TREND MICRO™

10.6 OfficeScan™

SP3 Data Loss Prevention Policy Creation

For Enterprise and Medium Business

Document Part No.: OSEM115885_130313

Release Date: March 2014

Protected by U.S. Patent No.: 5,951,698

This documentation introduces the main features of the product and/or provides installation instructions for a production environment. Read through the documentation before installing or using the product.

Detailed information about how to use specific features within the product may be available at the Trend Micro Online Help Center and/or the Trend Micro Knowledge Base.

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.

Evaluate this documentation on the following site:

http://www.trendmicro.com/download/documentation/rating.asp

Data Loss Prevention Policies

OfficeScan evaluates a file or data against a set of rules defined in DLP policies. Policies determine files or data that requires protection from unauthorized transmission and the action that OfficeScan performs after detecting a transmission.

Note

OfficeScan does not monitor data transmissions between the server and OfficeScan agents.

OfficeScan allows administrators to configure policies for internal and external OfficeScan agents. Administrators typically configure a stricter policy for external agents.

Administrators can enforce specific policies to agent groups or individual agents.

After deploying policies, agents use the location criteria set in the **Computer Location** screen (see the *OfficeScan Administrator's Guide*) to determine the correct location settings and the policy to apply. Agents switch policies each time the location changes.

Policy Configuration

Define DLP policies by configuring the following settings and deploying the settings to selected agents:

TABLE 1. Settings that Define a DLP Policy

SETTINGS	DESCRIPTION
Data Identifiers	Data Loss Prevention uses data identifiers to identify sensitive information. Data identifiers include expressions, file attributes, and keywords which act as the building blocks for DLP templates.
Rules	A DLP rule can consist of multiple templates, channels, and actions. Each rule is a subset of the encompassing DLP policy.

SETTINGS	DESCRIPTION
Templates	A DLP template combines data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement are subject to a DLP rule. Data Loss Prevention comes with a set of predefined templates and allows administrators to create customized templates. A DLP rule can contain one or several templates. Data Loss Prevention uses the first-match rule when checking templates. This means that if a file or data matches the data identifiers in a template, Data Loss Prevention no longer checks the other templates.
Channels	Channels are entities that transmit sensitive information. Data Loss Prevention supports popular transmission channels, such as email, removable storage devices, and instant messaging applications.
Actions	Data Loss Prevention performs one or several actions when it detects an attempt to transmit sensitive information through any of the channels.
Exceptions	Exceptions act as overrides to the configured DLP rules. Configure exceptions to manage non-monitored targets, monitored targets, and compressed file scanning.

Deploying a PCI-DSS Policy to a Domain

Tip

The following task describes the steps involved in creating and deploying a PCI-DSS rule in a Data Loss Prevention policy. To create other rules for different regulations or needs, select the appropriate template(s) and follow all other steps.

Procedure

1. Go to **Networked Computers** > **Client Management**.
2. In the agent tree, click the domain to deploy the PCI-DSS policy to.
3. Click **Settings** > **DLP Settings**.

Important

OfficeScan agents must install the Data Protection module before accepting DLP policies. OfficeScan informs administrators if any OfficeScan agents need to install the Data Protection module. After installing the module, OfficeScan prompts users to restart the OfficeScan agent endpoint to accept DLP policies.

The **Data Loss Prevention Policy Settings** screen appears.

4. Select **Enable Data Loss Prevention**.
5. Select **Apply all settings to external clients**.
6. On the **Rules** tab, click **Add**.
7. In the **Rule name** text box, type a name for the PCI-DSS rule.

   For example, type `PCI-DSS rule`.
8. Locate the PCI-DSS template.
   - In the search text box, type `pci` and click **Search**.
   - In the templates list, scroll down until the **PCI-DSS (Payment Card Industry Data Security)** template appears.
9. Click the template name and click **Add >**.
10. Click the **Channel** tab.
11. Select **Network Channels** to select all network channels.
12. Scroll down and select **System and Application Channels** to select all system and application channels.
13. Accept the default settings on the **Action** tab.
14. Click **Save**.
15. Click **Save and Apply the Setting to Clients**.

    A confirmation message appears.
16. Click **OK**.

The **Data Loss Prevention Policy Settings: Configuration changes have been applied** screen appears.

17. Click **Close**.

Checklist for Deploying a PCI-DSS Policy

STEP	SCREEN	ACTION	COMPLETED?
1, 2, 3	**Networked Computers** > **Client Management**	Select a domain in the agent tree.	
4	**Networked Computers** > **Client Management** then **Settings** > **DLP Settings**	Select **Enable Data Loss Prevention**.	
5		Select **Apply all settings to external clients**.	
6		**Add** a new rule.	
7	**Networked Computers** > **Client Management** then **Settings** > **DLP Settings** > **Add** > **Template**	Name the new rule.	
8, 9		Add the **PCI-DSS (Payment Card Industry Data Security)** template to the selected templates list.	
10, 11	**Networked Computers** > **Client Management** then **Settings** > **DLP Settings** > **Add** > **Channel**	Select **Network Channels**.	
12		Select **System and Application Channels**.	
13, 14		**Save** the rule.	

STEP	SCREEN	ACTION	COMPLETED?
15, 16, 17	**Networked Computers** > **Client Management Settings** > **DLP Settings**	Click **Save and Apply the Setting to Clients**.	

Associated Data Loss Prevention Documentation

For more information on Data Loss Prevention, policies, templates, data identifiers, channels, exceptions, and configurations, refer to the following documents.

Note

Choose the version of the documents that correspond to the version of OfficeScan installed on the server. Different versions of OfficeScan implement the Data Loss Prevention features in different ways.

TABLE 2. Data Loss Prevention Reference Material

MATERIAL	URL	DESCRIPTION
OfficeScan Administrator's Guide	http://docs.trendmicro.com/en-us/enterprise/officescan.aspx	Provides comprehensive information regarding the installation of the Data Protection module, deployment of policies to OfficeScan agents, rule and data identifier customization, channel descriptions, exception handling, and uninstallation

MATERIAL	URL	DESCRIPTION
Data Protection Lists	http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx	Provides descriptions of the prepackaged templates and data identifiers, lists of the supported applications, and supported device models (Device Control) **Note** The lists contained in this documents display the applications and devices that received specific testing by Trend Micro. Applications or devices not found in the lists may also be supported but did not receive specific testing.
Data Protection - Data Security Management	http://www.trendmicro.com/us/enterprise/data-protection/index.html?cm_mmc=VURL:USA-_-ENT-_-Data+Protection-_-Data+Protection	Provides an overview of data security and the Data Protection options available from Trend Micro
Best Practices for Deploying and Using a Data Loss Prevention Solution	http://trendedge.trendmicro.com/pr/tm/te/document/DLP_Best_Practices_110118.pdf	This document provides generic industry best practices on how to deploy and use a DLP solution in an enterprise environment. Where applicable, it presents Trend Micro Data Loss Prevention 5.x as a means to achieve these ends.
Data Discovery and Classification in Five Easy Steps	http://trendedge.trendmicro.com/pr/tm/te/document/DLP_Data_Discovery_and_Classification_in_5_Steps_090630.pdf	This document describes how to perform data discovery and classify data for use by a Data Loss Prevention (DLP) solution.

MATERIAL	URL	DESCRIPTION
Extending the LVM Partition in Trend Micro Data Loss Prevention 5.2 Virtual Appliances	http://trendedge.trendmicro.com/pr/tm/te/document/DLPVA5.2_LVM_Partition_Extension_Guide_100630.pdf	This document describes how to increase the amount of disk space available to Trend Micro Data Loss Prevention Management Server 5.2 by extending the LVM partition.
Working with Data Owners: A Guide for Data Security Professionals	http://trendedge.trendmicro.com/pr/tm/te/document/Working_with_Data_Owners_100121.pdf	This document contains a series of questions that information security professionals can pose to data owners implementing a DLP solution. These questions can help the professional gain an understanding of the data owner's critical data and business needs, and serve as the first step towards developing policies for the DLP solution.

TREND MICRO INCORPORATED

10101 North De Anza Blvd. Cupertino, CA., 95014, USA

Tel:+1(408)257-1500/1-800 228-5651 Fax:+1(408)257-2003 info@trendmicro.com

www.trendmicro.com

Item Code: OSEM106145/130910