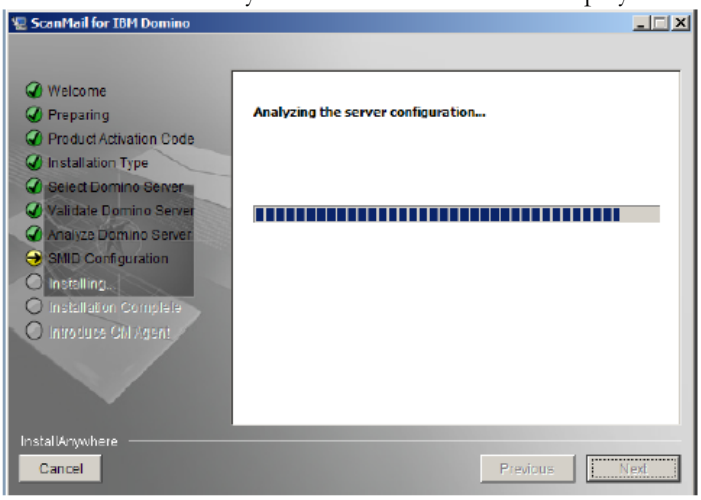


NOTE If you have a partitioned server, install SMID on the partitions that you want to protect.

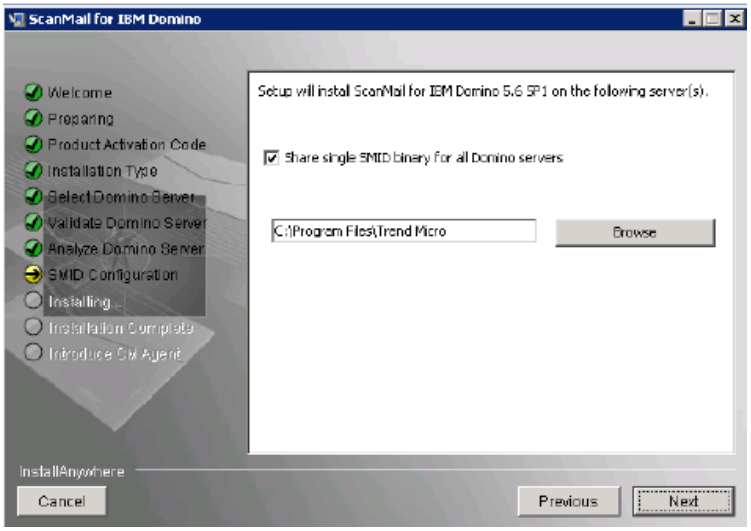
7. From the Validate Domino Server screen, verify the Domino and data directories path.



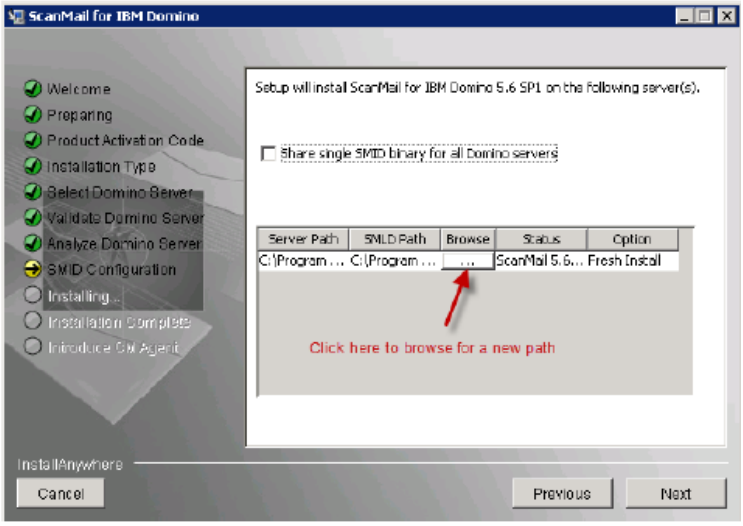
8. Click **Next**. The Analyze Domino Server screen displays.



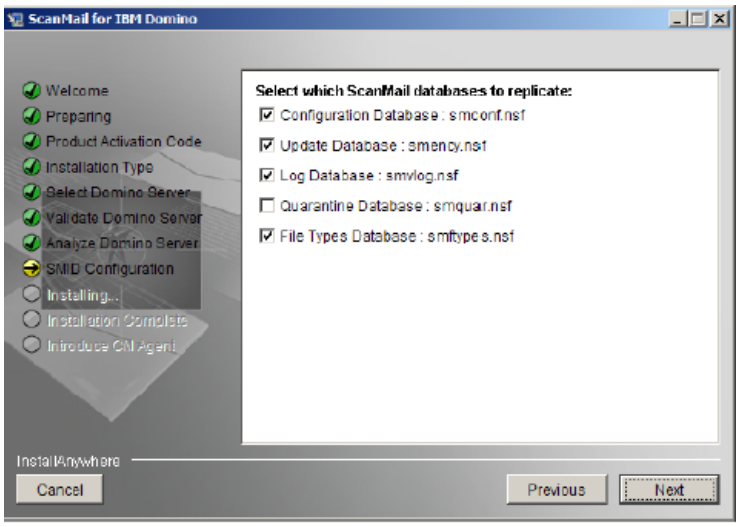
9. After the configuration analysis screen progress completes, click **Next**. The SMID configuration screen displays.



10. From the SMID configuration screen, type or browse for the location to install ScanMail for IBM domino. If you clear the **Share single SMID binary for all Domino servers** option. The screen will appear as shown below:

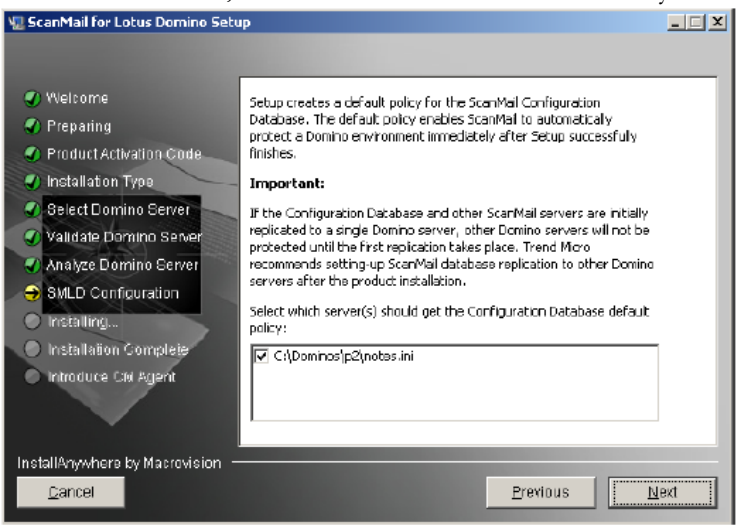


11. Click **Next.** The Database Replication Selection screen appears.
By default, Setup enables replicating all databases except for the Quarantine database. If you want to change the default settings, select or deselect the SMID databases you would want Setup to replicate.

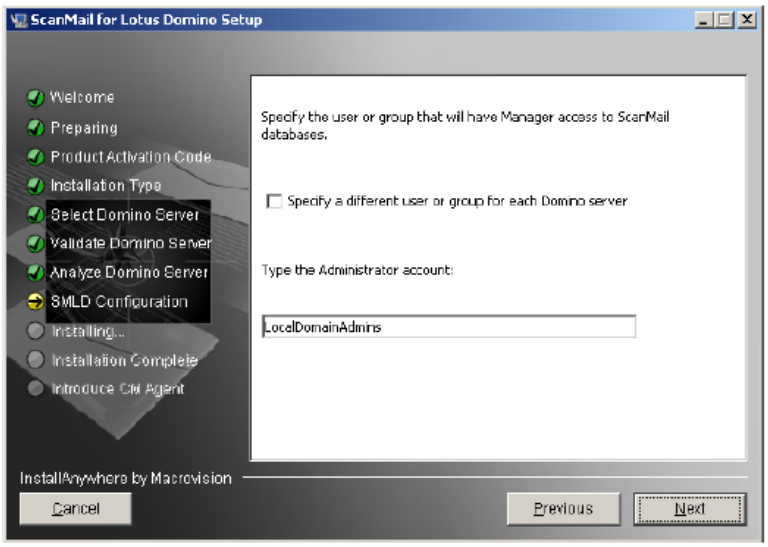


If you plan to install SMID on several servers and replicate databases, you may want to disable replication of the configuration database on subsequent servers. Select one server as the primary or administrative server to replicate it to all other servers.

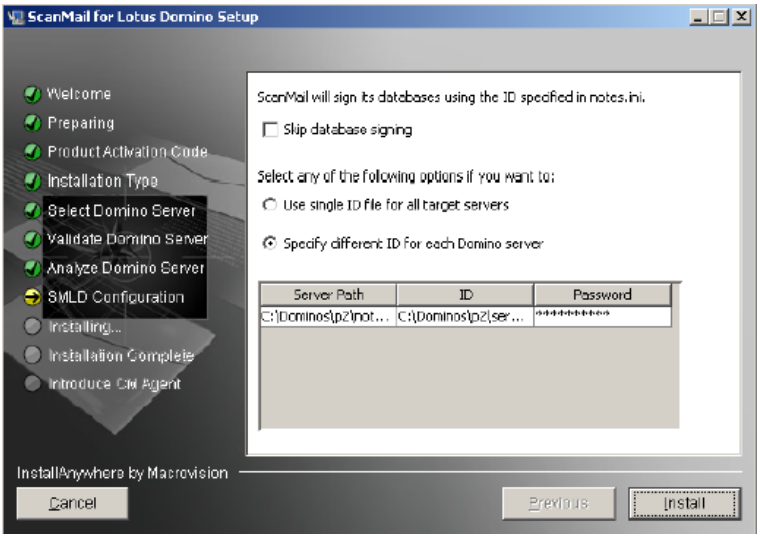
12. Click **Next.** The default Policy Selection screen appears. Select which server(s) should get the default policy. If there are server(s) with ScanMail installed and the configuration database is being replicated, you may skip this option on subsequent installations.
    A single ScanMail server,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



13. Click **Next.** The ScanMail Administrator screen appears.

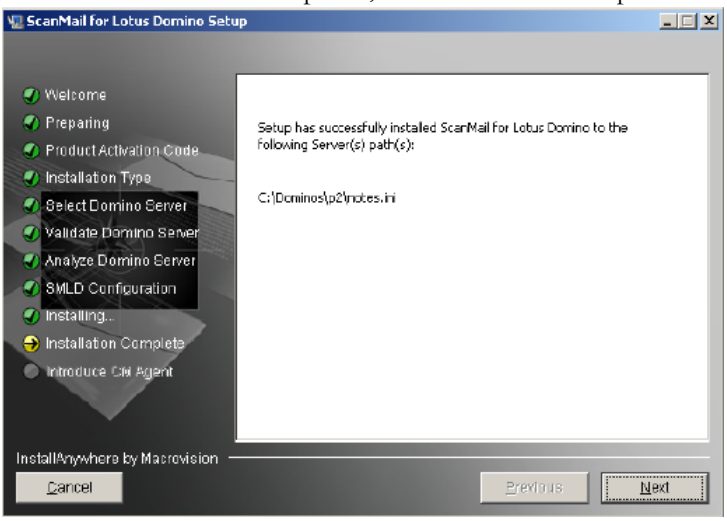


14. Click **Next**. The ScanMail Database Signing screen appears:
    - Select **Skip database signing** to prevent setup from signing ScanMail databases. You can sign the databases manually after the installation.
    - Select **Use single ID file for all target servers** to sign ScanMail databases with a single ID.
    - Select **Specify different ID for each Domino server** to sign ScanMail databases on each Domino server with a different ID.



15. Click **Install**. The installation begins.

16. After the installations completes, the Installation Complete screen displays.



17. Click **Next**. The Introduce CM Agent screen displays.
18. Click **Done** to close the setup screen.

Chapter 3: Deploy on Linux Platform

3.1 Recommended System Requirements

Hardware / Software	***Requirement***
Processor	Intel™ Pentium™ 4 Processor 1.3-GHz or higher
Memory	• 512 MB minimum • 512 MB or more recommended per CPU
Disk Space	• 1.5-GB minimum per partition • 500-MB for program files • 450-MB for the `/tmp` folder
Disk swap space	• Equal to the physical RAM installed required • Twice the physical RAM installed recommended
Protocols	TCP/IP (includes IPv6)
Domino Server	• Lotus Domino 8.0.1 32-bit • Lotus Domino 8.0.2 32-bit • Lotus Domino 8.5 32-bit • Lotus Domino 8.5.1 32-bit • Lotus Domino 8.5.2 32-bit • Lotus Domino 8.5.3 32-bit • IBM Domino 9.0 32-bit/64-bit • IBM Domino 9.0.1 32-bit/64-bit
Lotus Notes	• Lotus notes 8.0.1 • Lotus notes 8.0.2 • Lotus notes 8.5 • Lotus notes 8.5.1 • Lotus notes 8.5.2 • Lotus notes 8.5.3 • IBM notes 9.0 • IBM notes 9.0.1
Platform	• Novell SUSE Linux Enterprise Server (SLES) 10 • Novell SUSE Linux Enterprise Server (SLES) 11 • Novell SUSE Linux Enterprise Server (SLES) 12 • Red Hat Enterprise Linux (RHEL) 5 • Red Hat Enterprise Linux (RHEL) 6 • Red Hat Enterprise Linux (RHEL) 7
Browser	• Microsoft Internet Explorer 7.0 • Microsoft Internet Explorer 8.0
Trend Micro Control Manager	• Trend Micro Control Manager 5.0 with patch 8 • Trend Micro Control Manager 5.5 with hotfix 1273 • Trend Micro Control Manager 6.0
Other	• compat-libstdc++-33-3.2.3-69.el6.i686.rpm (on RHEL6 64-bit) • glibc-2.12-1.107.el6.i686.rpm (on RHEL6 64-bit) • nss-softokn-freebl-3.12.9-11.el6.i686.rpm (on RHEL6

	64-bit)

3.2 Pre-installation Tasks

Before installing SMID, perform the following tasks:

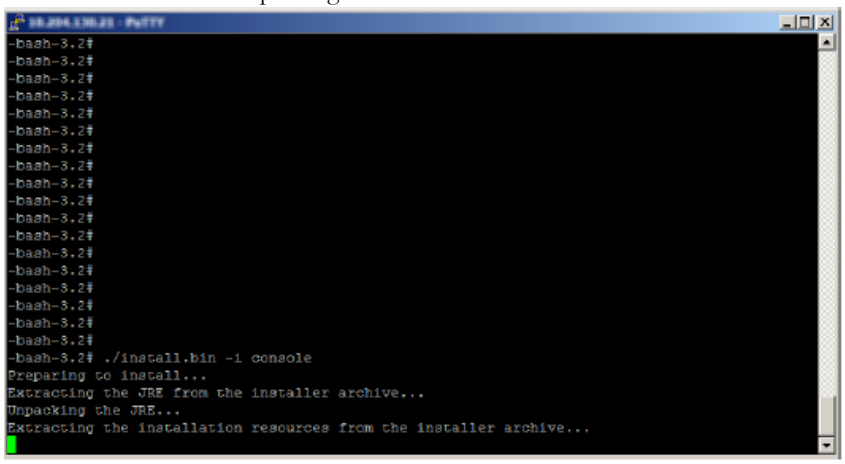
1. Log on to the Linux platform as root user.
2. Determine the **notes.ini** location(s) (including its location on partitioned servers, if applicable).
3. Determine the Domino Data and Domino Binary paths.
4. Ensure that the user/group that has the administrator authority used to manage the SMID database exists. The default group is **LocalDomainAdmins**.
5. Check the available disk space to verify there is at least 1.5GB of free space.
6. Close any open Notes Clients.
7. Close any open Notes account sessions.
8. Shut down all Domino servers.
9. Prepare the SMID activation Code.
10. Make sure the network connection between the Domino server and TMCM/Global AU (http://smid56-p.activeupdate.trendmicro.com/activeupdate/) is good.

3.3 Installing SMID for Linux

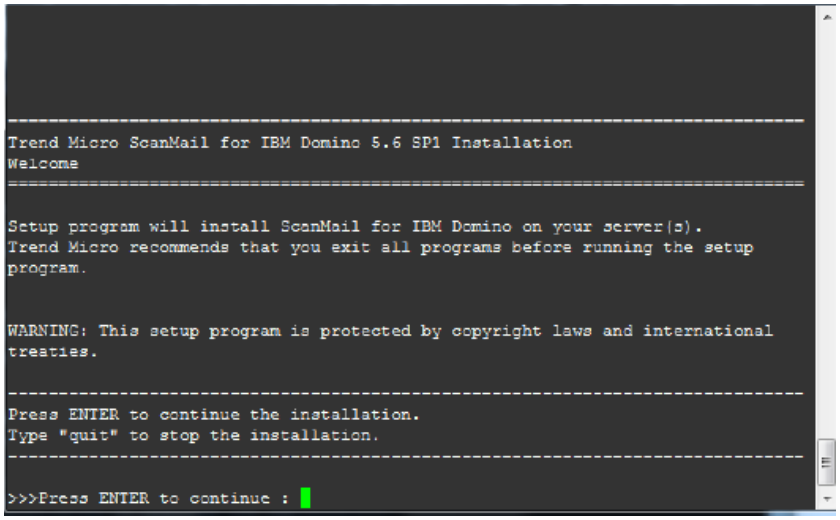
To install SMID for Linux, perform the following steps:

1. Open Terminal. To navigate to the installation program, do one of the following:
   - If you are installing from the Trend Micro Enterprise Protection CD, navigate to the SMID folder on the CD.
   - If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your server.
2. To make sure that the ***install.bin*** file has the execution privileges, type the following command:
   chmod 755 install.bin

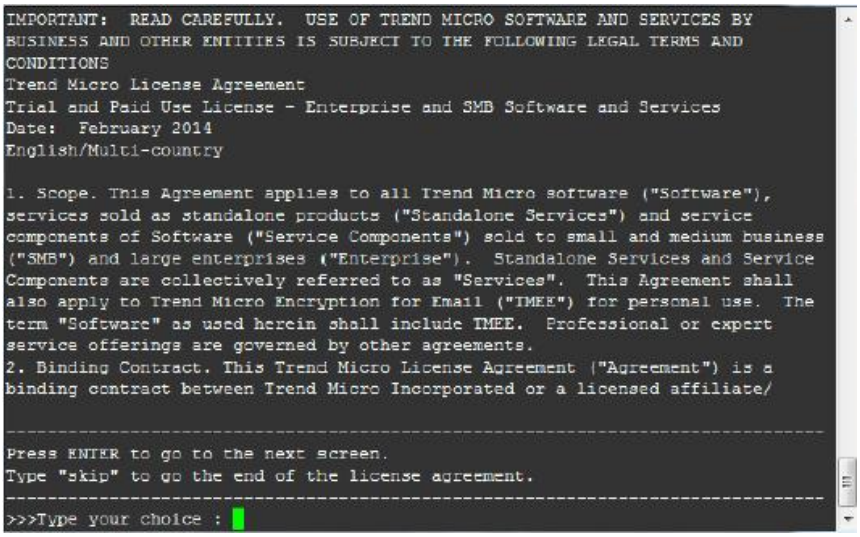
   NOTE If possible, we suggest to use chmod 777 install.bin
3. Run the installation file ***install.bin***, by typing the command:
   ./install.bin -i console
   The installer will start unpacking the file.



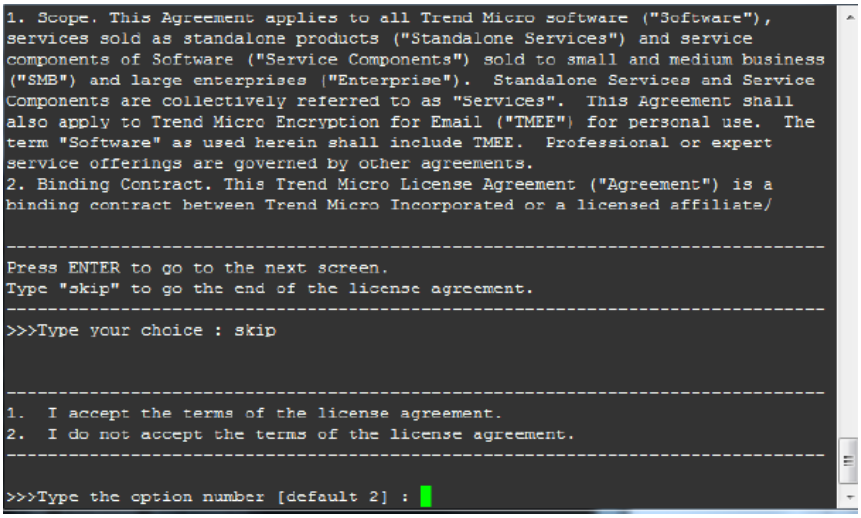
4. After the unpacking of the installation file is complete, the Welcome screen appears.



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

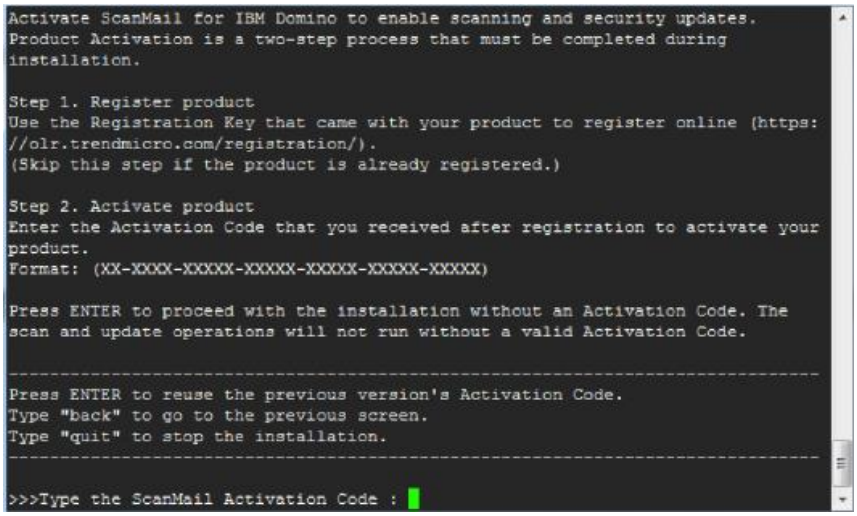


6. On the **Licence Agreement** screen, press **Enter** to continue scrolling on to the next screen of the **License Agreement**.. If you want to move to the end of the agreement, type ***skip*** or ***s*** then press **Enter**.



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

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

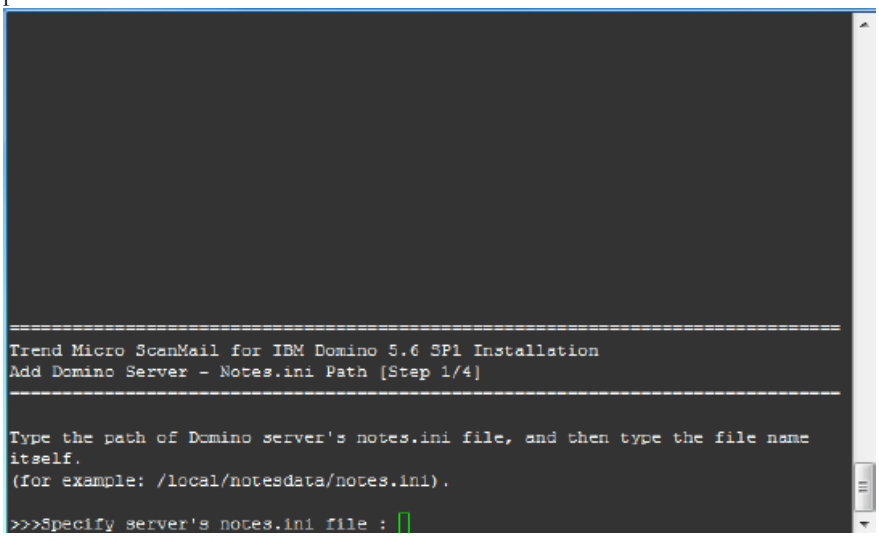


9. On the Product Activation screen, type the correct SMID activation code to activate SMID then press **Enter**.

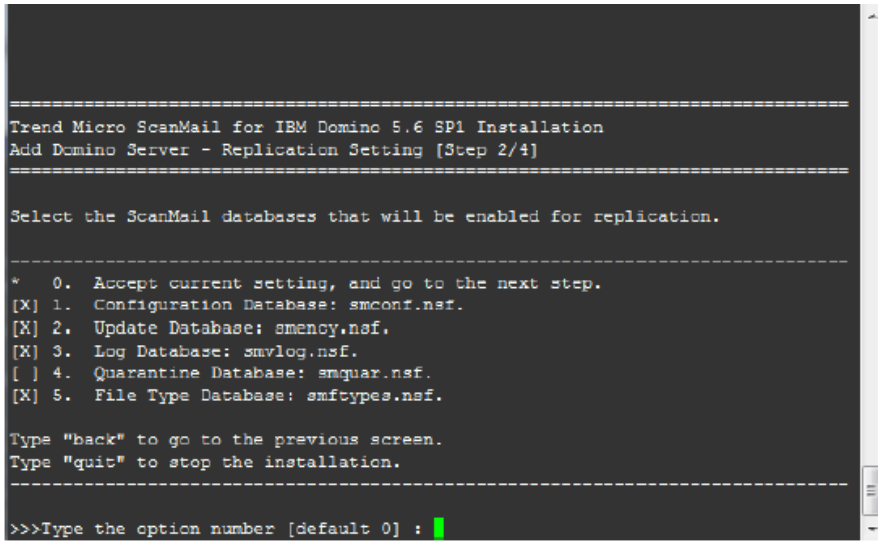
10. On the Add or Remove Domino Server screen, type *1* then press Enter to add the ***notes.ini*** server where you want to install SMID.

> **NOTE** If you have a partitioned server, install SMID on the partitions that you want to protect. The Accept current setting, and go to the next step option will start the installation of the selected Domino server (***notes.ini***). If you have not selected at least one ***notes.ini***, Accept current setting, and go to the next step option would be ineffective. You must select at least one Domino server (***notes.ini***) before starting the installation process.

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



b. Press Enter. The Add Domino Server - Replication Setting [Step 2/4] screen appears.



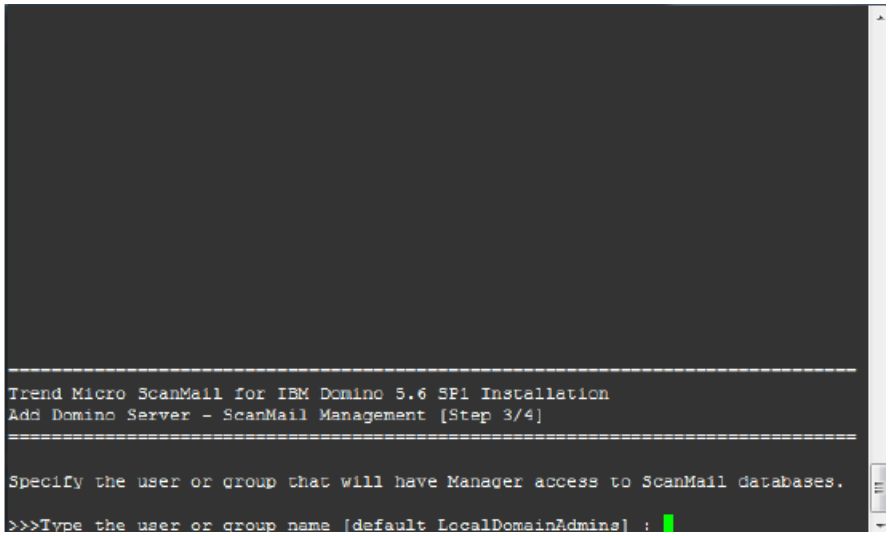
By default, Setup enables replicating all databases except for the Quarantine Database. If you want to change the default settings, select or deselect the SMID databases that you would want Setup to replicate or ignore. To select or deselect SMID database, do the following:

(1) Type the corresponding option, choose from numbers *1* ~ *5* (For example, if you want to select Quarantine Database, type *4*.).

(2) Press Enter.

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

c. Press Enter. The Add Domino Server - ScanMail Management [Step 3/4] screen appears.

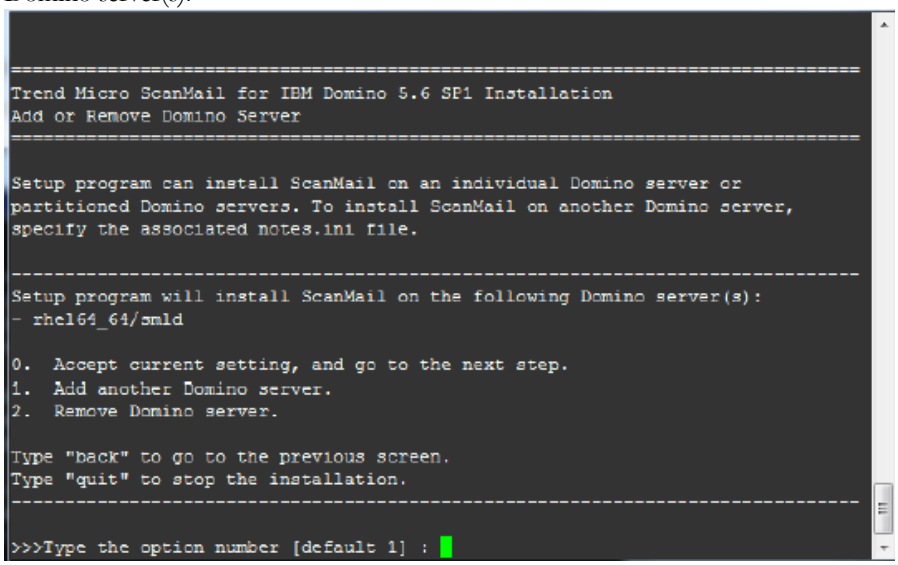


The default administrator group is LocalDomainAdmins. If you want to specify another user or group for administration tasks, type a single administrator account or group that will have Manager access to all SMID databases.

d. Press Enter. The Add Domino Server - Install Path [Step 4/4] screen appears.

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

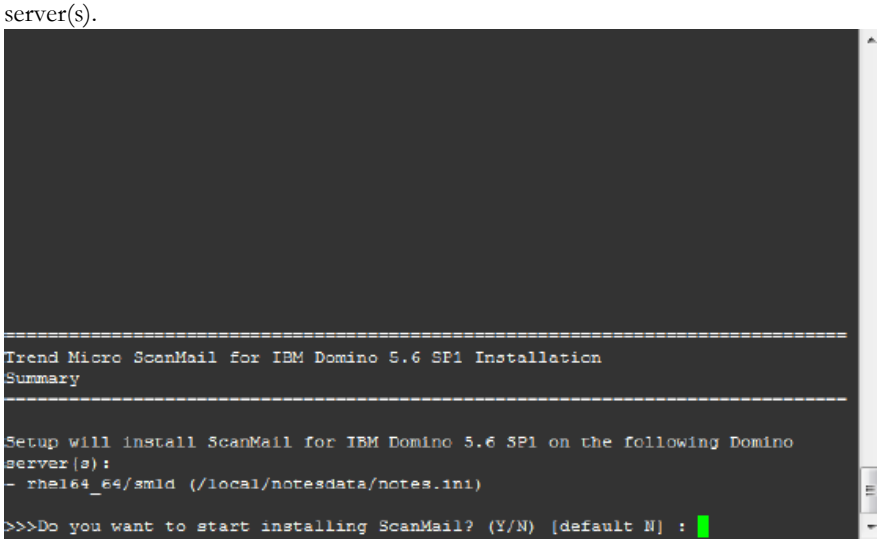
e. After typing the installation path, press Enter. The selection of one Domino Server completes and the Add or Remove Domino Server screen will appear again, displaying the list of selected Domino server(s).



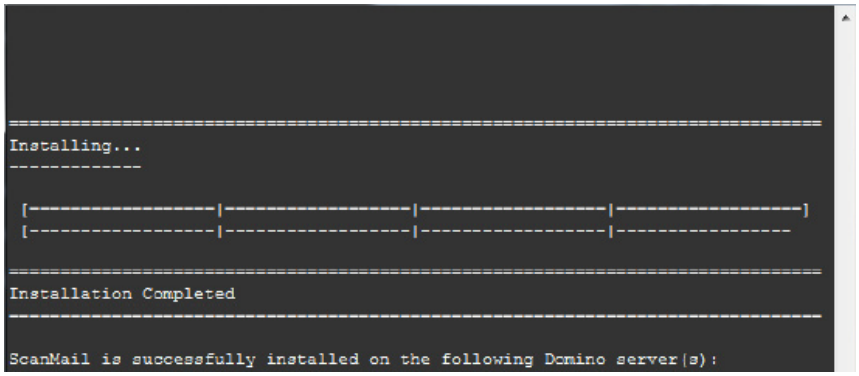
On the Add or Remove Domino Server screen, select one the following:

- Type *0* (zero) to select the current settings and start the installation of selected Domino server(s).
- Type *1* to add another Domino server (***notes.ini***) then follow the substep of step 10.
- Type *2* to remove the previously selected Domino server(s).

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



12. Press Enter. The installation begins. After that, the **Installation Complete** message displays on the screen.


Installing...
[----------|----------|----------|----------]
Installation Completed
ScanMail is successfully installed on the following Domino server(s):

Chapter 4: Deploy on AIX Platform

4.1 Recommended System Requirements

Hardware / Software	***Requirement***
Processor	Power 4 and higher
Memory	• 512 MB minimum • 512 MB or more recommended per CPU
Disk Space	• 1.5-GB minimum per partition • 500-MB for program files • 450-MB for ***/tmp*** file system
Disk swap space	• Equal to physical RAM installed required • Twice the physical RAM installed recommended
Protocols	• TCP/IP (includes IPv6)
Domino Server	• Lotus Domino 8.0.1 64-bit • Lotus Domino 8.0.2 64-bit • Lotus Domino 8.5 64-bit • Lotus Domino 8.5.1 64-bit
Lotus Notes	• Lotus notes 8.0.1 • Lotus notes 8.0.2 • Lotus notes 8.5 • Lotus notes 8.5.1
Platform	• 64-bit IBM AIX 5.3, TL7 0815 (5300-07-04-0815) • 64-bit IBM AIX 6.1, Service Pack 4, APAR • 64-bit IBM AIX 7.1 IZ10223, APAR IZ09961, APAR IZ10284, APAR IZ08022
Trend Micro Control Manager	• Trend Micro Control Manager 5.5 • Trend Micro Control Manager 6.0
Other	• XL C/C++ runtime lib 9.0.0.1 or later

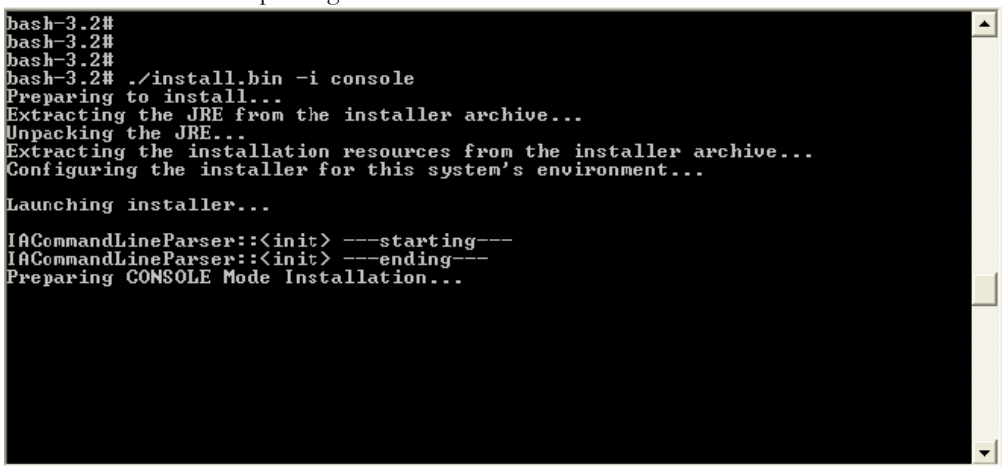
4.2 Pre-installation Task

1. Log on to the AIX platform as root user.
2. Determine the **notes.ini** location(s) (including its location on partitioned servers, if applicable).
3. Determine the Domino Data and Domino Binary paths.
4. Ensure that the user/group that has the administrator authority used to manage the SMID database exists. The default group is **LocalDomainAdmins**.
5. Check the available disk space to verify there is at least 1.5GB of free space.
6. Close any open Notes Clients.
7. Close any open Notes account sessions.
8. Shut down all Domino servers.
9. Prepare the SMID activation Code.
10. Make sure that the network connection between the Domino server and TMCM/Global AU (http://smid5-p.activeupdate.trendmicro.com/activeupdate) is good.

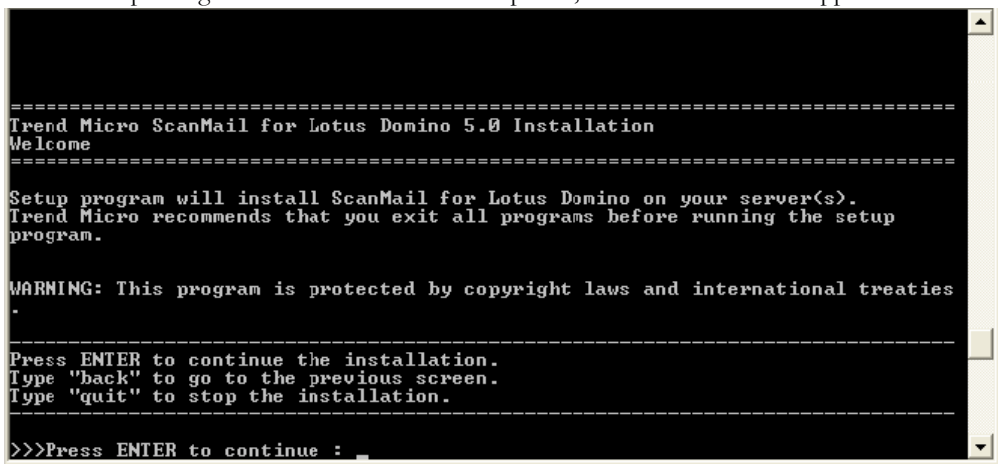
4.3 Installing SMD for AIX

To install SMD for AIX, perform the following steps:

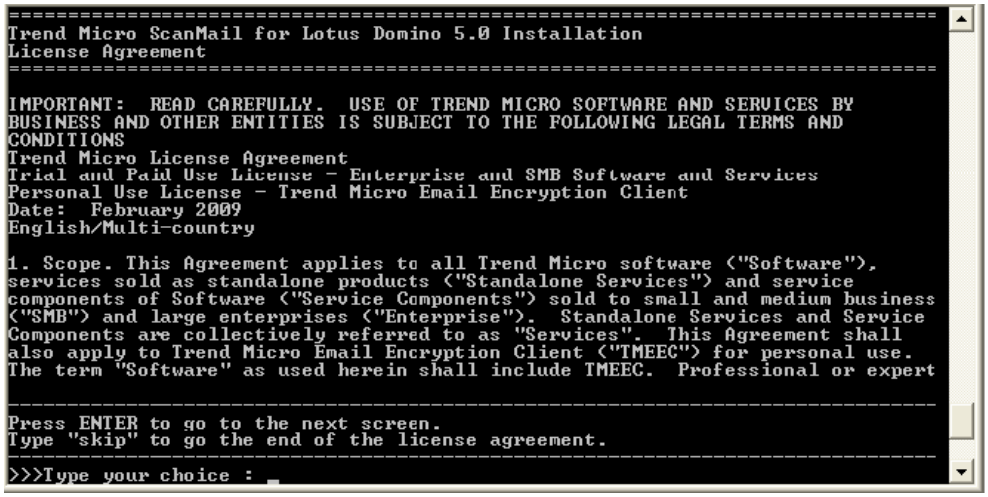
1. Open Terminal. To navigate to the installation program, do one of the following:
   - If you are installing from the Trend Micro Enterprise Protection CD, navigate to the SMID folder on the CD.
   - If you downloaded the software from the Trend Micro Web site, navigate to the relevant folder on your server.
2. Run the installation file (***SMID5SetupAIX.bin***) by typing the following command: **./SMID5SetupAIX.bin -i console**.
   The installer will start unpacking the file.



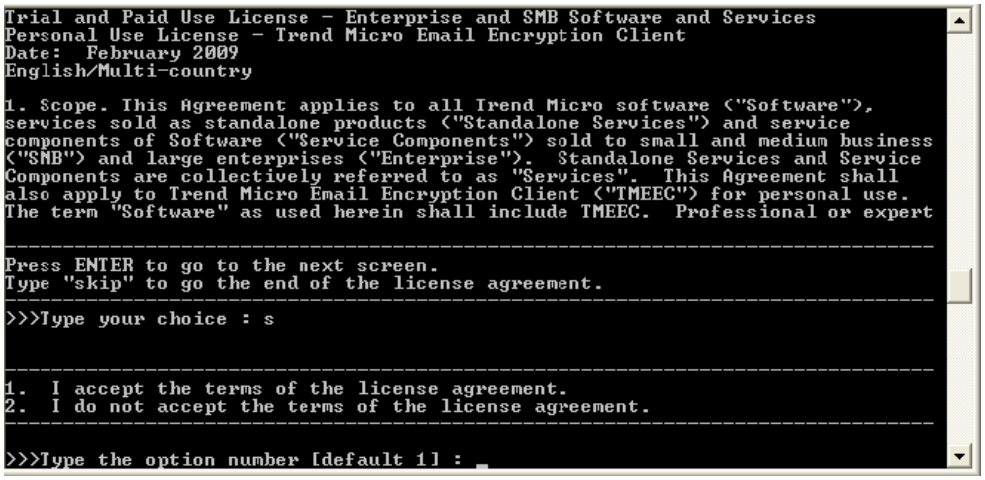
   After the unpacking of the installation file is completed, the **Welcome** screen appears.



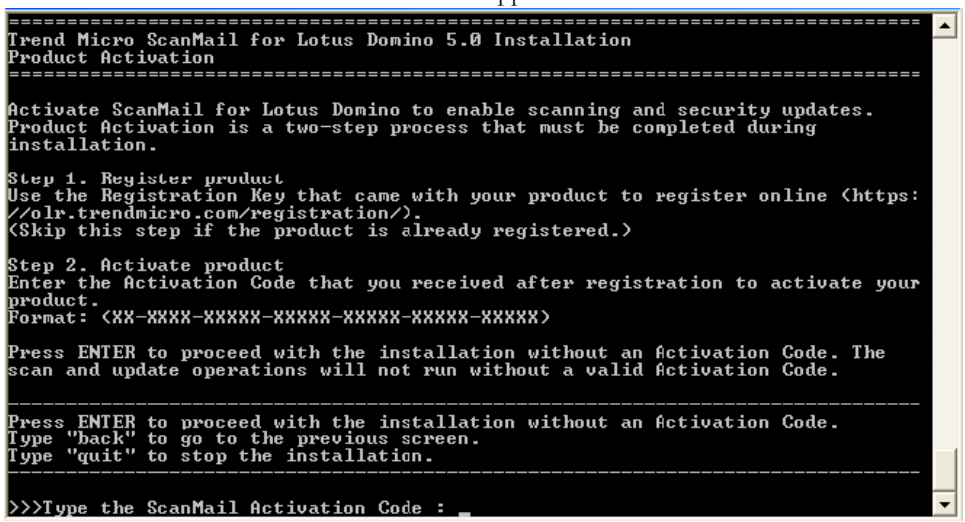
   Press **Enter** to continue the installation. The **License Agreement** screen appears.



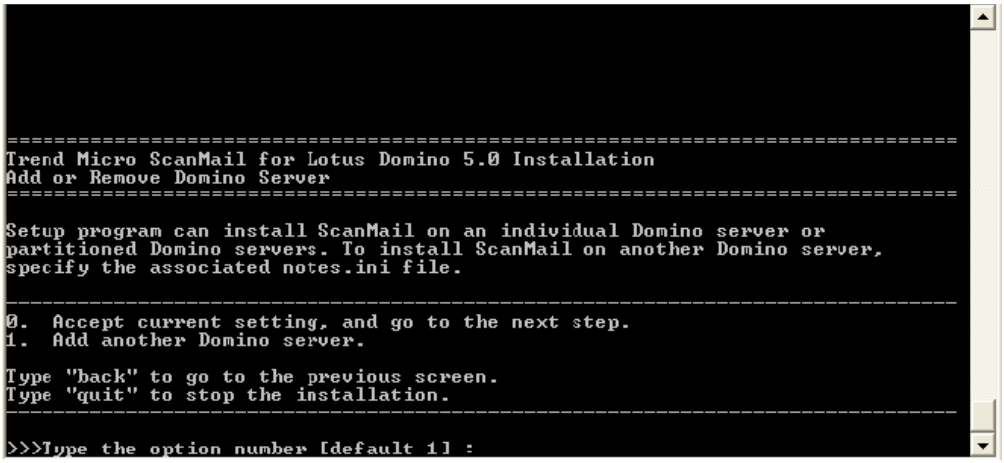
3. On the **License Agreement** screen, press **Enter** to continue to scroll on to the next screen of the **License Agreement**. If you want to move to the end of the agreement, type *skip* or *s* then press **Enter.**



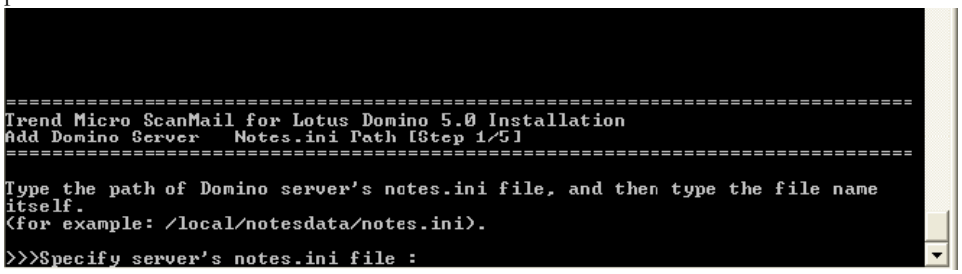
4. At the end of the **License Agreement**, Type *1* if you agree and accept the terms of the license agreement. If you do not agree with the terms of the license, type *2*; the installation then stops after the confirmation.
5. Press **Enter**. The **Product Activation** screen appears.



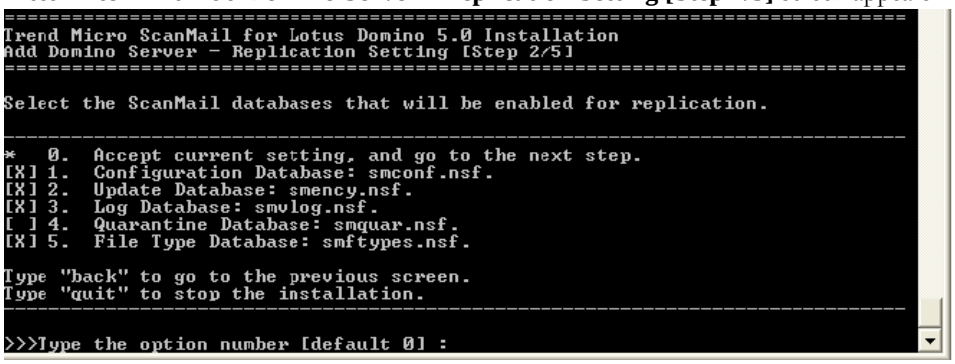
6. On the Product Activation screen, type the correct SMID activation code to activate SMIDthen press **Enter**.
7. On the **Add or Remove Domino Server** screen, type *1* to add the ***notes.ini*** server where you want to install SMID.



a. Press **Enter**. The **Add Domino Server - Notes.ini Path [Step 1/5]** screen appears. Type the path where the ***notes.ini*** file is located.



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

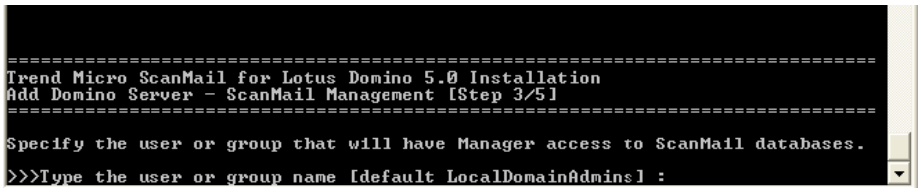


By default, Setup enables replicating all databases except for the **Quarantine Database**. If you want to change the default settings, select or deselect the ScanMail databases that you would want Setup to replicate or ignore. To select or deselect ScanMail database, do the following:

i. Type the corresponding option, choose from numbers *1* ~ *5* (For example, if you want to select **Quarantine Database**, type *4*.).
ii. Press **Enter**.

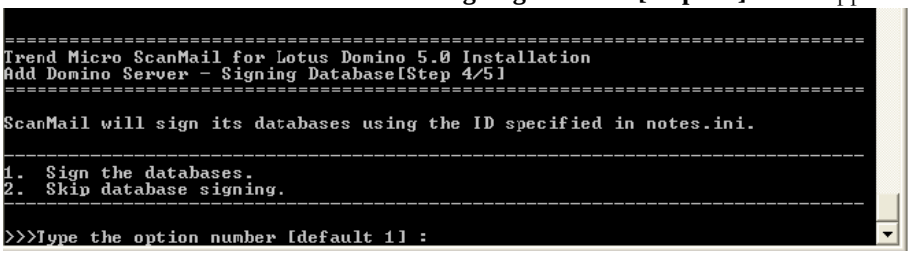
After making your selection, type 0 (zero) to accept the setting then proceed to the next step.

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



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

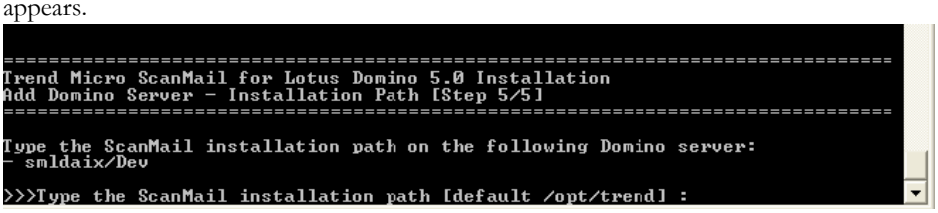
d. Press **Enter**. The **Add Domino Server - Signing Database[Step 4/5]** screen appears.



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

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

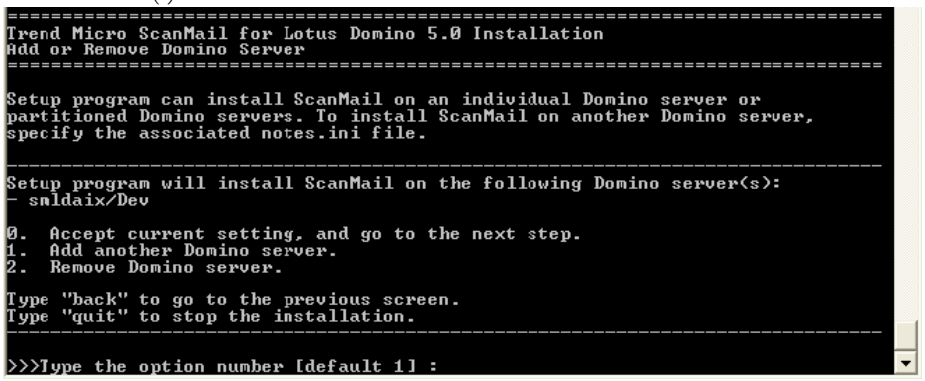
e. After the **Database Signing** screen, the **Add Domino Server - Install Path [Step 5/5]** screen appears.



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

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

f. After typing the installation path, press **Enter**. The selection of one Domino Server completes and the **Add or Remove Domino Server** screen appears again, displaying the list of selected Domino serve(s).



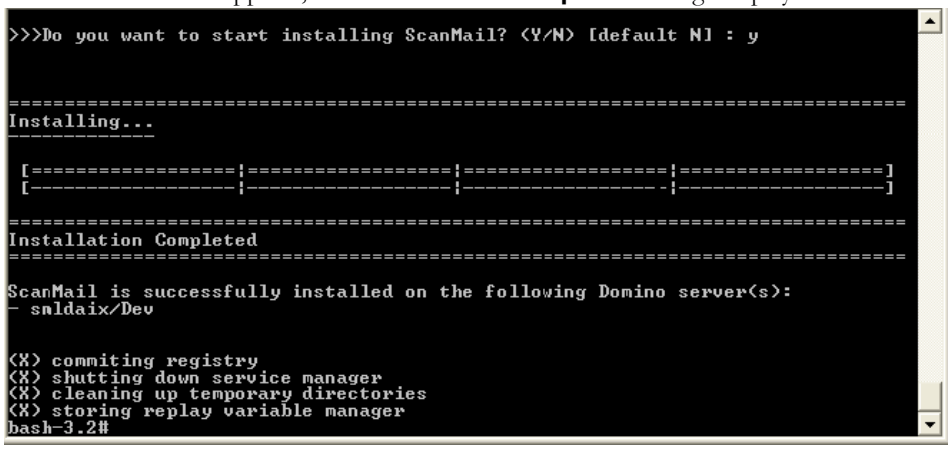
On the **Add or Remove Domino Server** screen, select one the following:

- Type *0* (zero) to select the current settings and start the installation of the selected Domino server(s).
- Type *1* to add another Domino server (***notes.ini***).
- Type *2* to remove the previously selected Domino server(s).

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

9. Press **Enter**. The installation begins.

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



Chapter 5: Troubleshooting

5.1 Manually update components

As a workaround, manually copy the components to SMID to solve the SMID update issue.

5.1.1 How to manually update components for AIX

1. Download the engine and pattern files from the following links:
   http://smid5-p.activeupdate.trendmicro.com/activeupdate/engine/<engine_verion.zip>
   http://smid5-p.activeupdate.trendmicro.com/activeupdate/pattern/<pattern_verion.zip>

   NOTE
   a. You can get the components version from the link: http://smid5-p.activeupdate.trendmicro.com/activeupdate/server.ini
   b. The AU URL is for SMID 5.0
   c. Some engine's address is not http://smid5-p.activeupdate.trendmicro.com/activeupdate/engine/<engine_verion.zip>
   d. For example: http://smid5-p.activeupdate.trendmicro.com/activeupdate/antispam/tmaseng_win32_vs2005_v82-1013.zip , you need confirm this in the server.ini file.

2. Create the following directory:
   a. /opt/trend/SMID/engine/<engine_type>/<engine_version>
   b. /opt/trend/SMID/pattern/<pattern_type>

3. Copy the contents of the extracted <engine_version.zip> to the following directory:
   /opt/trend/SMID/engine/<engine_type>/<engine_version>

4. Copy the contents of the extracted <pattern_version.zip> to the following directory:
   /opt/trend/SMID/pattern/<pattern_type>

   NOTE If you use FTP to transfer the files to AIX machine , use "bin" mode to transfer, otherwise the binary will be corrupted.

5. Run the following command:
   ln -s /opt/trend/SMID/engine/<engine_type>/<engine_version> latest

6. To reload and start the new components, go to the Domino console and run the following command:

tell smdreal reload

7. Do the above steps for the other components.

5.1.2 How to manually update components for Linux

1. Download the engine and pattern files from the following links:
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/engine/<engine_verion.zip>
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/pattern/<pattern_verion.zip>

2. Create the following directory:
   a. /opt/trend/SMID/engine/<engine_type>/<engine_version>
   b. /opt/trend/SMID/pattern/<pattern_type>

3. Copy the contents of the extracted <engine_version.zip> to the following directory:
   /opt/trend/SMID/engine/<engine_type>/<engine_version>

4. Copy the contents of the extracted <pattern_version.zip> to the following directory:
   /opt/trend/SMID/pattern/<pattern_type>

   NOTE If you use FTP to transfer the files to Linux machine , use "bin" mode to transfer, otherwise the binary will be corrupted.

5. To reload and start the new components, go to the Domino console and run the following command :
6. tell smdreal reload Do the above steps for the other components.

5.1.3 How to manually update components for Windows

1. Download the engine and pattern files from the following links:
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/engine/<engine_verion.zip>
   http://smid56-p.activeupdate.trendmicro.com/activeupdate/pattern/<pattern_verion.zip>

2. Create the following directory:
   a. \Trend Micro\ScanMail for Domino\engine\<engine_type>\<engine_version>
   b. \Trend Micro\ScanMail for Domino\pattern\<pattern_type>

3. Copy the contents of the extracted <engine_version.zip> to the following directory:
   \Trend Micro\ScanMail for Domino\engine\<engine_type>\<engine_version>

4. Copy the contents of the extracted <pattern_version.zip> to the following directory:
   \Trend Micro\ScanMail for Domino\pattern\<pattern_type>

5. To reload and start the new components, go to the Domino console and run the following command :
   tell smdreal reload
6. Do the above steps for the other components.

5.2 ScanMail For Domino Database

5.2.1 Databases

During installation, ScanMail for IBM Domino creates ten (10) NSF files which store the product's necessary operational information. SMID's scan settings, pattern and engine details, detection logs, quarantined files, help file and other data are all contained in one of these databases. They are created in a subfolder named *smd* under <Domino data directory>.

File Name	Database Name	Description
SMConf.nsf	Configuration Database	Stores the mail and database scanning settings as well as other configurations that define the product's behavior. **NOTE:** From the Configuration Database, the following databases can also be accessed: Log Database, Quarantine Database and Update Database
SMDApproved.nsf	Approve Database	Stores messages that must be approved by the Administrator before delivery.
SMDDtas.nsf	Deep Discovery Advisor's Quarantine Database	Advance Persistent Threat (APT) Prevention scanner uses the Deep Discovery Advisor Quarantine Database (smddtas.nsf) to temporarily store messages with suspicious attachments. The APT Prevention scanner uploads the suspicious attachments to Deep Discovery Advisor server for analysis and then takes the required pre-configured action based on the scan results.
SMEncy.nsf	Update Database	Stores all the engine, pattern and application files (for example, hotfixes for SMID) that are currently available on the SMID server.
SMFtypes.nsf	File Types Database	Stores all the file types that are recognized by SMID for scanning. It also highlights which among these types may contain a virus.
SMHelp.nsf	Help Database	Stores SMID's help files.
SMMsg.nsf	Message Database	Stores all the messages used by the SMID tasks that can appear either on SMID's console or notification.
SMQuar.nsf	Quarantine Database	Stores mails and attachments that have been quarantined by SMID.

SMTime.nsf	Delay Database	Stores mails whose delivery has been delayed by SMID.
SMVlog.nsf	Log Database	Stores the scan logs and statistics collected by SMID.

Some of the SMID database has a corresponding template file (*.*NTF*). Template files are used to rebuild databases if they get deleted or have become corrupted. These files have the same filename as the database (for example, the template for the configuration database is *smconf.ntf*) and are also stored in the *smd* subfolder.

File Name	Database Name	Description
SMConf.ntf	Configuration Template	Creates configuration database layout
SMDApproved.ntf	Approve Template	Creates approve database layout
SMDDtas.ntf	Deep Discovery Advisor Quarantine Template	Creates Deep Discovery Advisor quarantine database layout
SMEncy.ntf	Update Template	Creates update database layout
SMQuar.ntf	Quarantine Template	Creates quarantine database layout
SMTime.ntf	Delay Template	Creates delay database layout
SMVlog.ntf	Log Template	Creates log database layout

5.2.2 Recovering a Corrupt ScanMail Database

5.2.2.1 Use Domino Command to do the recovery

Type the following command at the Domino server console:

load fixup {database path and file name}

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

load fixup smd\smconf.nsf

5.2.2.2 Use the DB template to recreate the DB

If the ScanMail database becomes corrupted and is irrecoverable, use the corresponding ScanMail database templates to recreate these databases:

NOTE Recreating a ScanMail database does not restore the original database contents. If the corrupted database was the Configuration database, then the Administrator needs to redefine the policies, rules, and filters (or replicate the configuration database from another ScanMail server after the local Configuration Database is

Here's an example for SMConf.nsf database:

1. Open Domino then go to **Admin**>**File**>**Application**>**New**.
2. Specify the New Application Name and Location:
   Server: Your Server
   Title: ScanMail Configuration database
   Fle: smd\smconf.nsf
3. Specify the Template for New Application:
   Server: Your Server
   Template:ScanMail Configuration Database
   (Select the **Show advanced templates** check box.)
4. Click **Ok** to start recreating the DB.
5. Resign the DB if necessary.

5.3 Database Replication

The following table shows the replication ID for SMD major databases:

Database	Replication ID
smconf.nsf	4925408A:003D3550
smency.nsf	852552F9:001E96E4
smftypes.nsf	85256441:00561C7D
smquar.nsf	8525844A:005B4E9F
smvlog.nsf	852773FC:003F7460

The only supported way to change a replica ID within Lotus Notes or Domino is to create a new copy of the database using Notes client. From the File menu, choose **Database** > **New Copy**. This creates a random (based on the current system time) new replica ID for the new database.

Disclaimer:
There are third party applications available on the web that can also change the replica ID of a Notes Database. There are also agent samples and LotusScript code suggestions available on the internet that may be able to accomplish this. However, these applications and agents are not supported by IBM Lotus Technical Support and no recommendations or assistance with their use can be provided.

5.4 Update the SMID License

1. Open the SMID configuration database.
2. Go to **Administration** > **Product License**.
3. On the right pane, open the license profile or create a new license profile.
4. Verify or type in the activation code on the license profile.
5. Click **Save and Close**.
   Note: Do not delete the existing profile yet. Doing this may stop the smdreal task and stop the mail flow.
6. Open the Domino console either on the Domino Administrator or on the CLI itself.
7. Execute the following command:
   tell smdreal status
8. Update the license using the following command:
   tell smdreal checkac
   A confirmation message will appear.
9. Go back to the configuration database then go to **Administration** > **Product License** or go to the Summary Page. The status should be "Activated" and the product should now be licensed for a number of days.
   Note: Click the **Refresh** button if the page has not yet updated. It may take a while to replicate it to other servers.
10. Delete the old license profile.

Appendix Ⅰ: How To Collect SMD Logs

Refer to the following steps to collect the SMID logs:

1. On the Domino console, type the following:
   >start console log
   >te smdreal quit
   >lo smdreal -debug 3
   >lo smdupd -debug 3 (For AU update issue only)
   >lo smdsch -debug 3
2. Reproduce the issue.
3. Provide a zip file containing the following files based on your system:
   - For Linux or AIX users
     - List of Domino data folder (e.g. ls -lsR /local/notesdata/ > domino_listing.txt
     - List of SMD folder (e.g. ls –lsR /opt/trend/SMD/ > trend_listing.txt)
     - <domino_data>notes.ini
     - All <domino_data>/IBM_TECHNICAL_SUPPORT/
     - <domino_data>/smd/smency.nsf
     - <domino_data>/smd/smconf.nsf
     - <domino_data>/smd/smvlog.nsf
     - <domino_data>/smd/smquar.nsf (For spam and blocked email issues only)
     - All <domino_data>/smdtemp/*.dbg
     - /etc/smdsys.ini
     - /opt/trend/SMD/smdins.log
     - /opt/trend/SMD/smdspins.log
     - /opt/trend/SMD/TMPatch.log
     - <SMID installation directory>/program/<version>/AU_Data/AU_Log/TmuDump.txt (For AU update issue only)
     - mail.box and/or database involved in crash
   - For Windows users:
     - List of the Domino data folder (e.g. c:\Domino>dir /s > domino_listing.txt)
     - List of SMD folder (e.g. c:\Program Files\TrendMicro>dir /s > trend_listing.txt)
     - Windows System Information (i.e. msinfo32.exe output in .nfo format)
     - <domino_data>\notes.ini
     - All <domino_data>\IBM_TECHNICAL_SUPPORT/
     - <domino_data>\smd\smency.nsf
     - <domino_data>\smd\smconf.nsf
     - <domino_data>\smd\smvlog.nsf
     - <domino_data>\smd\smquar.nsf (For spam and blocked email issues only)
     - All <domino_data>\smdtmp*.dbg
     - c:\windows\smdsys.ini
     - c:\smdins.log
     - c:\smdspins.log
     - c:\TMPatch.log

- <SMID installation directory>\program\<version>\AU_Data\AU_Log\TmuDump.txt (For AU update issue only)
- mail.box and/or database involved in crash

4. Turn off the debug mode in Domino console using the following commands:
   >stop console log
   >te smdreal quit
   >te smdupd quit (if applicable only)
   >te smdsch quit
   >lo smdreal

Appendix Ⅱ Hidden Key

Here're some SMD related hidden keys in notes.ini:

KeyName	Explanation	Syntax	Available Since
DisableSecureUpdate	For updating engine or pattern from the AU server that does not support secure updates, e.g. locale AU server.	DisableSecureUpdate=1	N/A
SMDDelayMinutesWhenUpdate	Sleep for x minutes before reloading the SMD task.	SMDDelayMinutesWhenUpdate= value	N/A
SMDExcludeFQIN	Disable the checking of FQIN.	SMDExcludeFQIN=1	Release HF4038 for ISD3.0 for Windows
SMDExcludeGlobalDomain	Disable the checking of Global domain	SMDExcludeGlobalDomain=1	Release HF4038 for ISD3.0 for Windows
SMDKeepDebugLogs	Specify the number (x) of days to keep the SMD debug log files in the temp folder before they are purged.	SMDKeepDebugLogs=x Default value =7	Release HF3562 for SMD3.0 for AIX
SMDSkipScanBySize_MB	Pass the mail whose size exceeds the value (x). This valid value varies from 10 to 9999. If the number is smaller than 10 or larger than 9999, SMD sees it as an invalid value. If it is an invalid value, SMD will set this configuration as the default: 0 (disable)	SMDSkipScanBySize_MB=x (Unit:MB)	Release HF3135 for SMD3.0 for Solaris
SMDAttQuarMail	Enable SMD to quarantine the entire email messages instead of only the attachments when email messages trigger the content, attachment, or virus filter's "Quarantine" action.	SMDAttQuarMail=1	Release HF3062 for SMID5.0 for Windows
SMDAutoDebug	To set the ScanMail for IBM Domino debug log to be automatically enabled after the Domino server recovers from stopping unexpectedly.	SMDAutoDebug=1 By default this key is disabled and is set to "0"	Release HF3073 for SMID5.0 for AIX
SMDWriteOSEventLog	To enable SMDreal to record the SMID malicious violation log on Windows application event log as well as on smvlog.nsf	SMDWriteOSEventLog=1	Release HF3091 for SMLID5.0 for Windows
SMDSPAMLog	To enable TMASE engine logging.	SMDSPAMLog=1	Release Patch3 for SMID5.0 for Windows
SMDCMLogInterval	To enable users to set the interval with which SMID 5.0 communicates with TMCM server when the malicious logs has been generated by SMID.	SMDCMLogInterval=x Where "x" is the preferred interval period in seconds. You can set this value between 1 and 3600. (Unit:Second)	Release HF3094 for ISLD5.0 for Windows

BYPASS_RESEND_ UNSCANNABLE_ ATTACHMENT	To enable ScanMail for IBM Domino to not scan the mail that was resent from the quarantine database after the mail was filtered by Scan Restriction.	BYPASS_RESEND_ UNSCANNABLE_ATTACHMENT=1	Release HF3115 for SMID5.0 for AIX
SMD_MAX_SCAN_URLS	Allows users to specify the number of URLs that ScanMail for Domino should scan in each email message.	SMD_MAX_SCAN_URLS=5	Release HF3404 for SMID5.6
SMD_UPD_START_NEW _SCANNER	Sometimes, SMDreal processes stop unexpectedly during pattern updates. This issue is more likely to affect 32-bit Windows systems than 64-bit systems.	SMD_UPD_START_ NEW_SCANNER =1	Release Patch 6 for SMID5.0
TMUFEDebug	Enables the eManager debug log.	TMUFEDebug=x where X: 1 – Show all fatal information 2 – Show all error information 3 – Show all warning information 4- Show detailed information 5 – Show detailed debug information NOTE: To trigger TMUFE debugging, nSMDreal must be loaded with the –debug option	N/A
CMDebug	Enables the CM Agent debug log.	CMDebug=x where X: 1 – Show all fatal information only 2 – Show abbreviated debug information 3 – Show detailed debug information	N/A
eManagerDebugEnabled	Enables the eManager debug log.	eManagerDebugEnabled=1	N/A
SMDEMDEBUG	Enables the Extension Manager and EMFilter debug log.	SMDEMDEBUG =1	N/A

Appendix III Auto-Generated Key

KeyName	Explanation	Syntax	Available Since
ScanMailInstallPath	The install Path for SMD.	ScanMailInstallPath=%Path	N/A
SMDSkipTaskList	Enables SMD to skip the event of the task.	SMDSkipTaskList=%TaskName	N/A
SmStopMail	Enables SMD to hold messages in MAIL.BOX until they can be scanned by the Real-Time Scanner.	SmStopMail=1	N/A
EXTMGR_ADDINS	Enables the functionality of the Extension Manager plug-in.	EXTMGR_ADDINS=SMDex	N/A
ServerTasks	Enables the add-in server tasks to automatically start and be terminated together with the Domino Server.	ServerTasks=%TaskName	N/A
TrustedServerList	This parameter contains a list of servers belonging to the same cluster and is checked by the Extension Manager (nSMDext). When the Real-time Scanner starts up, it reads the setting inside smconf.nsf to determine if Cluster Trusting is enabled or not. If it is, it writes an entry in the notes.ini called TrustedServerList.	TrustedServerList=%server_name	N/A