Trend Micro Incorporated reserves the right to make changes to this document and to the products described herein without notice. Before installing and using the software, please review the readme files, release notes, and the latest version of the applicable user documentation, which are available from the Trend Micro website at:

http://docs.trendmicro.com

Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.

Copyright © 2012 Trend Micro Incorporated. All rights reserved.

Document Part No.: LPEM54473/ 100607

Release Date: June 2012


The user documentation for Trend Micro Data Loss Prevention introduces the main features of the software and installation instructions for your production environment. Read through it before installing or using the software.

Detailed information about how to use specific features within the software are available in the online help file and the online Knowledge Base at the Trend Micro website.

Trend Micro always seeks to improve its documentation. If you have questions, comments, or suggestions about this or any Trend Micro document, please contact us at docs@trendmicro.com.

Please evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp
# Table of Contents

**Chapter 1: Introduction**

Data Loss ......................................................................................................................... 1-2
Trend Micro Data Loss Prevention .................................................................................. 1-2
  Trend Micro Data Loss Prevention Endpoint 5.6 .................................................. 1-3
  Trend Micro Data Loss Prevention Network Monitor 2.0 .................................. 1-4
Infrastructure .................................................................................................................. 1-5
Key Terminology ............................................................................................................. 1-6
Content-aware Mechanisms ......................................................................................... 1-7
New in this Release ....................................................................................................... 1-8
System Requirements .................................................................................................... 1-8

**Chapter 2: Summary**

Web Console Access .......................................................................................................... 2-2
  Browser Prerequisites ............................................................................................... 2-3
Web Console Navigation .................................................................................................. 2-6
Summary Tabs ................................................................................................................... 2-7
  Executive Summary Tab .......................................................................................... 2-7
  DLP Incidents Tab ................................................................................................. 2-9
  Refreshing Summary Data .................................................................................... 2-11
  Printing Summary Reports ................................................................................... 2-12

**Chapter 3: Data Protection**

Data Protection ............................................................................................................... 3-2
  Data Identifiers ....................................................................................................... 3-2
    Expressions .......................................................................................................... 3-3
    File Attributes ..................................................................................................... 3-10
    Fingerprints ......................................................................................................... 3-13
    Keyword Lists ...................................................................................................... 3-21
### Chapter 4: Reports

- Generate Reports ................................................................. 4-2
  - Generating a New Report .................................................. 4-2
- Archived Reports ................................................................. 4-6
  - Viewing Archived Reports ................................................. 4-6

### Chapter 5: Logs

- Log Query ............................................................................... 5-2
  - Querying Logs ................................................................. 5-2
- Log Cleanup ........................................................................... 5-3
  - Cleaning Up Logs ............................................................. 5-4
- Log Restore ........................................................................... 5-5

### Chapter 6: Update

- Agents ..................................................................................... 6-2
Chapter 7: Administration

Server Configuration ................................................................. 7-2
   Fingerprint Settings ................................................................. 7-2
   Application Settings ................................................................. 7-5
Agent Settings ................................................................................. 7-6
   Configuring Agent Settings ....................................................... 7-6
Advanced Settings ........................................................................ 7-10
   Configuring the Alert Dialog Box .......................................... 7-10
   Configuring Agent Module Logging ....................................... 7-12
   Activating the UDP Listener ................................................... 7-13
Global Exceptions ....................................................................... 7-15
Remote Crawler Management ....................................................... 7-18
Remote Crawler Installation and Configuration ............................ 7-19
   Installing the Remote Crawler ............................................... 7-19
   Adding Repositories to Scan ............................................... 7-22
   Adding Fingerprint Definitions for the Remote Crawler ....... 7-25
   Reconfiguring the DLP Manager Server Address .................. 7-27
   Deleting Remote Crawler Agents ......................................... 7-27
Data Management ....................................................................... 7-28
   Exporting DLP Data ............................................................... 7-29
   Importing DLP Files Under 200MB ....................................... 7-29
   Importing DLP Files Over 200MB .......................................... 7-30
   Viewing and Downloading Exported Files ............................. 7-30
Agent Management .................................................................... 7-31
   Viewing and Editing Agent Information ................................. 7-32
Deleting Agents from the Agent Management List ......................... 7-33
Managing Agent Groups ...................................................................... 7-33
Creating New Groups ......................................................................... 7-34
Web Console Password ........................................................................ 7-35
Management Console .......................................................................... 7-36
User Account Management .................................................................. 7-36
Role Management ................................................................................. 7-38
Configuring LDAP Settings ................................................................. 7-40
Product License .................................................................................... 7-42
About Licenses ....................................................................................... 7-43
Viewing Existing Licenses .................................................................. 7-44
Activating DLP Products ..................................................................... 7-44
Renewing Licenses ............................................................................... 7-45
System Monitoring ............................................................................... 7-46

**Chapter 8: Command Line Interface Commands**

DLP Endpoint CLI Command Overview ................................................. 8-2
Accessing the Privileged CLI Mode .................................................... 8-2
Accessing the OS Shell ........................................................................ 8-3
DLP Endpoint CLI Commands ............................................................. 8-4
DLP Network Monitor CLI Commands ............................................... 8-13

**Index**

Index ................................................................................................. IN-1
Introduction

Trend Micro™ Data Loss Prevention is an enterprise-class information loss prevention solution. Depending on your implementation, Trend Micro Data Loss Prevention includes Data Loss Prevention Endpoint and Data Loss Prevention Network Monitor.
Data Loss

Traditional security solutions are focused on preventing external security threats from reaching the network. In today’s security environment, this is only half the story. Data breaches are now commonplace, exposing an organization’s confidential and sensitive data—referred to as digital assets—to unauthorized parties. A data breach may occur as a result of internal employee mistakes or carelessness, data outsourcing, stolen or misplaced computing devices, or malicious attacks.

Data breaches can:

• Damage brand reputation
• Erode customer trust in the organization
• Introduce unnecessary remediation and non-compliance costs
• Lead to lost business opportunities and revenue when intellectual property is stolen

With the prevalence and damaging effects of data breaches, organizations now see digital asset protection as a critical component of their security infrastructure.

Trend Micro Data Loss Prevention

Trend Micro™ Data Loss Prevention (DLP) safeguards an organization’s digital assets against accidental or deliberate leakage. DLP allows you to:

• Identify the digital assets to protect
• Create policies that limit or prevent the transmission of digital assets through common channels, such as email and external devices
• Enforce compliance to established privacy standards

The complete Trend Micro Data Loss Prevention solution includes the following components:

• Trend Micro Data Loss Prevention Endpoint 5.6
• Trend Micro Data Loss Prevention Network Monitor 2.0
Trend Micro Data Loss Prevention Endpoint 5.6

Trend Micro Data Loss Prevention Endpoint helps organizations protect sensitive information from accidental disclosure and intentional theft. DLP Endpoint prevents loss of sensitive data through endpoint-based enforcement and accurate fingerprinting and content matching technology. DLP Endpoint detects digital assets and automatically takes actions specified in your company policies, from blocking and logging to encrypting and alerting.

DLP Endpoint 5.6 Features

• Data identifier and template libraries for easy policy creation
• File type recognition, with support for:
  • Executable files
  • Documents and encoding methods
  • Graphics
  • Vector Graphics
  • Multimedia files
  • Compressed files
  • Databases
  • Spreadsheets
  • Presentation and diagram files
  • Desktop publishing files
  • Linked and embedded files
  • Encrypted files
• Data discovery capabilities that locate digital assets stored on laptops, desktops, and servers
• End user device control, with support for:
• Storage devices: CD/DVD, USB
• Non-storage devices: COM and LPT ports, infrared and imaging devices, modems, PCMCIA card, print screen key
• Expanded privacy protection that includes filters for:
  • Network channels: Network protocols, such as HTTP and FTP
  • System and application channels: A local computer’s applications and peripherals
• Multiple matching engines to detect structured and unstructured data
• Policy enforcement actions, such as block, allow, alert, encrypt, justify, and log
• Continuous data monitoring
• Active Directory integration and delegated administration
• Web-based management console for policy configuration and deployment, consolidated endpoint reporting, fingerprint extraction, and updates

**Trend Micro Data Loss Prevention Network Monitor 2.0**

Trend Micro Data Loss Prevention Network Monitor is an optional network monitoring component delivered in appliance mode for fast and easy implementation. This component captures network traffic and matches the intercepted content to fingerprint data and DLP security policies.

DLP Network Monitor also acts as an agent, and is configured and managed using the DLP Endpoint web console. Each Network Monitor must be registered with the DLP management server to be able to monitor network traffic.

---

**Note**

DLP Network Monitor is sold separately.

**DLP Network Monitor 2.0 Features**

• Fast, easy deployment with software appliance-based delivery and no third-party applications
• Little to no load or performance impact on the network device to which it is attached

• Monitors and detects sensitive content in network traffic, including:
  • Content whose loss might result in non-compliance with regulations
  • Company confidential information or intellectual property
  • Data stealing malware (DSM)

• Easy, regular updates for detecting new malware

• Data filtering across the most common protocols for internal to external network data transfer: SMTP, HTTP, FTP, IM, Webmail

• Data filtering across the most common protocol for transmitting inter-departmental traffic: Server Message Block (SMB)

• Centrally managed from the DLP management server with a simple command line interface (CLI) console for basic network configuration and troubleshooting

**Infrastructure**

The complete DLP Endpoint solution employs a client-server architecture with a software agent, server, remote crawler, and Web-based console.

• **Endpoint agent:** Non-intrusive monitoring and enforcement software installed on client machines. The agent receives policy and fingerprint updates from the server and sends back incident details.

• **Network agent:** Refers to each DLP Network Monitor device. The agent must be registered with the DLP management server to be able to monitor network traffic.

• **Management server:** An appliance that handles the overall administration of the solution, and stores all relevant data and configurations.

• **Remote crawler:** Scans for digital assets stored on desktops and laptops even if users are not connected to the company network. The remote crawler can acquire fingerprints for files stored on systems other than the management server and forwards generated fingerprints to the management server. This protects files
stored locally (on computers where the Remote Crawler is installed) or in a document management environment that the server may or may not have access to.

- **Web console**: Supports an administrative workflow for defining digital assets, creating confidential rules, deploying policies to agents, performing data discovery scans, monitoring, and reporting.

**Key Terminology**

- **Acquisition**: The process of creating and storing document fingerprints.
- **Data Discovery**: An automated scan that locates digital assets on laptops, desktops, and servers.
- **Data identifier**: An object that helps identify digital assets and serves as building blocks for templates. They are matched against existing data to determine if it is sensitive data that requires action.
- **DSM**: Data-stealing malware.
- **Expression**: Structured text elements that define a digital asset. Text is defined by regular expressions.
- **File attribute**: File metadata, such as file size and file type.
- **Fingerprint**: A DLP-generated document pattern that can survive a moderate content change. DLP generates multiple fingerprints per document, and then analyzes transmitted documents to identify potential data leaks.
- **Keyword list**: List of words or phrases that can identify sensitive data sets.
- **NCCE**: Network Content Correlation Engine. Analyzes network packages for threat-related network traffic.
- **NCCP**: Network Content Correlation Pattern. Works with NCCE.
- **Policy**: A set of rules that defines the actions DLP should take after identifying digital assets.
• **Remote Crawler**: A software module that fetches and generates document fingerprints from document repositories.

• **Template**: A condition statement comprised of data identifiers and logical operators (AND, OR, EXCEPT)

---

### Content-aware Mechanisms

Trend Micro Data Loss Prevention uses five content-aware mechanisms to identify digital assets stored on laptops, desktops, servers, and (with Network Monitor) in network traffic.

• **Expression matching**: DLP identifies digital assets using predefined and customized expressions. Expression matching is best used with structured content, such as credit card numbers, national ID numbers, or phone numbers.

• **File attribute matching**: DLP identifies digital assets using file attributes, such as file type and file size. DLP performs true file type detection to determine the correct file type even if the extension is altered.

• **Fingerprint matching**: DLP acquires fingerprints from a stored document and compares these with fingerprints acquired from a transmitted file. If the number of common fingerprints matches the number specified in a template, DLP determines that the transmitted file is sensitive. Fingerprint matching works best with unstructured content.

• **Keyword list matching**: DLP identifies digital assets using predefined and customized keyword lists.

• **Template matching**: DLP identifies digital assets using predefined and customized templates that combine data identifiers (expressions, file attributes, fingerprints, and keyword lists) with operators (such as AND and OR) to form condition statements. If conditions are met, DLP takes actions based on policy settings.
New in this Release

Trend Micro Data Loss Prevention Endpoint 5.6 includes enhancements to the following:

- Predefined data identifier library: Includes expressions and keyword lists that support common digital assets from different countries
- Predefined template library: Includes regulatory compliance templates, expression and keyword list specific templates, and general purpose templates
- Supported applications: Includes Outlook 2010 and HTTPS over Internet Explorer 9
- Supported operating systems: Includes Windows 64-bit operating systems
- Global exceptions: Includes support for fully qualified domain names (FQDN)

System Requirements

Management Server

The Management Server can be delivered as either a physical or virtual appliance.

The physical appliance is built on one of two types of purpose-built 1U rack-mountable Dell-based appliance.

Table 1-1. Physical Appliance System Requirements

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Dell R610</th>
<th>Dell PE1950-III</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Xeon-E5506, 2.13GHz</td>
<td>Xeon E5410, 2.33GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>6GB</td>
<td>2GB or 4GB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>250GB</td>
<td>160GB or 250GB</td>
</tr>
<tr>
<td>Network Interface Card (NIC)</td>
<td>Gigabit Ethernet</td>
<td></td>
</tr>
<tr>
<td>Operating System</td>
<td>CentOS Version 4.6</td>
<td></td>
</tr>
</tbody>
</table>

The following VMware versions are supported for the virtual appliance:
- VMware Workstation 6.0, 6.5, 7.0, 8.0
- VMware ESX(i) 3.5, 4.0, 4.1

### Table 1-2. Virtual Appliance System Requirements

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1024MHz Intel Pentium or equivalent</td>
<td>2048MHz Intel Pentium</td>
</tr>
<tr>
<td>RAM</td>
<td>2048MB</td>
<td>4096MB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>30GB</td>
<td>200GB</td>
</tr>
<tr>
<td>Network Interface Card (NIC)</td>
<td>10/100Mbps</td>
<td>1Gbps</td>
</tr>
</tbody>
</table>

### Endpoint Agent

### Table 1-3. Endpoint Agent System Requirements

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Minimum</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>300MHz Intel Pentium or equivalent</td>
<td>1024MHz Intel Pentium</td>
</tr>
<tr>
<td>RAM</td>
<td>128MB</td>
<td>1024MB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>300MB</td>
<td>1GB</td>
</tr>
<tr>
<td>Network Interface Card (NIC)</td>
<td>10/100 Mbps</td>
<td></td>
</tr>
<tr>
<td>SPECIFICATIONS</td>
<td>MINIMUM</td>
<td>RECOMMENDED</td>
</tr>
<tr>
<td>---------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating System</td>
<td><strong>32-bit</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 7 Ultimate SP1, Enterprise SP1, Professional SP1, Starter SP1,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Home Premium SP1, Home Basic SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Vista Enterprise SP1/SP2, Business SP1/SP2, Home Premium SP1/SP2,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ultimate SP1/SP2, Home Basic SP1/SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional SP2/SP3, Home SP2/SP3, Tablet 2005, Media Center</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SP2/SP3</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 Datacenter SP1/SP2, Enterprise SP1/SP2, Standard SP1/SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise SP1/SP2, Datacenter SP2, Standard SP1/SP2,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Standard R2 SP1/SP2, Standard R2 SP1/SP2, Web Edition SP2, Enterprise R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>SP1/SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>64-bit</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 7 Ultimate SP1, Enterprise SP1, Professional SP1, Starter SP1,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Home Premium SP1, Home Basic SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows Vista Enterprise SP1/SP2, Business SP1/SP2, Home Premium SP1/SP2,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ultimate SP1/SP2, Home Basic SP1/SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional SP1/SP2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 Datacenter SP1/SP2, Enterprise SP1/SP2, Standard SP1/SP2,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise R2 SP1, Standard R2 SP1</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise SP1/SP2, Datacenter SP2, Standard SP1/SP2,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Standard R2 SP1/SP2, Standard R2 SP1/SP2, Web Edition SP2, Enterprise R2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise SP1/SP2, Datacenter SP2, Standard SP1/SP2,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Standard SP1/SP2, Standard R2 SP1/SP2, Web Edition SP2, Enterprise R2</td>
<td></td>
</tr>
</tbody>
</table>

**Network Agent**
### Table 1-4. Network Agent System Requirements

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Dell R710</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>2 x Intel Quad Core Xeon-X5550, 2.66 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>8GB (4 x 2GB)</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>300GB</td>
</tr>
<tr>
<td>Network Interface Card (NIC)</td>
<td>Intel PRO 1000PT 1GbE Dual Port, PCIe-4</td>
</tr>
<tr>
<td>Maximum Throughput</td>
<td>80Mbps</td>
</tr>
<tr>
<td>Operating System</td>
<td>CentOS Version 5.3</td>
</tr>
</tbody>
</table>

### Remote Crawler

### Table 1-5. Remote Crawler System Requirements

<table>
<thead>
<tr>
<th>Specifications</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAM</td>
<td>512MB</td>
</tr>
<tr>
<td>Available Disk Space</td>
<td>20GB</td>
</tr>
<tr>
<td>Specifications</td>
<td>Recommended</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Operating System</td>
<td>32-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 Ultimate SP1, Enterprise SP1, Professional SP1, Starter SP1, Home Premium SP1, Home Basic SP1</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista Enterprise SP1/SP2, Business SP1/SP2, Home Premium SP1/SP2, Ultimate SP1/SP2, Home Basic SP1/SP2</td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional SP2/SP3, Home SP2/SP3, Tablet 2005, Media Center SP2/SP3</td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 Datacenter SP1/SP2, Enterprise SP1/SP2, Standard SP1/SP2</td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Datacenter SP2, Enterprise SP1/SP2, Enterprise R2 SP1/SP2, Standard SP1/SP2, Standard R2 SP1/SP2, Web Edition SP2</td>
</tr>
<tr>
<td></td>
<td>64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 2008 Enterprise SP1/SP2</td>
</tr>
<tr>
<td></td>
<td>• Windows 2003 Enterprise SP1/SP2, Enterprise R2 SP1/SP2</td>
</tr>
</tbody>
</table>
Summary

The **Summary** screen is a robust dashboard for viewing executive summaries of incident and system reports.
Web Console Access

Access the web console at: http://<serverMachineName>:8080/dsc/

![Logon screen](image)

**Figure 2-1. Logon screen**

**Note**
Set the `<serverMachineName>` to the machine name or IP address of the machine running the management server.

These are the default users:

- admin
- root, enable, dgate (for Linux command usage)

If you installed the management server as a virtual appliance, use the password that you set up during installation. If the management server came pre-installed on a physical appliance, use the default password. Be sure to change the password after logging on.
Tip
Trend Micro recommends that you log off the web console when you are not using it. An idle user session automatically times out after 30 minutes.

Browser Prerequisites

Note
In order to access all features provided by the UI, cookie support is required.

The following browsers can be used to access the web console.

- Microsoft Internet Explorer™ 9
- Microsoft Internet Explorer™ 8
- Microsoft Internet Explorer™ 7
- Microsoft Internet Explorer™ 6 SP2/SP3
- Mozilla Firefox™ 12
- Mozilla Firefox™ 11
- Mozilla Firefox™ 10

Note
The web console does not support multiple sessions on a single machine at any given time.

Configuring Internet Explorer Security Settings

1. On Internet Explorer, select Tools > Internet Options and then click the Security tab.
2. Set the zone security level to Medium-low.

3. Click the Privacy tab and set privacy settings to Medium.

4. Click Apply and click OK.

**Configuring Mozilla Firefox Security Settings**

1. On the Tools > Options > Content screen, select Enable JavaScript.
2. On the **Tools > Options > Privacy** screen, select **Firefox will: Remember history**.
Web Console Navigation

The web console defaults to the Summary screen.

![Summary screen](image)

**Figure 2-4. Summary screen**

The left navigation bar accesses six functional areas:

- **Summary**: Displays summaries of DLP incidents over a range of time (seven days by default) plus system status.

- **Data Protection**: Enables you to configure data identifiers, templates, company policies, data discovery scans, and device control.

- **Reports**: Enables you to define and generate reports.

- **Logs**: Enables you to query and view various logs for specific dates or a range of dates.

- **Updates**: Enables you to test and deploy new versions of patches, plug-ins and fingerprints.

- **Administration**: Enables you to configure and/ or manage the server configuration, agents, crawlers, data, endpoints, user accounts and roles.
Summary Tabs

The Executive Summary and DLP Incidents tabs display customized UIs based on your role and account permissions. Data is pulled from logs uploaded from agents to the management server. DLP summarizes data in near real-time (10 minutes by default) on the Executive Summary tab and in real-time on the DLP Incidents tab.

Note

If an agent is disconnected from the network, such as a laptop working offline, agents continue to monitor and protect the disconnected machine. After the machine reconnects, the agent uploads offline incident logs to the management server. Offline incidents are then counted in the DLP Incidents summary charts and reports.

If an offline agent log uploads after a Summary report runs, you can go to Reports > Generate Reports to run a one-time report for the latest information.

Executive Summary Tab

Executive summary charts display the number of DLP incidents per channel. Channels are color-coded for easy viewing. DLP summarizes data in near real-time (10 minutes by default).

Note

“This Week” on the x-axis of the executive summary charts refers to data gathered since Monday of the current week.
Figure 2-5. Executive Summary tab
An account with full permissions displays the following executive summary charts:

**TABLE 2-1. Executive Summary Charts**

<table>
<thead>
<tr>
<th>Chart</th>
<th>Time Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Incident Summary Trend by Channel</td>
<td>Includes data from the current week and the previous seven weeks. The current week starts on Monday.</td>
</tr>
<tr>
<td>Data Stealing Malware DLP Incident Summary Trend by Channel</td>
<td>Includes data from the current week and the previous seven weeks. The current week starts on Monday.</td>
</tr>
<tr>
<td>Incident Distribution</td>
<td>Includes data from Monday of the current week.</td>
</tr>
<tr>
<td>Top 5 Department DLP Incidents</td>
<td>Includes data for the last 4 weeks and the current week.</td>
</tr>
<tr>
<td>Top 5 Policy DLP Incidents</td>
<td>Includes data for the last 4 weeks up to the current week. The current week starts on Monday.</td>
</tr>
<tr>
<td>Top 5 High Risk Users</td>
<td>Includes data from the previous and current weeks. The current week starts on Monday.</td>
</tr>
</tbody>
</table>

**Note**

High-risk users trigger more incidents than other users.

<table>
<thead>
<tr>
<th>Chain</th>
<th>Time Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Top 5 Users Infected by Data Stealing Malware</td>
<td>Includes data from Monday to the current week. The current week starts on Monday.</td>
</tr>
<tr>
<td>Top 5 IPs Infected by Data Stealing Malware</td>
<td>Includes data from Monday of the current week. The current week starts on Monday.</td>
</tr>
<tr>
<td>Top 5 Email Account DLP Incidents</td>
<td>Includes data from Monday of the current week.</td>
</tr>
</tbody>
</table>

**DLP Incidents Tab**

The **Incidents** tab summarizes incidents over time, by channel and agent. The time span is seven days by default, and data is summarized in real time. If your
implementation includes DLP Network Monitor, you can view summaries for both network agents and endpoint agents. Otherwise, DLP sets network agent values to zero (0).

**Figure 2-6. DLP Incidents tab**
### Table 2-2. DLP Incidents Tab Charts

<table>
<thead>
<tr>
<th>Chart</th>
<th>Notes</th>
</tr>
</thead>
</table>
| Top Agents and DLP Incidents Summary       | • For the Endpoint Agents tab, the Top Agents and Incidents Summary report displays the top 5 endpoints with the most incident logs reported in the past 90 days. The report is color-coded by online/offline incidents.  
• For the Network Agents tab, the Top Agents and Incidents Summary report displays the top 5 IP sources with the most incident logs reported in the past 90 days. |
| DLP Incidents Over Time                    | This chart is color-coded by agent type: Endpoint Agent and Network Agent. If you are not running DLP Network Monitor, only one line displays. You can select to view this chart by 1 week or 1 month.                           |
| Security Events                            | This table displays information about the last 10 incidents.                                                                                                                                               |
| DLP Incidents                              | This table displays the total number of incidents by channel over the last 90 days. “Total” is the total number of incidents found by both endpoint and network agents (if your implementation includes DLP Network Monitor).    |
| Agent Status                               | This table displays the number of agents that are offline or online.                                                                                                                                       |
| Top DLP Incident Sources                   | This table displays information about the top 5 incident sources over the last 90 days.                                                                                                                 |

### Refreshing Summary Data

1. Click **Refresh** on the **Summary** screen to update report data. See **Executive Summary Tab** on page 2-7 to view the time periods for the reports.

---

**Note**

Summary report data is pulled from agent logs. If agents upload logs to the server while you are on the Summary page, there may be a 10-minute delay before they are counted in the Executive Summary tab.
Printing Summary Reports

You can click Print on the Summary screen to print the Summary reports.

---

**Note**
The Summary print function directly calls the browser print function. To maintain the web page formatting style, you must configure the print background and layout settings in your browser.

---

**Configuring Microsoft Internet Explorer Print Settings**

1. Open your browser and click **Tools > Internet Options > Advanced**.
2. Scroll down to Printing and select **Print background colors and images**.

---

**Note**
If you are using Microsoft Internet Explorer 6, select **Landscape** in **File > Page Setup > Orientation**.

---

**Configuring Mozilla Firefox Print Settings**

1. Open your browser and click **File > Page Setup**.
2. Select **Print Background (color & images)**.
3. Select **Shrink to Fit Page Width**.
Data Protection

This chapter describes how to configure data identifiers, templates, policies, data discovery, and device control.
Data Protection

Before you can monitor digital assets for potential loss, you must be able to answer the following questions:

• What data needs protection from unauthorized users?
• Where does the sensitive data reside?
• How is the sensitive data transmitted?
• What users are authorized to access or transmit the sensitive data?
• What action should be taken if a DLP incident occurs?

This important audit typically involves multiple departments and personnel familiar with the digital assets in your organization.

If you already defined your digital assets and security strategy, you can begin to define data identifiers, templates, and policies.

Data Identifiers

DLP uses data identifiers to define and recognize digital assets. Data identifiers combine with actions in policies.

DLP uses the following data identifiers.

• Expressions: Data that has a certain structure.
• File attributes: File properties such as file type and file size.
• Fingerprints: Document pattern used for unstructured content.
• Keyword lists: A list of special words or phrases.
Note
You can define or modify any type of data identifier at any time. However, new or modified data identifiers do not take effect until you manually deploy them through the Policies screen.

Expressions

An expression is data that has a certain structure. For example, credit card numbers typically have 16 digits and appear in the format "nnnn-nnnn-nnnn-nnnn", making them suitable for expression-based detections.
You can use predefined and customized expressions. For details, see Predefined Expressions on page 3-4 and Customized Expressions on page 3-5.

**Figure 3-1. Expressions screen**

**Predefined Expressions**

DLP comes with a set of predefined expressions. After DLP matches potential digital assets with an expression, the data may undergo additional verification checks.

**Expression Validators**

Data units follow semantic rules. Not every 9-digit number is a valid social security number and not every 15 or 16-digit number is a valid credit card number. To reduce false positives, expression validators check if the extracted data units follow these rules.

For a list of predefined expressions and expression validators, see:
Customized Expressions

Create customized expressions if none of the predefined expressions meet your requirements.

Expressions are a powerful string-matching tool. Ensure that you are comfortable with expression syntax before creating expressions. Poorly written expressions can dramatically impact performance.

When creating expressions:

- Refer to the predefined expressions for guidance on how to define valid expressions. For example, if you are creating an expression that includes a date, you can refer to the expressions prefixed with "Date".

- Note that DLP follows the expression formats defined in Perl Compatible Regular Expressions (PCRE). For more information on PCRE, visit the following website:
  
  http://www.pcre.org/

- Start with simple expressions. Modify the expressions if they are causing false alarms or fine tune them to improve detections.

Expression Criteria

There are several criteria that you can choose from when creating expressions. An expression must satisfy your chosen criteria before DLP subjects it to a policy. Choose one of the following criteria for each expression:

**Table 3-1. Expression Criteria**

<table>
<thead>
<tr>
<th>CRITERIA</th>
<th>RULE</th>
<th>EXAMPLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>None</td>
<td>Names of U.S. citizens</td>
</tr>
<tr>
<td>CRITERIA</td>
<td>RULE</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>------------------</td>
<td>----------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Specific characters</td>
<td>An expression must include the characters you have specified.</td>
<td>US: ABA Routing Number</td>
</tr>
<tr>
<td></td>
<td>In addition, the number of characters in the expression must be</td>
<td>• Expression: <code>[^\w\\\{&quot;\}\-=&amp;&quot;] ([0123678]\d{8})[^\w-]+</code></td>
</tr>
<tr>
<td></td>
<td>within the minimum and maximum limits.</td>
<td>• Characters: 0123456789</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Minimum number of digital asset characters: 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maximum number of digital asset characters: 9</td>
</tr>
<tr>
<td>Suffix</td>
<td>Suffix refers to the last segment of an expression. A suffix</td>
<td>Home address, with zip code as the suffix</td>
</tr>
<tr>
<td></td>
<td>must include the characters you have specified and contain a certain</td>
<td>• Expression: `[^D[^d+[^s[a-z.]+[^s([a-z]+[^s\s[0,2]{lane</td>
</tr>
<tr>
<td></td>
<td>number of characters.</td>
<td>• Suffix characters: 0123456789-</td>
</tr>
<tr>
<td></td>
<td>In addition, the number of characters in the expression must be</td>
<td>• Number of suffix characters: 5</td>
</tr>
<tr>
<td></td>
<td>within the minimum and maximum limits.</td>
<td>• Minimum number of digital asset characters: 25</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maximum number of digital asset characters: 80</td>
</tr>
<tr>
<td>CRITERIA</td>
<td>RULE</td>
<td>EXAMPLE</td>
</tr>
<tr>
<td>--------------------------</td>
<td>----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Single-character separator | An expression must have two segments separated by a character. The character must be 1 byte in length. In addition, the number of characters left of the separator must be within the minimum and maximum limits. The number of characters right of the separator must not exceed the maximum limit. | Email address
  • Expression: `[^\w.][\w.] {1,20}@[a-z0-9]{2,20}[\.][a-z]{2,5}[a-z.]{0,10})[^\w.]`
  • Separator: @
  • Minimum characters to the left: 3
  • Maximum characters to the left: 15
  • Maximum characters to the right: 30 |

**Adding Expressions**

1. Navigate to **Data Protection > Data Identifiers > Expressions**.
   
The Expressions screen appears.

2. Click **Add**.
A new screen appears.

**Figure 3-2. Add Expression screen**

3. Type a name for the expression. The name must not exceed 100 bytes in length and cannot contain the following characters:

   $ > < * ^ | & ? /$

4. Type a description for the expression. The description must not exceed 256 bytes in length and cannot contain the following characters:

   $ > < * ^ | & ? /$

5. Choose one of the following criteria and configure additional settings for the chosen criteria:
   - None
6. Type the expression and specify whether it is case-sensitive.

7. Type the displayed data. For example, if you are creating an expression for ID numbers, type a sample ID number. This data is used for reference purposes only and will not appear elsewhere in the product.

8. Select a validator for the expression. See Predefined Expressions on page 3-4 for details.

9. Test the expression against an actual data. For example, if the expression is for a national ID, type a valid ID number in the Test data text box, click Test, and then check the result.

10. Click Save if you are satisfied with the result.
Note
Save the settings only if the testing was successful. An expression that cannot identify any data wastes system resources and may impact performance.

Modifying Expressions
1. Navigate to Data Protection > Data Identifiers > Expressions.
2. Click the name of the expression that you want to modify.
   A new screen appears.
3. Modify the settings.
4. Click Save.

Deleting Expressions

Note
It is not possible to delete a data identifier that is being used in a template. Delete the template before deleting the data identifier.

1. Navigate to Data Protection > Data Identifiers > Expressions.
2. Select the expressions that you want to delete and click Delete.
3. Click OK.

File Attributes
File attributes are specific properties of a file. You can use two file attributes when defining digital assets, namely, file type and file size.

By themselves, file attributes are poor identifiers of sensitive files. Trend Micro therefore recommends combining file attributes with other data identifiers for a more targeted detection of digital assets.

For a list of supported file types, see:
Adding File Attribute Lists

1. Navigate to **Data Protection > Data Identifiers > File Attributes**.
   
The *File Attributes* screen appears.

2. Click **Add**.
   
   A new screen appears.

3. Type a name for the file attribute list. The name must not exceed 100 bytes in length and cannot contain the following characters:

   $ > < * ^ | & ? \ /$

---

3-11
4. Type a description that does not exceed 256 bytes in length.

5. Select the file attributes that you want to include.

6. If you selected **File type**, click **Edit**.

   A new screen appears.

7. Select the file types that you want to include. Click the file type to see the supported file extensions.

8. If a file type you want to include is not listed, select **Others** and then type the file type’s extension. DLP checks files with the specified extension but does not check their true file types.

Guidelines when specifying file extensions:

- Each extension must start with an asterisk (*), followed by a period (.), and then the extension. The asterisk is a wildcard, which represents a file’s actual name. For example, *.pol matches 12345.pol and test.pol.

- You can include wildcards in extensions. Use a question mark (?) to represent a single character and an asterisk (*) to represent two or more characters. See the following examples:

  *.*m matches the following files: ABC.dem, ABC.prm, ABC.sdc

  *.m*r matches the following files: ABC.mgdr, ABC.mtp2r, ABC.mdmr

  *.fm? matches the following files: ABC.fme, ABC.fml, ABC.fmp

- Be careful when adding an asterisk at the end of an extension as this might match parts of a file name and an unrelated extension. For example: *.do* matches abc.doctor_john.jpg and abc.donor12.pdf.

- Use semicolons (;) to separate file extensions. There is no need to add a space after a semicolon.

9. Type the minimum and maximum file sizes in bytes. Both file sizes must be whole numbers larger than zero.

10. Click **Save**.
**Modifying File Attribute Lists**

1. Navigate to **Data Protection > Data Identifiers > File Attributes**.

   The **File Attributes** screen appears.

2. Click the name of the file attribute list that you want to modify.

   A new screen appears.

3. Modify the settings.

4. Click **Save**.

**Deleting File Attribute Lists**

- **Note**
  It is not possible to delete a data identifier that is being used in a template. Delete the template before deleting the data identifier.

1. Navigate to **Data Protection > Data Identifiers > File Attributes**.

   The **File Attributes** screen appears.

2. Select the file attributes that you want to delete and click **Delete**.

3. Click **OK**.

**Fingerprints**

Use the Fingerprints screen to register sensitive content for fingerprinting, acquire fingerprints, or schedule fingerprint acquisitions. Fingerprints can be acquired by both the local crawler and the remote crawler.

Fingerprint definitions specify the location and types of sensitive information for DLP to fingerprint. After you register and schedule sensitive content for document fingerprinting, DLP uses a mathematical algorithm to extract multiple fingerprint patterns per document. Fingerprints help identify the document later even if the
document is partially altered. Fingerprinting works best with unstructured content, such as reports, email, and articles.

**Figure 3-5. Fingerprints screen**

Fingerprinting documents is a two-step process:

1. Create a fingerprint definition.
2. Acquire the fingerprints.

**Adding Fingerprints**

1. Navigate to Data Protection > Data Identifiers > Fingerprints.
   
   The Fingerprints screen appears.

2. Click Add.
A new screen appears.

**Figure 3-6. Add Fingerprints Screen**

3. Enter the Source information. The source information describes the content to fingerprint and tells the system where to locate the content.

**Table 3-2. Source Information Fields and Options**

<table>
<thead>
<tr>
<th>Field/Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name accepts up to 100 alphanumeric characters. Special characters are not allowed.</td>
</tr>
<tr>
<td>Description</td>
<td>Description accepts up to 256 alphanumeric characters. Special characters are not allowed.</td>
</tr>
<tr>
<td>Repository Type</td>
<td>Different information is required depending on the repository type.</td>
</tr>
<tr>
<td><strong>FIELD/OPTION</strong></td>
<td><strong>DESCRIPTION</strong></td>
</tr>
<tr>
<td>------------------</td>
<td>----------------</td>
</tr>
</tbody>
</table>
| Local or NFS repository | Local is the local file system on the management server. If the repository is part of the local file system or a mounted file system on the management server, you must set the Path (for example, `/home/dgate/tmp`). Host is not required when files to be acquired are located in the local file directory on the server.  
NFS: If the repository is part of an exported directory on an NFS server, you must set the following parameters:
  - Host
  - Path
The Local/NFS folder must have “execute” permission. Otherwise, the DLP server cannot acquire fingerprints for files in local/NFS folder. This is due to the fact that a Linux system requires execution permissions of a folder in order to list files in the folder. The DLP server needs to list the files to acquire the fingerprints. |
| Windows™ Share | If the repository is a shared drive or directory on a remote machine that is running Windows™, set the following parameters:
  - Host (for example, myHostName or myHostIP)
  - Path (for example, /path1/path2)
  - Logon credentials for the remote machine (UserID and password) |
| SharePoint | If the repository is Microsoft SharePoint™, you must set the following parameters:
  - Repository Type: SharePoint
  - Host (for example, http://ishare.example.com/eng/dlp/)
  - Path (for example, shared documents/path)
  - Logon credentials for SharePoint (UserID and password) |

**Note**

If the repository type is Remote Crawler, a drop-down list field appears so that you can select the Host (the remote crawler registered to the management server).

Machines names where your remote crawlers are installed can be viewed at Administration > Crawler Management.

**Note**

“Windows™ Share” and “Sharepoint” using the “Remote Crawler” is preferred because it is more dependable and private. DLP does not need a password to access the source configured on the remote crawler but requires a separate Remote Crawler download and configuration. See Remote Crawler Management on page 7-18.

4. Click **Test Connection** to ensure that DLP can access the repository.

**Note**

Skip this step if you selected a Remote Crawler repository type, since DLP hides the Test button. You already tested the repository connection when you installed the remote crawler and configured the repository for the remote crawler.

5. Enter Filter criteria to apply limits to the content being fingerprinted. This prevents unnecessary acquisitions that could affect crawler performance or cause you to exceed the fingerprints storage limit of 2GB.

**Table 3-3. Source Information Fields and Options**

<table>
<thead>
<tr>
<th>Field/Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote Crawler</td>
<td>If the repository type is Remote Crawler, a drop-down list field appears so</td>
</tr>
<tr>
<td></td>
<td>that you can select the Host (the remote crawler registered to the management</td>
</tr>
<tr>
<td></td>
<td>server). Machines names where your remote crawlers are installed can be</td>
</tr>
<tr>
<td></td>
<td>viewed at Administration &gt; Crawler Management.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Filter Criteria</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include</td>
<td>Includes specific files or file extensions for the fingerprint acquisition.</td>
</tr>
<tr>
<td></td>
<td>For example, you could specify one or multiple files.</td>
</tr>
<tr>
<td></td>
<td>• DLP does not support folders since you specify the path/folder in the Path</td>
</tr>
<tr>
<td></td>
<td>field.</td>
</tr>
<tr>
<td></td>
<td>• Separate multiple entries with a comma but do not place a space after the</td>
</tr>
<tr>
<td></td>
<td>comma.</td>
</tr>
<tr>
<td></td>
<td>• You can use up to 200 characters.</td>
</tr>
<tr>
<td></td>
<td>Example: example.doc,* .docx</td>
</tr>
<tr>
<td>FILTER CRITERIA</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Exclude        | Excludes specific folders, files, or file types during the acquisition.  
|                | • You can use up to 200 characters.  
|                | • Separate multiple entries with a comma but do not place a space after the comma. |
| Date Restriction| Restricts the acquisition to files that have been modified within the specified date range. |
| Source File Size | Specifies that fingerprints should only be acquired for files within a file size range (in bytes, KB or MB). By default, the minimum file size is 61 bytes and the maximum file sizes are as follows:  
|                | • Binary file: 32MB  
|                | • Archive file: 32MB  
|                | • Document: 75MB but only the first 6MB of extracted text is fingerprinted |

Note
You can reconfigure the default minimum and maximum fingerprint settings at Administration > Server Configuration > Fingerprint Settings.

6. Choose from the following options:

• **Save**: Saves the settings only. Fingerprints will be acquired according to a schedule.

• **Save & Acquire**: Saves the settings and then runs the fingerprint acquisition.

The fingerprint definition appears in the Fingerprint Source list along with the acquisition status.
Scheduling Fingerprint Acquisition (Non-remote Crawler Source)

1. Navigate to **Data Protection > Data Identifiers > Fingerprints**.

   The **Fingerprints** screen appears.

2. Select the fingerprint and click **Schedule Acquisition**.

   A new screen appears.

   ![Figure 3-7. Scheduling Fingerprints screen](image)

3. Select the schedule for the fingerprint and click **Save**.

   The fingerprint is acquired at the scheduled time.

   **Note**
   
   To immediately acquire a fingerprint, select the fingerprint from the list and click **Acquire Documents**.

4. On the Fingerprints Source list, click the icon in the History column to view the acquisition status.

   A new screen appears.
View the acquisition status, including the Failure Reason if the acquisition was unsuccessful.

5. Click the **Acquired** link to view details about files that were not fingerprinted.

**Scheduling Fingerprint Acquisition (Remote Crawler Source)**

1. Navigate to **Data Protection > Data Identifiers > Fingerprints.**
   
   The **Fingerprints** screen appears.

2. Select the fingerprint and click **Schedule Acquisition.**
   
   A new screen appears.

3. Select the schedule for the fingerprint.

4. Specify which repositories on the remote crawler will be fingerprinted, and click **Save.**
   
   The fingerprints are acquired at the scheduled time.

**Deleting Fingerprints**

---

**Note**

It is not possible to delete a data identifier that is being used in a template. Delete the template before deleting the data identifier.

---

1. Navigate to **Data Protection > Data Identifiers > Fingerprints.**
   
   The **Fingerprints** screen appears.

2. Select the fingerprints that you want to delete and click **Delete.**

3. Click **OK.**
Keyword Lists

Keywords are special words or phrases. You can add related keywords to a keyword list to identify specific types of data. For example, "prognosis", "blood type", "vaccination", and "physician" are keywords that may appear in a medical certificate.

Commonly used words can be combined to form meaningful keywords. For example, "end", "read", "if", and "at" can be combined to form keywords found in source code, such as "END-IF", "END-READ", and "AT END".

![Keyword Lists screen](image)

**Figure 3-8.** Keyword Lists screen

**Predefined Keyword Lists**

DLP comes with a set of predefined keyword lists. Each keyword list has built-in conditions that determine if the template should trigger a DLP incident.

For a list of predefined keyword lists, see:

3-21
**Customized Keyword Lists**

Create customized keyword lists if none of the predefined keyword lists meet your requirements.

There are several criteria that you can choose from when configuring a keyword list. A keyword list must satisfy your chosen criteria before DLP subjects it to a policy. Choose one of the following criteria for each keyword list:

**Table 3-4. Keyword List Criteria**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any keyword</td>
<td>A file must contain at least one keyword in the keyword list.</td>
</tr>
<tr>
<td>All keywords</td>
<td>A file must contain all the keywords in the keyword list.</td>
</tr>
</tbody>
</table>
| All keywords within `<x>` characters | A file must contain all the keywords in the keyword list. In addition, each keyword pair must be within `<x>` characters of each other. For example, your 3 keywords are ABCDE, FGHIJ, and WXYZ and the number of characters you specified is 20. If DLP detects all keywords in the order FGHIJ, ABCDE, and WXYZ, the number of characters from F to A and from A to W must be 20 characters at most.  • The following data matches the criteria:  
  `FGHIJ####ABCDE############WXYZ`
  • The following data does not match the criteria:  
  `FGHIJ**************ABCDE****WXYZ`

When deciding on the number of characters, remember that a small number, such as 10, will usually result in faster scanning time but will only cover a relatively small area. This may reduce the likelihood of detecting sensitive data, especially in large files. As the number increases, the area covered also increases but scanning time might be slower.
### Criteria vs. Rule

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combined score for keywords exceeds threshold</td>
<td>A file must contain one or more keywords in the keyword list. If only one keyword was detected, its score must be higher than the threshold. If there are several keywords, their combined score must be higher than the threshold. Assign each keyword a score of 1 to 10. A highly confidential word or phrase, such as &quot;salary increase&quot; for the Human Resources department, should have a relatively high score. Words or phrases that, by themselves, do not carry much weight can have lower scores. Consider the scores that you assigned to the keywords when configuring the threshold. For example, if you have five keywords and three of those keywords are high priority, the threshold can be equal to or lower than the combined score of the three high priority keywords. This means that the detection of these three keywords is enough to treat the file as sensitive.</td>
</tr>
</tbody>
</table>

### Adding Keyword Lists

1. Navigate to Data Protection > Data Identifiers > Keyword Lists. The **Keyword Lists** screen appears.
2. Click Add.
A new screen appears.

**Figure 3-9. Add Keyword List screen**

3. Type a name for the keyword list. The name must not exceed 100 bytes in length and cannot contain the following characters:

   > < * ^ | & ? /

4. Type a description that does not exceed 256 bytes in length.

5. Choose one of the following criteria and configure additional settings for the chosen criteria:
   - Any keyword
   - All keywords
   - All keywords within <x> characters
• Combined score for keywords exceeds threshold

See Customized Keyword Lists on page 3-22 for details about the criteria.

6. To import keywords:
   a. Select Import keywords.
   b. Click Import and then locate the file containing the keywords.
   c. Click Open.

7. To manually add keywords to the list:
   a. Select Add/update keywords.
   b. Type a keyword that is 3 to 40 bytes in length and specify whether it is case-sensitive.
   c. Type a description that does not exceed 256 bytes in length.
   d. Click Add.

8. Click Save.

Preparing Keyword Import Files

**Note**

Use the JavaScript Object Notation (JSON) format:

```json
[{
  "description": "description0",
  "caseSensi": "1",
  "name": "key0",
  "score": 1
},
{
  "description": "1:description",
  "caseSensi": "0",
  "name": "key1",
  "score": 2
},
{
  "description": "2:description",
  "caseSensi": "1",
  "name": "key2",
  "score": 3
}]
```

1. Type a keyword that is 3 to 40 bytes (single-byte characters) or 1 to 40 (multi-byte characters) in length.

2. Type a description for the keyword. This is optional.

3. Specify case sensitivity.
4. Set a score threshold. Specify a value between 1 and 10. This is optional and is only used when the condition is “Combined score for keywords exceeds threshold”.

5. Save the file as UTF-8.

Modifying Keyword Lists

1. Navigate to Data Protection > Data Identifiers > Keyword Lists.

   The **Keyword Lists** screen appears.

2. Click the name of the keyword list that you want to modify.

   A new screen appears.

3. Modify the settings.

4. Click **Save**.

Deleting Keywords

---

**Note**

It is not possible to delete a data identifier that is being used in a template. Delete the template before deleting the data identifier.

---

1. Navigate to Data Protection > Data Identifiers > Keyword Lists

   The **Keyword Lists** screen appears.

2. Select the keyword lists that you want to delete and click **Delete**.

3. Click **OK**.

Templates

A template combines data identifiers and logical operators (And, Or, Except) to form condition statements. Only data that satisfy a certain condition statement will be subject to a policy.
For example, a file must be a Microsoft Word document (file attribute) AND must contain specific legal terms (keywords) AND must contain ID numbers (expressions) for it to be subject to the "Employment Contracts" policy. This policy allows Human Resources personnel to transmit the file to a network printer so that a copy can be signed by an employee. Transmission through all other possible channels, such as email, is blocked.

You can create your own templates if you have configured data identifiers. You can also use predefined templates.

Figure 3-10. Templates screen

Predefined Templates

DLP comes with a set of predefined templates that you can use to comply with various regulatory standards.
**Note**

Predefined templates cannot be modified or deleted.

For a list of predefined templates, see:


**Customized Templates**

Create your own templates if you have configured data identifiers. A template combines data identifiers and logical operators (And, Or, Except) to form condition statements.

**Condition Statements and Logical Operators**

DLP evaluates condition statements from left to right. Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

**Table 3-5. Sample Condition Statements**

<table>
<thead>
<tr>
<th>Condition Statement</th>
<th>Interpretation and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Definition 1] And ![Definition 2] Except ![Definition 3]</td>
<td>A file must satisfy ![Definition 1] and ![Definition 2] but not ![Definition 3]. For example: A file must be [an Adobe PDF document] and must contain [an email address] but should not contain [all of the keywords in the keyword list].</td>
</tr>
<tr>
<td>![Definition 1] Or ![Definition 2]</td>
<td>A file must satisfy ![Definition 1] or ![Definition 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].</td>
</tr>
</tbody>
</table>
As the last example in the table illustrates, the first data identifier in the condition statement can have the "Except" operator if a file must not satisfy all of the data identifiers in the statement. In most cases, however, the first data identifier does not have an operator.

### Adding Templates

1. Navigate to **Data Protection > Templates**.

   The **Templates** screen appears.

2. Click **Add**.

   A new screen displays.

   ![Figure 3-11. Add Template screen](image)

3. Type a name for the template. The name must not exceed 100 bytes in length and cannot contain the following characters:

   > < * ^ | & ? \ /

4. Select the type of data identifier, and then the actual data identifier name.
5. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before DLP subjects it to a policy.

6. If you selected a fingerprint, select one of the following match types:
   - Low-level Match: If the number of matched fingerprints is > 0 and < 12.5%, the document is sensitive.
   - Medium Match: If the number of matched fingerprints is >= 8 or >= 12.5%, the document is sensitive.
   - High-Level Match: If the number of matched fingerprints is >= 20 or over 33.3%, the document is sensitive.

   **Note**
   DLP compares the fingerprints of registered and transmitted digital assets, counts the number of matches, and then determines the match level.

7. Click + to add condition statements.

8. Select a logical operator for each condition statement.

   **Note**
   Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results.

9. Click **Add**.

   The rule is displayed in the Template Definitions list.

10. Select a logical operator for each rule.

11. Click **Save**.

### Importing Templates

1. Navigate to **Data Protection > Templates**.

   The **Templates** screen appears.
2. Click **Import** and select the format of the file to be imported.

3. Select the template to be imported and click **Open**.

4. Click **Import**.

5. Click **Yes** to complete the import.

   A message appears, informing you if the import was successful. If a template to be imported already exists, it will be overwritten.

### Exporting Templates

**Note**

Use the export option to back up templates, import them to another DLP 5.6 server, or use with other Trend Micro data protection products.

1. Navigate to **Data Protection > Templates.**

   The **Templates** screen appears.

2. Select the templates that you want to export and click **Export**.

   - Select **Binary Format** if you intend to import the selected templates to another DLP 5.6 server.
   - Select **XML Format** if you intend to use the selected templates with other Trend Micro data protection products.

3. Select the format of the exported file.

4. Save the file to your preferred location.

### Deleting Templates

**Note**

It is not possible to delete a template that is being used in a policy. Remove the template from the policy before deleting it.
1. Navigate to Data Protection > Templates.
2. Select the templates that you want to delete and click Delete.
3. Click OK.

Policies

Use the Policies screen to combine templates with rules for handling the digital assets when detected.

Tip
Trend Micro recommends that you first create a policy that imposes the strictest rules for as many targets (users or endpoints) as possible. Then create policies for a few endpoints or users as the exception from “All Endpoints” or “All Users.”

If you purchased DLP Network Monitor, you can define separate polices for network monitoring.

Although the process of setting up policies is the same whether you set up an endpoint agent policy or a network agent policy, the available options on the screens differ. Consequently, adding policies is split into two procedures:

- Adding Endpoint Agent Policies on page 3-33
- Adding Network Agent Policies on page 3-43
Adding Endpoint Agent Policies

To add an Endpoint Agent Policy, define the following:

<table>
<thead>
<tr>
<th>ITEM</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target</td>
<td>Set the endpoint targets for DLP to monitor. You can specify targets from domains, endpoint groups, LDAP users, and all targets.</td>
</tr>
<tr>
<td>Channel</td>
<td>Set the channel for DLP to monitor, such as ActiveSync filter, CD/DVD, HTTP, and so forth.</td>
</tr>
<tr>
<td>Condition</td>
<td>Set the condition for DLP to detect as defined in your templates. Also enable DLP to monitor for data-stealing malware.</td>
</tr>
<tr>
<td>Action</td>
<td>Set the network boundary for DLP to filter and the action for DLP to take when an incident is triggered.</td>
</tr>
</tbody>
</table>

1. Navigate to **Data Protection > Policies**.

   The **Policies** screen appears.

2. Click **Add > Endpoint Agent Policy**.
The **Step 1: Target** screen appears.

**FIGURE 3-13. Add Policy (Step 1: Target) screen**

**Defining Endpoint Agent Policy Targets**

1. On the Add Policy (Step 1: Target) screen, configure template settings:

   **TABLE 3-6. Template Settings**

<table>
<thead>
<tr>
<th>FIELD</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Name</td>
<td>Type up to 245 alphanumeric characters.</td>
</tr>
<tr>
<td>Copy from an existing policy</td>
<td>This field is optional. If you select to copy a policy, a field displays so that you can type the new policy name. Then you can modify additional policy screens.</td>
</tr>
</tbody>
</table>

2. Configure target settings. DLP matches captured data against the targets to determine if DLP needs to filter the content.
### TABLE 3-7. Target Settings

<table>
<thead>
<tr>
<th><strong>FIELD</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Target Scope</td>
<td>Enables you to search for targets by Groups/Endpoints, Domain/Endpoints, LDAP/Users, or All Targets.</td>
</tr>
<tr>
<td></td>
<td>Groups/Endpoints: Enables you to select from the available groups that you set up in Administration &gt; Agent Management &gt; Groups.</td>
</tr>
<tr>
<td></td>
<td>LDAP/Users: To select LDAP/Users, the LDAP server must be configured and in use. See Configuring LDAP Settings on page 7-40.</td>
</tr>
<tr>
<td>Search</td>
<td>After you select an option in the Select By field, you can type a search term and click Search to drill down to specific targets.</td>
</tr>
<tr>
<td></td>
<td>If you add an asterisk at the end of your search term, DLP returns all target entities that start with your search term.</td>
</tr>
<tr>
<td>Selected</td>
<td>Click the Add or Remove buttons to add and / or remove targets to monitor or targets that are exceptions to monitoring.</td>
</tr>
</tbody>
</table>

3. Click Next.
The **Add Policy (Step 2: Channel)** screen appears.

![Digital assets can be transmitted through various channels. Select the channels for this policy.](image)

**Figure 3-14. Add Policy (Step 2: Channel) screen**

**Defining Endpoint Agent Policy Channels**

1. On the Add Policy (Step 2: Channel) screen, select or enter the channels for DLP to monitor.

   **Note**

   For all channels, the endpoint agent bypasses one path, especially for Printer (C:\Windows\Fonts\).

   For performance tuning, define policy rules only for channels that you need to filter.

The channels below have additional specifications to consider:
### TABLE 3-8. Channel Specifications

<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Email                                | • Click the **Email Clients down arrow** to display the Monitored and Non-monitored Targets fields.  
• Type monitored and non-monitored email domain names in X400, email address domain, or individual address format. Separate multiple entries with commas. For example, “/O=Trend/OU=USA, /O=Trend/OU=China, trendmicro.com,test@example.com”  |
| **Note**                             | The endpoint agent supports monitored and non-monitored email domain names for Microsoft Exchange, Lotus Notes, and SMTP. |
| Removable Storage (FileWrite)        | • Click the **Removable Storage down arrow** to display the Non-monitored USB Devices field.  
• Type non-monitored USB devices. Separate each USB device with commas. Use the format: `<Vendor Name>|<Model>|<Serial ID>`. For example, ZTE|6025|30101106703D310, GENERIC|8012|*, GENERIC|*|*, *|*|*. You can use asterisks (*). |
<p>| Instant Messengers                   | Click the <strong>IM Applications down arrow</strong> to view the filtered IM channels.  |</p>
<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| P2P     | • Click the **Peer-to-peer Applications down arrow** to view the filtered peer-to-peer channels.  
• For the P2P and Skype channels, the endpoint agent bypasses files with these extensions: .dll, .ttf, .lnk, .ico, .gpd, .bud, .ini, .gif, .jpg, .png, .ime, .dbb, .manifest, .torrent, .ezlog, .mlsxml, and .ttc.  
• For Skype channels, the endpoint agent bypasses the special file names, etilqs_XXXXXXXXXXXXXXXX  
• For the P2P and Skype channels, the endpoint agent also bypasses these system directories:  
  Cookies 
  Local settings (long version)  
  Application data  
  appdata\local\ (skip for Win7 feature - Libraries)  
  appdata\roaming\ (skip for Win7 feature - Libraries)  
  windows  
  winnt |
| Printer | Click **Printer** to detect sensitive content in documents sent to print. |
| SMB     | • Click the **SMB Protocol down arrow** to display the Monitored and Non-monitored Targets.  
• Type monitored and non-monitored IP addresses, IP address ranges (for example: 192.168.2.1/10), host names, and Fully Qualified Domain Names (FQDN). Separate multiple entries with commas. |

**Note**

The endpoint agent bypasses files with these file extensions: .dll, .pf, .dic, .exe and the system font path, `C:\windows\fonts\`. 
2. Click Next.

The Add Policy (Step 3: Conditions) screen appears.

![Figure 3-15. Add Policy (Step 3: Conditions) screen](image)

**Defining Endpoint Agent Policy Conditions**

1. On the Add Policy (Step 3: Conditions) screen, select or import one or more templates for the policy condition. The policy is activated if these conditions are met.

2. Select **Enable data-stealing malware detection** to detect unmonitored transmissions of sensitive data, including:
   - Keyloggers, spyware, and trojans that collect and post sensitive data on the Internet
   - Phone-home malware (DSM)
   - Hidden FTP processes that transfer stolen data to remote hacker sites
• Botnet data collectors

3. Click Next.

The Add Policy (Step 4: Action) screen appears.

![Add Policy (Step 4: Action) screen](image)

**FIGURE 3-16. Add Policy (Step 4: Action) screen**

**Defining Endpoint Agent Policy Actions**

### Table 3-9. Transmission Scope Radio Buttons

<table>
<thead>
<tr>
<th>Radio Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>All transmissions</strong></td>
<td>DLP monitors all files transmitted outside the local host.</td>
</tr>
<tr>
<td></td>
<td><strong>WARNING!</strong></td>
</tr>
<tr>
<td></td>
<td>This is strict filtering that is only recommended for offline agents.</td>
</tr>
<tr>
<td><strong>Only transmissions outside the Local Area Network</strong></td>
<td>DLP monitors all files transmitted outside the LAN.</td>
</tr>
<tr>
<td></td>
<td>The LAN boundary includes only private IP address ranges, including 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16.</td>
</tr>
<tr>
<td></td>
<td>However, if a destination IP address is a private IP address but is listed in Global Exceptions as a Monitored Target, DLP considers it as outside the LAN.</td>
</tr>
<tr>
<td></td>
<td>DLP approves private IP ranges by default. Even if you use a 10.0.0.0/24 network for your LAN, the private IP addresses 172.16.x.x, 192.168.x.x and every other 10.x.x.x IP are also approved by default. Subnet boundary checking is not currently supported.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>This is the recommended setting for online agents.</td>
</tr>
</tbody>
</table>

“Network” is the company network, including traffic to standard private IP addresses:

- A: 10.0.0.0~10.255.255.255
- B:172.16.0.0~172.31.255.255
- C:192.168.0.0~192.168.255.255

The Transmission Scope that you select impacts network-related channels: SMB, FTP, HTTP, HTTPS and IM. The impact to IM channel traffic is for File Transfer only (since the message channel is always sent out to the global IM server with an IP outside the company network).
Transmission Scope impacts Email channels (Outlook, Lotus, and SMTP) with some differences. When Transmission Scope is set to Only transmissions outside the local area network, DLP only scans email in which recipients are not in the internal email domain. You can configure the internal email domain at **Administration > Global Exceptions**.

---

**Note**

When DLP checks for incidents, DLP complies with the settings of your Monitored Targets, Non-monitored Targets, and Transmission Scope. When these settings conflict, Monitored Targets is the first priority for DLP checking, followed by Non-monitored Targets. The last priority is Transmission Scope checking.

In other words, the destination listed in Monitored Targets will always be an incident source even if the destination is a local machine or within the LAN boundary. If the destination is not on the Monitored Targets list and is on the Non-monitored Targets list, the destination is in compliance and no checking will occur. If the destination is not in the Monitored Targets or Non-monitored Targets lists, DLP determines if the destination does not comply with the Transmission Scope setting.

---

2. **Specify the System Action when Online.** This is the action for DLP to take if an incident is triggered while the agent is connected to the management server.

3. **Specify the System Action when Offline.** This is the action for DLP to take if an incident is triggered while the agent is not connected to the management server.

**Table 3-10. System Action Considerations**

<table>
<thead>
<tr>
<th>System Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notify the customer</td>
<td>You can set a policy-based URL in the client side alert screen instead of setting a global URL at <strong>Administration &gt; Agent Configuration &gt; Advanced Settings</strong>. This way, you can set different URLs for different policies.</td>
</tr>
<tr>
<td>Encrypt; Prompt user to enter justification</td>
<td>You can only select <strong>Encrypt</strong> and <strong>Prompt user to enter justification</strong> if you selected only the Removable Storage channel.</td>
</tr>
</tbody>
</table>
If you select **Record data**, DLP automatically encrypts the forensic data with a pre-defined password and securely stores the data on the DLP server. The default password for encrypted files is 12345678. It is recommended that you change this password at **Administration > Agent Configuration > Agent Settings**.

**WARNING!**

**Record data** uploads files to the DLP server which could occupy too much hard disk space. Trend Micro highly recommends that you only record highly sensitive information.

4. Click **Finish** to save the policy.

   The policy appears on the Policy List.

5. On the Policy List, click the **Status** icon to disable or enable the policy.

6. Click **Deploy Now**. DLP deploys all enabled policies in the list to the agents.

   Click the up or down arrows in the Order column to change the policy priority. When multiple policies are involved in an incident, DLP executes the most strict rules. However, when matching block and encryption actions, DLP takes actions based on order. The lowest number has the highest priority and is executed first.

   Moving the mouse over a policy name displays a snapshot of the policy content.

   **Note**

   The management server waits an interval of one minute for each policy deployment. If you continually click Deploy Now, DLP waits one minute and redeployes the policies. In this case, Deploy Now is disabled after one minute and a message displays, “Policies have been deployed.”

---

### Adding Network Agent Policies

To add a Network Agent Policy, define the following:
**ITEM** | **DESCRIPTION**
---|---
Target | Set the targets for DLP to monitor. You can type IP address ranges or IP addresses.
Channel | Set the channel for DLP to monitor.
Condition | Set the condition for DLP to detect as defined in your templates. Also enable DLP to monitor for data stealing malware.
Action | Set the network boundary for DLP to filter and the action for DLP to take when an incident is triggered.

1. Navigate to **Data Protection > Policies**.
   
The **Policies** screen appears.

2. Click **Add > Network Agent Policy**.
   
The **Step 1: Target** screen appears.

**Defining Network Agent Policy Targets**

1. On the **Add Policy: Step 1: Target** screen, configure template settings:
2. Enter the targets for DLP to protect or monitor. Select by All IP Addresses or a specific IP address or range. DLP matches captured data against the targets to determine if DLP needs to filter the content.

3. Click Next. The Add Policy Channel screen appears.

Defining Network Agent Policy Channels

1. On the Add Policy: Step 2: Channel screen, select the channels for DLP to monitor.
For performance tuning, define policy rules only for channels that you need to filter.

The channels below have additional specifications to consider:

Table 3-12. Channel Specifications

<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| Email    | • Click the Email Clients down arrow to display the Non-monitored domain names box.  
|          | • Type email domain names. Separate the names with commas. For example, admin@yahoo.com,admin@gmail.com. |

Note

The network agent supports non-monitored email domain names for SMTP.
<table>
<thead>
<tr>
<th>CHANNEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</table>
| FTP            | • Click the FTP down arrow to display the Non-monitored domain names or IP addresses box.  
 • Type the approved Fully Qualified Domain Name (FQDN) or IP addresses. Separate multiple entries with commas. For example, www.example.com,192.168.2.1/10. |
| Note           | The network agent only supports IP and FQDN for the FTP and HTTP approved list, not a host name via NetBIOS. |
| HTTP           | • Click the HTTP down arrow to display the Non-monitored domain names or IP addresses box.  
 • Type the approved FQDN or IP addresses. Separate multiple entries with a comma. For example, www.example.com,192.168.2.1/10. |
| Instant Messengers | Click the IM Applications down arrow to view the filtered IM channels. |
| SMB            | Select SMB Protocol to monitor SMB traffic. The network agent does not support Monitored and Non-monitored lists. |
| Web mail       | Click the Webmail down arrow to view the filtered web mail channels. |

2. Click Next.  
The Add Policy Conditions screen appears.

**Defining Network Agent Policy Conditions**

1. On the Add Policy: Step 3: Conditions screen, select or import one or more templates for the policy condition. The policy is activated if these conditions are met.
2. Select **Enable data-stealing malware detection** to detect unmonitored transmissions of sensitive data, including:
   - Keyloggers, spyware, and trojans that collect and post sensitive data on the Internet
   - Phone-home malware (DSM)
   - Hidden FTP processes that transfer stolen data to remote hacker sites
   - Botnet data collectors

3. Click **Next**.
   
   The **Add Policy Action** screen appears.

**Defining Network Agent Policy Actions**

1. On the **Add Policy: Step 4: Action** screen, select the **Transmission Scope**:
Figure 3-20. Add Policy: Step 4: Action screen

- **Only transmissions outside the local area network** is the recommended setting. Select this if you want DLP to inspect only data transmitted outside the LAN.

- **All transmissions** enables DLP to inspect all data transmitted outside the local machine.

“Network” is the company network, including traffic to standard private IP addresses:

- A: 10.0.0.0~10.255.255.255
- B: 172.16.0.0~172.31.255.255
- C: 192.168.0.0~192.168.255.255

**Only transmissions outside the local area network** includes only private IP address ranges, including 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. However, if a destination IP address is a private IP address but is listed in Global Exceptions on the Monitored Targets list, DLP considers it as outside the LAN.

Note that DLP approves private IP ranges by default. Even if you use a 10.0.0.0/24 network for your LAN, the private IP addresses 172.16.x.x, 192.168.x.x and every other 10.x.x.x IP are also approved by default. Subnet boundary checking is not currently supported.
When DLP checks for incidents, DLP complies with the settings of your Monitored Targets, Non-monitored Targets, and Transmission Scope. When these settings conflict, Monitored Targets is the first priority for DLP checking, followed by Non-monitored Targets. The last priority is Transmission Scope checking.

In other words, the destination listed in Monitored Targets will always be an incident source even if the destination is a local machine or within the LAN boundary. If the destination is not on the Monitored Targets list and is on the Non-monitored Targets list, the destination is in compliance and no checking will occur. If the destination is not in the Monitored Targets or Non-monitored Targets lists, DLP determines if the destination does not comply with the Transmission Scope setting.

Transmission Scope impacts network-related channels: SMB, FTP, HTTP, and IM. The impact to the IM channel traffic is for File Transfer only (since the message channel is always sent out to the global IM server with an IP outside the company network).

Transmission Scope also impacts Email channels with some differences. For Email (SMTP), when Transmission Scope is set to Only transmissions outside the local area network, DLP only scans email in which recipients are not in the internal email domain. You can configure the internal email domains at Administration > Global Exceptions.

2. Specify the System Actions for DLP Network Monitor to take if an incident is triggered.

If you select Record data, the network agent automatically encrypts the forensic data with a predefined password and securely uploads the data to the DLP server. The default password for encrypted files is 12345678. It is recommended that you change this password at Administration > Agent Configuration > Agent Settings.

WARNING!

Record data uploads files to the DLP server which could occupy too much hard disk space. Trend Micro highly recommends that you only record highly sensitive information.

3. Click Finish to save the policy.
The network agent policy appears on the Policy List.

4. On the Policy List, click the **Status** icon to disable or enable the policy.

5. Click **Deploy Now**. DLP deploys all enabled policies in the list to the agents.

Click the up or down arrows in the **Order** column to change the policy priority. When multiple policies are triggered in an incident, DLP executes the most strict rules. However, when matching block and encryption actions, DLP takes actions based on order. The lowest number has the highest priority and is executed first.

Moving the mouse over a policy name displays a snapshot of the policy content.

---

**Note**

The DLP server waits an interval of one minute for each policy deployment. If you continually click **Deploy Now**, DLP waits one minute and redeploy the policies. In this case, **Deploy Now** is disabled after one minute and a message displays, “Policies have been deployed.”

---

**Data Discovery**

Use the Data Discovery screen to configure and run data discovery tasks that scan and locate sensitive content in data at rest on your network.

A data discovery scan is a two-step process:

1. Specify scan targets in data discovery task definitions.

2. Run or schedule the discovery task.

---

**WARNING!**

Performing a full scan of an endpoint drive or directory could cause a noticeable system slowdown for the user.
Note

Due to security and performance issues, DLP does not scan the autoexec.bat file and the following file paths:

?:\Documents and Settings\*\Application Data\n
?:\Documents and Settings\*\Local Settings\n
?:\Documents and Settings\*\Cookies\n
?:\Program Files\n
?:\Windows\n
?:\Winnt\n
?:\Users\*\AppData\n
?:\ProgramData\n
![Data Discovery screen](image)

**FIGURE 3-21. Data Discovery screen**

**Defining a Data Discovery Task**

1. Navigate to **Data Protection > Data Discovery**.
   
The **Data Discovery** screen appears.

2. On the Data Discovery toolbar, click **Add**.
The Add Discovery Task Target screen appears.

3. Select the targets to scan and click Add >>.

**Note**
You can only add endpoint agents as targets for a Data Discovery scan. DLP Network Monitor does not support Data Discovery scans.

4. Click Next.
The Add Discovery Task (Step 2: Condition) screen appears.

Figure 3-23. Add Discovery Task (Step 2: Condition)

5. Select templates with which to filter the target locations. Include:
   - Root path to the target location. The root folder cannot be a Windows Share folder or removable device, such as a USB device or DVD.
   - Priority of the scan. “High” moves this scan to the front of the queue.

6. Type the Scan Exceptions:

   Note
   Click the information icon next to the Scan Exceptions fields to display examples.

   - Include: Includes specific file types for the scan. Identify file types by *.<file type>, such as *.exe. Separate multiple file types with a “|”.
   - Exclude: Excludes specific files, file types, or folders during the scan. Identify file types by “*.<file type>”, such as *.exe. Separate multiple file types with “|”.

   Specify an absolute path, if any. For example, c:\test\ or c:\test\example.doc
Note
DLP supports wildcard characters * and ?. * means all char. ? means one char or double byte word. For example, c:\ test* matches any files whose absolute path begins with c:\ test, such as c:\test\test.doc or c:\testXX\test.doc.
 *	est* matches all files whose path contains \	est\ . c:\test?test\*.* matches all files whose path contains c:\test?test\, such as c:\testXtest\1.doc.

7. Click Next.

The Add Discovery Task (Step 3: Action) screen appears.

8. Select the system action to trigger in the event that DLP discovers sensitive information:
   - Log: Combine “Log” with any one of the remaining actions. However, you cannot combine “Log” with more than one other action.
   - Move to security folder: Type the security folder to which to move detected files upon discovery. The security folder cannot be a Windows Share folder or removable device, such as a USB device or DVD.
DLP does not scan the security folder. Consequently, once DLP moves files to 
the security folder (including sub-folders), DLP does not scan or move those 
files again.

- Encrypt: DLP automatically encrypts the detected files with sensitive data 
  (using a pre-defined password) and stores the encrypted file on the DLP agent 
side.

  * If action=encrypt for the file, c:\ test.doc, the DLP agent scans and encrypts 
it as c:\ test.doc.exe. When a user double-clicks c:\ test.doc.exe, the alert screen 
appears and asks for a password to decrypt the file.

  The default password for encrypted files is 12345678. It is recommended that 
you change this password at Administration > Agent Configuration > 
Agent Settings.

Note

Trend Micro highly recommends that you not use Move or Encrypt actions for 
whole drive scans. Only use Move or Encrypt when scanning specific folders. 
With Move and Encrypt actions, the original detected files no longer exist. If 
the detected files are important system files or configuration files for 
applications, Move or Encrypt could make the system or certain applications 
unstable.

9. Click Finish.

  DLP adds the Data Discovery task to the tasks on the Data Discovery page.

10. To run the data discovery task immediately, select the task and click Run. You can 
also select the task and click Schedule Scan to schedule the scan for later.

Note

When an Endpoint agent receives multiple data discovery tasks, the agent performs 
the tasks one-by-one, in order. If you pause a data discovery task on the endpoint 
agent, the agent cannot execute any other data discovery task until the paused task 
resumes and completes.
Scheduling Data Discovery Scans

Note
When an endpoint agent receives multiple data discovery tasks, the agent performs the tasks one by one, in order. If you pause a data discovery task on the endpoint agent, the agent cannot execute any other data discovery task until the paused task resumes and completes.

1. Navigate to Data Protection > Data Discovery.
   The Data Discovery screen appears.

2. Select the scan task to schedule, and click Schedule Scan.
   The Scheduling Data Discovery screen appears.

3. Specify the scan schedule, and click Save.
   The scan starts at the scheduled time.

Tip
To start a scan immediately, select the discovery task from the list and click Run.

Viewing Data Discovery Task Reports

1. Navigate to Data Protection > Data Discovery.
The **Data Discovery** screen appears.

2. View the status of the discovery tasks:
   - In Progress
   - Completed: Scan completed without errors.
   - Completed with Errors: Scan completed with errors, such as:
     * User cancelled the task when in progress.
     * Some target agents are offline when the task starts.
     * Some agents encounter errors when running the tasks, such as “root folder does not exist.”

   **Note**
   When starting a task on targeted machines, if an online endpoint machine shuts down during scanning, the DLP agent continues scanning when the machine reboots. The agent reports the scan results to the management server. While scanning is “in progress,” you can still view the report and check scan results for other targeted agents.

3. Select the discovery task and click **Report**.

   The **Data Discovery Report** screen appears.

4. Select an **Output Format** and click **Get Report**.
Device Control

Use the **Device Control** screen to limit user access to specific devices and network shared folders. You can limit device access by group or endpoint. To limit access by group, select the group and then configure the device access for the group.

![Device Control screen](image)

**Figure 3-25. Device Control screen**

**Configuring Device Control by Group**

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If Endpoint A has a device control policy and is a member of Group B which has another device control policy, Endpoint A merges the device control policy set of A and B.</td>
</tr>
</tbody>
</table>

1. Navigate to **Data Protection > Device Control > Groups**.

   The Device Control Groups tab appears with a list of groups that you set up on the **Administration > Agent Management > Agents > Groups** tab. For more information, see *Managing Agent Groups* on page 7-33.

2. Click the group name that you want to configure device control for.
The Device Control Configuration screen appears.

![Device Control Configuration screen](image)

**Figure 3-26. Device Control Configuration screen**

3. Select the devices for which to restrict access.

If you enable device control on Removable disk drives, and a user plugs a USB device into a machine with the DLP agent, DLP takes the following actions:

- Disables the USB device.
- Displays an alert for the user.
- Logs the event to the DLP server.

You can view event details at **Logs > Query > Log Type: System Events**.

You can also click the down arrow next to **Removable disk drives** to define exceptions for removable disk devices. The exception list includes three fields for each removable disk drive: vendor, model number, and serial number. If you leave any one or two fields empty, DLP matches all of the empty fields.

**Note**

Trend Micro provides a tool for checking the vendor, model, and serial number of USB devices. Click the **Removable disk drives** down arrow and download the Auto-detect Assistance tool.
4. Select **Enable Network Device Control**.
   - Select **Enable Network Device Control** to prevent machines without the DLP agent from copying network shared files.
   - Clear **Enable Network Device Control** to allow machines without the DLP agent to copy network shared files.
   - Click **Add** to create a list of approved IP addresses.

5. Click **Save**.

### Configuring Device Control by Endpoint

1. Click **Data Protection > Device Control > Endpoints** tab.
   
The **Device Control Endpoints** tab appears with a list of endpoints.

2. Click the endpoint that you want to configure device control for. You can search for endpoints by clicking **Filter** on the toolbar.
   
The **Device Control Configuration** screen appears.

   ![Device Control Configuration screen](image)

   **Figure 3-27. Device Control Configuration screen**

3. Select the devices to restrict access to.
If you enable device control on Removable disk drives, and a user plugs a USB device into a machine with an endpoint agent, DLP takes the following actions:

- Disables the USB device.
- Displays an alert for the user.
- Logs the event to the management server.

You can view event details by selecting Log > Query > System Event.

Click the down arrow next to Removable disk drives to define exceptions for USB devices. You can enter vendor, model number, and serial number for one or more USB devices.

**Note**

Trend Micro provides a tool for checking the vendor, model, and serial number of USB devices. Click the Removable disk drives down arrow and download the Auto-detect Assistance tool.

4. Specify Network Device Control:

- Select the **Enable Network Device Control** to prevent machines without the DLP agent from copying network shared files.
- Clear **Enable Network Device Control** to allow machines without the DLP agent to copy network shared files.
- Click **Add** to create a list of approved IP addresses.

5. Click **Save**.

DLP saves and implements your device control settings.

**Note**

DLP retains the agent’s device control settings even if the agent is disconnected from the network and deleted from the agent management screen. When the agent is back online and registered again with the server, the device control settings are recovered.
Reports

This chapter describes the DLP report functions.
Generate Reports

Use the **Generate Reports** screen to create new report definitions and generate scheduled or one-time reports. Reports retrieve data from logs that agents upload to the DLP management server.

![Generate Report screen](Image)

**Figure 4-1. Generate Reports screen**

**Generating a New Report**

1. Navigate to **Reports > Generate Reports**.

   The **Generate Report** screen appears.

2. Click **Add**.
The Add Reports screen appears.

![Add Reports Screen](image)

**Figure 4-2. Add Reports screen**
3. Define the report:

Report Name accepts up to 100 alphanumeric characters and must be a unique name. These special characters are not accepted: <>*\&?/

Report Title accepts up to 40 characters.

- DLP supports these special characters: @^&*()-_.
- DLP does not support these special characters: `~!#$%+=\[\]';/}{:"<>?

Recurrence Pattern specifies how often to run the report. When you select a recurrence type, additional fields appear so you can enter report details:

- One-time: specify the date range for the report.
- Daily: specify how often to run the report, such as every 1 day, every 2 days, and so forth. The Range of Recurrence group box appears so you can specify when to start and end the daily reports.
- Weekly: specify the day of the week and how often to run the report, such as every 1 weeks, every 2 weeks, and so on. The Range of Recurrence group box appears so you can specify when to start and end the weekly report.
- Monthly: specify whether the report should run on the last day of the month or whether it should run on a specific day. Specify how often to run the report, every 1 month, every 2 months, and so on. Also, the Range of Recurrence group box appears so you can specify when to start and end the monthly report.

**Note**
For Executive Summary Information reports, you can only select One-time or Weekly.

Report By specifies users and agents to report and the report data to include.

- Select whether to report by endpoint agents, network agents, or both, as well as whether to report on a specific user, endpoint, or network device.

Network Agent details are only available if you are running DLP Network Monitor. If you are running Network Monitor and select All Network Devices, one report aggregates and displays all detection by connecting DLP
Network Monitor devices. The report identifies the devices that detect the data.

- Select report data from the following categories:
  * Top Incident Source Information
  * Summary Information
  * Executive Summary Information
  * Compliance Audit Report

Time to Keep This Report specifies how long to keep this report in archived reports. When the time limit expires, DLP purges the report.

Email This Report specifies email address, subject and recipient list. If this option is enabled, the To and Subject fields are required.

---

**Note**
Except for email recipients, DLP reuses SMTP account settings configured at Administration > Application Settings > Server Side Alert Email Notification to send the report.

---

4. Click **Save** or **Preview Report**.

---

**Note**
If DLP Network Monitor is unable to upload a log to the DLP management server, DLP Network Monitor sends the log again.

---
Archived Reports

Use the **Archived Reports** screen to view archived reports stored in PDF, HTML, or Microsoft Excel. The duration for storing the reports depends on the value you set in the Time to Keep field when you generated the report.

**Figure 4-3. Archived Reports screen**

## Viewing Archived Reports

1. **Navigate to** Reports > Archived Reports.

   The **Archived Reports** screen appears.

2. **Click Filter** to search for a report by type or name.
Logs

This chapter describes the DLP log functions.
Log Query

Use the Log Query screen to query the following logs that DLP has generated over time:

- Policy Deployment
- DLP Incidents
- Server Status
- System Events
- Security Audit

![Log Query Screen](image)

**Figure 5-1. Log Query screen**

**Querying Logs**

1. Navigate to **Logs > Query**.
   
The Log Query screen appears.

2. Select the date period or the date range of the logs.
3. Select the log type and click **Show Log**.

   The results appear under the Log Query form.

   **Tip**
   - Clicking **Filter** narrows log search results by description and operators.
   - Clicking the plus symbol expands the log information.
   - Clicking the ID down arrow sorts the logs in ascending or descending order.

4. Select the log and click **Export**.

   DLP exports the log in CSV format to a zip file for saving to your hard drive or network.

5. Click **Refresh** to update the log queries with current information.

   **Note**
   In FTP server mode, the DLP Endpoint agent is installed on the FTP server. In FTP client mode, the DLP agent is installed on a separate machine from the FTP server. DLP logs FTP incidents differently depending on the mode. In FTP server mode, if another machine downloads a sensitive file from the FTP server, the DLP agent logs the incident but displays the user as "**NT AUTHORITY\SYSTEM**."

---

**Log Cleanup**

The DLP Server stores both incident logs and forensic data in a local file system. Over time, the logs and data could occupy too much hardware space. To reduce the impact on server performance, DLP provides CLI commands for backing up, cleaning, and restoring incident logs and recorded data. You must be logged on as root.

By default, DLP stores incident logs on the local file system in the backup folder, `/backup/violationlogs`. Incident logs are scheduled for a purge daily by default. During the log purge, DLP purges incident logs from the database if they are older than 90 days.
Cleaning Up Logs

1. Set the log backup destination by executing one of the following commands.

   • admin log config backup ftp [host] [user] [password] [path]
   • admin log config backup local
   • admin log config backup smb [host] [user] [password] [path]

   Command Parameters
   • Host: If FTP or SMB, type the server FTP IP address or SMB IP address.
   • User: Type the user name. For a domain account, type '/' instead of '\' (such as trend/test).
   • Password: If there is no password, type "none" (case sensitive).
   • Path: If FTP or SMB, type the relative path on the FTP or SMB/SAMBA server. DLP does not support the following special characters: ~`!* and white space.

   **Note**
   When the backup destination is the FTP server, and the FTP backup destination does not exist, DLP backs up the logs to the root folder on the FTP server.
   
   If DLP cannot access the FTP and SMB servers, DLP backs up files to the local directory at /backup/violationlogs.

2. Purge logs or set the schedule for purging logs by executing one of the following commands:

   CLI commands for cleaning up incident logs and forensic data
   • admin log config schedule [none/ day mon week]
   
   Sets the schedule for automatically running the log purge.
   
   • admin log config purge [days]
Sets the maximum number of days to save the backup incident logs after a purge. Valid values are 0 to 180. After exceeding the time limit, the logs are cleaned up. This parameter must be an integer. If set to 0, all incident logs in the database are deleted.

- **admin log purge**

Immediately purges incident logs in the database. The time it takes to purge log files depends on the number of log files to purge. The purge is not finished until the command prompt returns. You must wait until the purge is complete.

## Log Restore

Follow these steps to restore logs to the DLP server database.

1. Log on to the DLP server as root.
2. Execute the following command:

   ```
   admin log restore <file name>
   ```
Chapter 6

Update

This chapter describes the DLP update functions.
Agents

Use the **Agents** screen to update agents with the latest patches, add-ons, fingerprints, and data-stealing malware patterns.

The system is divided into two environments:

- Staging
- Production

---

**Note**

By default, you can set the server part of your system within the staging environment. Any operation performed in the staging environment affects only the server and all available agents within the staging environment. If you perform any operation within the production environment, it affects only the agents within the production environment.
Staging Environment

Use the staging environment to test and review new patches, add-ons, fingerprints, and data-stealing malware patterns before deploying to production. You can also check for outdated agents.

![Staging Environment screen](image)

**Figure 6-1. Staging Environment screen**

**Updating Agents in the Staging Environment**

1. Navigate to **Update > Agents > Staging Environment**.
The **Staging Environment** screen appears. The update details about agents in the **Staging Environment** screen apply to the selected tabs (Patches, Add-ons, Fingerprints, or Data-stealing Malware).

![Staging Environment screenshot](image)

**Figure 6-2. Staging Environment screen**

2. View updated and outdated agents to determine if a manual update is needed. Or, view the Available Updates list to determine if you need to take action on available updates.

   **Note**
   
   If you did not add DLP Network Monitor to your DLP system, network agent details are set to zero (0).

3. Click the following tabs to take action as needed:
   
   - Patches automatically download and display on the console. When you deploy patches, all agents in the staging environment should install (unless the agent is offline). You can also deploy them to production, rollback to the last patch status, or manually update a patch.
- Add-ons are sent by email or communication channel. Since only some customers require add-ons, they are not automatically downloaded from the official server. After receiving an add-on, upload it manually to the console and add it to your environment. You can also deploy it to production or delete it.

- Fingerprints are automatically created by DLP by the server or remote crawler. Auto-update is selected by default causing the fingerprints to auto-install when generated to all staging environment agents. However, if you clear the Auto-update checkbox, you can select the fingerprint on the Available Updates list and click Deploy to install to all staging environment agents.

- Patterns are data stealing malware patterns. Patterns are automatically downloaded and installed.

4. On the Updates: Staging Environment screens, click the number of Outdated Agents.

![Note]

**Outdated agents are agents that failed to install an update (perhaps they were offline during the installation).**

A list of agents whose updates did not install appears.

5. On the Outdated Agents list, click **Deploy Update** to attempt the install again.

![Tip]

**Tip**

For patches, add-ons, and fingerprints, clicking **Deploy to Production** synchronizes production environment versions with the staging environment versions. Patterns are automatically installed.
## Table 6-1. Available Updates Quick Reference Table

<table>
<thead>
<tr>
<th>Update Type</th>
<th>Sources</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patches</td>
<td>Trend Micro ActiveUpdate Server</td>
<td>• Install updates to all agents in the staging environment</td>
</tr>
<tr>
<td></td>
<td>• Automatically</td>
<td>• Roll back to last patch status</td>
</tr>
<tr>
<td></td>
<td>• Click Manually Upload Update</td>
<td>• Deploy to production</td>
</tr>
<tr>
<td>Add-ons</td>
<td>Trend Micro Email or Other</td>
<td>• Add (install) to agents in the staging environment</td>
</tr>
<tr>
<td></td>
<td>• Click Manually Upload Update</td>
<td>• Deploy to production</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Delete from agents in the staging and production environments</td>
</tr>
<tr>
<td>Fingerprints</td>
<td>Data Loss Prevention Server</td>
<td>• Deploy (install) to all agents in the staging environment</td>
</tr>
<tr>
<td></td>
<td>• Created automatically</td>
<td>• Deploy to production</td>
</tr>
<tr>
<td>DSM Patterns</td>
<td>Trend Micro ActiveUpdate Server</td>
<td>• View data-stealing malware patterns</td>
</tr>
<tr>
<td></td>
<td>• Automatically</td>
<td></td>
</tr>
</tbody>
</table>

## Production Environment

Use the production environment to:

- Install and roll back patches and hot fixes
- Install and delete add-ons
- Deploy fingerprints
• View data-stealing malware patterns in the production environment

**Figure 6-3. Production Environment screen**

**Updating Agents in the Production Environment**

1. Navigate to **Update > Agents > Production Environment.**
The **Production Environment** screen displays the update status.

**Figure 6-4. Production Environment screen**

2. Select a tab to view update status and available updates for that tab.
   - Patches or hot fixes are installed to all production agents from the staging environment. Click Rollback if you need to roll back to the prior version.
   - Add-ons are installed to all production agents from the staging environment. However, you can click Delete to delete them from the production agents.
   - Fingerprints are generated by the server or remote crawler and are downloaded from the server. Clicking Deploy deploys all fingerprints to the production environment agents. Or, select Auto-update to auto-install fingerprints to all production environment agents when generated.
   - Patterns are data-stealing malware patterns updated automatically from the ActiveUpdate server. Click a pattern to view details about when it was installed.

3. On the Updates - Production Environment screens, click the number of Outdated Agents.
Note
Outdated agents are agents that failed to install an update (perhaps they were offline during the install).

A list of agents whose updates did not install appears.

4. From the Outdated Agents list, click **Deploy Update** to attempt the install again.

**Active Updates**

Use the Configuration screen to configure the server address for downloading patches and hot fixes. The server address can be the Trend Micro ActiveUpdate Server or another server address. You can also configure a proxy to connect to this server address and a download schedule.

![Configuration screen](image)

**FIGURE 6-5.** Configuration screen
Configuring Active Updates

1. On the left navigation bar, click **Update > Configuration**.

   The **Configuration** screen appears.

   ![Configuration screen](image)

   **Figure 6-6. Configuration screen**

2. Enter the Server Update Source from which to download patches and hot fixes.

3. Enter the Proxy Settings to connect to the update server through a proxy. The proxy is disabled by default.

   **Note**
   
   If you enable the proxy, it is used for license verification as well.

4. Enter the **Download Update Schedule** to schedule the patch and hot fix downloads. This is enabled by default. The default schedule is 01:00 AM daily.

   **Note**
   
   Click **Download Now** to trigger an auto-download from the update source.
Configuring Silent Reboot

Sometimes endpoints require a reboot after a patch or hot fix installation. This may interrupt the normal work of the users. Consequently, DLP adds a Silent Reboot feature for more control over the installation reboot, including:

- Scheduling the endpoint restart time.
- Configuring a confirmation screen to appear to the user prior to an automated restart, giving the user a choice of restarting immediately or manually restarting later.

Configuring Silent Reboot Properties

1. Open the bootcfg.properties configuration file at the following location:

   /home/dgate/ prod/ common/ cfg/ bootcfg/ bootcfg.properties

2. Edit bootcfg.properties.

   **Table 6-2. Silent Reboot Properties (Continued)**

<table>
<thead>
<tr>
<th>PROPERTY</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>reboot_schedule_flag</td>
<td>Specifies whether to enable silent reboot:</td>
</tr>
<tr>
<td></td>
<td>• 1 is the default. A scheduled restart will occur after a patch or hot fix installation.</td>
</tr>
<tr>
<td></td>
<td>• * 0 restarts the endpoint immediately after installation (as in DLP 5.0).</td>
</tr>
<tr>
<td>reboot_schedule_time</td>
<td>Specifies the time for the scheduled restart in the format “hh:mm” where hh is hour and mm is minute.</td>
</tr>
<tr>
<td></td>
<td>“02:00” is the default.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>reboot_popup_flag</td>
<td>Specifies whether or not to display a pop-up screen prior to restart, offering users the option of accepting an immediate restart or a manual restart later.</td>
</tr>
<tr>
<td></td>
<td>• 0 is the default. No DLP screen displays when the restart occurs.</td>
</tr>
<tr>
<td></td>
<td>• 1 displays a pop-up screen prior to restart so users can choose an immediate restart or not.</td>
</tr>
<tr>
<td>reboot_popup_title</td>
<td>Specifies what to display in the title and body of the pop-up screen set with the reboot_popup_flag configuration.</td>
</tr>
<tr>
<td>reboot_popup_body</td>
<td></td>
</tr>
</tbody>
</table>

**Note**

If you use multi-byte characters (such as Japanese characters), save this configuration file in UTF-8 encoding format.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reboot_prompt</td>
<td>Specifies the text string to display in the body of the Windows™ shutdown prompt screen.</td>
</tr>
<tr>
<td>reboot_delay_sec</td>
<td>Specifies how many seconds to delay the system restart after the DLP agent triggers the restart command. This must be an integer.</td>
</tr>
<tr>
<td></td>
<td>30 seconds is the default value.</td>
</tr>
</tbody>
</table>

Once you save the bootcfg.properties file, the DLP management server notifies endpoints to apply this change.

---

**WARNING!**

Silent reboot restarts the system with the force reboot option.
Administration

This chapter describes the DLP administration functions.
Server Configuration

Use the **Server Configuration** screen to configure the following items:

- Fingerprint settings for fingerprint acquisition and sensitive content detection
- File decompression rules for fingerprint acquisition
- Server-side alert box

Fingerprint Settings

Use the Fingerprint Settings screen to perform the following configurations:

- Fingerprint Settings: File and repository size limits for acquiring fingerprints and detecting sensitive content.
- Fingerprint Decompression Control Settings: Decompression rules for acquiring fingerprints in compressed files, such as .zip files.

![Fingerprint Settings screen](image)

**FIGURE 7-1. Fingerprint Settings screen**

**Configuring Fingerprint Settings**

1. Navigate to **Administration > Server Configuration > Fingerprint Settings**.
The **Fingerprints Settings** screen appears.

**Figure 7-2. Fingerprint Settings screen**

2. Set fingerprint settings as described in the table below.

**Table 7-1. Fingerprint Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum File Size</td>
<td>Valid values: 62 Bytes to 32KB. This sets the file's minimum size for DLP to scan the file for fingerprinting. DLP does not scan files smaller than the minimum value set in this field.</td>
</tr>
<tr>
<td>Maximum Text File Size</td>
<td>Valid values: 1MB to 75MB. DLP converts documents to plain text before scanning the content for fingerprint generation or sensitive content detection. If the plain text exceeds the Maximum Text File Size set here, any content that exceeds this value is not fingerprinted or scanned for sensitive content. For example, if the maximum text file size limit is 6MB (the default setting) and the text file is 6.1MB, DLP only scans the first 6MB of the plain text document to detect sensitive content or acquire fingerprints. The .1MB over the 6MB is ignored.</td>
</tr>
<tr>
<td>Maximum Binary File Size</td>
<td>Valid values: 1MB to 75MB. If a binary file exceeds the value set in the Maximum Binary File Size field, DLP does not scan the file for fingerprinting or sensitive content detection.</td>
</tr>
</tbody>
</table>
### Maximum Archive File Size

Valid values: 1MB to 75MB. If an archive file exceeds the value set in the Maximum Archive File Size field, DLP does not scan the file for fingerprinting or sensitive file detection.

### Maximum Repository size to download the agent

Valid values: 1MB to 2GB. DLP uses the maximum repository size limitation for the fingerprints update. If the total fingerprints size exceeds the maximum repository size, the agent does not download the fingerprints. Instead, the agent performs a remote match.

---

3. **Set the Fingerprint Decompression Control Settings for Acquisition.**

<table>
<thead>
<tr>
<th><strong>FIELD</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
</table>
| Decompressed file size       | Valid values: 1MB to 512MB. To acquire fingerprints in a compressed file, DLP decompresses the file before scanning. If the decompressed file size exceeds the value that is set here, DLP only scans up to the decompressed file size setting. For example, suppose DLP encountered these two values:  
  - Decompressed file size setting: 512MB  
  - Archive file size after DLP extracts files: 600MB  
  DLP extracts the archived files and handles the first 512MB of files (ordered by alphabet). Files after 512MB are ignored. |
| Number of embedded layers    | Valid values: 1 to 20 layers. An archive file could be embedded in another archive file which is embedded in another, and so on. DLP scans and acquires fingerprints for the number of layers specified here.                                           |
| Number of decompressed files | Valid values: 1 to 2000. DLP scans and acquires fingerprints for the number of decompressed files (decompressed from archive files) specified here.                                                          |

4. **Click Save.**
Any change to the defaults or previous fingerprint settings do not take effect until the next fingerprint acquisition process.

Application Settings

Use the **Application Settings** screen to view or configure the email SMTP account settings for automated alert emails triggered by policy actions or for system alerts. In addition, except for Recipient email, DLP reuses these email settings to send reports.

**Note**

DLP supports simple password authentication only.

The email name of the sender displays in the alert mail.

![Application Settings screen](image)

**Figure 7-3. Application Settings screen**
Agent Settings

Use the **Agent Settings** screen to configure agent encryption rules and passwords, as well as the local LDAP cache time to live (TTL).

![Agent Settings screen](image)

**FIGURE 7-4. Agent Settings screen**

**Configuring Agent Settings**

1. Navigate to **Administration > Agent Configuration > Agent Settings**.
The **Agent Settings** screen appears.

![Agent Settings screen](image)

**FIGURE 7-5. Agent Settings screen**

2. Set the Agent Settings as described in the table below:
### Table 7-2. Fingerprint Settings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent Batch Encryption Settings</td>
<td>Agent Batch Encryption/Justification Timeout: If a user copies multiple files and DLP blocks a file that requires a justification before copying, DLP prompts for the justification. To avoid having the user enter a justification for every file being copied, DLP sets a timeout for the justification. Multiple files can then be copied without interruption, until the timeout expires.</td>
</tr>
</tbody>
</table>

**Note**

DLP only displays the justification prompt if you set “justification” as a company policy action.

Also, if you set a policy action to encrypt files copied to a USB device and require that the user enter a justification and password to avoid the encryption action, DLP prompts the user for the justification and password. Again, the Agent Batch Encryption/Justification Timeout sets the timeout so that the user does not need to provide a justification and password for every file. When the timeout expires, DLP prompts the user again for a justification and password.

Agent Batch Encryption Filename Prefix: When a user copies multiple files to a USB device and DLP encrypts the files, DLP adds the files to an existing encryption file. DLP names the encryption file with the \{filename prefix\} + the \{file name\} (with extension) + a variable \{counter\}.exe.

For example, an encryption file name, “dlp_encrypted_sample.doc.23.exe” is assembled as follows:

- Filename prefix: dlp_encrypted
- File name: sample.doc
- Counter: 23
- File extension: .exe
Local LDAP Cache

Local LDAP cache time to live (TTL) can be up to one week.

**Note**

The agent queries user or group information if a policy is based on LDAP or endpoint group targets. After receiving the query from the management server, the agent caches the query locally until the TTL expires or a new policy is deployed. If the TTL value is set to 0 days, the expiration time is automatically set to 30 minutes.

Decompression Control Settings

DLP decompresses compressed archive files before scanning them for sensitive data. Decompression control settings set the file size limit for decompressed files, number of layers for DLP to scan, and the number of decompressed files from an archive file for DLP to scan.

Change Password

This is the password for forensic data encryption and data discovery. The default password is 12345678. However, it is recommended that you change this password. Passwords for forensic data encryption can include letters, numbers, and some special characters, such as # and @.

3. Click Save.
Advanced Settings

Use the Advanced Settings screen to configure the client-side alert screen and logging. You can also activate the UDP listener.

![Advanced Settings Screen](image)

**Figure 7-6. Advanced Settings screen**

Configuring the Alert Dialog Box

Data Loss Prevention provides a default client-side, security alert dialog box that appears to users on the agent endpoint when:

- An incident occurs (depending on the company policy)
- For encryption justification

You can edit its XML code, such as importing a logo image file (.GIF).
1. Navigate to Administration > Agent Configuration > Advanced Settings > Dialog Configuration.

The Advanced Settings Dialog Configuration tab appears.

2. Click Load Dialog File.

The Dialog Configuration XML file loads into the text box.

![Figure 7-7. Dialog Configuration text box](image)

3. Modify the XML code, but do not use single quotation marks.
   - Browse to a logo file and upload it.
   - Use a GIF file type that is no larger than 450 by 200 pixels and does not exceed 3MB.
   - The GIF can contain a transparent background.
   - Change the tag from “<Logo Show="0"...” to “<Logo Show="1"...”

4. Click Deploy to Agent.
   - For online agents, changes take place within several minutes.
For offline agents, changes take place after the agents come online to get the latest configurations.

Configuring Agent Module Logging

Use the **Logging Configuration** tab to edit the debug logging configuration file and enable or disable debug logging of agent modules.

1. Navigate to **Administration > Agent Configuration > Advanced Settings > Logging Configuration**.

   The **Logging Configuration** tab appears.

2. Enter the agent module logging specifications:
   - Endpoints: Click **[Select endpoint(s)]** to select the endpoints to log.
• Modules: Select modules and click Add>>. You can select multiple items.
• Logging Level
• Type:
  * DebugView (Dbg) writes a debug log to a delegated channel that you can view using the DebugView tool. Download the DebugView tool from Microsoft.
  * File displays a text field so that you can type the full path of the log file to which the agent should write. For example, C:\dlpagent.log.
  * UDP displays a text field so that you can specify the IP address of the DLP server for UDP logging.

---

**Note**
Trend Micro recommends sending logs to File, since it is more stable than UDP where packets can be lost and since you can directly transfer the file to Trend Micro Support.

---

**3.** Click **Enable Agent Log**.

The system displays the following message: “Logging configuration information deployed successfully!”

### Activating the UDP Listener

If you enable debug logging for an agent module using UDP, the agent sends its debug log to the server directly through UDP. In the UDP listener tab, you can view the debug logs directly from the agent rather than getting the debug log file from disk on the agent side. Although this may be more convenient, Trend Micro recommends sending logs to
File instead. With UDP, packets may be lost. Also, a file can be directly transferred to Trend Micro Support.

**Figure 7-9. UDP Listener tab**

1. Navigate to Administration > Agent Configuration > Advanced Settings > UDP Listener.
2. Click **Start Listening** to activate the Internal UDP Listener.

**WARNING!**

udp logging for more than one endpoint is not recommended.
Global Exceptions

Use the Global Exceptions screen to change global DLP behavior for monitored and non-monitored targets, as well as internal email domains.

**Figure 7-10. Global Exceptions screen**

1. Navigate to **Administration > Agent Configuration > Global Exceptions**.
2. Type the global exceptions for digital asset scanning.
### Table 7-3. Global Exceptions

<table>
<thead>
<tr>
<th>Global Exception</th>
<th>Description</th>
</tr>
</thead>
</table>
| Non-monitored Targets  | Specify destinations outside your network where an endpoint is permitted to send sensitive data. DLP will not check sensitive data sent through this network service.  
  Define each target by:  
  - IP address or address range  
  - Host name  
  - FQDN  
  - Network address and subnet mask, such as 10.1.1.1/32  
  To target specific channels, include the default or company-defined port numbers for those channels. For example, port 21 is typically for FTP traffic, port 80 for HTTP, and port 443 for HTTPS. Use a colon to separate the target from the port numbers.  
  You can also include port ranges. To include all ports, ignore the port range.  
  Examples of targets with port numbers and port ranges:  
  - 10.1.1.1:80  
  - host:5-20  
  - host.domain.com:20  
  - 10.1.1.1/32:20  
  For the subnet mask, DLP only supports a classless inter-domain routing (CIDR) type port. That means that you can only type a number like 24 instead of 255.255.255.0.  
  Separate targets with commas. |

---

Trend Micro Data Loss Prevention Endpoint 5.6 Administrator’s Guide
<table>
<thead>
<tr>
<th><strong>GLOBAL EXCEPTION</strong></th>
<th><strong>DESCRIPTION</strong></th>
</tr>
</thead>
</table>
| Monitored Targets      | Specify destinations inside your network that do not have total clearance. DLP checks traffic but does not block content unless you specify blocking as the policy action. Define each target by:  
  • IP address or address range  
  • Host name  
  • FQDN  
  • Network address and subnet mask, such as 10.1.1.1/32  
To target specific channels, include the default or company-defined port numbers for those channels. For example, port 21 is typically for FTP traffic, port 80 for HTTP, and port 443 for HTTPS. Use a colon to separate the target from the port numbers.  
You can also include port ranges. To include all ports, ignore the port range.  
Examples of targets with port numbers and port ranges:  
  • 10.1.1.1:80  
  • host:5-20  
  • host.domain.com:20  
  • 10.1.1.1/32:20  
For the subnet mask, DLP only supports a classless inter-domain routing (CIDR) type port. That means that you can only type a number like 24 instead of 255.255.255.0.  
Separate targets with commas. |

**Note**  
If the global exceptions and transmission scope settings conflict, DLP recognizes the following priorities, in order of highest priority to lowest:  
Monitored Targets > Non-monitored Targets > Transmission Scope
Global Exception | Description
--- | ---
Internal Email Domains | Type all internal email domains to help DLP determine the email to monitor.

DLP checks the transmission scope, which you need to configure when specifying actions for a policy. DLP automatically monitors email traffic when:

- Transmission scope is set to “All transmissions”; or
- Transmission scope is set to “Only transmissions outside the local area network” AND the recipient is not in the list of Internal Email Domains

Specify domains using any of the following formats, separating multiple domains with commas:

- X400 format, such as /O=Trend/OU=USA, /O=Trend/OU=China
- Email domains, such as example.com

3. Click Save.

Remote Crawler Management

Use the Crawler Management screen to manage or deploy the Remote Crawler agent. The Remote Crawler agent performs the following functions:

- Scans for confidential data stored on desktops and laptops not connected to the company network
- Acquires fingerprints on systems other than the DLP server.

The Remote Crawler forwards generated fingerprints to the DLP server where they are merged with fingerprints already stored on the server.

The Remote Crawler can protect:

- Files stored locally (on computers where the Remote Crawler is installed). For locally stored files, the Remote Crawler computer does not require a shared folder that the DLP server can access.
• Files in a SharePoint server environment that the DLP server may or may not have access to.
• Files in a Windows Share environment.

**FIGURE 7-11. Crawler Management screen**

**Remote Crawler Installation and Configuration**

Installing and configuring the remote crawler is a four-part process:

**TABLE 7-4. High-Level Remote Crawler Installation Process**

<table>
<thead>
<tr>
<th><strong>STEP</strong></th>
<th><strong>WHERE PROCEDURE OCCURS</strong></th>
<th><strong>PROCEDURE</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>DLP web console</td>
<td>Install the remote crawler.</td>
</tr>
<tr>
<td>2</td>
<td>Remote Crawler console</td>
<td>Add a repository to scan.</td>
</tr>
<tr>
<td>3</td>
<td>DLP web console</td>
<td>Add a fingerprint definition for the acquisition source (with Remote Crawler as Repository Type and the Remote Crawler name as Host).</td>
</tr>
<tr>
<td>4</td>
<td>Remote Crawler console</td>
<td>Reconfigure the DLP Manager server address.</td>
</tr>
</tbody>
</table>

**Installing the Remote Crawler**

1. Navigate to Administration > Crawler Management.
The Crawler Management screen appears.

![Crawler Management Screen](image)

**Figure 7-12. Crawler Management screen**

2. Click **Download Remote Crawler**.
   The system prompts you to save or run RemoteCrawlerAgentSetUp.msi.

   The **Remote Crawler InstallShield Wizard** appears.

4. Navigate the InstallShield Wizard and complete the required screens:

**Table 7-5. Remote Crawler InstallShield Wizard Screens**

<table>
<thead>
<tr>
<th>Screens</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Agreement</td>
<td>Read and agree.</td>
</tr>
<tr>
<td>Destination Folder</td>
<td>Specify where to install the Remote Crawler.</td>
</tr>
<tr>
<td>Manager Server Address</td>
<td>Specify the host name or IP address of the DLP Manager server to which the remote crawler uploads fingerprints files.</td>
</tr>
<tr>
<td>Ready to Install Program</td>
<td>Click Install.</td>
</tr>
</tbody>
</table>
The **InstallShield Wizard Completed** screen appears.

![InstallShield Wizard Completed Screen](image)

**Figure 7-13. InstallShield Wizard Completed screen**

5. Clear **Launch DLP Remote Crawler Agent Console** and click **Finish**.

6. From Windows, navigate to **Start > Program Files > Trend Micro DLP Remote Crawler Agent**.

![Windows Program Files Menu](image)

**Figure 7-14. Windows Program Files Menu**

7. Click **Remote Crawler Agent Console**.
The **Trend Micro DLP Remote Crawler Agent** console appears.

![Image of the Trend Micro DLP Remote Crawler Agent Console](image)

**Figure 7-15. DLP Remote Crawler Agent Console**

**Adding Repositories to Scan**

1. On the **Remote Crawler Agent** console, click **Add**.
The **Add/ Edit Repository** screen appears.

![Add/Edit Repository screen](image)

**Figure 7-16. Add/Edit Repository screen**

2. Specify the details of the repository to scan:

**Table 7-6. Add/Edit Repository Fields**

<table>
<thead>
<tr>
<th>SCREENS</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Select Local if the sensitive documents reside in the local system. Select Windows Share Folder if the sensitive documents reside in a Windows share folder. Select SharePoint 2003 or 2007 if the sensitive documents reside on a Sharepoint 2003 or 2007 site.</td>
</tr>
<tr>
<td><strong>SCREENS</strong></td>
<td><strong>ACTION</strong></td>
</tr>
<tr>
<td>----------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recursive</td>
<td>Select Yes to have the crawler agent crawl the subdirectories. Note these “Recursive” rules to prevent duplicate file paths for fingerprint acquisitions:</td>
</tr>
<tr>
<td></td>
<td>• To configure both parent and child directories on the remote crawler, set “Recursive” to “No” on the parent directory. Otherwise, the parent and child directories cannot be configured in the same crawler. For example, if you add a repository of c:\abc with recursive=yes, you cannot add any more children folders, such as c:\abc\test.</td>
</tr>
<tr>
<td></td>
<td>• If you add a child repository and set “Recursive” to “Yes” on the parent repository, you cannot add more parent folders.</td>
</tr>
<tr>
<td>Site</td>
<td>Type the site IP address or host name for the repository.</td>
</tr>
<tr>
<td></td>
<td>• For a Share folder, you can type a host name or IP address. Example: for \10.64.10.1\test, you could just type the IP address, 10.64.10.1.</td>
</tr>
<tr>
<td></td>
<td>• For Microsoft SharePoint, type the SharePoint server site address, such as “<a href="http://ishare.trendmicro.com/enggroup/dlp%E2%80%9D">http://ishare.trendmicro.com/enggroup/dlp”</a>. In this case, “enggroup/dlp” is the SharePoint site. You would add “enggroup/dlp” to the Host field (rather than the Path field) on the DLP web console during fingerprint definition setup.</td>
</tr>
<tr>
<td>Path</td>
<td>Set the repository path, such as “Shared Document/Test”.</td>
</tr>
<tr>
<td>User Name and Password</td>
<td>User name and password are required to access the SharePoint server or Share folder. Leave these fields blank for the local repository.</td>
</tr>
</tbody>
</table>

3. Click **Test** to ensure that the Remote Crawler can access the repository.
When the test is complete, the test result appears in the bottom pane of the Add/Edit Repository screen.

![Add/Edit Repository screen - Test result](image)

**Figure 7-17. Add/Edit Repository screen - Test result**

1. Click **Save**.

---

**Note**

Cancel closes the window without saving.

---

### Adding Fingerprint Definitions for the Remote Crawler

1. Navigate to **Data Protection > Data Identifiers > Fingerprints**.
The **Fingerprints** screen appears.

**FIGURE 7-18. Fingerprints screen**

2. Click **Add**.

A new screen appears.

**FIGURE 7-19. Add Fingerprints screen**

3. Complete the fields for the fingerprint definition and make the following selections:
   - Select “Remote Crawler” for Repository Type.
• Select the Remote Crawler name for the Host.

4. Click **Save**.

---

### Reconfiguring the DLP Manager Server Address

Typically, the DLP server IP address is configured during remote crawler setup. However, in some cases, the DLP server IP may change. Or, if a remote crawler switches from one DLP server to another DLP server, the IP address will change. In this case, you may want to reconfigure the DLP manager server address.

**Note**

When switching from one DLP server to another, Trend Micro recommends that you reinstall the remote crawler rather than reconfigure the IP (since the cache may not be useful for the new server and should be removed).

1. From the **Remote Crawler Agent Console**, select **File > Configuration**.

   The **Remote Crawler file configuration** screen appears.

2. Type the server address and click **Save**.

   The Remote Crawler automatically registers to the server in several minutes.

   Schedule or run the remote crawler acquisition process from the DLP web console at **Data Protection > Data Identifiers > Fingerprints**.

### Deleting Remote Crawler Agents

You can delete an online remote crawler that a Fingerprint definition does not reference by source in **Adding Fingerprints > Source**. To delete a remote crawler, uninstall it from the Remote Crawler menu or through the Add/Remove program in the machine that the Remote Crawler is installed on.

**Note**

DLP simply deletes the crawler from the list. If the crawler is offline when you delete the it from the list, the crawler reappears when it comes back online.
1. Navigate to Administration > Crawler Management.

   The Crawler Management screen appears.

   **Note**
   View detailed information of a Remote Crawler Agent by clicking the hyperlink in the Host column.

2. Click Filter.

   The Crawler Criteria screen appears.

3. Select the filter criteria and click Find.

   The crawler appears.

4. Select the crawler and click Delete.

   The system asks if you are sure that you want to delete the remote crawler.

5. Click Yes.

   DLP deletes the remote crawler from the list.

---

## Data Management

Use the Data Management screen to export and import DLP Endpoint and Network Monitor data, such as security policies and user roles. Exporting the data provides a backup in the event of a system failure.

**Note**
During an export, DLP clears the DLP database. However, DLP does not export archived reports files, fingerprint scheduled job information, data discovery scheduled job information, and the Agent Settings log configuration.
To import data using the Data Management function, the import file must be less than 200MB. For larger file sizes, import the file using a script at the command line interface.

![Data Management screen](image)

**Figure 7-20. Data Management screen**

**Exporting DLP Data**

1. Navigate to **Administration > Data Management > Data Management Control**.
   
   The **Data Management Control** tab appears.

2. Select **Export file from system data repository**.

3. Select an item to export.

4. Click **Start**.

DLP dumps the specified data from the DLP database and downloads the file. When the export is complete, the system displays the message, “Data export a success!”

**Importing DLP Files Under 200MB**

1. Navigate to **Administration > Data Management > Data Management Control**.
2. Select **Import file to system data repository**.
3. Browse to and select the file to import.
4. Click **Start**.

DLP imports the data into the DLP database.

**Importing DLP Files Over 200MB**

1. Upload the import file to the DLP server using FTP or SSH.

---

**Note**
The import file should retain the export file name.

---

2. Open the command prompt box on the DLP server.
3. Log on to the DLP server shell as “dgate.” Use the default password if your DLP Endpoint application came pre-installed. Otherwise, use the password of the DLP service’s default account that you set up during the DLP server VA installation.
4. Go to the following directory:

```
/home/dgate/prod/common/scripts
```
5. Enter the following command to import the uploaded import file:

```
dg_import.sh {filepath/file name}
```
6. After the command finishes executing, restart the DLP server.

**Viewing and Downloading Exported Files**

1. Navigate to **Administration > Data Management > Exported Files**.
The list of exported files appears.

![Image of Exported Files tab]

**Figure 7-21. Exported Files tab**

2. Click the export file to download it.

**Agent Management**

Use the **Agent Management: Agents** tab to view agent status, to notify an agent to download the latest patch from the server (if it missed a prior notification), and to move the agent to the staging or production environment.

![Image of Agent Management screen]

**Figure 7-22. Agent Management screen**
Viewing and Editing Agent Information

1. Navigate to Administration > Agent Management > Agents.

The Agent tab appears with a list of agents. You can quickly view agent details and status, as well as whether the company policy for that agent is outdated or not.

2. Click an agent.

The Agent Information screen appears. You can take the following actions from the Agent Information screen:

![Agent Information Screen]

Figure 7-23. Agent Management - Agents Information
• Update Environment: Moves the agent to the staging or production environment.
• Update Endpoint: Notifies the agent to download the latest patch from the server. Click this if the agent missed a prior patch download notification.

3. Click Save.

Deleting Agents from the Agent Management List

1. Navigate to Administration > Agent Management > Agents.

The Agent tab appears with a list of agents.

2. Select the agent. The agent must be offline, not associated with a group, and not listed as a target of a policy or data discovery task.

3. Click Delete.

DLP deletes the agent from the list but does not remotely uninstall the agent. When the agent reconnects, its name reappears on the list.

---

**Note**

DLP retains the agent’s device control settings even if the agent is disconnected from the network and deleted from the agent management screen. When the agent is back online and registered again with the server, the device control settings are recovered.

---

Managing Agent Groups

Use the Agent Management: Group tab to group agents for the purpose of applying different incident control and device control policies by group. Groups created in the Group tab populate these two lists:

• Data Protection > Company Policies > Targets list for Group/ Endpoint targets
• Data Protection > Device Control > Groups
Creating New Groups

1. Navigate to **Administration > Agent Management > Group**.
   The **Group** tab displays a current list of groups.

2. Click **Add**.
   The **Add Group** screen appears.

3. Type the group information:
   - **Group Name** accepts up to 50 alphanumeric characters.
   - **Description** accepts up to 256 alphanumeric characters.

4. Select the agents for the group and click **Add>>**.
   The agents are moved to the **Selected** box.
Note
You can add multiple agents by selecting another existing group or domain and
adding the group as a member of the new group. If you add an existing group as a
member, DLP automatically expands the endpoints of the selected group/domain
and adds them one-by-one into the new group.

5. Click **Save**.

Note
To delete a group, select the group and click **Delete**. Note that you can only delete a
user-defined group that is not associated with a company policy or data discovery
target.

Web Console Password

Access the web console **Change Passwords** screen at **Administration > Password**.

Passwords must be between 8 and 32 characters. Passwords can include letters,
numbers, and some special characters, such as # and @.

![Change Password](image)

**Figure 7-25. Change Password screen**
Management Console

Use the Management Console to create, view, update, or delete user accounts and role definitions at runtime.

User Account Management

Use the User Accounts screen to reset user passwords and create, view, and delete user accounts. Assign one or more roles to each user. The default user is “Admin.”

---

**Note**
You cannot edit role permissions for the default admin user.

---

**Figure 7-26. User Accounts screen**

Adding Users

1. Navigate to Administration > Management Console > User Accounts.
The User Accounts screen appears.

**Figure 7-27. User Accounts screen**

2. Click **Add**.

The New Account screen appears.

**Figure 7-28. New Account screen**

3. Select **Enable account**.

4. Type user name and password information.
   - Username must less than 51 alphanumeric characters.
   - Password must be between 8 and 32 alphanumeric characters.

5. Select roles to assign to the user and click **Save**.
The new user account is added to the User Accounts list.

**Note**
To delete a user account, select the account and click **Delete**. To edit a user account, click the user name to display the **User Account** screen for editing.

### Role Management

Use the **Role Management** screen to create, view, update, or delete administrative roles at runtime. Define each role with permissions for system operations. The default roles are Administrator, Security Manager, and Account Manager.

![Role Management screen](image)

**Figure 7-29. Role Management screen**

#### Adding Roles

1. Navigate to **Administration > Management Console > Role Management**.
The **Role Management** screen appears.

![Role Management screen](image)

**FIGURE 7-30. Role Management screen**

2. Click **Add**.

The **New Role** screen appears.

![New Role screen](image)

**FIGURE 7-31. New Role screen**
3. Type the Role Information:
   - Name must be less than 51 alphanumeric characters.
   - Description is optional.

4. Select the permissions for the role and click **Save**. At least one permission must be selected.

The new role is added to the Role Management list.

---

**Note**

To delete a role, select the role from the Role Management list and click **Delete**.

---

### Configuring LDAP Settings

Use the LDAP Settings screen to integrate DLP user-group definitions with Microsoft Active Directory.

1. Navigate to **Administration** > **LDAP**.
The **LDAP Settings** screen appears.

![LDAP Settings Screen](image)

2. Select **Enable Primary LDAP Server** and type server details:

   - **Enable Primary LDAP server**
   - **Server name:**
     - Example: server1.us.example.org or 123.123.123.123
   - **Base DN:**
   - **Port:**
   - **Login User Name/DN:**
   - **Password:**
     - Enable SSL [Certificate Management]
     - Test Connection

   - **Enable Backup LDAP server**
   - **Server name:**
     - Example: server1.us.example.org or 123.123.123.123
   - **Base DN:**
   - **Port:**
   - **Login User Name/DN:**
   - **Password:**
     - Enable SSL [Certificate Management]
     - Test Connection

   **LDAP Cache Expiration**
   - **Time to Live (TTL):**
     - 60 minute(s)

   **CAUTION:** The DLP server MUST be restarted for any new changes to take effect.

**Figure 7-32. LDAP Settings screen**
• Server name accepts an IP address for the Active Directory (AD) or a DNS name.
• Base DN is the Distinguished Name (DN) where the AD search would begin.
• Port - 389 is the default. 3628 is used for the Global Catalog. Port numbers greater than 65535 or smaller than 1 are not valid.
• Login Domain name and Password authorizes logging into the Active Directory.
• Enable SSL transports AD data over the Secure Socket Layer.
  * When Enable SSL is selected, you must use port 3269 or 636.
  * When Enable SSL is not selected, you cannot use port 3269 or 636.

3. Select **Enable Backup LDAP Server** and configure its settings, if applicable.

4. Type the LDAP Cache Expiration. This is the duration that DLP caches LDAP information queried from the Active Directory. For the most current information, do not set the cache value for longer than one day. Alternately, do not set the cache value too short. Without the cache, the search query has to go round trip to the active directory.

5. Click **Save**.

A confirmation screen appears asking if you want to restart the DLP server so that changes can take effect.

6. Click **OK** so that DLP can implement the new changes.

---

**Note**

Check the Base DN and Server Name. When using a hostname/DNS name, make sure your DNS server query resolve is okay.

---

**Product License**

Use the **Product License** screen to:
• View licensing information
• Manage licenses
• Register and activate all DLP products

Note
DLP Endpoint is activated with one activation code for all DLP Endpoint features. However, multiple DLP Network Monitor devices must be activated one at a time, each with its own activation code.

**Figure 7-33. Product License screen**

**About Licenses**

A license for Trend Micro software usually includes the right to product updates, pattern file updates, and basic technical support (“Maintenance”) for one (1) year from the date of purchase only. After the first year, Maintenance must be renewed on an annual basis at Trend Micro’s most current Maintenance rate.

A Maintenance Agreement is a contract between your organization and Trend Micro. It establishes your right to receive technical support and product updates in return for the payment of applicable fees. When you purchase a Trend Micro product, the License Agreement you receive with the product describes the terms of the Maintenance Agreement for that product.
Note

The Maintenance Agreement has an expiration date. Your License Agreement does not. If the Maintenance Agreement expires, agent detection can still occur. However, you will not be able to download and update patches and DSM patterns from the update server. Nor will you be entitled to receive technical support from Trend Micro.

Typically, ninety (90) days before the Maintenance Agreement expires, you will start to receive email notifications, alerting you of the pending discontinuation. You can update your Maintenance Agreement by purchasing renewal maintenance from your Reseller, Trend Micro Sales, or on the Trend Micro Online Registration site URL:

https://olr.trendmicro.com/registration/

---

Viewing Existing Licenses

1. Navigate to Administration > Product License.

A brief summary of each license appears on the Product License screen.

2. Click the license to view details.

The following details appear:

- Product name
- Version (full or trial)
- Activation code
- Number of seats
- Status (activated or not activated)
- Maintenance expiration

3. To check the status of the license agreement on the Trend Micro Online Registration website, click Check Status Online.

Activating DLP Products

You must activate DLP products to use their features. To activate a product, you must have its activation code. You can obtain the activation code after registering the product
and receiving a registration code. To obtain a registration code, go to the Trend Micro online registration website:

https://olr.trendmicro.com/registration/

1. Navigate to Administration > Product License.
   A brief summary of each license appears on the Product License screen.

2. On the Product License screen, click the license to activate.
   The Product License details screen appears.

3. Click Enter a new code.
   The New Activation Code screen appears.

4. Type the new activation code and click Save.
   The Product Licenses screen appears with the number of days left before the product expires.

Renewing Licenses

To renew a license, DLP needs access to the Internet to connect with the Trend Micro servers.

1. Navigate to Administration > Product License.
   A brief summary of each license appears on the Product License screen.

2. Click the license to renew.
   The Product License details screen appears.

3. On the license details screen, click View renewal instructions.
   The Renewal Instructions screen appears.

   The Online Registration screen appears.
System Monitoring

When the hard disk drive on the DLP management server exceeds 80% usage, the DLP server sends alert email. The alert email goes to recipients configured in Administration > Server Configuration > Application Settings. DLP sends the alert every 30 minutes for as long as the hard disk drive continues to exceed 80% usage.

If hard disk drive usage exceeds 80%, take one or more of the following server maintenance operations:

• Add a hard disk drive to the DLP server.
• Reduce hard drive usage by taking the following actions:
  • Purge incident logs using the command line interface.
  • Delete other types of data, such as archived reports, from the web console.
Chapter 8

Command Line Interface Commands

This chapter describes the command line interface (CLI) commands used in DLP.
DLP Endpoint CLI Command Overview

Access to the DLP CLI is available through the DLP console (keyboard and monitor connected directly to the DLP server) or remotely using an SSH v2 connection to the management IP address.

CLI commands enable you to perform additional configuration tasks and to perform debug and troubleshooting functions. The CLI also provides additional commands to monitor critical resources and functions, such as the traffic that flows to and from the DLP server.

To access the CLI, you will need to have the administrator account and password. DLP CLI commands are separated into two categories: nonprivileged and privileged commands.

- Nonprivileged commands are basic commands that allow you to obtain specific low-security-risk information and to perform simple tasks.
- Privileged commands provide full configuration control and advanced monitoring and debugging features.

Privileged commands are protected by an additional layer of credentials: the Enable account and password.

---

**Note**

You must configure system configurations, such as network settings, through the DLP VA command line interface. You cannot configure system configurations using Linux commands. If you do, settings will not be saved in the configuration file and the agent will not be able to register with the server.

---

Accessing the Privileged CLI Mode

The DLP CLI is secured through an industry-standard architecture using several levels of authentication and passwords. To gain access to the CLI, the administrator level account credentials are required. This can be the default "admin" account or it can be any administrator equivalent account created in the DLP server.
After you authenticate to the CLI with an authorized administrator level account, you are placed into the nonprivileged mode of the CLI. The nonprivileged level enables you to perform basic commands.

To enter the privileged CLI mode in which administration and system level commands are executed, you must authenticate using the Enable account credentials while in the nonprivileged CLI mode. This prevents unauthorized administrators from gaining access to the critical system commands.

1. Access the CLI from the local DLP console or through a remote SSH v2 connection.
2. Authenticate to the nonprivileged CLI using the “admin” account and password.
3. To see a list of available commands, type ? and press Enter.
   A list of available nonprivileged commands displays.
4. Authenticate to the privileged CLI by typing the enable command and press Enter.
5. Type the Enable account password.
   If your account and passwords were properly entered, you will be placed into the privileged CLI mode.
6. To see a list of available privileged commands, type ? and press Enter.
   A list of available privileged commands appears. This list contains more system commands than the list for the nonprivileged CLI level.

Accessing the OS Shell

You should never need to access the OS Shell under normal operating conditions as the DLP management UI and the Privileged CLI modes provide all of the routine configuration functions to set up and maintain DLP on a day-to-day basis. On the rare occasion when you might be required to enter the OS shell interface, use the following procedure to authenticate to the OS shell.

1. Access the CLI from the local DLP console or through a remote SSH v2 connection.
2. Authenticate to the nonprivileged CLI using the “admin" account and password (or any administrator equivalent account.)

3. To authenticate to the privileged CLI, type the enable command and press Enter.

4. Type the Enable account password.
   
   If you entered your account and passwords properly, you are placed into the privileged CLI mode.

5. To gain access to the OS shell, type the admin shell command and press Enter.

6. Enter the root password.
   
   If you entered your root password correctly, you are placed into the OS shell and the CLI prompt changes to the OS Shell prompt. You can now perform native operating system commands.

7. To exit from the OS shell and go back to the privileged CLI, type the exit command and press Enter.

   The exit command moves you back up one CLI shell level at a time until it logs you out of the CLI.

---

**Note**

If you received DLP Endpoint pre-installed, use the default password. You can change the passwords for each of these accounts by using the configure password CLI command.

---

**DLP Endpoint CLI Commands**

---

**Note**

You must configure system configurations, such as network settings, through the DLP VA command line interface. You cannot configure system configurations using Linux commands. If you do, settings will not be saved in the configuration file and the agent will not be able to register with the server.

---

The following commands are available in DLP.
<table>
<thead>
<tr>
<th>CLI COMMAND</th>
<th>DESCRIPTION</th>
<th>NOTES</th>
</tr>
</thead>
</table>
| admin log config backup ftp [host] [user] [password] [path] | Configures FTP as a backup destination for the log file.                    | host: type FTP server IP address  
user: type the user name. For a domain account, type ‘/’ instead of ‘\’ (such as trend/test)  
password: if there is no password, type "none" (case sensitive)  
path: type the relative path on the FTP server. DLP does not support the following special characters: ~`!* and white space |
| admin log config backup local    | Configures local as a backup destination for the log file.                  |                                                                                                                                         |
| admin log config backup smb [host] [user] [password] [path] | Configures the Server Message Block (SMB) as a backup destination for the log file.                                | host: type smb/samba server IP address  
user: type the user name. For a domain account, type ‘/’ instead of ‘\’ (such as trend/test)  
password: if there is no password, type "none" (case sensitive)  
path: type the relative path on the smb/samba server. DLP does not support the following special characters: ~`!* and white space |
<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin log config purge [days]</td>
<td>Sets the maximum number of days to save the backup incident logs after a purge. Valid values are 0 to 180. After exceeding the time limit, the logs are cleaned up.</td>
<td>This parameter must be an integer. If set to 0, all incident logs in the database are deleted.</td>
</tr>
<tr>
<td>admin log config purge [days]</td>
<td>Sets the maximum number of days to save the backup incident logs after a purge. Valid values are 0 to 180. After exceeding the time limit, the logs are cleaned up.</td>
<td>This parameter must be an integer. If set to 0, all incident logs in the database are deleted.</td>
</tr>
<tr>
<td>admin log config schedule [none/ day mon week]</td>
<td>Sets the schedule for automatically running the log purge.</td>
<td></td>
</tr>
<tr>
<td>admin log config show</td>
<td>Shows the log configuration parameters.</td>
<td></td>
</tr>
<tr>
<td>admin log delback [file name]</td>
<td>Deletes the backup log file.</td>
<td>You can use the CLI (log show backup) to check the backup files, which are located at /backup/ violationlogs</td>
</tr>
<tr>
<td>admin log purge</td>
<td>Purges incident logs in the database.</td>
<td>DLP may take more time to purge log files depending on the number of log files to purge. The purge is not finished until the command prompt returns. You must wait until the purge is complete.</td>
</tr>
<tr>
<td>CLI COMMAND</td>
<td>DESCRIPTION</td>
<td>NOTES</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>admin log restore [file name]</td>
<td>Restores the backup log and forensic data to the DLP server database.</td>
<td>You can use the CLI (log show backup) to check the backup files, which are located at /backup/violationlogs</td>
</tr>
<tr>
<td>admin db backup [db name] [destination] [option] ...</td>
<td>db_backup.sh – backs up the database.</td>
<td></td>
</tr>
<tr>
<td>admin db checkconf [configuration file] [option] ...</td>
<td>admin_checkconf.sh – performs an integrity check on the database.</td>
<td></td>
</tr>
<tr>
<td>admin db checksize [db file] [option] ...</td>
<td>admin_checksize.sh – used to verify the amount of disk space allocated to the database.</td>
<td></td>
</tr>
<tr>
<td>admin db clean [db file] [option] ...</td>
<td>Performs VACUUM (on the database.)</td>
<td></td>
</tr>
<tr>
<td>admin db reindex [db file] [option] ...</td>
<td>admin_reindex.sh – re-indexes the database.</td>
<td></td>
</tr>
<tr>
<td>admin db restore [source] [db name] [option] ...</td>
<td>db_restore.sh – restores the database from the backup file.</td>
<td></td>
</tr>
<tr>
<td>capture interface [interface value] [option 1] [option 2] [option 3] ...</td>
<td>tcpdump – Captures network traffic passing through the interfaces on the system.</td>
<td>Suggested Options: Src IP Dst IP Protocol Interface Port Packet Count Output Location Leverages v3.1’s GUI to manage the dump files used by FTP to transport. Have a maximum hard limit to prevent dump files from taking over the disk.</td>
</tr>
<tr>
<td>config.properties</td>
<td>Specifies parameters for cleaning and backing up logs.</td>
<td></td>
</tr>
<tr>
<td>CLI Command</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>configure date</td>
<td>Specifies parameters for cleaning and backing up logs.</td>
<td></td>
</tr>
<tr>
<td>configure DLP network</td>
<td>Configures the IP and firewall settings.</td>
<td></td>
</tr>
<tr>
<td>configure dns</td>
<td>Configures the dns settings.</td>
<td></td>
</tr>
<tr>
<td>configure hostname</td>
<td>Configures the hostname or FQDN.</td>
<td></td>
</tr>
<tr>
<td>configure interface</td>
<td>Configures the interface.</td>
<td></td>
</tr>
<tr>
<td>configure password enable</td>
<td>Changes the enable user's password.</td>
<td></td>
</tr>
<tr>
<td>configure route</td>
<td>Adds, deletes, or sets a default route.</td>
<td></td>
</tr>
<tr>
<td>configure timezone</td>
<td>Allows you to change the time zone to the chosen region.</td>
<td></td>
</tr>
<tr>
<td>dg_import.sh [file name]</td>
<td>Imports Data Loss Prevention files that are over 200MB.</td>
<td></td>
</tr>
<tr>
<td>enable</td>
<td>Command to enable mode.</td>
<td></td>
</tr>
<tr>
<td>enable shell</td>
<td>Launches the Native OS shell.</td>
<td></td>
</tr>
<tr>
<td>exit</td>
<td>Exits the session.</td>
<td></td>
</tr>
<tr>
<td>ftp (support same OS format and syntax)</td>
<td>ftp – Helpful when you need to transfer files to a remote system via FTP.</td>
<td></td>
</tr>
<tr>
<td>help</td>
<td>Displays an overview of the CLI syntax.</td>
<td></td>
</tr>
<tr>
<td>CLI COMMAND</td>
<td>DESCRIPTION</td>
<td>NOTES</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>history</td>
<td>Displays the current session's command line history.</td>
<td></td>
</tr>
<tr>
<td>Logout</td>
<td>Logs out of the current CLI session.</td>
<td></td>
</tr>
<tr>
<td>ping [ip address][fqdn]</td>
<td>ping – Helpful when checking if a remote machine is reachable or not. Also uses ICMP messages.</td>
<td></td>
</tr>
<tr>
<td>reboot</td>
<td>Reboots the server.</td>
<td></td>
</tr>
<tr>
<td>rescue</td>
<td>Rescue the system and software. Sets DLPback to the factory defaults.</td>
<td></td>
</tr>
<tr>
<td>resolve</td>
<td>Resolves an IP address on the network.</td>
<td></td>
</tr>
<tr>
<td>scp (support same OS format and syntax)</td>
<td>scp – Helpful when you need to transfer files to a remote system via Secure Copy.</td>
<td></td>
</tr>
<tr>
<td>setupEnv.sh</td>
<td>Sets up a proper shell environment.</td>
<td></td>
</tr>
<tr>
<td>show arp [ip address / hostname]</td>
<td>arp – obtains arp table values for troubleshooting.</td>
<td></td>
</tr>
<tr>
<td>show boot message</td>
<td>dmesg - displays the kernel debug messages.</td>
<td></td>
</tr>
<tr>
<td>show capture [file name]</td>
<td>Shows the directory where dump files are stored.</td>
<td></td>
</tr>
<tr>
<td>show connections</td>
<td>Displays network connections.</td>
<td></td>
</tr>
<tr>
<td>CLI Command</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>show conntrack</td>
<td>cat /proc/net/sockstat - displays the used socket information.</td>
<td></td>
</tr>
<tr>
<td>show conntrack expect</td>
<td>cat /proc/net/ ip_conntrack_expect - displays the FW expect connection tables (root access required).</td>
<td></td>
</tr>
<tr>
<td>show database backup</td>
<td>Shows database backup files.</td>
<td></td>
</tr>
<tr>
<td>show date</td>
<td>Shows current date and time.</td>
<td></td>
</tr>
<tr>
<td>show disk partition [optional partition]</td>
<td>df – Displays the disk space usage of the different partitions on the system.</td>
<td></td>
</tr>
<tr>
<td>show disk space [optional directory or file name]</td>
<td>du – Estimates the disk space usage of each file recursively for the directories.</td>
<td></td>
</tr>
<tr>
<td>show file [option] ...</td>
<td>lsof – List all the files open on the system.</td>
<td>Need to get the list of popular options used with this command.</td>
</tr>
<tr>
<td>show firewall filter</td>
<td>uses the iptables –t filter –L -v</td>
<td></td>
</tr>
<tr>
<td>show firewall nat</td>
<td>iptables - displays the firewall rules if any (needs root equivalence).</td>
<td>uses the iptables –t nat-L -v</td>
</tr>
<tr>
<td>show hostname</td>
<td>Displays the hostname.</td>
<td></td>
</tr>
<tr>
<td>show ip [options]</td>
<td>Displays the DNS or IP settings.</td>
<td></td>
</tr>
<tr>
<td><strong>CLI COMMAND</strong></td>
<td><strong>DESCRIPTION</strong></td>
<td><strong>NOTES</strong></td>
</tr>
<tr>
<td>-----------------</td>
<td>-----------------</td>
<td>-----------</td>
</tr>
<tr>
<td>show log backup</td>
<td>Displays log files to be backed up on the local file system. Normally, log files are located at /backup/violationlogs</td>
<td></td>
</tr>
<tr>
<td>show module</td>
<td>lsmod – displays the kernel modules loaded.</td>
<td></td>
</tr>
<tr>
<td>show process [optional name/ID with wildcard support]</td>
<td>ps – Lists the active processes running on the system. Helpful when checking which processes are running and their statuses.</td>
<td></td>
</tr>
<tr>
<td>show process library [active process name/id]</td>
<td>ltrace – Attaches to an active process and prints out the dynamic library calls it is using during its run time.</td>
<td></td>
</tr>
<tr>
<td>show process stack [active process name/id]</td>
<td>pstack – Attaches to an active process and prints out an execution stack trace.</td>
<td>Just use the ID instead of the process name.</td>
</tr>
<tr>
<td>show process top</td>
<td>top – Lists the top processes running on a system at any specific time.</td>
<td></td>
</tr>
<tr>
<td>show process trace [active process name/id]</td>
<td>strace – Attaches to an active process and prints out the system calls it’s using during its run time.</td>
<td></td>
</tr>
<tr>
<td>show resource [process name/id]</td>
<td>plimit – Sets or gets the resource limits of a running process.</td>
<td></td>
</tr>
<tr>
<td>CLI Command</td>
<td>Description</td>
<td>Notes</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------</td>
</tr>
<tr>
<td>show statistic [interval]</td>
<td>vmstat – Reports information about processes, memory paging blocks, I/O traps, and CPU activity.</td>
<td>n – not to resolve IP address to hostnames.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>a – displays all sockets: listening and nonlistening.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>all – displays all Ethernet interfaces.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>default – displays packet information.</td>
</tr>
<tr>
<td>show statistic block_io</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show statistic cpu</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show statistic ethernet [Ethernet interface] [all] [n] [a]</td>
<td>netstat – Shows network statistics of the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>show statistic IO [interval]</td>
<td>iostat – Reports the I/O performance of the system.</td>
<td></td>
</tr>
<tr>
<td>show statistic memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show statistic paging</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show statistic process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show statistic traps</td>
<td></td>
<td></td>
</tr>
<tr>
<td>show system</td>
<td>sysctl – displays the kernel parameters.</td>
<td></td>
</tr>
<tr>
<td>show timezone</td>
<td>Displays the current time zone.</td>
<td></td>
</tr>
<tr>
<td>show uptime</td>
<td>Displays how long the system has been running.</td>
<td></td>
</tr>
</tbody>
</table>
DLP Network Monitor CLI Commands

You can access the DLP Network Monitor CLI through the DLP Network Monitor console (keyboard and monitor connected directly to the DLP Network Monitor) or remotely using an SSH v2 connection to the DLP Network Monitor IP address.

CLI commands enable you to perform additional configuration tasks and to perform debug and troubleshooting functions.

To access the CLI, you will need to have the administrator account and password.

The following commands are available in DLP.

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>show version</td>
<td>Command to list the version of the appliance software – includes both the DLPserver version and the OS version.</td>
<td></td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the server.</td>
<td></td>
</tr>
<tr>
<td>stop process [process id] [core]</td>
<td>kill – Used force-kill a process. Helpful in situations where you want to force-generate a core file from a process.</td>
<td>If stop process is used without options - just kill the process using -9. If stop process is used with options [core] they will generate the core using -6. You must add the file management to allow Trend Micro to transfer the core file out.</td>
</tr>
<tr>
<td>tftp (support same OS format and syntax)</td>
<td>tftp – Helpful when you need to transfer files to a remote system via TFTP.</td>
<td></td>
</tr>
<tr>
<td>traceroute [ip address] [fqdn]</td>
<td>traceroute – tracks where the packet is dropped on the network using ICMP messages.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-2. Command Line Interface Commands

<table>
<thead>
<tr>
<th>CLI Command</th>
<th>Description</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure dglink &lt;DLP management server IP address&gt;</td>
<td>Configures the IP address of the DLP management server.</td>
<td></td>
</tr>
<tr>
<td>configure dns &lt;dns1&gt;[dns2]</td>
<td>Configures the primary and secondary domain name servers.</td>
<td></td>
</tr>
<tr>
<td>configure gateway &lt;gateway&gt;</td>
<td>Configures the gateway for the Network Monitor device.</td>
<td></td>
</tr>
<tr>
<td>configure hostname &lt;hostname&gt;</td>
<td>Configures the Network Monitor hostname.</td>
<td>Type a unique hostname for DLP Network Monitor, since you will register the hostname with the DLP Management Server. The name will display in the DLP web console.</td>
</tr>
<tr>
<td>configure interface ip &lt;ip&gt; &lt;mask&gt;</td>
<td>Configures the interface running IP address.</td>
<td></td>
</tr>
<tr>
<td>configure interface mode &lt;interface&gt;&lt;mode&gt;</td>
<td>Configures the interface running mode.</td>
<td></td>
</tr>
<tr>
<td>configure interface type &lt;type&gt;</td>
<td>Configures interface running type.</td>
<td></td>
</tr>
<tr>
<td>configure max_file_size {max file size in bytes}</td>
<td>Configures the default maximum file size that DLP Network Monitor can scan. The default is 20MB. Example: configure max_file_size 30000000</td>
<td>Access in privileged mode.</td>
</tr>
<tr>
<td>configure password &lt;password&gt;</td>
<td>Configures the account password.</td>
<td></td>
</tr>
</tbody>
</table>
Index

A
accessing the web console, 2-2
activation, 7-44
adding
   company policies, 3-33, 3-34, 3-36, 3-44
   compliance templates, 3-29
   data discovery, 3-52
   file attributes, 3-11
   fingerprints, 3-14
administration, 7-1
agent
   modules, 7-12
alert configuration, 7-10
application settings
   SMTP account settings, 7-5
available updates, 6-5

C
company policies, 3-32
   adding, 3-33, 3-34, 3-36, 3-44
   deleting, 3-33, 3-34, 3-36, 3-44
compliance templates
   adding, 3-29
   deleting, 3-29
configure
   alert, 7-10
   console password, 7-35
   device control, 3-59
   fingerprint settings, 7-2
   server, 7-2
   SMTP account settings, 7-5
   user accounts, 7-36
crawler management, 7-18

d data discovery, 3-51
   adding, 3-52
   scheduling data discovery tasks, 3-57
data management
   import DLP data, 7-29
deleting
   company policies, 3-33, 3-34, 3-36, 3-44
   compliance templates, 3-29
   file attributes, 3-13
   fingerprints, 3-14
device control, 3-59
digital assets, 3-2
DLP activation, 7-44
DLP registration, 7-44

e exported files, 7-30

F
file attributes
   deleting, 3-13
file extensions, 3-12
fingerprints, 3-14
   adding, 3-14
   deleting, 3-14
fingerprint settings, 7-6

I
import data, 7-29

L
licenses
   renewing, 7-45
   viewing, 7-44
license status online, 7-44
logging modules, 7-12
logs, 5-1
  incidents, 5-2
  policy deployment, 5-2
  security audit, 5-2
  server status, 5-2
  system events, 5-2

M
maintenance agreement, 7-43
management
  console, 7-36
  crawler, 7-18
  user accounts, 7-36

P
policy actions, 3-40, 3-48
product registration, 7-44

R
registering products, 7-44
registration, 7-44
reports, 4-1

S
server configuration
  application settings, 7-5
SMTP account settings, 7-5

T
targets, 3-34, 3-36

U
UDP listener, 7-13
UDP logging, 7-14
update, 6-1
updates, 6-5
user accounts, 7-36

V
viewing product licenses, 7-44