TREND MICRO™

Securing Your Web World

Trend Micro LeakProof 3.0

Evaluator’s Guide

ENTERPRISE TECHNICAL MARKETING

Revision History

Rev. No.	Publication Date	Change Description
1	12 February 2008	Initial publication.

Contents

About This Document 1
Introduction to Trend Micro LeakProof 3.0 1
Evaluator's Guide Requirements 1
Assumptions 2
Sample Data Set 2
LeakProof 3.0 Scenarios List 2
Exploration 4
LeakProof 3.0 Evaluation Scenarios 5
A: Protecting Sensitive Company Data Using LeakProof 3.0 5
Scenario A1 — Sending a sensitive document to an external email address using company email 5
Scenario A2 — Copying and pasting a sensitive document and sending it to an external email address using company email 6
Scenario A3 — Sending part of a sensitive document to an external email address using company email 6
Scenario A4 — Copying the content of a sensitive document into an email and sending it to an external email account using a company email address 7
Scenario A5 — Sending a sensitive document to an external email address using Webmail 7
Scenario A6 — Sending a sensitive document to an external email account using Webmail 8
Scenario A7 — Copying part of a sensitive document, pasting the content into a new document and sending the document to an external email account using Webmail 8
Scenario A8 — Copying part of a sensitive document, pasting it in an email and sending the mail to an external email account using a company email address 9
Scenario A9 — Copying a sensitive document to an external USB storage device 9
Scenario A10 — Copying non-sensitive data document to an external USB storage device 10
Scenario A11 — Viewing a clients' notifications during violations 10
Scenario A12 — Viewing the LeakProof 3.0 server's notifications during violations 10
Scenario A13 — Verifying that LeakProof 3.0 client files are hidden from users 11
Scenario A14 — Viewing the size of LeakProof 3.0 Fingerprints 11
Scenario A15 — Enable/Disable Devices 12
B: Protecting Unstructured Sensitive Data Using Fingerprints 13
Scenario B1 — Adding Sensitive Information Classifications 13
Scenario B2 — Entering sensitive document definitions 14
Scenario B3 — Adding sensitive documents source definitions 15
Scenario B4 — Create a Security Policy 16
Scenario B5 — Validate your Configuration 16
C: Protecting Sensitive Structured Data Using Entities 17
Scenario C1 — Using the Entity Definitions page to add or edit new entities 17
Scenario C2 — Creating a Security Policy 18
Scenario C3 — Creating a Matching Level Rule 18
Scenario C4 — Validating your LeakProof 3.0 Configuration 18
D: Protecting Sensitive Structured Data Using Category Definitions 19
Scenario D1 — Adding a Category Definition 19
Scenario D2 — Creating a Security Policy 20
Scenario D3 — Creating a Matching Level Rule 20
Scenario D4 — Validating your LeakProof 3.0 Configuration 20
E: Using LeakProof 3.0 Reporting 21
Scenario E1 — Adding a New Report 21
Scenario E2 — Alternate Definition 22
F: Administering LeakProof 3.0 23

Scenario F1 — Monitoring Server Status 23
Scenario F2 — Managing Endpoints 23
Scenario F3 — Assigning a management role to a user....24
Appendix A: Creating a Security Policy....26
How to create or change the current security policy....26
Appendix B: Creating a Matching Level Rule 28
Creating an Entity-based Matching Level Rule....28
Creating a Keyword-based Matching Level Rule....28
Appendix C: Adding Sensitive Information You Want to Protect 29
How to add sensitive documents to DNA server and client 30
Appendix D: How to Clean up the LeakProof 3.0 DNA Server After the Scenarios are Complete 31
About Trend Micro Incorporated....32

Information contained in this document is provided "as-is" and subject to change without notice. This report is for informational purposes only and is not part of the documentation supporting Trend Micro products.

TRENDMICRO MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS REPORT.
[RG01LP30_080212USZWO]

This document is a product of Trend Micro Technical Sales Services.

About This Document

The intent of this document is to give customers a guide for evaluating Trend Micro™ LeakProof™ 3.0 (LeakProof). It will give the evaluator scenarios that will highlight the key benefits of the product as well as its ease of use.

Introduction to Trend Micro LeakProof 3.0

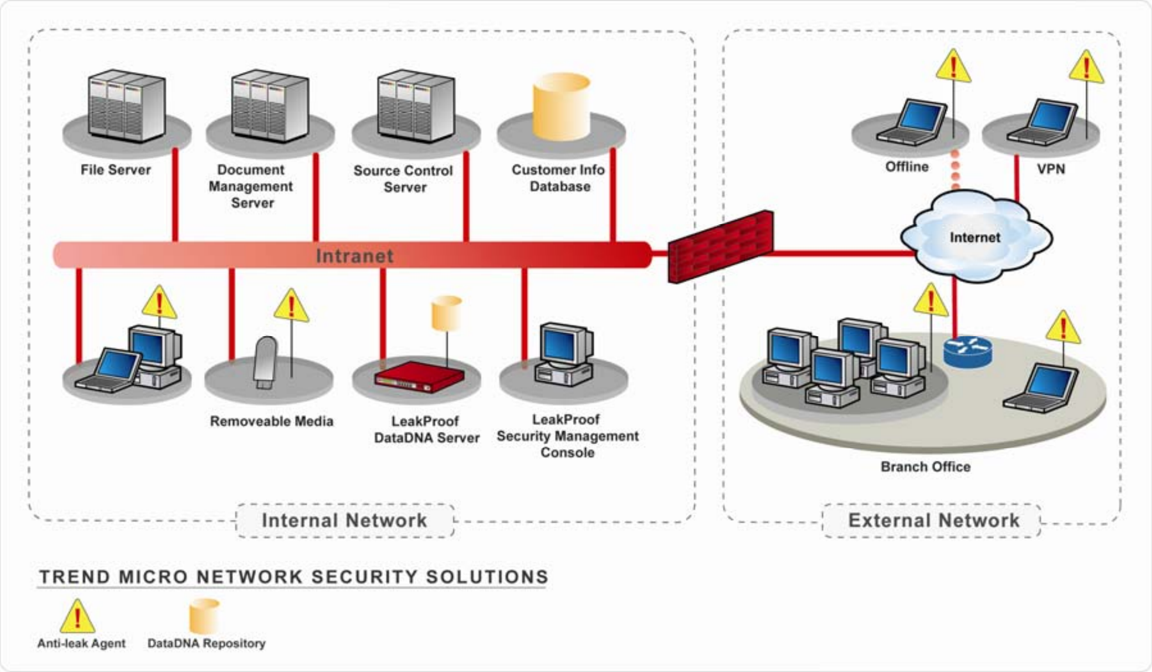
Trend Micro LeakProof 3.0 is a comprehensive software solution designed to help organizations protect sensitive information from accidental disclosure and intentional theft. With LeakProof 3.0, you will be at peace knowing that all insider threats are blocked and/or logged.

LeakProof 3.0 provides four levels of content filtering capabilities:

- DataDNA match engine based on document fingerprinting
- Entity match engine based on regular expression
- Keyword match
- Meta data match

Evaluator's Guide Requirements

- A LeakProof 3.0 DNA Server
  - You have a choice:
    - DL100/DL500
    - VMware version
- A Windows client such as Windows XP Professional
- A test network



Assumptions

This document assumes that the LeakProof 3.0 server and client are installed prior to starting the evaluation. The high-level requirements are:

1. All network configurations should be set with the LeakProof 3.0 DNA server. The server could be the VMware version or an appliance (DL100 or DL500).
2. Agent software has been installed on at least one endpoint and has been configured to connect to the LeakProof DNA server.

Sample Data Set

Trend Micro Inc. has prepared sample documents to be fingerprinted for this evaluation. The documents include five different file formats (Microsoft Word, Adobe Acrobat, Microsoft Excel, Microsoft PowerPoint, and text) and 17 different languages including English, Chinese, Japanese, French, Russian, and Greek. These sample documents are stored in following directory of the LeakProof DNA server.

```
/home/dgate/EvalDataDNADocRep/EvalDataDNADocSource
```

We also provide another set of documents that will be used for testing leakage from the client. These documents are included with the agent package in a folder named “Leaked-Documents”. These test samples include “sensitive documents” organized into the following categories:

- DataDNA match
  - All fingerprinted documents
  - One .rar file that contains some of the fingerprinted files
- Keyword match
  - files containing C/C++ and Java source code
  - One .rar file that contains several Java and C/C++ source files
- Entity match
  - 1 Excel file, 1 Word file, 1 PowerPoint file, 1 Rich Text (.rtf) file and 1 text file. All these files contain U.S. Social Security Number and credit card numbers information in them.
  - One .zip file—Contains 2 files: 1 zipped Word and 1 zipped Excel file

Table 1 identifies the test information included with Trend Micro LeakProof 3.0 and its location on the LeakProof 3.0 client:

Table 1 *Location and Function of Pre-defined LeakProof 3.0 Client Test Documents*

Location	Protection Method	Classification	Test Channel	Policy Rule Actions Taken During Transactions
C:\LeakedDocuments\ DataDNA-Match	Fingerprint DNA Match	Super Secret	All (email, USB)	Block, Notification, Justification
C:\LeakedDocuments\ Entity-Match	Entity Match/ Regex based	Personal Information	All (email, USB)	Encryption, Justification
C:\LeakedDocuments\ Keyword-Match	Keyword Match	Intellectual Property	All (email, USB)	Block
C:\LeakedDocuments\ Non-Sensitive-Doc	None	None	All (email, USB)	None

LeakProof 3.0 Scenarios List

The following table has the list of Scenarios we will use to evaluate the LeakProof 3.0. Each of these scenarios has a set of subsidiary scenarios.

Note: After you complete the scenarios, use the procedures in Appendix D to restore the test environment to the condition it was in before you began testing.

Table 2 *Trend Micro LeakProof 3.0 Scenario Summary*

Section	Description	Purpose
A: Protecting sensitive data:	These scenarios include violation tests such as sending sensitive information through email, copying sensitive files to a USB device, and other device control activities.	The purpose of these tests is to demonstrate how LeakProof 3.0 protects sensitive information. **Note**: The evaluator can do just these scenarios to understand the functionality and benefits of LeakProof 3.0. To see reporting capabilities, do the Reporting Scenarios. These scenarios should be enough to give overview of the product and its benefits.
B: Protecting Unstructured Sensitive Data Using Fingerprints	These scenarios include configuration steps and tests such as: • Adding your own sensitive documents • Preparing documents for protection • Adding documents to repositories • Scheduling the acquisition of documents • Validating the LeakProof 3.0 configuration	The purpose of these tests is to show how easy it is to configure LeakProof 3.0 to protect sensitive information based on Fingerprinting.
C: Protecting Sensitive Structured Data Using Entities	These scenarios include configuration steps and tests such as: • Add New entity Definitions • Validating the LeakProof 3.0 configuration	The purpose of these tests is to show how easy it is to configure LeakProof 3.0 to protect sensitive information based on entities .
D: Protecting Sensitive Structured Data Using Category Definitions	These scenarios include configuration steps and tests such as: • Creating keyword lists • Validating the LeakProof 3.0 configuration	The purpose of these tests is to show how easy it is to configure LeakProof 3.0 to protect sensitive information based on keywords
E: Using LeakProof 3.0 Reporting	These scenarios include configuration steps and tests such as: • Creating reports • Scheduling reports	The purpose of these tests is to show how easy it is to configure LeakProof 3.0 to create and schedule reports.
F: Administering LeakProof 3.0	These scenarios include configuration steps and tests such as: • Viewing events • Role-based access control • Client management	The purpose of these tests is to show how easy it is to configure LeakProof 3.0 to administer and manage users, systems, and clients.

Exploration

You are encouraged to explore the new features more fully.

LeakProof 3.0 Evaluation Scenarios

A: Protecting Sensitive Company Data Using LeakProof 3.0

Business Benefits	• LeakProof 3.0 protects internal users from unintentional or intentional transmission of a company's sensitive data. • LeakProof 3.0 protects sensitive data from being transmitted out of your company's possession while the client is ON or OFF your network.
Scenario Goals	These scenarios will show that LeakProof 3.0 prevents users from: • Attaching sensitive data to a document; copying sensitive data to a new document; copying sensitive data into the body of an email and transmitting it. This protection is both while client is ON or OFF the company's network • Copying sensitive data to external storage peripherals such as a USB storage device. We will also show that notifications will be sent to both client and administrator when there are policy violations: • We will show the LeakProof 3.0 Agent behavior in the clients • We will show the small size of the fingerprints

Note: There are two sets of sample documents shipped with the product. The sample document set for fingerprinting is located on the DNA server in the following directory:

```
/home/dgate/EvalDataDNADocRep/EvalDataDNADocSource
```

The sample document set to test data leaks from the client computer is located in the following directory on the test computer:

```
c:/LeakProof/Leaked-Documents
```

These tests can be conducted while the client is either ON or OFF-line.

Important Note:

1. The customer will need to PUSH the **Acquire** radio button in the LeakProof 3.0 Administrative console before starting these test scenarios to fingerprint the required pre-defined documents.
2. For Scenarios A1 through A9, make sure you try to leak information from DataDNA-Match, Keyword Match and Entity-Match directories NOT Non-Sensitive-Doc directory.

Scenario A1 — Sending a sensitive document to an external email address using company email

1. Login to the client computer that has LeakProof 3.0 agent installed.
2. Compose an email.
3. Attach a sensitive document from `c:/LeakProof/Leaked-Documents/` and try to send it.
    a. LeakProof will take the following actions:
        i. Issue a notification stating that this document contains company-sensitive information.
        ii. If the "Block" and "Justification" rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.

iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A2 — Copying and pasting a sensitive document and sending it to an external email address using company email

1. Open a sensitive document in `c: /LeakProof/Leaked-Documents/` and copy the contents.
2. Create a new document and paste the contents you just copied into it. Save the document and name it whatever you want.
3. Compose an email.
4. Attach a copy of the document you just created and send it.
    a. LeakProof will take the following actions:
        i. Issue a notification stating that this document contains company-sensitive information.
        ii. If the “Block” and “Justification” rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
        iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A3 — Sending part of a sensitive document to an external email address using company email

1. Open a sensitive document in `c:/LeakProof/Leaked-Documents/`.
2. `C`opy part of the document’s content.
3. Create a new document (name the document to whatever you want).
4. Compose an email.
5. Attach the document you just created to the email.
6. Send the email.
    a. LeakProof will take the following actions:
        i. Issue a notification stating that this document contains company-sensitive information.
        ii. If the “Block” and “Justification” rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
        iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A4 — Copying the content of a sensitive document into an email and sending it to an external email account using a company email address

1. Open a sensitive data document in `c:/LeakProof/Leaked-Documents/` .
2. Copy the content.
3. Compose an email.
4. Paste the content into the email body
5. Send the email.
    a. LeakProof will take the following actions:
        i. Issue a notification stating that this document contains company-sensitive information.
        ii. If the “Block” and “Justification” rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
        iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A5 — Sending a sensitive document to an external email address using Webmail

1. Login to the client computer that has LeakProof 3.0 agent installed.
2. Compose an email using a Webmail client.
3. Attach a sensitive document from `c:/LeakProof/Leaked-Documents/` to the email.
4. Send the email.
    a. LeakProof will take the following actions:
        i. Issue a notification stating that this document contains company-sensitive information.
        ii. If the “Block” and “Justification” rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
        iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A6 — Sending a sensitive document to an external email account using Webmail

1. Open a sensitive document in `c:/LeakProof/Leaked-Documents/.`
2. Copy the contents of the document.
3. Create a new document
4. Paste the contents into the new document.
5. Name the document whatever you want and save it.
6. Compose an email.
7. Attach the document you just created
8. Send the email.
   a. LeakProof will take the following actions:
      i. Issue a notification stating that this document contains company-sensitive information.
      ii. If the "Block" and "Justification" rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
      iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A7 — Copying part of a sensitive document, pasting the content into a new document and sending the document to an external email account using Webmail

1. Open a sensitive document in `c:/LeakProof/Leaked-Documents/`
2. copy part of the content.
3. Create a new document.
4. Save the document (name it whatever you want).
5. Compose an email.
6. Attach the document you just created.
7. Send the email.
   a. LeakProof will take the following actions:
      i. Issue a notification stating that this document contains company-sensitive information.
      ii. If the "Block" and "Justification" rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
      iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A8 — Copying part of a sensitive document, pasting it in an email and sending the mail to an external email account using a company email address

1. Open a sensitive document in `c:/LeakProof/Leaked-Documents/`.
2. Copy the content.
3. Compose an email.
4. Paste the content into the body of the email.
5. Send the email.
    a. LeakProof will take the following actions:
        i. Issue a notification stating that this document contains company-sensitive information.
        ii. If the “Block” and “Justification” rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
        iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A9 — Copying a sensitive document to an external USB storage device

1. Login to the client computer that has LeakProof 3.0 agent installed.
2. Copy a sensitive data document from `c:/LeakProof/Leaked-Documents/` and try to copy it to an external USB storage device.
3. Open a sensitive data document in `c:/LeakProof/Leaked-Documents/` and copy the content and create a new document (name the document what ever you wanted). Then try to copy it to an external USB storage device.
4. Open a sensitive data document in `c:/LeakProof/Leaked-Documents/` and copy part of the content and create a new document (name the document what ever you wanted). Then try to copy it to an external USB storage device.
5. Disconnect your Ethernet cable from your client and try to copy a sensitive document from `c:/LeakProof/Leaked-Documents/` to a USB storage device.
    a. LeakProof will take the following actions:
        i. Issue a notification stating that this document contains company-sensitive information.
        ii. If the “Block” and “Justification” rules in the policy are set, LeakProof 3.0 displays a Justification window that allows you to enter the reason you want to copy or move the sensitive document.
        iii. Encrypt the document. This happens only if the sensitive document is being copied to removable media such as a USB device or CD/DVD.

Scenario A10 — Copying non-sensitive data document to an external USB storage device

1. Login to the client computer that has LeakProof 3.0 agent installed.
2. Copy a known non-sensitive data document from `c:/LeakProof/Leaked-Documents/Non-Sensitive-Doc` and try to copy it to an external USB storage device.
3. Disconnect your Ethernet cable from your client and try to copy a sensitive document from `c:/LeakProof/Leaked-Documents/Non-Sensitive-Doc` to an external USB storage device.
4. Notice nothing happens if the information is NOT sensitive.

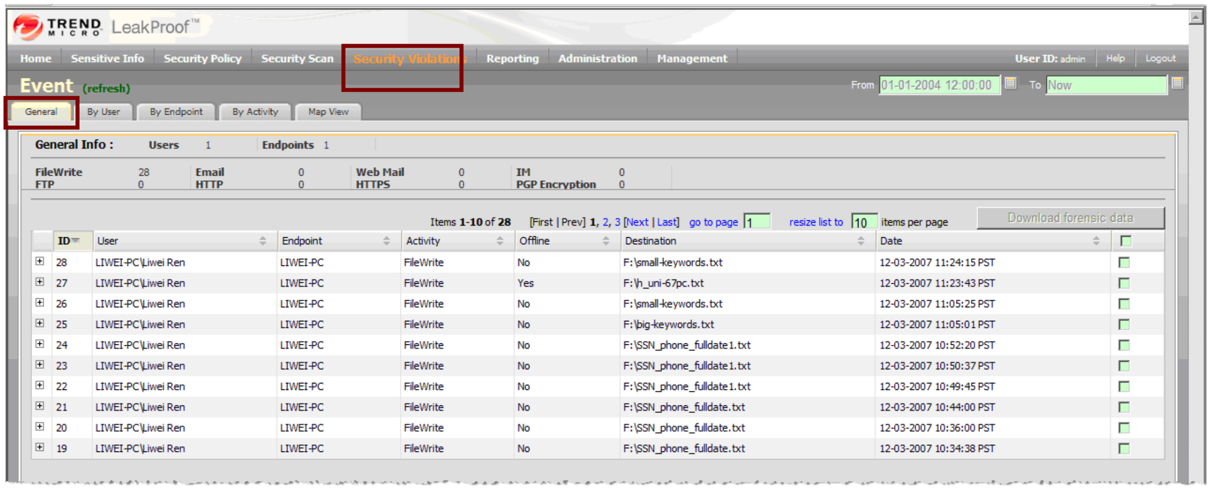
Scenario A11 — Viewing a clients' notifications during violations

1. Login to the client computer that has LeakProof 3.0 agent installed
2. Copy a sensitive data document and try to copy it to an external USB storage device.
3. Look for a popup educational window. This window will give the details of what the company policy is for copying a sensitive data, etc.
4. If the justification policy is set, and the user is doing this action for a business reason, the LeakProof client will give the user an option to justify and then continue with the action. However, the action is logged and a notification sent to the administrator.

Scenario A12 — Viewing the LeakProof 3.0 server's notifications during violations

1. Click the **Security Violations** tab of the menu bar on top of the administrative console.
2. Click the **General** tab.

Trend Micro LeakProof 3.0 Administrative Console



From 01-01-2004 12:00:00 To Now

General Info : Users 1 Endpoints 1

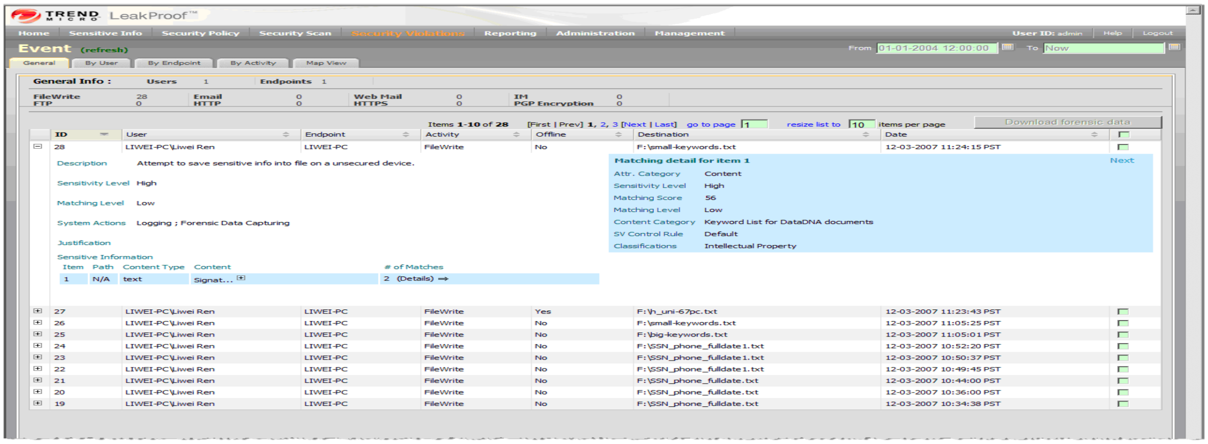
FileWrite	28	Email	0	Web Mail	0	IM	0
FTP	0	HTTP	0	HTTPS	0	PGP Encryption	0

Items 1-10 of 28 [First | Prev] 1, 2, 3 [Next | Last] go to page 1 resize list to 10 items per page

	ID	User	Endpoint	Activity	Offline	Destination	Date	□
⊞	28	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\small-keywords.txt	12-03-2007 11:24:15 PST	□
⊞	27	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	Yes	F:\h_uni-67pc.txt	12-03-2007 11:23:43 PST	□
⊞	26	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\small-keywords.txt	12-03-2007 11:05:25 PST	□
⊞	25	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\big-keywords.txt	12-03-2007 11:05:01 PST	□
⊞	24	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate1.txt	12-03-2007 10:52:20 PST	□
⊞	23	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate1.txt	12-03-2007 10:50:37 PST	□
⊞	22	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate1.txt	12-03-2007 10:49:45 PST	□
⊞	21	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate.txt	12-03-2007 10:44:00 PST	□
⊞	20	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate.txt	12-03-2007 10:36:00 PST	□
⊞	19	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate.txt	12-03-2007 10:34:38 PST	□

3. Click the expansion icon on the left side of each violation record to see the details of each violation event. Administrator will be able to see detail information such as what the violation was, what time it happened, if it happened ON or OFF the network, etc.

Figure 1 *Expanded Event Page*



From 01-01-2004 12:00:00 To Now

General Info : Users 1 Endpoints 1

FileWrite	28	Email	0	Web Mail	0	IM	0
FTP	0	HTTP	0	HTTPS	0	PGP Encryption	0

Items **1-10** of **28** [First | Prev] **1**, 2, 3 [Next | Last] go to page 1 resize list to 10 items per page

	ID	User	Endpoint	Activity	Offline	Destination	Date	□
⊟	28	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\small-keywords.txt	12-03-2007 11:24:15 PST	□

Description Attempt to save sensitive info into file on a unsecured device.

Sensitivity Level High

Matching Level Low

System Actions Logging ; Forensic Data Capturing

Justification

Sensitive Information

Item	Path	Content Type	Content	# of Matches
1	N/A	text	Signat... ⊞	2 (Details) ⇒

Matching detail for item 1

Attr. Category	Content
Sensitivity Level	High
Matching Score	56
Matching Level	Low
Content Category	Keyword List for DataDNA documents
SV Control Rule	Default
Classifications	Intellectual Property

	ID	User	Endpoint	Activity	Offline	Destination	Date	□
⊞	27	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	Yes	F:\h_uni-67pc.txt	12-03-2007 11:23:43 PST	□
⊞	26	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\small-keywords.txt	12-03-2007 11:05:25 PST	□
⊞	25	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\big-keywords.txt	12-03-2007 11:05:01 PST	□
⊞	24	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate1.txt	12-03-2007 10:52:20 PST	□
⊞	23	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate1.txt	12-03-2007 10:50:37 PST	□
⊞	22	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate1.txt	12-03-2007 10:49:45 PST	□
⊞	21	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate.txt	12-03-2007 10:44:00 PST	□
⊞	20	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate.txt	12-03-2007 10:36:00 PST	□
⊞	19	LIWEI-PC\Liwei Ren	LIWEI-PC	FileWrite	No	F:\SSN_phone_fulldate.txt	12-03-2007 10:34:38 PST	□

Scenario A13 — Verifying that LeakProof 3.0 client files are hidden from users

1. Login to the client computer that has LeakProof 3.0 agent installed.
2. Check for the process in Windows Task Manager. You should not see any LeakProof 3.0 processes as the client process is hidden.
3. Search the registry to see if you can find any entries for the LeakProof client. You will not be able to see any because the registry entries are hidden.
4. Check to see if you can view the violation logs. These files are also hidden.
5. Login to the LeakProof administrative console.
6. Click the **Management** tab in the menu bar at the top of the administrative console.
7. Use the arrow keys to look for the name of the client. The name of the client appears indicating that it is protected.

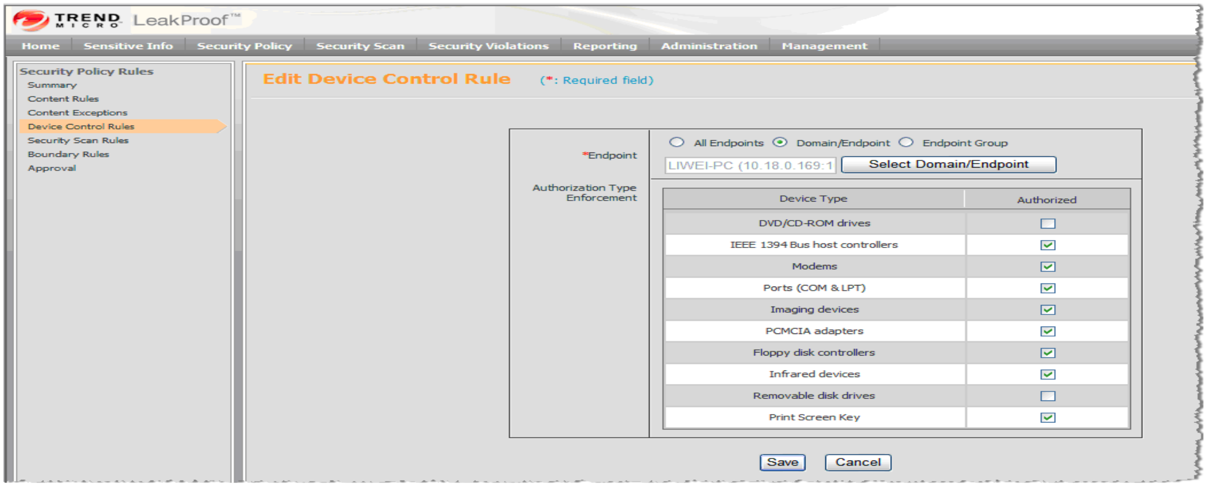
Scenario A14 — Viewing the size of LeakProof 3.0 Fingerprints

1. Login into the appliance with user “dgate”
2. **cd** to the directory `/home/dgate/prod/common/data/index`.
3. The user should find some sub-directories with names in format “RepoN” where “N” is a number. For example, “Repo2”, “Repo3”, etc.
4. **cd** to the directory with the largest number, For example, if you see directories named “Repo4” and “Repo5”, cd to “Repo5”.
5. Type **du** and you will see the fingerprint size in KBytes.

Scenario A15 — Enable/Disable Devices

1. Go to **Security Policy → Device Control Rules**.
2. Click **Add Rule**.
3. Create a rule similar to that in the example below, which disables the DVD, CD, and removable disk drivers on "PC-Liwei".

Figure 2 *Edit Device Control Rule Page*



Edit Device Control Rule (*: Required field)

*Endpoint: ○ All Endpoints ● Domain/Endpoint ○ Endpoint Group

LIWEI-PC (10.18.0.169:1

Authorization Type Enforcement

Device Type	Authorized
DVD/CD-ROM drives	□
IEEE 1394 Bus host controllers	☑
Modems	☑
Ports (COM & LPT)	☑
Imaging devices	☑
PCMCIA adapters	☑
Floppy disk controllers	☑
Infrared devices	☑
Removable disk drives	□
Print Screen Key	☑

4. Click **Save** after you complete editing the rule.

B: Protecting Unstructured Sensitive Data Using Fingerprints

Business Benefits	• LeakProof 3.0 protects unstructured sensitive company data using the DataDNA™ match engine. This match engine uses document fingerprinting to identify documents.
Scenario Goals	• In these scenarios, we will show how to configure and set policies in Trend Micro LeakProof 3.0 to protect unstructured sensitive documents using scanning and fingerprinting techniques. These scenarios include procedures that enable users to: o Classify information o Define sensitive documents, including creating a ▪ Document source repository ▪ Document acquisition job definition o Create Policies o Perform functionality tests

Note: Before you start your scenarios:

1. Create a directory in the DNA server under:

   `/Home/dgate/Directory name`

2. Make sure that you have added the data you wanted to protect to the DNA Server in the directory you just created:

   `/home/dgate/Directory name`

Also, make sure you have some of these sensitive documents copied in the client system with LeakProof agent installed so you can use them for testing.

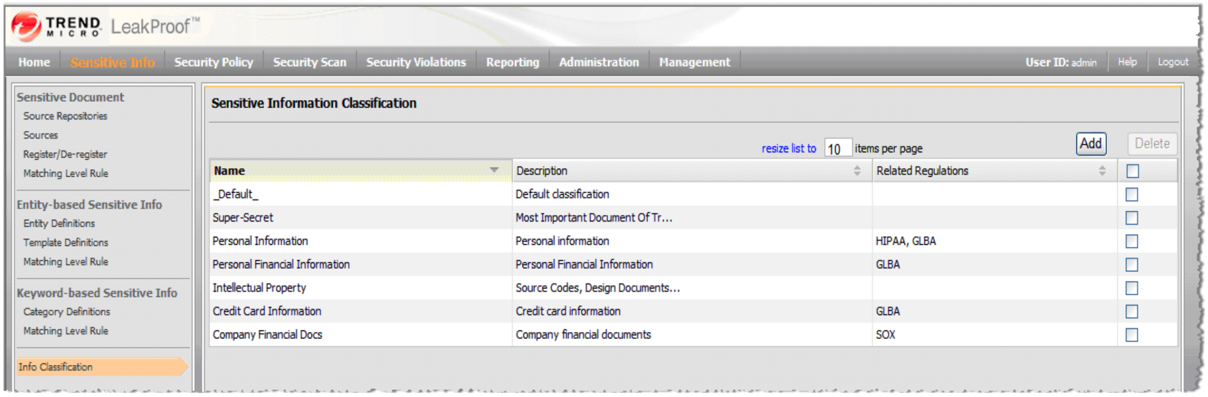
Scenario B1 — Adding Sensitive Information Classifications

1. Open a Web Browser from a computer that is in the same network as the DNA server.
2. Login to DNA server Web interface by typing “http://<DNA server IP address:8080/dsc>”

   LoginID = admin

   Password = yourpassword
3. Go to **Sensitive Info → Info Classification**.
4. Click **Add**.
5. Enter the Name and Description of the classification you would like to add. The classification will be added.

Figure 3 *Sensitive Information Classification Page*



Sensitive Information Classification

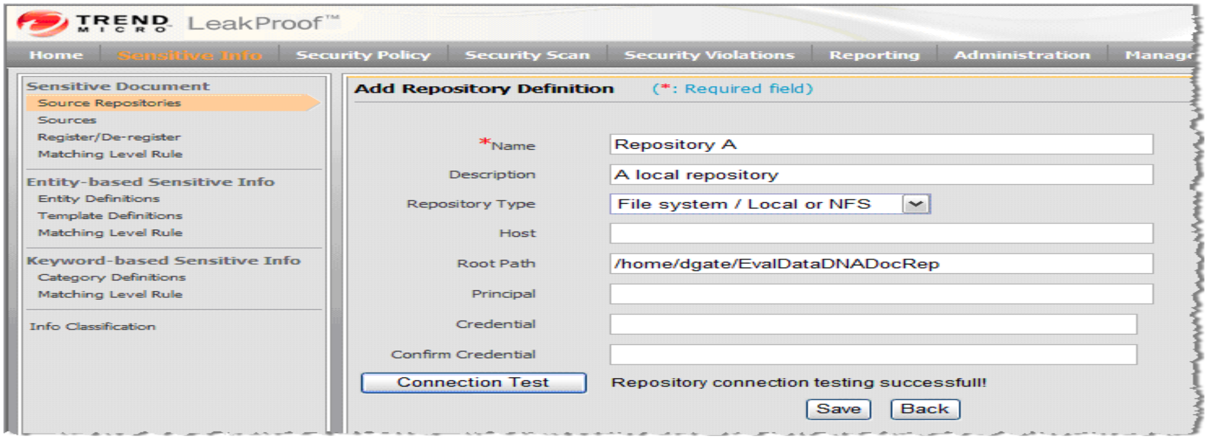
resize list to 10 items per page

Name	Description	Related Regulations	□
Default	Default classification		□
Super-Secret	Most Important Document Of Tr…		□
Personal Information	Personal information	HIPAA, GLBA	□
Personal Financial Information	Personal Financial Information	GLBA	□
Intellectual Property	Source Codes, Design Documents…		□
Credit Card Information	Credit card information	GLBA	□
Company Financial Docs	Company financial documents	SOX	□

Scenario B2 — Entering sensitive document definitions

1. Click **Add** above the repository list to take you to the Add Repository Definition page which allows you to add a new repository definition. For a repository definition, a name and repository type are always required.
2. Define repository type. If the repository is part of a local file system or a mounted file system on the LeakProof server, the Repository Type should be set to **File system / Local or NFS**..

Figure 4 *Add Repository Definition Page*



Add Repository Definition (*: Required field)

*Name: Repository A

Description: A local repository

Repository Type: File system / Local or NFS

Host:

Root Path: /home/dgate/EvalDataDNADocRep

Principal:

Credential:

Confirm Credential:

Repository connection testing successfull!

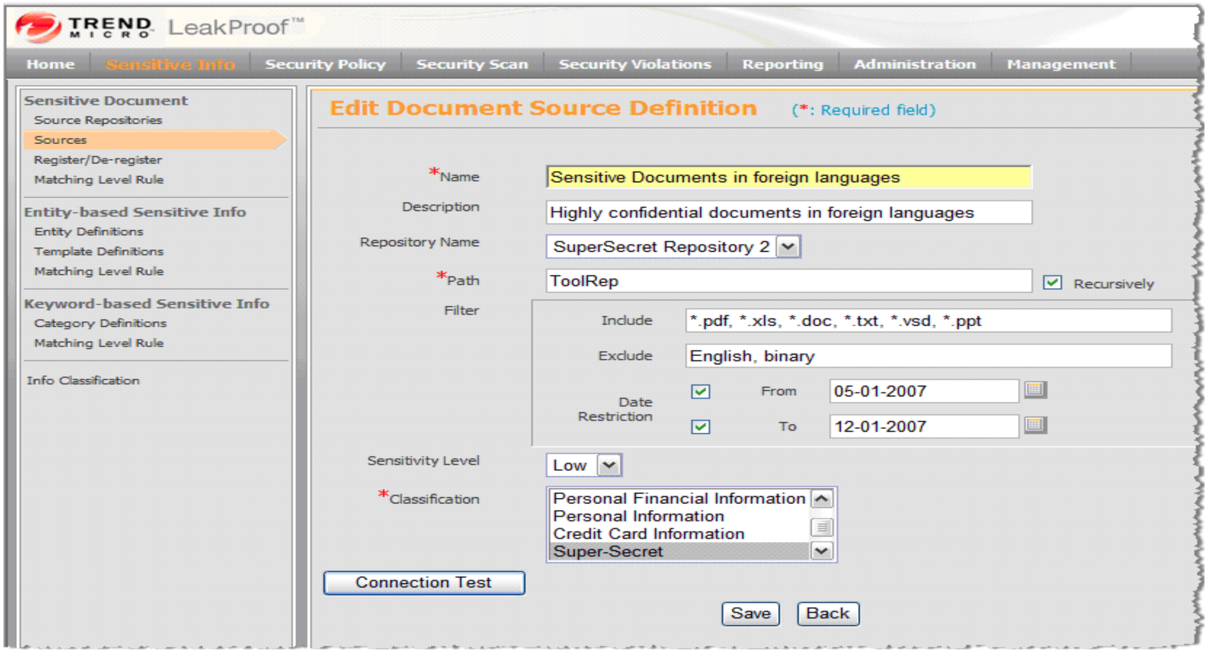
Scenario B3 — Adding sensitive documents source definitions

1. Go to **Sensitive Info → Sources → Add** to add a new source definition and you will get to *"Edit Document Source Definition page".*
2. Enter a Name and a Repository Name. For sensitive document source definitions, the Name and Repository Name fields are required.
3. Enter the Path (relative to the root of the repository directory selected).
4. By default, all subdirectories will be included recursively. Deselecting the Recursively checkbox excludes all subdirectories (this is strongly recommended, but optional). Enter the data for the Filter feature: Select only those files with names that satisfy the Include and Exclude criteria. Exclude those directories with names that match the patterns specified in the Exclude field.
5. Specify last modified dates to satisfy the Date Restriction criterion.

Filter Example:	Only files satisfying the following criteria will be selected: • Include criteria — To include the file name matches for *.doc, *.pdf, *.xls, *.txt, *.ppt, *.vsd. • Exclude criteria — To exclude folder names with "English" and "binary" • Date Restriction criterion — mm/dd/yyyy to mm/dd/yyyy

6. (Optional) Select the sensitivity level.
7. Specify one or more classifications for the source definition with the Control key.
8. While adding or editing a source definition, press **Connection Test** to see whether the source is accessible.
9. Click **Save** to save the new source definition.
10. Select the source you have created and acquire it by clicking the **Acquire** button.

Figure 5 *Edit Document Source Definition Page*



Edit Document Source Definition (*: Required field)

*Name: Sensitive Documents in foreign languages

Description: Highly confidential documents in foreign languages

Repository Name: SuperSecret Repository 2

*Path: ToolRep ☑ Recursively

Filter

Include: *.pdf, *.xls, *.doc, *.txt, *.vsd, *.ppt

Exclude: English, binary

Date Restriction: ☑ From 05-01-2007 ☑ To 12-01-2007

Sensitivity Level: Low

*Classification: Personal Financial Information, Personal Information, Credit Card Information, Super-Secret

Scenario B4 — Create a Security Policy

See Appendix A on how to create a policy.

Scenario B5 — Validate your Configuration

Perform the tests in Scenarios A1 through A15 to validate your configuration.

C: Protecting Sensitive Structured Data Using Entities

Business Benefits	• LeakProof 3.0 can protect structured sensitive company data using the Entity Match engine. Entities are based on regular expressions .
Scenario Goals	• These scenarios will show how to configure and set policies in Trend Micro LeakProof 3.0 to protect structured sensitive data based on regular expressions. The scenarios include procedures for: o Defining entities o Creating Policies o Performing functionality tests

Important Note: **Before you start your scenarios:**

Make sure you have some of the test sensitive documents copied to the client system. The test documents are installed with LeakProof agent and are contained in the `C:/LeakProof/Leaked-Documents/` directory.

Scenario C1 — Using the Entity Definitions page to add or edit new entities

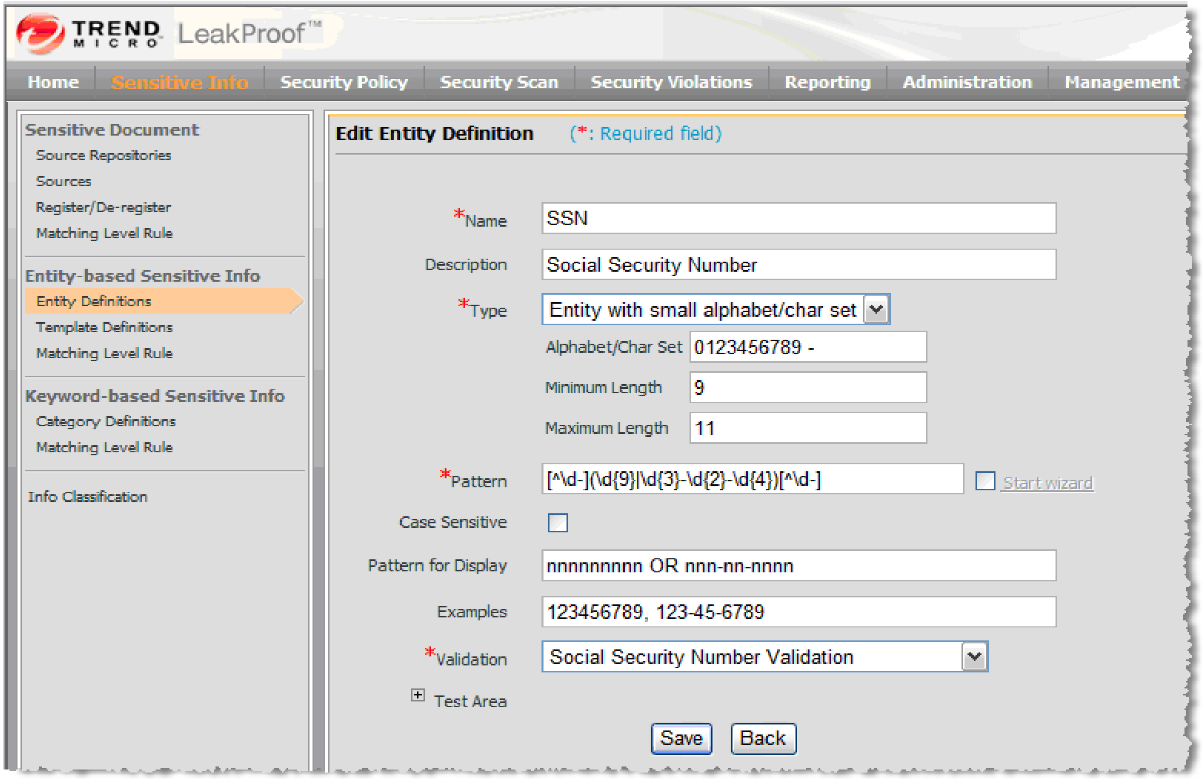
1. Go to **Sensitive Info → Entity-based Sensitive Info → Entity Definitions**. Click **Add**.

2. Type data in the following fields:

- o **Name** — Any name is allowed.
- o **Type** — Select either a Generic type or one of the three Optimized types. It is strongly recommended that you select appropriate optimized type if possible.
- o **Pattern** — Follow the guidelines that we described when writing the pattern in regular expression. You can use the test area to validate the pattern.
- o **Validation** — LeakProof provides validation methods for most of the 16 predefined entities. There is no general validation method for all entities. The validation method has to be built individually for each entity. When adding a new entity other than the 16 predefined ones, select the “No Validation” option.

3. Click **Save**.

Figure 6 *Entity Definition Page*



Edit Entity Definition (*: Required field)

*Name: SSN

Description: Social Security Number

*Type: Entity with small alphabet/char set

Alphabet/Char Set: 0123456789 -

Minimum Length: 9

Maximum Length: 11

*Pattern: [^\d-](\d{9}|\d{3}-\d{2}-\d{4})[^\d-]

Case Sensitive: □

Pattern for Display: nnnnnnnnn OR nnn-nn-nnnn

Examples: 123456789, 123-45-6789

*Validation: Social Security Number Validation

Scenario C2 — Creating a Security Policy

See Appendix A on how to create a Security Policy.

Scenario C3 — Creating a Matching Level Rule

See Appendix B on how to create a Matching Level Rule.

Scenario C4 — Validating your LeakProof 3.0 Configuration

Perform the functionality tests in Scenario 1.

D: Protecting Sensitive Structured Data Using Category Definitions

Business Benefits	• LeakProof 3.0 protects structured sensitive company data using the Entity Match engine and category definitions.
Scenario Goals	• These scenarios show how to configure and set policies in Trend Micro LeakProof 3.0 to protect structured sensitive data using keywords. They include procedures for: o Defining categories o Assiging category names o Entering category descriptions o Assiging a sensitivity level o Classifying categories o Entering keywords

Important Note:	**Before you start your scenarios:** Make sure you have some of the test sensitive documents copied to the client system. The test documents are installed with LeakProof agent and are contained in the `C:/LeakProof/Leaked-Documents/` directory.

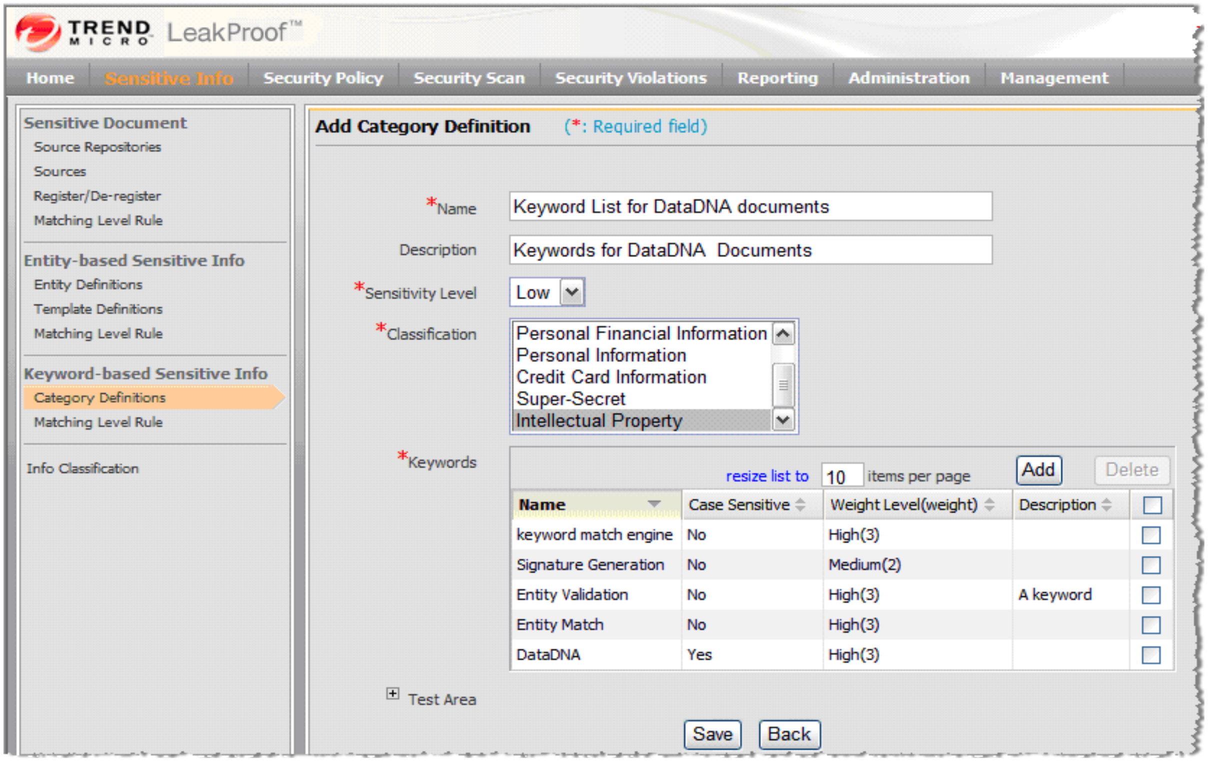
Scenario D1 — Adding a Category Definition

1. Click **Sensitive Info → Keyword-based Sensitive Info → Category Definitions**.
2. Click **Add** to bring up the Add Category Definition page.

Note:	Each category definition has a Name, Description, Sensitivity Level, one or more Classifications, and a set of keywords.

3. Enter a name for the category.
4. Enter each keyword you wish to associate with the category.
5. Select the case sensitivity you wish to associate with the category.
6. Select the weight level you wish to assign to the category.

Figure 7 *Add Category Definition Page*



Add Category Definition (*: Required field)

*Name: Keyword List for DataDNA documents

Description: Keywords for DataDNA Documents

*Sensitivity Level: Low

*Classification:
Personal Financial Information
Personal Information
Credit Card Information
Super-Secret
Intellectual Property

*Keywords: resize list to 10 items per page [Add] [Delete]

Name	Case Sensitive	Weight Level(weight)	Description	□
keyword match engine	No	High(3)		□
Signature Generation	No	Medium(2)		□
Entity Validation	No	High(3)	A keyword	□
Entity Match	No	High(3)		□
DataDNA	Yes	High(3)		□

⊞ Test Area

[Save] [Back]

Scenario D2 — Creating a Security Policy

See Appendix A on how to create a policy.

Scenario D3 — Creating a Matching Level Rule

See Appendix B on how to create a Matching Level Rule.

Scenario D4 — Validating your LeakProof 3.0 Configuration

Do the tests in Scenarios A1 through A15 to validate your LeakProof 3.0 configuration.

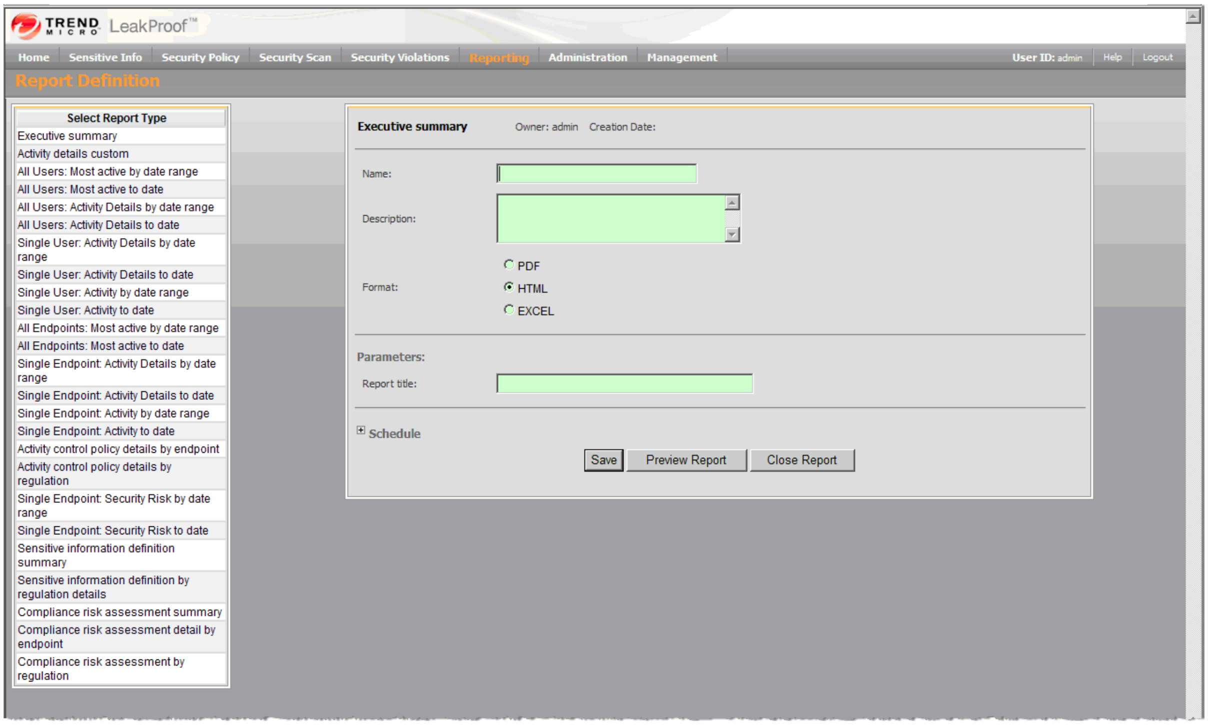
E: Using LeakProof 3.0 Reporting

Business Benefits	• LeakProof 3.0 comes with four predefined reports. You can customize these reports or schedule the time the reports are generated and have them sent to a specific email address. • LeakProof 3.0 includes a drilldown capability that enables users to look at reports based on client, classification, etc.
Scenario Goals	• These scenarios show how to: o Create reports o Schedule reports

Scenario E1 — Adding a New Report

1. Go to **Reporting → Report Definition.**
2. Click the **Add New Report** button for adding a new report. The following four default report definitions are provided
   - Executive summary
   - Top Users
   - Last month activity details
   - Top endpoints
3. From the left panel, select the report type you would like to define to create a report.
4. On the right side, type a report name and definition.
5. Click the radio button for the report format you want:
   - **PDF**
   - **HTML**
   - **Excel**
6. Enter the other necessary parameters for the report:
   - **Report title** — Title to appear in the report.
   - **Last** — Select the interval for the report from the drop-down list
   - **Max # of records** — Enter the number of maximum number of records between 1 and 1,000 that the report can contain. Any number larger than 1,000 will be treated the same as 1,000.
7. Click **Preview Report** to preview the report you have created.
8. Click **Save**.

Figure 8 *Report Definition Page*



Select Report Type

- Executive summary
- Activity details custom
- All Users: Most active by date range
- All Users: Most active to date
- All Users: Activity Details by date range
- All Users: Activity Details to date
- Single User: Activity Details by date range
- Single User: Activity Details to date
- Single User: Activity by date range
- Single User: Activity to date
- All Endpoints: Most active by date range
- All Endpoints: Most active to date
- Single Endpoint: Activity Details by date range
- Single Endpoint: Activity Details to date
- Single Endpoint: Activity by date range
- Single Endpoint: Activity to date
- Activity control policy details by endpoint
- Activity control policy details by regulation
- Single Endpoint: Security Risk by date range
- Single Endpoint: Security Risk to date
- Sensitive information definition summary
- Sensitive information definition by regulation details
- Compliance risk assessment summary
- Compliance risk assessment detail by endpoint
- Compliance risk assessment by regulation

Executive summary Owner: admin Creation Date:

Name:

Description:

Format: ○ PDF ● HTML ○ EXCEL

Parameters:

Report title:

Scenario E2 — Alternate Definition

Another way to run a report is to schedule it using the **Administration → Scheduled → Job** feature. This feature is useful when you need to schedule reports to run on a regular basis or at a later time.

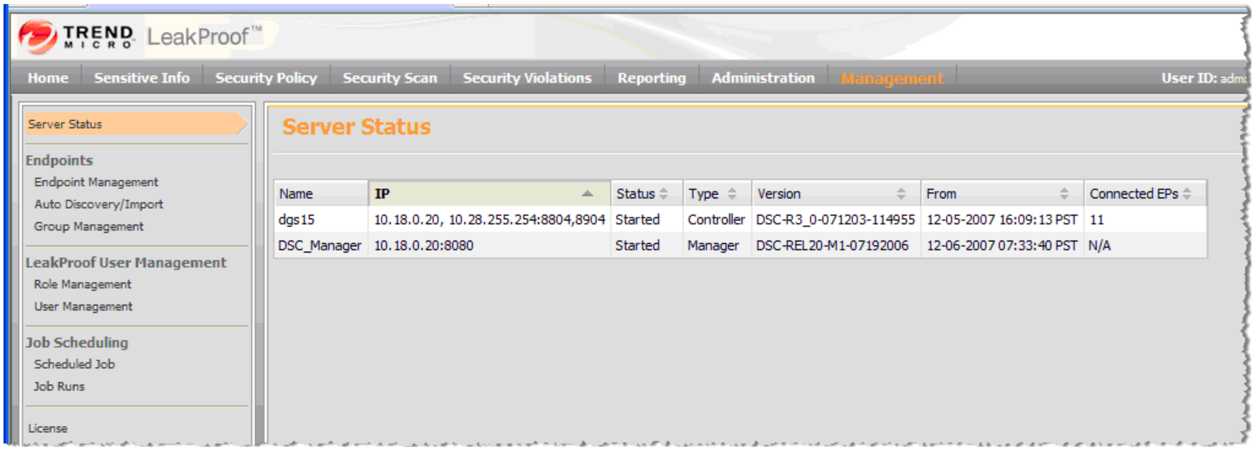
F: Administering LeakProof 3.0

Business Benefits	• Trend Micro LeakProof 3.0 administrators can manage all clients and the LeakProof server through a centralized, Web-based interface. • Administrators can give users role-based access control, monitor system events, manage data, etc.
Scenario Goals	• These scenarios show how to: o Monitor the server o Manage endpoints o Assign a management role to a user

Scenario F1 — Monitoring Server Status

The following shows the Server Status page. This page allows an administrator to monitor the status of the LeakProof 3.0 server.

Figure 9 *Server Status Page*



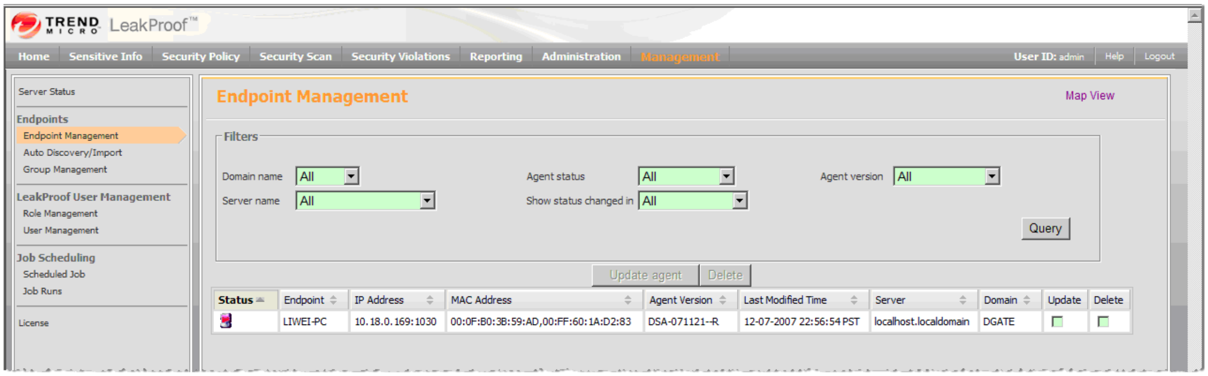
Server Status

Name	IP	Status	Type	Version	From	Connected EPs
dgs15	10.18.0.20, 10.28.255.254:8804,8904	Started	Controller	DSC-R3_0-071203-114955	12-05-2007 16:09:13 PST	11
DSC_Manager	10.18.0.20:8080	Started	Manager	DSC-REL20-M1-07192006	12-06-2007 07:33:40 PST	N/A

Scenario F2 — Managing Endpoints

The LeakProof 3.0 Endpoint Management functionality allows administrators to browse or edit the endpoints in the network.

Figure 10 *Endpoint Management Page*



Endpoint Management

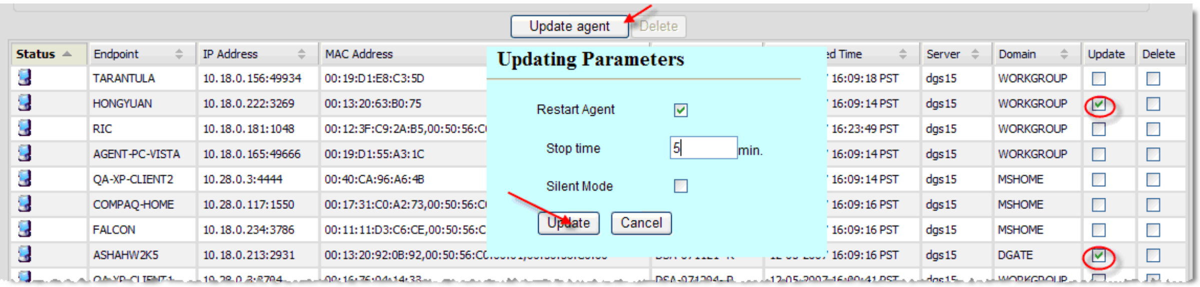
Filters

Domain name: All
Server name: All
Agent status: All
Show status changed in: All
Agent version: All

Status	Endpoint	IP Address	MAC Address	Agent Version	Last Modified Time	Server	Domain	Update	Delete
	LIWEI-PC	10.18.0.169:1030	00:0F:B0:3B:59:AD,00:FF:60:1A:D2:83	DSA-071121--R	12-07-2007 22:56:54 PST	localhost.localdomain	DGATE	□	□

A server can update the agent if the agent version on the endpoint does not match the server build.

Figure 11 *Updating Agent Parameters*



Updating Parameters

Restart Agent ☑

Stop time 5 min.

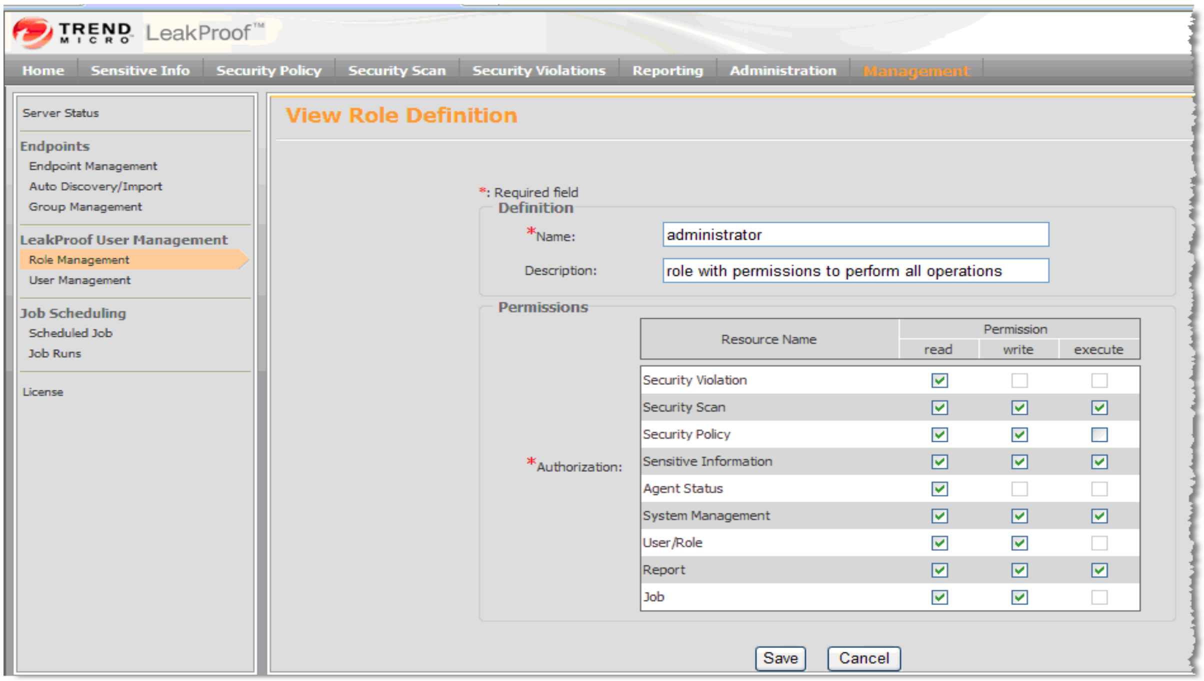
Silent Mode □

Status	Endpoint	IP Address	MAC Address	...ed Time	Server	Domain	Update	Delete
	TARANTULA	10.18.0.156:49934	00:19:D1:E8:C3:5D	16:09:18 PST	dgs15	WORKGROUP	□	□
	HONGYUAN	10.18.0.222:3269	00:13:20:63:B0:75	16:09:14 PST	dgs15	WORKGROUP	☑	□
	RIC	10.18.0.181:1048	00:12:3F:C9:2A:B5,00:50:56:C	16:23:49 PST	dgs15	WORKGROUP	□	□
	AGENT-PC-VISTA	10.18.0.165:49666	00:19:D1:55:A3:1C	16:09:14 PST	dgs15	WORKGROUP	□	□
	QA-XP-CLIENT2	10.28.0.3:4444	00:40:CA:96:A6:4B	16:09:14 PST	dgs15	MSHOME	□	□
	COMPAQ-HOME	10.28.0.117:1550	00:17:31:C0:A2:73,00:50:56:C	16:09:16 PST	dgs15	MSHOME	□	□
	FALCON	10.18.0.234:3786	00:11:11:D3:C6:CE,00:50:56:C	16:09:16 PST	dgs15	MSHOME	□	□
	ASHAHW2K5	10.18.0.213:2931	00:13:20:92:0B:92,00:50:56:C	16:09:16 PST	dgs15	DGATE	☑	□

Scenario F3 — Assigning a management role to a user

1. Go to **Management → LeakProof User Management → Role Management**.
2. Click **Add Role** to create a new role definition.
3. Type a name for the new role in the Name field.
4. (Optional) Type a description of the role in the Description field.
5. Mark the appropriate **Authorization** checkbox(es) in the appropriate **Permission** (read, write or execute) column.
6. Click **Save**.

__Figure 12__ View (and Add) Role Definition Page



View Role Definition

*: Required field

Definition

*Name: administrator

Description: role with permissions to perform all operations

Permissions

*Authorization:

Resource Name	Permission		
	read	write	execute
Security Violation	☑	□	□
Security Scan	☑	☑	☑
Security Policy	☑	☑	□
Sensitive Information	☑	☑	☑
Agent Status	☑	□	□
System Management	☑	☑	☑
User/Role	☑	☑	□
Report	☑	☑	☑
Job	☑	☑	□

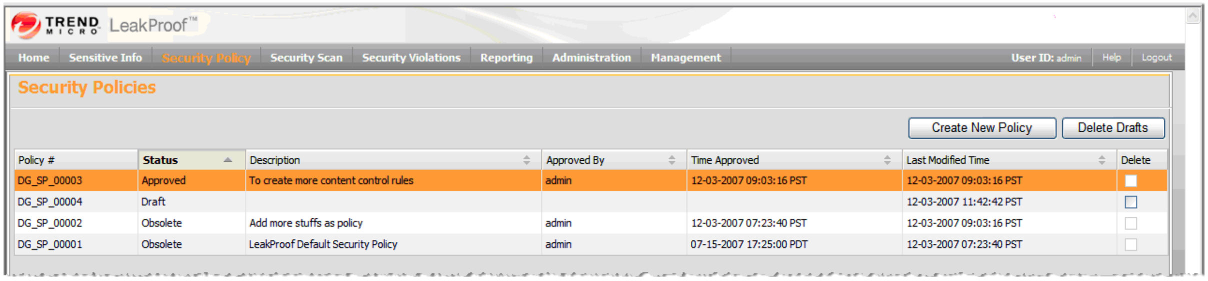
Appendix A: Creating a Security Policy

LeakProof is shipped with a default **Approved** security policy. An Approved policy cannot be changed.

How to create or change the current security policy

1. Click the Security Policy tab on the menu bar on the top of the GUI console.

Figure 13 *Security Policies Page*

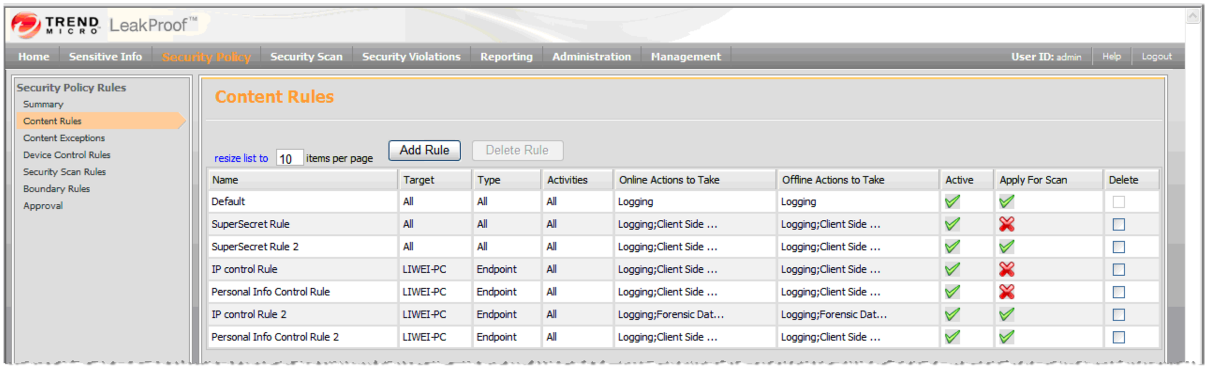


Security Policies

Policy #	Status	Description	Approved By	Time Approved	Last Modified Time	Delete
DG_SP_00003	Approved	To create more content control rules	admin	12-03-2007 09:03:16 PST	12-03-2007 09:03:16 PST	□
DG_SP_00004	Draft				12-03-2007 11:42:42 PST	□
DG_SP_00002	Obsolete	Add more stuffs as policy	admin	12-03-2007 07:23:40 PST	12-03-2007 09:03:16 PST	□
DG_SP_00001	Obsolete	LeakProof Default Security Policy	admin	07-15-2007 17:25:00 PDT	12-03-2007 07:23:40 PST	□

2. Select an existing **Approved** or **Obsolete** policy as a template to create a new draft policy.
3. Click **Create New Policy**.
4. Select a policy name from the drop-down list of the Create New Policy dialog box.
5. Click **Create**. A new policy appears with "Draft" in the status column.
6. Click the **Policy #** field of the new draft policy.
7. Click **Content Rules**. The Content Rules page appears.

Figure 14 *Content Rules Page*



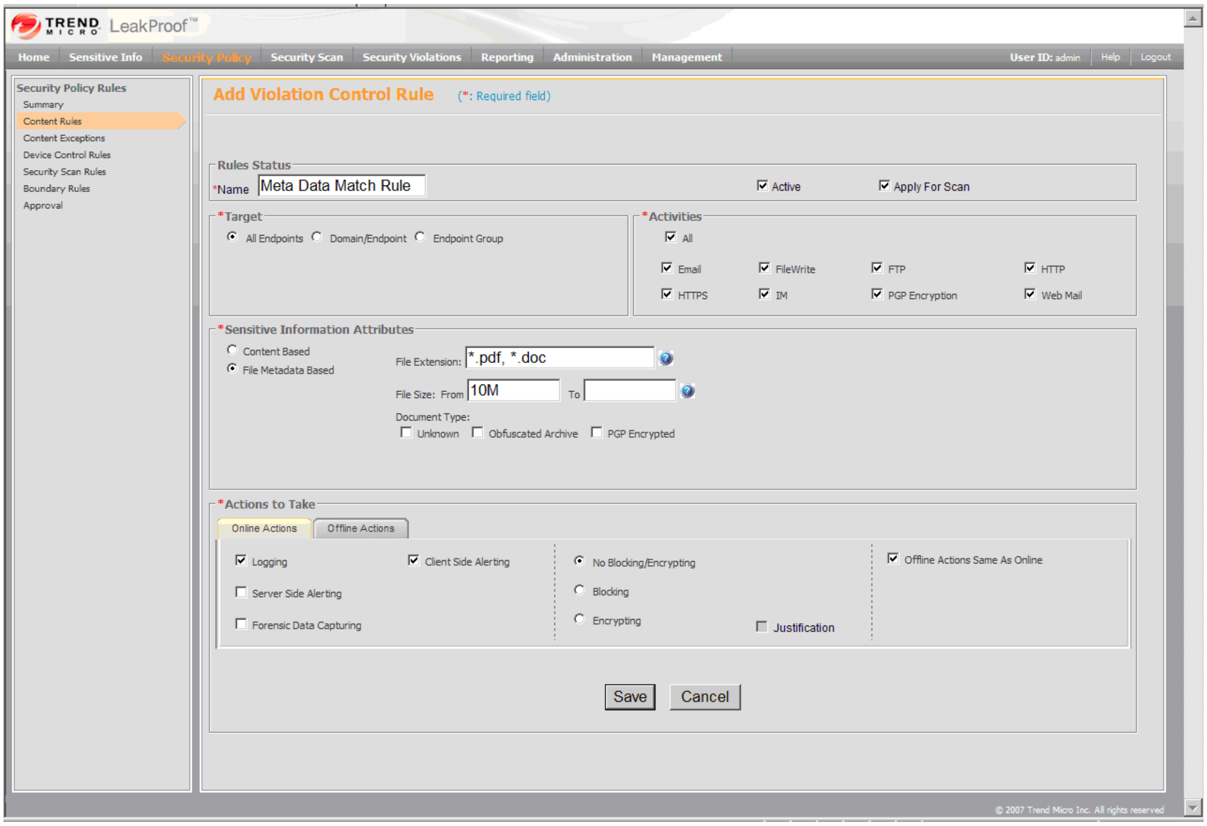
Content Rules

resize list to 10 items per page

Name	Target	Type	Activities	Online Actions to Take	Offline Actions to Take	Active	Apply For Scan	Delete
Default	All	All	All	Logging	Logging	✓	✓	□
SuperSecret Rule	All	All	All	Logging;Client Side ...	Logging;Client Side ...	✓	✗	□
SuperSecret Rule 2	All	All	All	Logging;Client Side ...	Logging;Client Side ...	✓	✓	□
IP control Rule	LIWEI-PC	Endpoint	All	Logging;Client Side ...	Logging;Client Side ...	✓	✗	□
Personal Info Control Rule	LIWEI-PC	Endpoint	All	Logging;Client Side ...	Logging;Client Side ...	✓	✗	□
IP control Rule 2	LIWEI-PC	Endpoint	All	Logging;Forensic Dat...	Logging;Forensic Dat...	✓	✓	□
Personal Info Control Rule 2	LIWEI-PC	Endpoint	All	Logging;Client Side ...	Logging;Client Side ...	✓	✓	□

8. Go to **Security Policy → Content Rules** and click **Add Rule**.
9. In the "Rules Status" section, type in a name.
   - o Check the rule as **Active**.
   - o Check the rule as **Apply for Scan**, which means this rule is applied to a data-at-rest scan.
10. In the "Target "section, select **All Endpoints**.
11. In the "Activities" section, select **All Activities**. That means all leakage channels will be inspected by LeakProof 3.0.
12. In the "Sensitive Information Attributes" section, select the **Content Based** radio button. This allows you to apply three matching capabilities.
    - **a.** Select the sensitivity level as **High** or above.
    - **b.** Select the matching level as **Medium** or above.
    - **c.** Select the information classification **Super-Secret**, which was defined previously.
13. In the "Actions to Take" section, select the actions **Logging**, **Client Side Alert**, and **Blocking and Justification** for both online and offline use.
14. Click **Save** to save the new content rule.

Figure 15 *Add Violation Control Rule Page*



Add Violation Control Rule (*: Required field)

Rules Status

*Name Meta Data Match Rule ☑ Active ☑ Apply For Scan

*Target

● All Endpoints ○ Domain/Endpoint ○ Endpoint Group

*Activities

☑ All

☑ Email ☑ FileWrite ☑ FTP ☑ HTTP

☑ HTTPS ☑ IM ☑ PGP Encryption ☑ Web Mail

*Sensitive Information Attributes

○ Content Based

● File Metadata Based

File Extension: *.pdf, *.doc

File Size: From 10M To

Document Type:

□ Unknown □ Obfuscated Archive □ PGP Encrypted

*Actions to Take

Online Actions | Offline Actions

☑ Logging ☑ Client Side Alerting ● No Blocking/Encrypting ☑ Offline Actions Same As Online

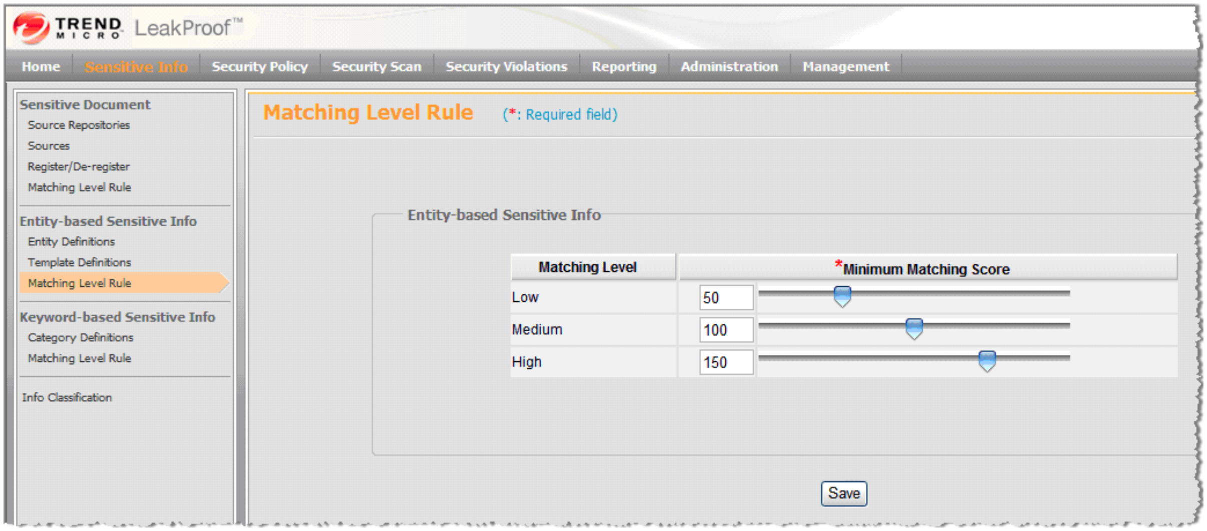
□ Server Side Alerting ○ Blocking

□ Forensic Data Capturing ○ Encrypting □ Justification

Appendix B: Creating a Matching Level Rule

When LeakProof matches a document and its content against a well-defined template, it calculates a matching score based on the matching scoring rules in the template. LeakProof determines the matching level based on the matching score and the matching rules. The administrator can set Matching Level Rules for both Entity-based sensitive Information and Keyword-based sensitive information.

Figure 16 *Matching Level Rule Page*



Matching Level Rule (*: Required field)

Entity-based Sensitive Info

Matching Level	*Minimum Matching Score
Low	50
Medium	100
High	150

Creating an Entity-based Matching Level Rule

When LeakProof matches a document and its content against a well-defined template, it calculates a matching score based on the scoring rules in the template. LeakProof determines the matching level based on the matching score and matching rules.

1. Click **Sensitive Info → Entity-based Sensitive Info → Matching Level Rule**.
2. Set the matching rule by defining the matching levels as **High**, **Medium**, or **Low**.
3. Set the score ranges by either typing in the numbers or moving the scroll bars.

Creating a Keyword-based Matching Level Rule

When LeakProof matches a document and its content against a keyword category, it calculates a matching score by summing up the scores of all keyword occurrences according to an assigned keyword weight. LeakProof then determines the matching level based on the matching score and the matching rules.

To access the Matching Level Rule Page:

1. Click **Sensitive Info → Keyword-based Sensitive Info → Matching Level Rule.**
2. Set the matching rule by defining the matching levels as **Low**, **Medium**, and **High**.
3. Set the score ranges by either typing in the numbers or moving the scroll bars.

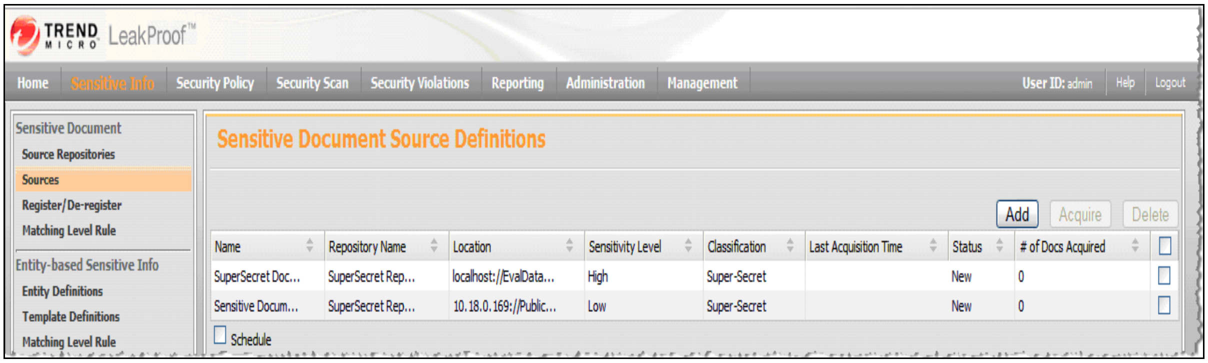
Appendix C: Adding Sensitive Information You Want to Protect

Important Note: Before you start using LeakProof 3.0 to block and log, you must define sensitive data because LeakProof 3.0 works by:

1. Acquiring and fingerprinting the sensitive documents you wanted to protect. By scanning the sensitive documents using the DNA server, you will make sure that these sensitive documents are protected from leaking out of your company regardless if the client is ON or OFF your network. The DNA Server will scan these documents and create fingerprint which can be pushed to the clients along with the policies you have created. Thus, the client will be blocked and or logged when trying to copy to a USB device, email, etc.
2. Defining regular expression based entities: By building a well-defined regex-based entity templates, these templates along with the policies you have created can be pushed to the clients. LeakProof 3.0 will protect documents that contain part or whole of these defined templates.
3. Defining keyword lists. By building well-defined keyword lists, LeakProof 3.0 will protect documents that contain part or all of the specified keywords.

Note: For this evaluation, pre-defined document acquisition tasks and policies have been prepared and shipped with the product. .

Figure 17 *LeakProof 3.0 Sensitive Document Source Definition Page*



Sensitive Document Source Definitions

Name	Repository Name	Location	Sensitivity Level	Classification	Last Acquisition Time	Status	# of Docs Acquired	□
SuperSecret Doc...	SuperSecret Rep...	localhost://EvalData...	High	Super-Secret		New	0	□
Sensitive Docum...	SuperSecret Rep...	10.18.0.169://Public...	Low	Super-Secret		New	0	□

How to add sensitive documents to DNA server and client

For this evaluation, you will put the sensitive information on the DNA server.

1. Copy the documents using SCP to the server.
2. Start WinSCP and start a session with the following information:
   - Host IP or name
   - user name of the DNA server (dgate)
   - password
3. Start WinSCP and start a session with the following information:
   - Transfer the files you wanted to protect to */home/dgate/Directory name you have created*
   - Copy some of these sensitive documents to the local drive of the client with LeakProof agent installed for testing purposes. Put the sensitive documents in the following directory:

     ```
     C:\LeakedDocuments\
     ```

Appendix D: How to Clean up the LeakProof 3.0 DNA Server After the Scenarios are Complete

You can clean up the system after you are done with the scenarios as follows:

1. Create a policy based on the approved policy and remove all rules except the default rule.
2. Go to **Sensitive Info** and delete the following settings:
    - Sensitive Documents:
        - Source repositories
        - Source
    - Entity-based Sensitive Information:
        - Template definition
    - Keyword-based Sensitive Information:
        - Category definitions

About Trend Micro Incorporated

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our Web site at www.trendmicro.com.