



LeakProof Agent Demo (LPAD) Getting Started Guide

Legal Notice

Copyright ©2007 Provilla, Inc. All rights reserved. No reproduction in whole or in part is permitted without prior written approval from Provilla, Inc.

Provilla, the Provilla logo and all other trademarks are properties of their respective owners.

The software provided by Provilla is provided on an "as is" basis without any representations, warranties or conditions of any kind, whether express or implied, statutory, out of a course of dealing or usage, trade or otherwise including any implied warranties or conditions of merchantability, merchantable quality, fitness for any particular purpose or use or non-infringement. Provilla does not represent or warrant that the software will be free of defect, uninterrupted, accurate, complete, current, stable, bug-free, error-free, or available at any time.

To the maximum extent permitted by law, in no event shall Provilla be liable for any direct, indirect, consequential, incidental, special, reliance, punitive or other damages or expenses of any kind, including but not limited to any loss of profits or revenue, lost savings, lost business, lost business opportunities, lost data, lost goodwill, loss from work stoppage, costs of overhead, costs of cover, loss of anticipated benefits hereunder, arising out of or related to this agreement, however caused and on any theory of liability, even if the party has been advised of the possibility of such damages, and notwithstanding the failure of the essential purpose of any limited remedy stated herein.

For more information about Provilla, contact us at:



Address: 1240 Villa St.
Mountain View, CA 94041
USA

TEL: 650-903-9600

Email: info@provilla-inc.com

Website: www.provilla-inc.com

Support: support@provilla-inc.com

1. Introduction

LeakProof from Provilla is a comprehensive solution designed to help organizations protect sensitive information from accidental leak or disclosure, as well as intentional theft. While the full product consists of the LeakProof DataDNA server and LeakProof anti-leak (A/L) Agent, the LeakProof Agent Demo (LPAD) is a stand-alone version of the LeakProof agent. With a pre-built policy, the LPAD demonstrates how the LeakProof agent performs content matching at the endpoint using Provilla's patented content matching technology.

Once LPAD is installed into the endpoint computer, it uses the pre-built policy to filter all outbound content activities involving file copying to external drives (such as USB), or network activity including :

- HTTP/HTTPS post
- email (Outlook exchange and Lotus Notes)
- web-mail bodies
- web-mail attachments
- FTP, SMTP, Instant Messaging and PGP encryption

If sensitive content is detected by LPAD, the user is alerted, via a client dialog box, that the operation is not recommended.

2. Installation

2.1 Hardware Requirements

LPAD should be installed on a system with the following minimum hardware requirements:

- CPU - Intel Pentium II or above
- At least 128 MB RAM
- Free hard disk space: 100 MB
- Agent requires approximately 7MB RAM

2.2 Software Requirements

- Windows 2000 Professional/Server/Advanced Server
- Windows XP Home/Professional
- Windows Server 2003

2.3 Installation of LPAD

The download package of LPAD is a zip file. There are three parts to the LPAD package:

- LeakProofDemo v1.msi – LPAD installation file
- Provilla LeakProof Agent Demo Users Guide – This document

- Directory “LeakProofDemo-TestFiles” - Sample files for LPAD testing

After unzipping the LPAD package and extracting the MSI file, double-click on the installation file (LeakProofDemo1.0.msi). This will take you through the easy to use installation process. At the end of installation, you will need to restart the machine.

2.4 Un-installation of LPAD

To uninstall LPAD, you can double-click on the installation file (LeakProofDemo1.0.msi), to begin the un-installation process.

3. Pre-Built Policy

In the full LeakProof product, these policies are configured in the server and pushed to each agent endpoint. Unlike the full product, LPAD is shipped with a pre-built policy to detect the following types of violations.

- **Password Protected Archive**

If LPAD detects an outbound archive that is password protected, it will alert the user. The LPAD test file shipped with LPAD contains one sample file (importing.rar) in the “\LPAD\LPAD Test Files\ArchiveWithPassword” directory.

- **Large File**

If LPAD detects an outbound file larger than 5M, it will alert the user. The LPAD test file shipped with LPAD contains one sample file (gaim-1.3.1.exe) in the “\LPAD\LPAD Test Files\Big Files” directory.

- **Fingerprinted Samples Files with DataDNA**

One of LeakProof’s core technologies is signature generation of DataDNA. This enables the generation of DataDNA from files to detect matches of sensitive data. Detection takes place even when the content has been changed, including adding, deleting, shuffling, name changing, extension changing, etc. As long as at least 50% of the original content exists within the file, LPAD will detect it. The test files shipped with LPAD contain fifty sample files (10 each in MS Word, MS Excel, MS PPT, PDF and plain text format) in the “\LPAD\LPAD Test Files\DNAFiles” directory.

- **Entity Data**

LPAD can detect entity data such as Social Security Numbers (SSN), Credit Card numbers, Dates, Phone Number, email addresses, mailing addresses and any data that can be detected by a regular expression. LPAD is pre-packaged to detect the following entity data combinations, which are designed to represent customer confidential data (two samples):

Sample 1: SSN + Credit Card Number + Phone Number + Email address + Home address + CA Driver's License Number (all must be present)

Sample 2: Customer Account Number (e.g. ABCD-12345678 or CNDF12345678) + Credit Card Number + Phone Number + Email address + Home address + CA Driver's License Number (all must be present)

The test file shipped with LPAD contains three sample files in the “\LPAD\LPAD Test Files\EntityFiles” directory. One of the entity files, “CustomerData_BadSSN.xls,” shows that LPAD actually is further validating the SSN using a SSN rule to eliminate false positives.

- **Keyword Matching**

LPAD will detect any content that contains “ABCDCompany Confidential” or “ABCDCompany Top Secret” or “ABCDCompany Proprietary”. The LPAD test file shipped with LPAD contains three sample files in the “\LPAD\LPAD Test Files\KeywordFiles” directory.

4. Using LPAD to Evaluate the LeakProof Solution

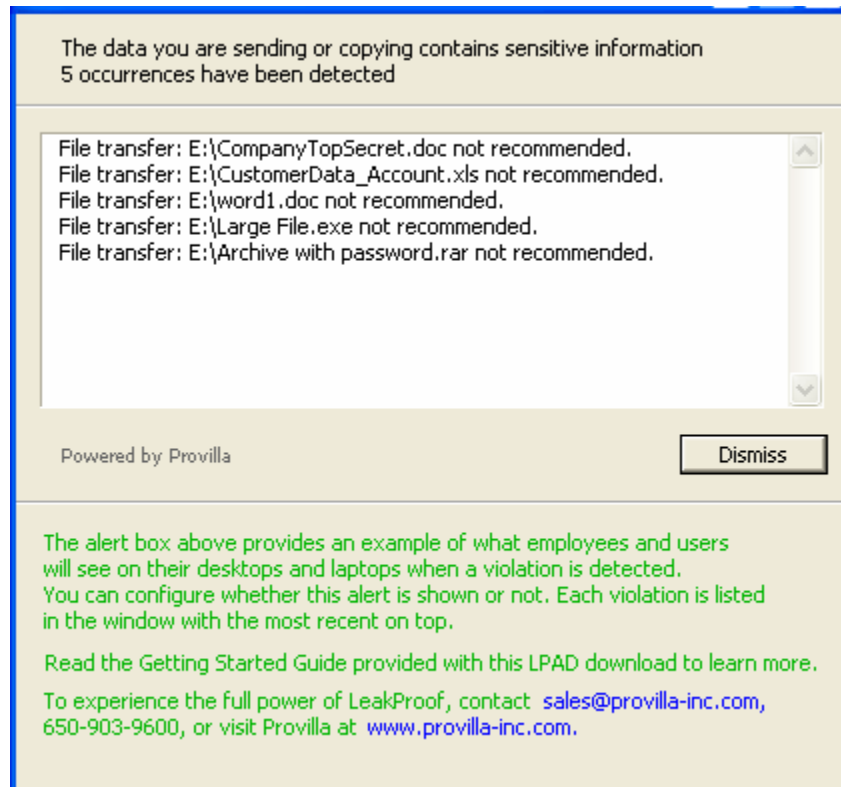
The LPAD client software is an ideal way to see the LeakProof Agent in action at the client (endpoint). After successfully installing LPAD and the sample files, the best way to observe the agent in action, and to experience the power of the DataDNA technology, is to try various activities using the sample files. Some suggested examples include:

- Open one of the DataDNA files and edit it, saving the file under a different name and in a different directory. Then attempt to copy the file to your USB drive.
- Create an email and attach one of the Entity data sample files to the email, then send.
- Create an email and cut/paste the keyword content from a KeywordFiles file into the body of the email, then send.

For each violation, the Client Alert window will pop up on your system.

5. The Client Alert Window

Performing any outbound activities using sensitive data as described in the examples above will result in the activity being detected by LPAD. Once an activity is detected, a client alert window being displayed. This window demonstrates that the LPAD agent has successfully detected the leakage activity.



LeakProof enables the administrator to configure whether or not a client side alert is presented after detection of a policy infraction. If enabled, the client alert can simply notify the user that the action involves sensitive information, and let the user proceed while logging the incident on the server. Alternatively, the client alert can block the user's activity from completion while logging it on the server.

6. Limitations

LPAD provides a subset of the full feature set available with the LeakProof product. It is intended to demonstrate the content matching capabilities of the agent and the DataDNA technology *after a policy has been established*. LPAD does not demonstrate the **server-based** features of LeakProof. LPAD does not demonstrate the following features that the full LeakProof product provides:

- **Sensitive Information Repository Scanning.** Sensitive data can be scanned by the appliance in order to extract the signature of each document. Repositories include file servers and document management systems.
- **Security Policy Configuration.** This takes place on the DataDNA server and provides ultimate flexibility and granularity for endpoint based policies.
- **Security Incident Logging.** The events captured by the LeakProof Agent are logged on the server. A summary is presented in the Dashboard.
- **Security Incident Forensic Capturing.** Full records of the actual content and files attempted to be sent or copied can be captured on the server for later analysis.
- **Security Incident Blocking.** The client is able to be configured to block any activity, such as file copying or emails which contain sensitive information, depending upon the policy configured on the server.
- **Security Incident Reporting.** The server is able to produce a number of valuable reports to enhance analysis.

The policy file may be customized for any environment in order to perform further testing or demonstrate LPAD to others. For changes to the pre-built security policy or to evaluate the full LeakProof product, please contact Provilla for further assistance at 650.903.9600 or sales@provilla-inc.com.

7. LPAD License

LPAD's trial is limited to 30 days from the date of install. In order to extend the license, evaluate the full LeakProof solution, or buy the full product, please contact Provilla for further information.