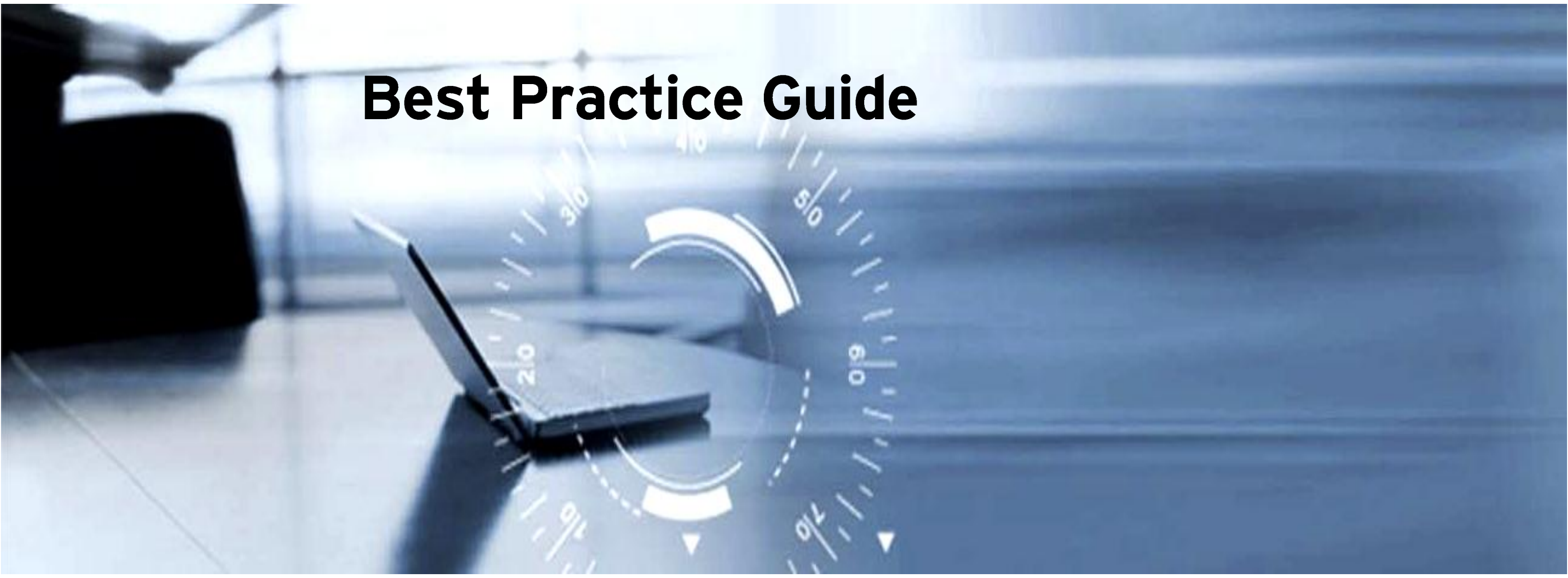
Trend Micro™
OfficeScan iDLP



Best Practice Guide

Anti-Spyware Anti-Spam Antivirus Anti-Phishing Content & URL Filtering

Information in this document is subject to change without notice. The names of companies, products, people, characters, and/or data mentioned herein are fictitious and are in no way intended to represent any real individual, company, product, or event, unless otherwise noted. Complying with all applicable copyright laws is the responsibility of the user.

Author: Julin Shao

Released: March 31, 2016

Table of Contents

Chapter 1: Product Introduction

Integrated Data Loss Prevention (iDLP) in OfficeScan safeguards an organization's sensitive data against accidental or deliberate leakage.

The OfficeScan server can manage the DLP settings to prevent clients from leaking private/confidential data. If some clients violate the DLP rule, an iDLP client detects the action and sends a log to the server.

There are two main features of iDLP:

- Device Control
- Data Loss Prevention

Chapter 2: System Requirements

Since iDLP is a plug-in of OfficeScan, it has the same set of minimum system requirements as the OfficeScan server and agent.

For more information on the minimum system requirements, see the OfficeScan *Installation and Deployment Guide* or the OfficeScan *Readme*.

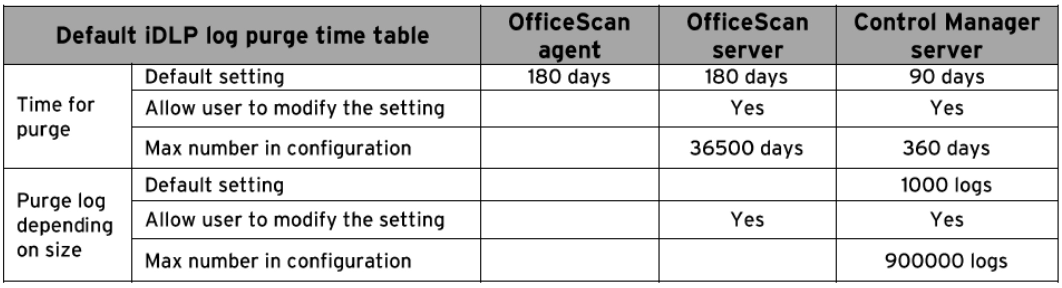
Chapter 3: Deployment

3.1 > Deploying and Testing Agents

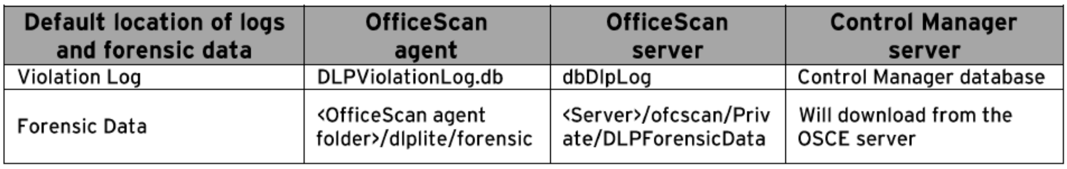
DLP agents should be deployed without any policies enabled. Trend Micro recommends testing policies before deploying to the production environment. Poorly configured and tested policies may lead to the disruption of daily work routines and might end up in computers, flooding the OfficeScan server with a large number of false positives.

3.2 > Calculating Disk Space

To determine the required disk space for the server, you must decide if there is a need to capture the files when a policy violation occurs. The files captured during the violation are called "forensic data". Capturing forensic data allows you to quickly identify why the alert occurred and whether it was a false positive. While the forensic data function is helpful when tuning policies, you can still gather this information by reviewing the alerts. The alerts contain the path to the file that triggered it.



Default iDLP log purge time table		OfficeScan agent	OfficeScan server	Control Manager server
Time for purge	Default setting	180 days	180 days	90 days
	Allow user to modify the setting		Yes	Yes
	Max number in configuration		36500 days	360 days
Purge log depending on size	Default setting			1000 logs
	Allow user to modify the setting		Yes	Yes
	Max number in configuration			900000 logs



Default location of logs and forensic data	OfficeScan agent	OfficeScan server	Control Manager server
Violation Log	DLPViolationLog.db	dbDlpLog	Control Manager database
Forensic Data	<OfficeScan agent folder>/dlplite/forensic	<Server>/ofcscan/Private/DLPForensicData	Will download from the OSCE server

3.3 > Pre-Deployment

DLP Installation and activation are performed from the Plug-in Manager.

> **NOTE** 🗎 You do not need to install the Data Protection module if the standalone Trend Micro Data Loss Prevention software is already installed and running on endpoints.

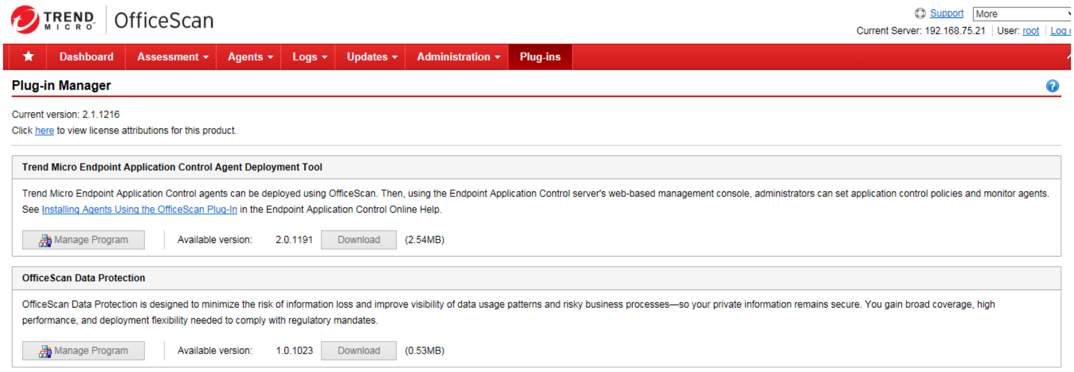
The Data Protection module can be installed on a pure IPv6 Plug-in Manager. However, only the Device Control feature can be deployed to pure IPv6 agents.

Data Loss Prevention does not work on pure IPv6 agents.

1. Download the DLP package.
   a. Go to **Plug-ins** > **OfficeScan Data Protection**.
   b. Click **Download**.

The size of the file to be downloaded displays beside the **Download** button.

Plug-in Manager stores the downloaded file to `<Server installation folder>\PCCSRV\Download\Product`.



Plug-in Manager

Current version: 2.1.1216
Click here to view license attributions for this product.

Trend Micro Endpoint Application Control Agent Deployment Tool

Trend Micro Endpoint Application Control agents can be deployed using OfficeScan. Then, using the Endpoint Application Control server's web-based management console, administrators can set application control policies and monitor agents. See Installing Agents Using the OfficeScan Plug-In in the Endpoint Application Control Online Help.

Manage Program | Available version: 2.0.1191 Download (2.54MB)

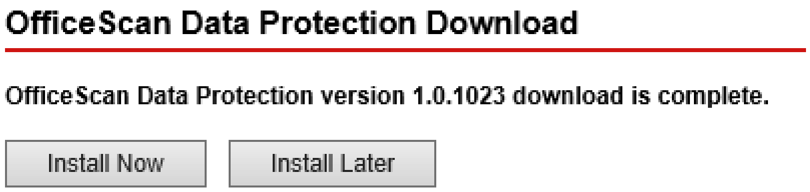
OfficeScan Data Protection

OfficeScan Data Protection is designed to minimize the risk of information loss and improve visibility of data usage patterns and risky business processes—so your private information remains secure. You gain broad coverage, high performance, and deployment flexibility needed to comply with regulatory mandates.

Manage Program | Available version: 1.0.1023 Download (0.53MB)

> **NOTE** 🗎 If Plug-in Manager is unable to download the file, it automatically re-downloads after 24 hours. To manually trigger Plug-in Manager to download the file, restart the OfficeScan Plug-in Manager service from the Microsoft Management Console.

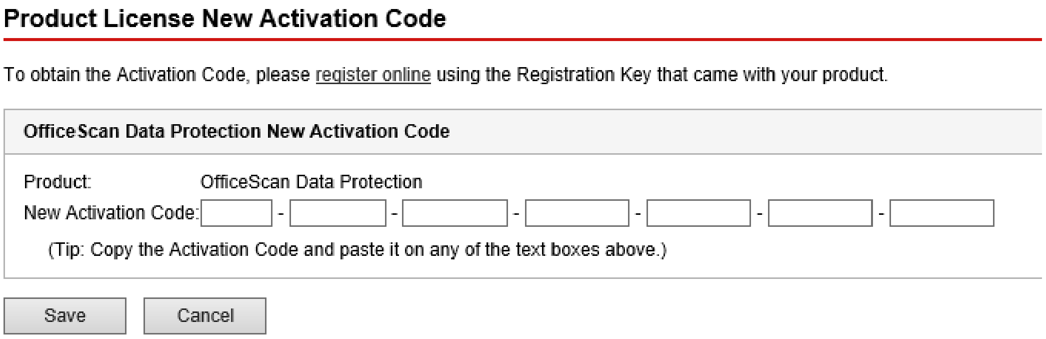
2. To install OfficeScan Data Protection immediately, click **Install Now**. To install at a later time:
   a. Click **Install Later**.
   b. Open the Plug-in Manager screen.
   c. Go to the OfficeScan Data Protection section and then click **Install**.


OfficeScan Data Protection Download

OfficeScan Data Protection version 1.0.1023 download is complete.

3. Read the license agreement and accept the terms by clicking **Agree**. The installation starts.

4. Monitor the installation progress. After the installation, the OfficeScan Data Protection version displays.



Product License New Activation Code

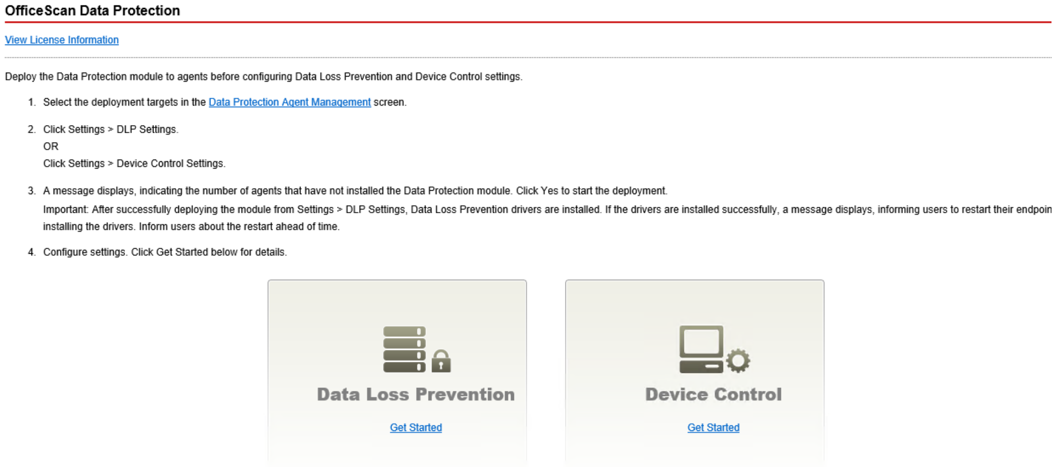
To obtain the Activation Code, please register online using the Registration Key that came with your product.

OfficeScan Data Protection New Activation Code

Product: OfficeScan Data Protection

New Activation Code: □ - □ - □ - □ - □ - □ - □

(Tip: Copy the Activation Code and paste it on any of the text boxes above.)



OfficeScan Data Protection

View License Information

Deploy the Data Protection module to agents before configuring Data Loss Prevention and Device Control settings.

1. Select the deployment targets in the Data Protection Agent Management screen.
2. Click Settings > DLP Settings.
   OR
   Click Settings > Device Control Settings.
3. A message displays, indicating the number of agents that have not installed the Data Protection module. Click Yes to start the deployment.
   Important: After successfully deploying the module from Settings > DLP Settings, Data Loss Prevention drivers are installed. If the drivers are installed successfully, a message displays, informing users to restart their endpoin
   installing the drivers. Inform users about the restart ahead of time.
4. Configure settings. Click Get Started below for details.

5. Deploy the Data Protection module to OfficeScan Agents.

NOTES 🗎

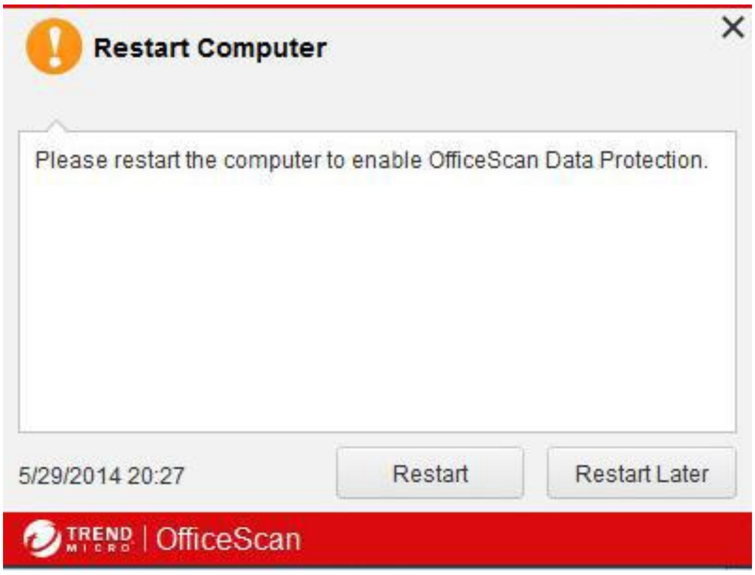
- By default, the module is disabled on Windows Server 2003, Windows Server 2008, and Windows Server 2012 to avoid impacting the performance of the host machine.
- Data Protection now supports an x64 environment.
- Online agents install the Data Protection module immediately. Offline and roaming agents install the module when connection is restored.
- User must restart their computers to finish installing Data Loss Prevention drivers. Inform users about the restart ahead of time.

   a. Go to **Agents** > **Agent Management** > **<domain or agent>**.

   b. Deploy the module using one of the following methods:

      - Go to **Settings** > **DLP Settings**.
      - Go to **Settings** > **Device Control Settings**.

NOTE 🗎 If you use this method and the Data Protection module is deployed successfully, Data Loss Prevention drivers will be installed. If the drivers are installed successfully, a message displays informing users to restart their endpoints and finish installing the drivers.



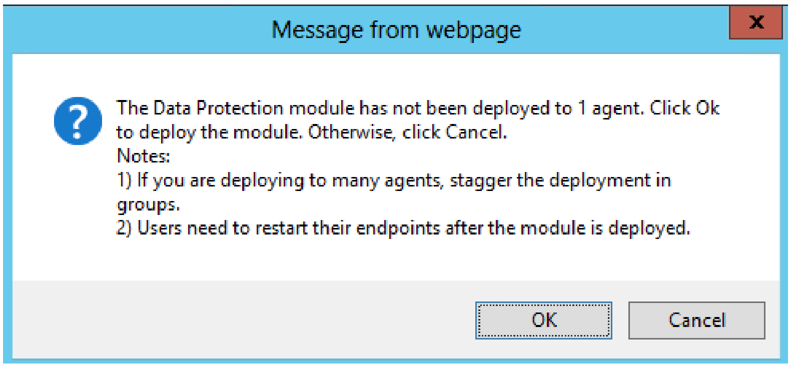
Restart Computer

Please restart the computer to enable OfficeScan Data Protection.

5/29/2014 20:27

c. A message displays, indicating the number of agents that were unable to install the module. Click **Yes** to start the deployment.

OfficeScan agents start to download the module from the server.

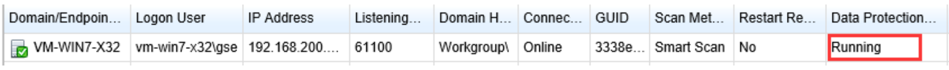


Message from webpage

The Data Protection module has not been deployed to 1 agent. Click Ok to deploy the module. Otherwise, click Cancel.
Notes:
1) If you are deploying to many agents, stagger the deployment in groups.
2) Users need to restart their endpoints after the module is deployed.

6. Check if the module was deployed to agents using any of the following methods:

a. On the agent tree, select a domain or agent and then verify that the Data Protection Status is *Running*.



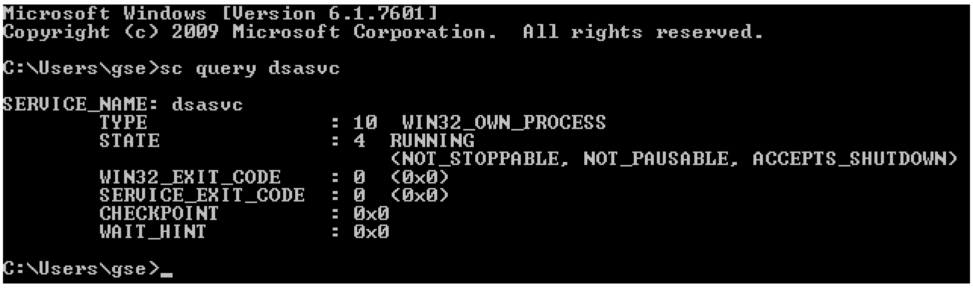
Domain/Endpoin...	Logon User	IP Address	Listening...	Domain H...	Connec...	GUID	Scan Met...	Restart Re...	Data Protection...
VM-WIN7-X32	vm-win7-x32\gse	192.168.200....	61100	Workgroup\	Online	3338e...	Smart Scan	No	Running

The deployment status can be any of the following:

- Running – The module was deployed successfully and its features have been enabled.
- Requires restart – Data Loss Prevention drivers have not been installed because users have not restarted their computers. If the drivers are not installed, Data Loss Prevention will not be functional.
- Stopped – The service for the module has not been started or the target endpoint has been shut down normally. To start the Data Protection service, go to **Agents** > **Agent Management** > **Settings** > **Additional Service Settings** and then enable Data Protection Services.
- Cannot install – There was a problem deploying the module to the agent. You will need to re-deploy the module from the agent tree.

- Cannot install (Data Loss Prevention already exists) – The Trend Micro Data Loss Prevention software already exists on the endpoint. OfficeScan will not replace it with the Data Protection module.
- Not installed – The module has not been deployed to the agent. This status displays if you chose not to deploy the module to the agent or if the agent's status is offline or roaming during deployment.

b. On the OSCE client, open the command prompt using administrator privilege and run the following command: `sc query dsasvc`. The state should be *Running*.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\gse>sc query dsasvc

SERVICE_NAME: dsasvc
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 4  RUNNING
                                (NOT_STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0

C:\Users\gse>_
```

3.4 > Deploying the iDLP template and policy

Before monitoring sensitive information for potential loss, it would be better to answer the following questions:

- What data needs to be protected from a leak?
- Where does the sensitive data reside?
- How is the sensitive data transmitted?
- Which users are authorized to access or transmit the sensitive data?
- What action should be taken if a security violation occurs?

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

Data Identifier Types

Digital assets are files and data that an organization must protect against unauthorized transmission. Administrators can define digital assets using the following data identifiers:

- File Attributes – File attributes are specific properties of a file. You can use two file attributes when defining data identifiers, namely, file type and file size. For File Type, you can use true file type recognition or define an extension. For File Size, it must be more than 0 bytes but not more than 2GB.
- Keywords – Data Loss Prevention comes with a set of predefined keyword lists. These keyword lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.
- 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.

Predefined Keyword Lists, Expressions Lists and File Attribute Lists

DLP comes with a set of predefined keyword lists, expressions lists, and file attribute lists for different target users including banks, educational institutions, healthcare or enterprises. These data identifier lists cannot be modified or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation. Customers can deploy a policy according to their specific requirements.

For more information on the data identifier lists, see the *Data Protection Lists* document at http://docs.trendmicro.com/en-us/enterprise/data-protection-reference-documents.aspx.

Predefined DLP Templates

DLP comes with the following set of predefined templates that you can use to comply with various regulatory standards. These data identifier lists cannot be modified or deleted.

- GLBA **–** Gramm-Leach-Billey Act
- HIPAA – Health Insurance Portability and Accountability Act
- PCI-DSS – Payment Card Industry Data Security Standard
- SB-1386 – US Senate Bill 1386
- US PII – United States Personally Identifiable Information

Customized Keyword Lists, Expressions Lists, File Attribute Lists, and Templates

We can create customized keyword lists, expressions lists, file attribute lists and create templates if none of the predefined lists meets your requirement.

Example:

```
A word file   which     contains   Trend Micro

File Attribute            And       Keyword
```

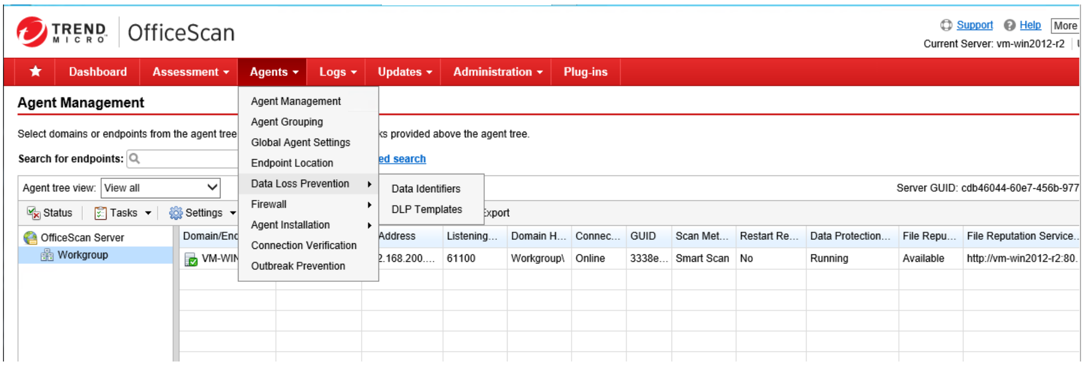
```
A text which looks like xxxx-xxxx-xxxx-xxxx, where x is any number between 0 and 9
Regular expression: [^\d-](\d{4}-\d{4}-\d{4}-\d{4})[^\d-]
```

The following section describes the steps on how to create a policy.

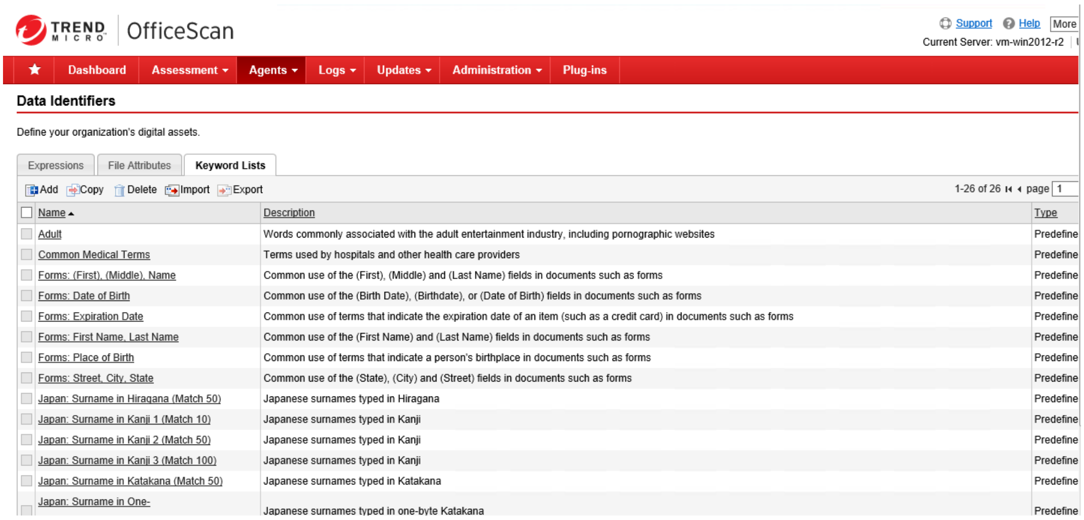
3.4.1 Defining an iDLP Identifier

Creating a Keyword List

1. On the OfficeScan management console, go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.



2. Go to Keyword Lists and then click **Add** to create a keyword data identifier.



Data Identifiers

Define your organization's digital assets.

□	Name ▲	Description	Type
□	Adult	Words commonly associated with the adult entertainment industry, including pornographic websites	Predefine
□	Common Medical Terms	Terms used by hospitals and other health care providers	Predefine
□	Forms: (First), (Middle), Name	Common use of the (First), (Middle) and (Last Name) fields in documents such as forms	Predefine
□	Forms: Date of Birth	Common use of the (Birth Date), (Birthdate), or (Date of Birth) fields in documents such as forms	Predefine
□	Forms: Expiration Date	Common use of terms that indicate the expiration date of an item (such as a credit card) in documents such as forms	Predefine
□	Forms: First Name, Last Name	Common use of the (First Name) and (Last Name) fields in documents such as forms	Predefine
□	Forms: Place of Birth	Common use of terms that indicate a person's birthplace in documents such as forms	Predefine
□	Forms: Street, City, State	Common use of the (State), (City) and (Street) fields in documents such as forms	Predefine
□	Japan: Surname in Hiragana (Match 50)	Japanese surnames typed in Hiragana	Predefine
□	Japan: Surname in Kanji 1 (Match 10)	Japanese surnames typed in Kanji	Predefine
□	Japan: Surname in Kanji 2 (Match 50)	Japanese surnames typed in Kanji	Predefine
□	Japan: Surname in Kanji 3 (Match 100)	Japanese surnames typed in Kanji	Predefine
□	Japan: Surname in Katakana (Match 50)	Japanese surnames typed in Katakana	Predefine
□	Japan: Surname in One-	Japanese surnames typed in one-byte Katakana	Predefine

3. To create a new keyword list, perform the following tasks.

   a. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.

   b. Click the Keyword tab.

   c. Click **Add**.

   A new screen displays.

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

   > < * ^ | & ? \ /

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

   f. 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

   g. To manually add keywords to the list:

i. Type a keyword that is 3 to 40 bytes in length and specify whether it is case-sensitive.

ii. Click **Add**.

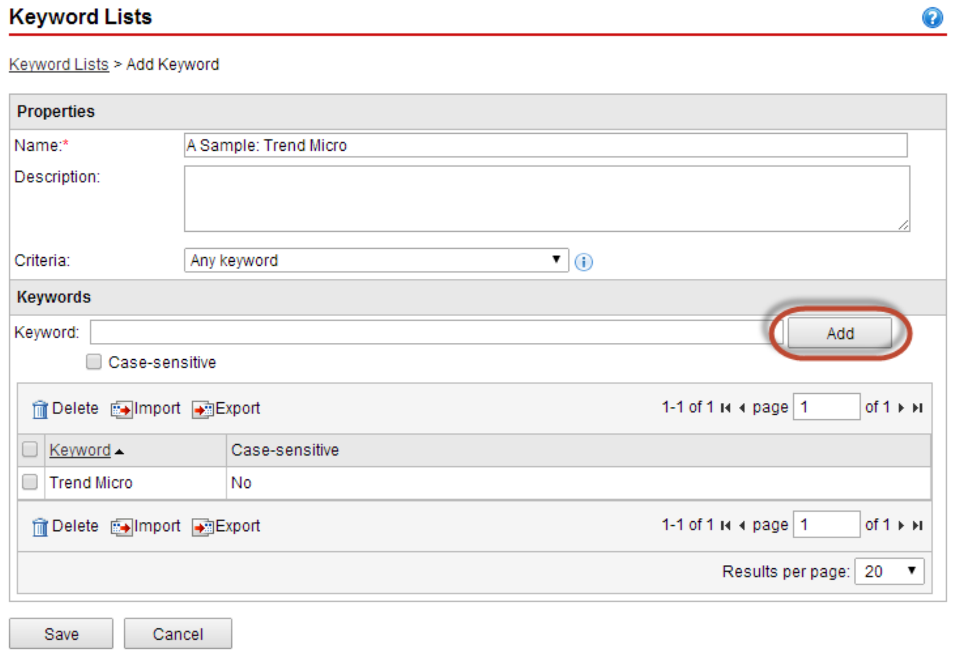
h. To add keywords by using the "import" option:

i. Click **Import** and then locate the .csv file containing the keywords.

ii. Click **Open**.

A message appears, informing you if the import was successful. If a keyword to be imported already exists in the list, it will be skipped.

i. Click **Save**.



Keyword Lists

Keyword Lists > Add Keyword

Properties

Name:* A Sample: Trend Micro

Description:

Criteria: Any keyword ▾

Keywords

Keyword: [Add]

□ Case-sensitive

Delete Import Export 1-1 of 1 ⏮ ◀ page 1 of 1 ▶ ⏭

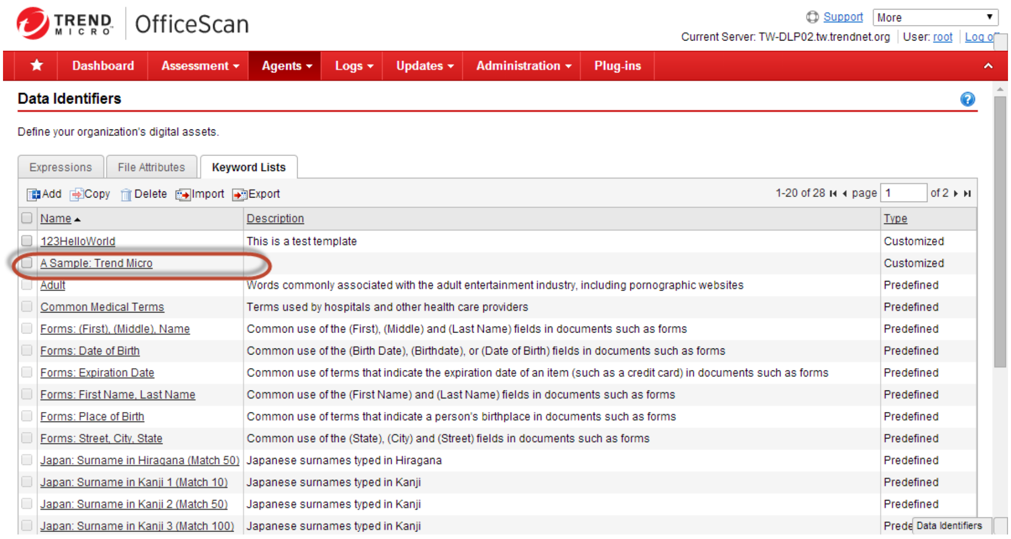
□	Keyword ▲	Case-sensitive
□	Trend Micro	No

Delete Import Export 1-1 of 1 ⏮ ◀ page 1 of 1 ▶ ⏭

Results per page: 20 ▾

[Save] [Cancel]

Keyword Lists



Current Server: TW-DLP02.tw.trendnet.org | User: root | Log o

Data Identifiers

Define your organization's digital assets.

Expressions | File Attributes | Keyword Lists

Add Copy Delete Import Export 1-20 of 28 ⏮ ◀ page 1 of 2 ▶ ⏭

□	Name ▲	Description	Type
□	123HelloWorld	This is a test template	Customized
□	A Sample: Trend Micro		Customized
□	Adult	Words commonly associated with the adult entertainment industry, including pornographic websites	Predefined
□	Common Medical Terms	Terms used by hospitals and other health care providers	Predefined
□	Forms: (First), (Middle), Name	Common use of the (First), (Middle) and (Last Name) fields in documents such as forms	Predefined
□	Forms: Date of Birth	Common use of the (Birth Date), (Birthdate), or (Date of Birth) fields in documents such as forms	Predefined
□	Forms: Expiration Date	Common use of terms that indicate the expiration date of an item (such as a credit card) in documents such as forms	Predefined
□	Forms: First Name, Last Name	Common use of the (First Name) and (Last Name) fields in documents such as forms	Predefined
□	Forms: Place of Birth	Common use of terms that indicate a person's birthplace in documents such as forms	Predefined
□	Forms: Street, City, State	Common use of the (State), (City) and (Street) fields in documents such as forms	Predefined
□	Japan: Surname in Hiragana (Match 50)	Japanese surnames typed in Hiragana	Predefined
□	Japan: Surname in Kanji 1 (Match 10)	Japanese surnames typed in Kanji	Predefined
□	Japan: Surname in Kanji 2 (Match 50)	Japanese surnames typed in Kanji	Predefined
□	Japan: Surname in Kanji 3 (Match 100)	Japanese surnames typed in Kanji	Prede

Data Identifiers

Creating a Customized Expression

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.

2. Click the Expression tab.

3. Click **Add**.

   A new screen displays.

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

   > < * ^ | & ? \ /

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

6. Type an expression.

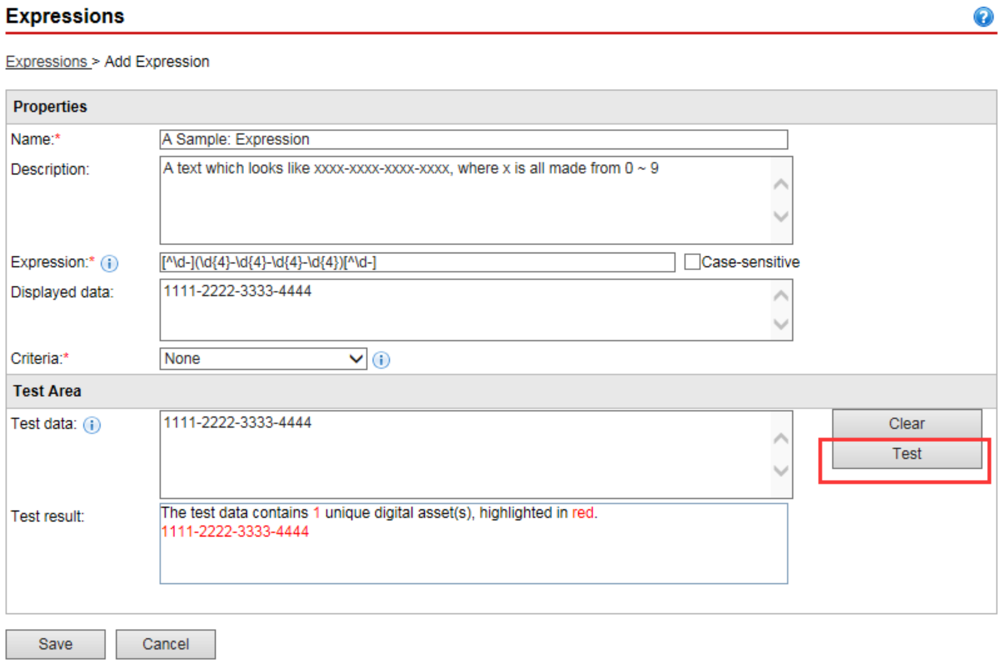
7. Type the displayed data.

8. Choose one of the following criteria and configure additional settings for the chosen criteria.

   For more information, see *Criteria for Customized Expressions* in the OfficeScan Administrator's Guide.

9. Test the expression against an actual data.

10. Click **Save** if you are satisfied with the result.



Expressions

Expressions > Add Expression

Properties

Name:* A Sample: Expression

Description: A text which looks like xxxx-xxxx-xxxx-xxxx, where x is all made from 0 ~ 9

Expression:* [^\d-](\d{4}-\d{4}-\d{4}-\d{4})[^\d-] □ Case-sensitive

Displayed data: 1111-2222-3333-4444

Criteria:* None

Test Area

Test data: 1111-2222-3333-4444

Test result: The test data contains 1 unique digital asset(s), highlighted in red.
1111-2222-3333-4444

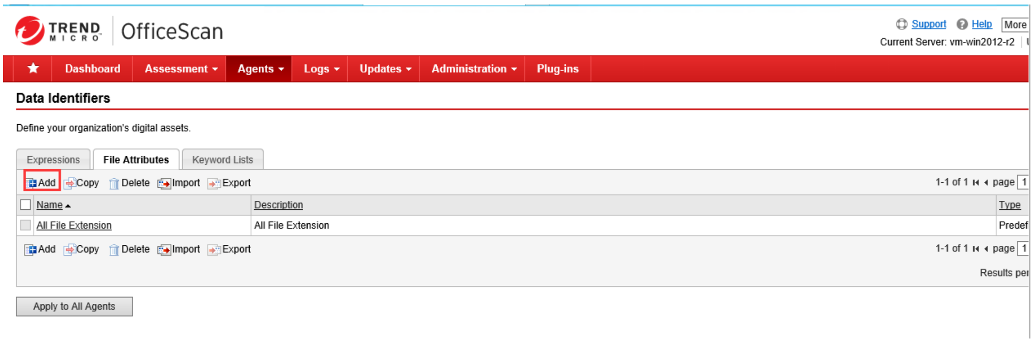
Creating a File Attribute List

1. Go to **Agents** > **Data Loss Prevention** > **Data Identifiers**.

2. Click the File Attribute tab.

3. Click **Add**.

A new screen displays.



Data Identifiers

Define your organization's digital assets.

Name	Description	Type
All File Extension	All File Extension	Predef

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

   > < * ^ | & ? \ /

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

6. Select your preferred true file types.

7. If a file type you want to include is not listed, select File extensions and then type the file type's extension.

   Data Loss Prevention checks files with the specified extension but does not check their true file types. Follow the guidelines below 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.sdcm
     - *.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.

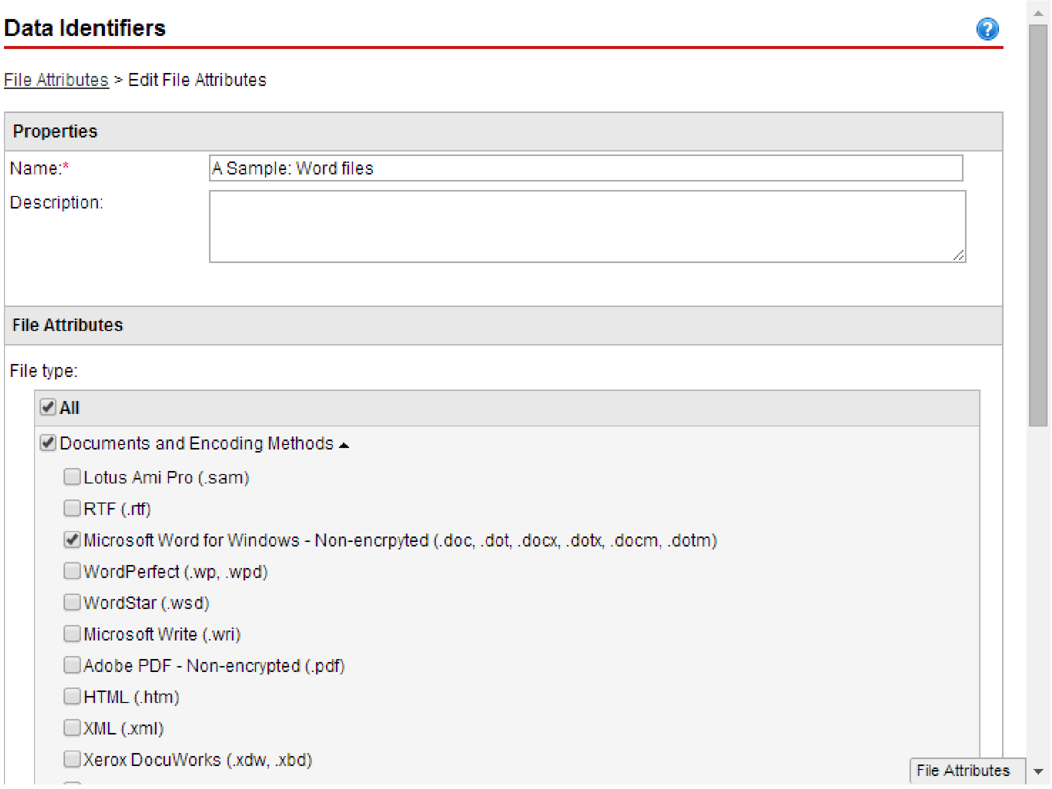
8. Type the minimum and maximum file sizes in bytes. Both file sizes must be whole numbers larger than zero.

9. Click **Save**.

   A message appears, reminding you to deploy the settings to agents.

10. Click **Close**.

11. Back in the DLP Data Identifiers screen, click **Apply to All Agents**.



Data Identifiers

File Attributes > Edit File Attributes

Properties

Name:* A Sample: Word files

Description:

File Attributes

File type:

☑ All

☑ Documents and Encoding Methods ▲

☐ Lotus Ami Pro (.sam)

☐ RTF (.rtf)

☑ Microsoft Word for Windows - Non-encrpyted (.doc, .dot, .docx, .dotx, .docm, .dotm)

☐ WordPerfect (.wp, .wpd)

☐ WordStar (.wsd)

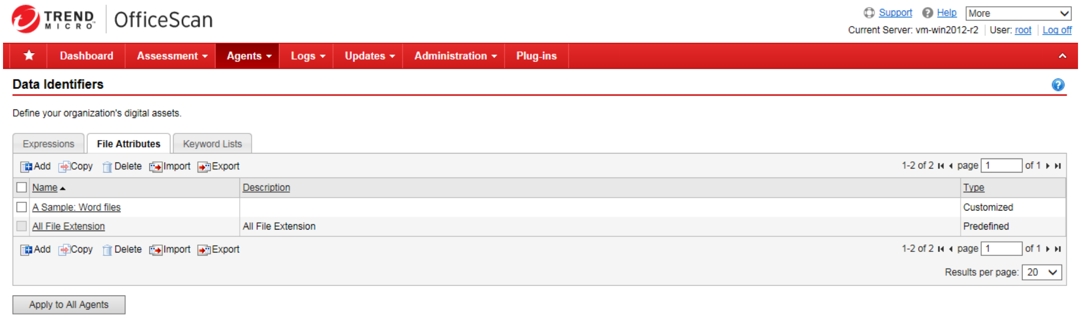
☐ Microsoft Write (.wri)

☐ Adobe PDF - Non-encrypted (.pdf)

☐ HTML (.htm)

☐ XML (.xml)

☐ Xerox DocuWorks (.xdw, .xbd)



Data Identifiers

Define your organization's digital assets.

☐	Name ▲	Description	Type
☐	A Sample: Word files		Customized
☐	All File Extension	All File Extension	Predefined

3.4.2 Defining a DLP Template

You must first configure data identifiers before defining the templates. Templates are defined based on data identifiers.

Procedure

1. Add a template using one of the following methods:

- From the Data Loss Prevention Policy Settings screen:

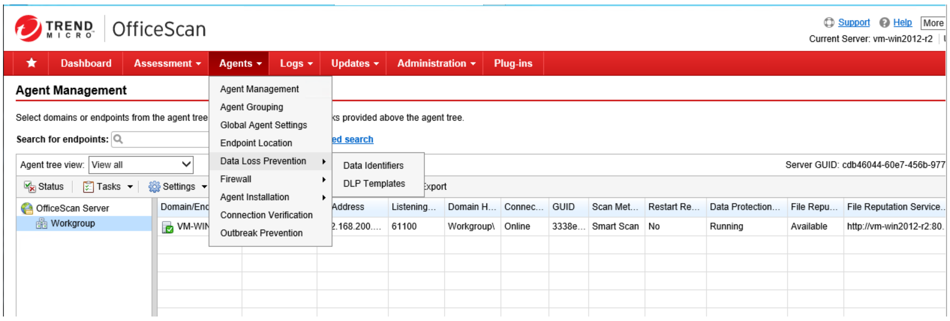
    a. Go to **Agents** > **Agent Management** > **<domain or agent>** > **Settings** > **DLP Settings**.

    b. Go to the External Agents or Internal Agents tab.

    c. On the Rules tab, click **Add**.

    d. Under Template, click **Add new template**.

- From the Data Loss Prevention Templates screen:



Current Server: vm-win2012-r2

Agent Management

Select domains or endpoints from the agent tree ks provided above the agent tree.

Search for endpoints: ed search

Agent tree view: View all

Server GUID: cdb46044-60e7-456b-977

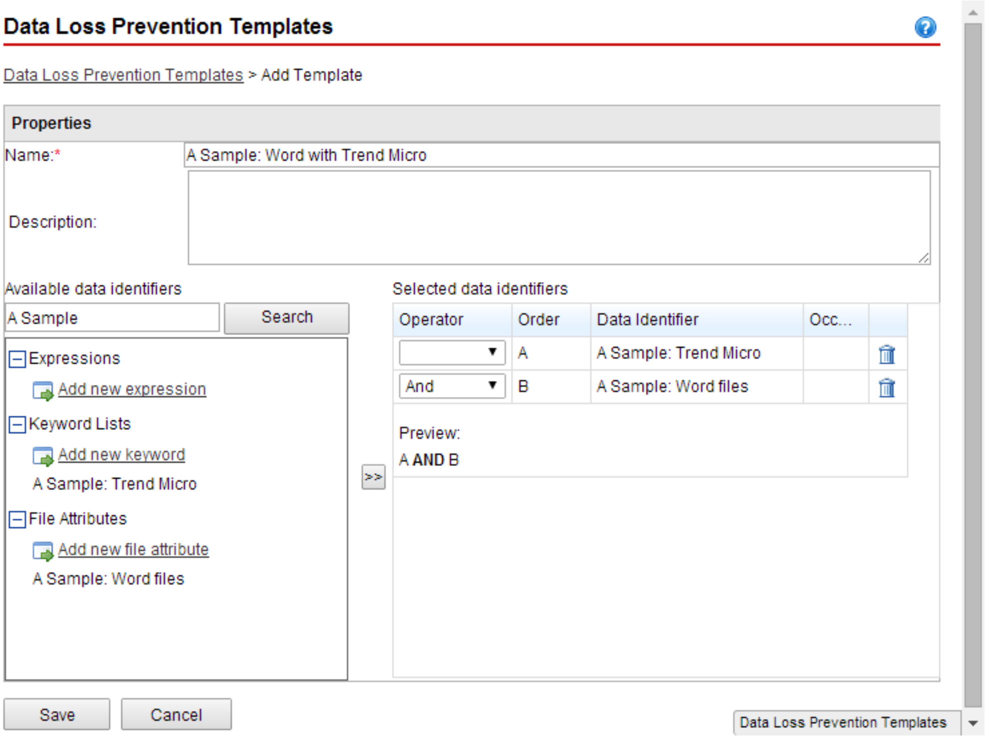
Domain/End	Address	Listening...	Domain H...	Connec...	GUID	Scan Met...	Restart Re...	Data Protection...	File Repu...	File Reputation Service...
VM-WIN	2.168.200....	61100	Workgroup\	Online	3338e...	Smart Scan	No	Running	Available	http://vm-win2012-r2:80.

   a. Go to **Agents** > **Data Loss Prevention** > **DLP Templates**.

   b. Click **Add**.

2. On the Add Template screen, provide the following information.

   - Name
   - Description
   - Data Identifiers



Data Loss Prevention Templates

Data Loss Prevention Templates > Add Template

Properties

Name:* A Sample: Word with Trend Micro

Description:

Available data identifiers

A Sample

Expressions

Keyword Lists

A Sample: Trend Micro

File Attributes

A Sample: Word files

Selected data identifiers

Operator	Order	Data Identifier	Occ...
	A	A Sample: Trend Micro	
And	B	A Sample: Word files	

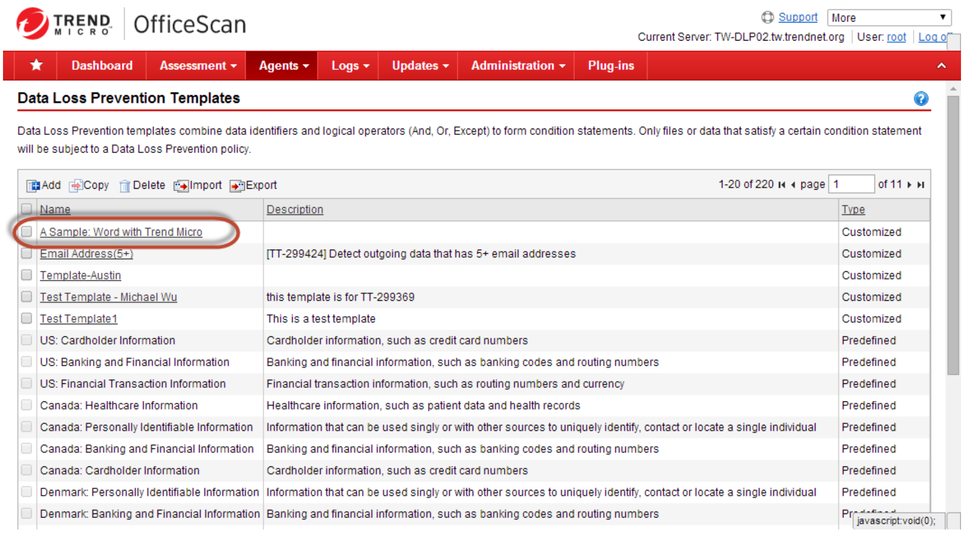
Preview:

A **AND** B

NOTE 🗎 For more information on condition statements, see "Condition Statements and Logical Operators" in the OfficeScan Help document. You can also check the preview displayed on the web console.

3. Click **Save**.

   A customized template has been created.


TREND MICRO | OfficeScan
Support
More
Current Server: TW-DLP02.tw.trendnet.org | User: root | Log off
★ Dashboard | Assessment ▾ | Agents ▾ | Logs ▾ | Updates ▾ | Administration ▾ | Plug-ins
Add | Copy | Delete | Import | Export
1-20 of 220 ⏮ ◀ page 1 of 11 ▶ ⏭
javascript:void(0);

Data Loss Prevention Templates

Data Loss Prevention templates combine data identifiers and logical operators (And, Or, Except) to form condition statements. Only files or data that satisfy a certain condition statement will be subject to a Data Loss Prevention policy.

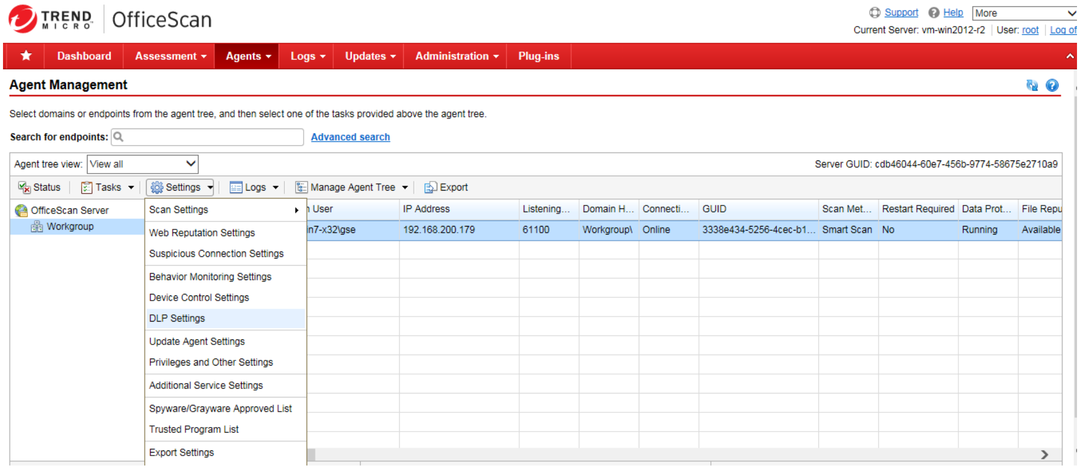
□	Name	Description	Type
□	A Sample: Word with Trend Micro		Customized
□	Email Address(5+)	[TT-299424] Detect outgoing data that has 5+ email addresses	Customized
□	Template-Austin		Customized
□	Test Template - Michael Wu	this template is for TT-299369	Customized
□	Test Template1	This is a test template	Customized
□	US: Cardholder Information	Cardholder information, such as credit card numbers	Predefined
□	US: Banking and Financial Information	Banking and financial information, such as banking codes and routing numbers	Predefined
□	US: Financial Transaction Information	Financial transaction information, such as routing numbers and currency	Predefined
□	Canada: Healthcare Information	Healthcare information, such as patient data and health records	Predefined
□	Canada: Personally Identifiable Information	Information that can be used singly or with other sources to uniquely identify, contact or locate a single individual	Predefined
□	Canada: Banking and Financial Information	Banking and financial information, such as banking codes and routing numbers	Predefined
□	Canada: Cardholder Information	Cardholder information, such as credit card numbers	Predefined
□	Denmark: Personally Identifiable Information	Information that can be used singly or with other sources to uniquely identify, contact or locate a single individual	Predefined
□	Denmark: Banking and Financial Information	Banking and financial information, such as banking codes and routing numbers	Pr[illegible]

> **NOTE** 🗎 OfficeScan supports importing and exporting templates. For more information, see the *OfficeScan Administrator's Guide.*

3.4.3 Defining and Deploying an iDLP Policy

A DLP policy is composed of three parts:

- Template – combines data identifiers and logical operators (And, Or, Except) to form condition statements.
- Channel – an entity that transmits sensitive information.
- Action – action taken when DLP detects an attempt to transmit sensitive information through any of the channels.


TREND MICRO | OfficeScan
Support | Help | More
Current Server: vm-win2012-r2 | User: root | Log of
★ Dashboard | Assessment ▾ | Agents ▾ | Logs ▾ | Updates ▾ | Administration ▾ | Plug-ins
Status | Tasks ▾ | Settings ▾ | Logs ▾ | Manage Agent Tree ▾ | Export
OfficeScan Server
Workgroup
Scan Settings ▸
Web Reputation Settings
Suspicious Connection Settings
Behavior Monitoring Settings
Device Control Settings
DLP Settings
Update Agent Settings
Privileges and Other Settings
Additional Service Settings
Spyware/Grayware Approved List
Trusted Program List
Export Settings

Agent Management

Select domains or endpoints from the agent tree, and then select one of the tasks provided above the agent tree.

Search for endpoints: Advanced search

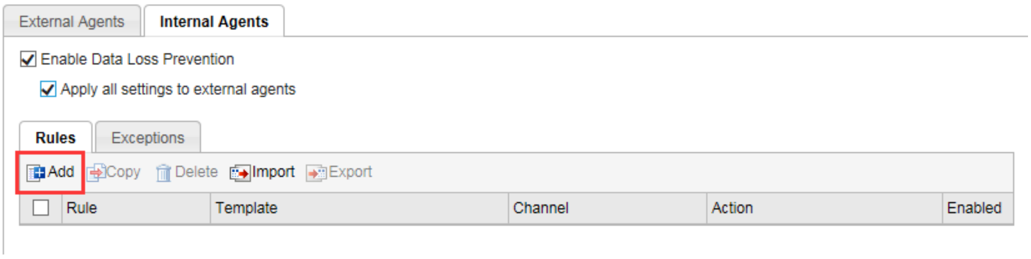
Agent tree view: View all

Server GUID: cdb46044-60e7-456b-9774-58675e2710a9

User	IP Address	Listening...	Domain H...	Connecti...	GUID	Scan Met...	Restart Required	Data Prot...	File Repu
n7-x32\gse	192.168.200.179	61100	Workgroup\	Online	3338e434-5256-4cec-b1...	Smart Scan	No	Running	Available

Defining an iDLP Policy

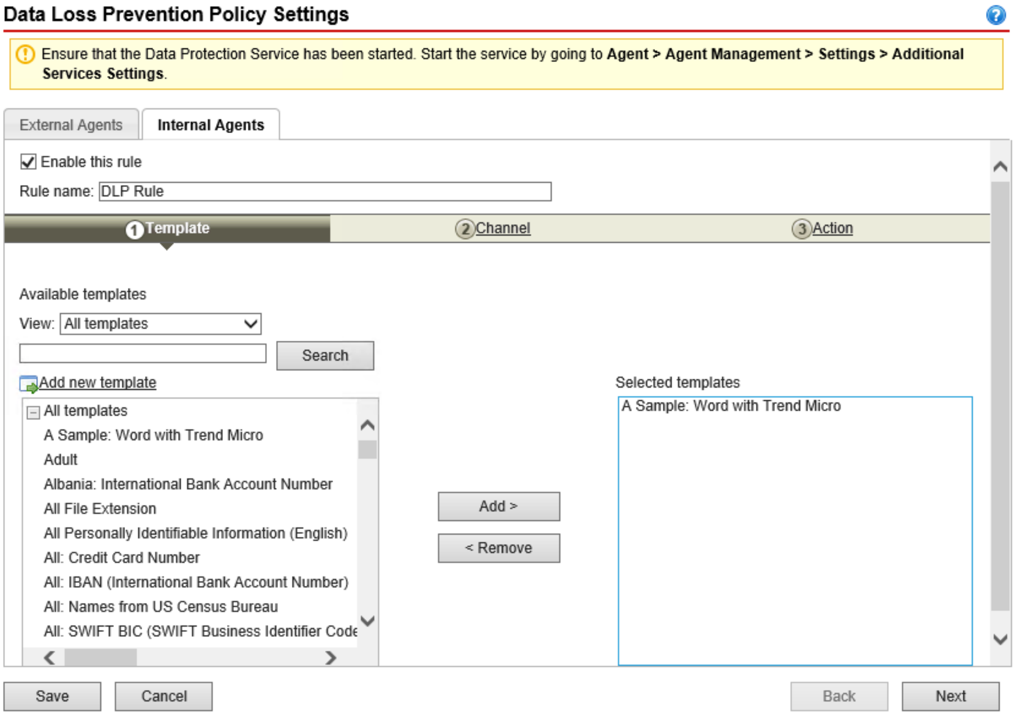
1. Go to **Agents** > **Agent Management** > **<domain or agent>** > **Settings** > **DLP Settings**.
2. Go to the External Agents or Internal Agents tab.
3. On the Rules tab, click **Add**.



☑ Enable Data Loss Prevention

☑ Apply all settings to external agents

4. Type a rule name.
5. From the templates list, select the template and then click **Add >**.



Data Loss Prevention Policy Settings

Ensure that the Data Protection Service has been started. Start the service by going to **Agent > Agent Management > Settings > Additional Services Settings**.

☑ Enable this rule

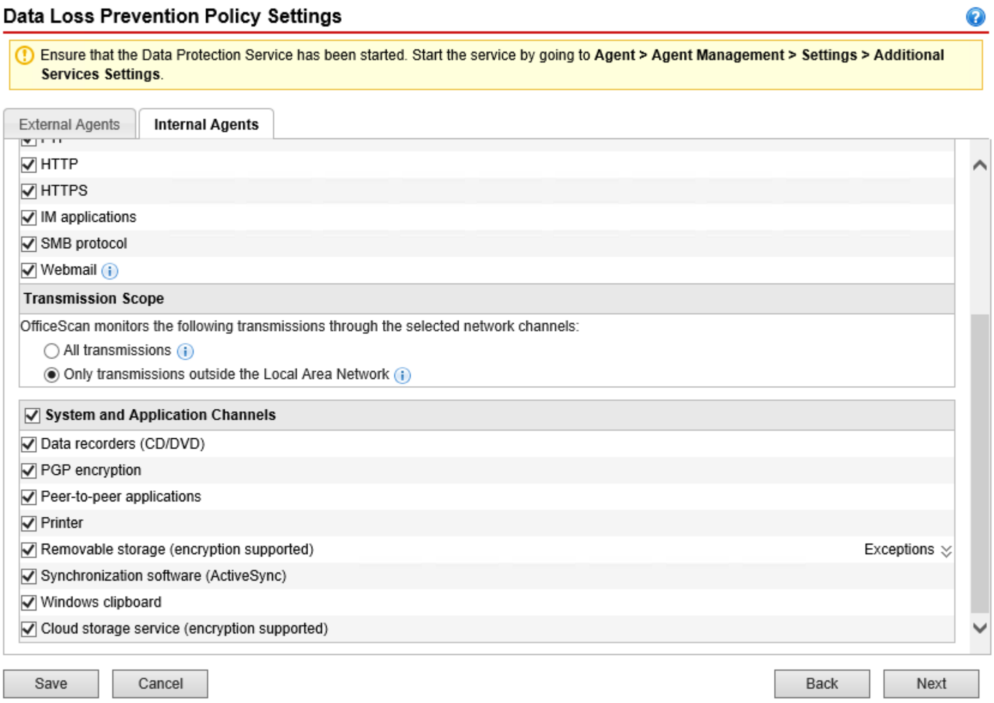
Rule name: DLP Rule

View: All templates

Selected templates: A Sample: Word with Trend Micro

External Agents
Internal Agents
1 Template
2 Channel
3 Action
Available templates
Search
Add new template
All templates
A Sample: Word with Trend Micro
Adult
Albania: International Bank Account Number
All File Extension
All Personally Identifiable Information (English)
All: Credit Card Number
All: IBAN (International Bank Account Number)
All: Names from US Census Bureau
All: SWIFT BIC (SWIFT Business Identifier Code
Add >
< Remove
Save
Cancel
Back
Next

6. Click **Next** or **(2) Channel**.
7. Select one or more channels.



Data Loss Prevention Policy Settings

Ensure that the Data Protection Service has been started. Start the service by going to **Agent > Agent Management > Settings > Additional Services Settings**.

☑ HTTP
☑ HTTPS
☑ IM applications
☑ SMB protocol
☑ Webmail

Transmission Scope

OfficeScan monitors the following transmissions through the selected network channels:

○ All transmissions
● Only transmissions outside the Local Area Network

☑ **System and Application Channels**

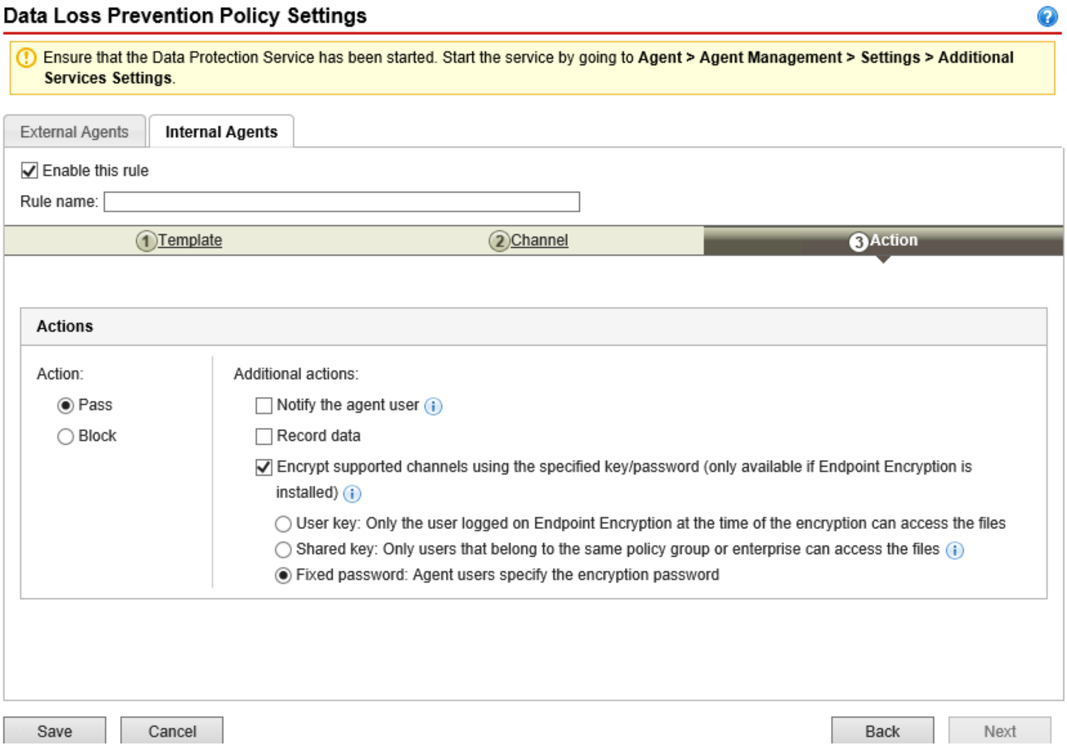
☑ Data recorders (CD/DVD)
☑ PGP encryption
☑ Peer-to-peer applications
☑ Printer
☑ Removable storage (encryption supported) Exceptions
☑ Synchronization software (ActiveSync)
☑ Windows clipboard
☑ Cloud storage service (encryption supported)

NOTES

- "Email clients" and "Removable storage" support the use of exceptions.
- Under Transmission Scope, you can choose to monitor data transmission outside the endpoint or outside the local access network (LAN).
- Under System and Application Channels, "Removable storage" and "Cloud storage service" support encryption.

8. Click **Next** or **(3) Action**.
9. Select **Pass** or **Block** and then specify the additional actions.

   For more information, see *Additional Actions* below.



Data Loss Prevention Policy Settings

Ensure that the Data Protection Service has been started. Start the service by going to **Agent > Agent Management > Settings > Additional Services Settings**.

☑ Enable this rule

Rule name:

Actions

Action:

● Pass

○ Block

Additional actions:

□ Notify the agent user

□ Record data

☑ Encrypt supported channels using the specified key/password (only available if Endpoint Encryption is installed)

○ User key: Only the user logged on Endpoint Encryption at the time of the encryption can access the files

○ Shared key: Only users that belong to the same policy group or enterprise can access the files

● Fixed password: Agent users specify the encryption password

10. Click **Save**.

Additional Actions

The administrator assigns specific additional actions to each. If a target document meets “n” number of policy criteria, all respective “n” additional action will be applied on the target.

Pass action and its additional actions

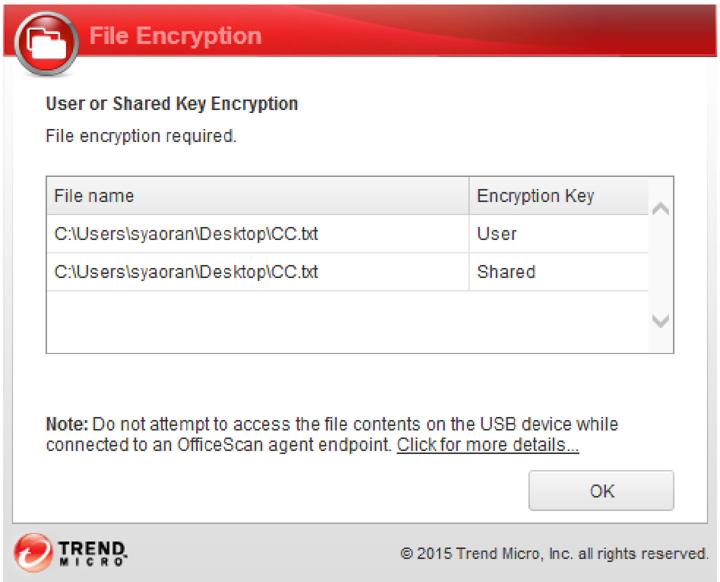
DLP integrates with Trend Micro Endpoint Encryption (TMEE) in automating the encryption of sensitive data on removable devices and cloud storage service channels.

- User key – Also known as a Local Key. This key is unique to each user and limits access to the encrypted file to the user that created the file.
- Shared key – This key refers to the Group Key or Enterprise Key and the Endpoint Encryption administrator configures the type using PolicyServer MMC.
- Fixed password – Users manually provide a fixed password using an on-screen prompt. Endpoint Encryption creates a self-extracting package that users can access on any endpoint after providing the decryption password.

If TMEE is not installed, Data Loss Prevention performs the *Block* action on files.

If TMEE is not logged in for User and Shared key, Data Loss Prevention applies the *Block* action on files. For Fixed Password, it encrypts the data and applies the *Pass* action.

Using the User Key/Share Key:



User or Shared Key Encryption

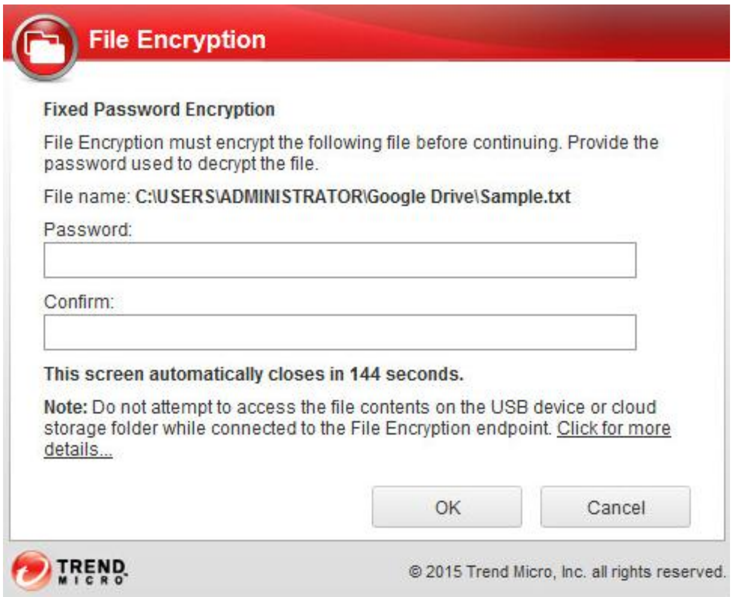
File encryption required.

File name	Encryption Key
C:\Users\syaoran\Desktop\CC.txt	User
C:\Users\syaoran\Desktop\CC.txt	Shared

Note: Do not attempt to access the file contents on the USB device while connected to an OfficeScan agent endpoint. Click for more details...

© 2015 Trend Micro, Inc. all rights reserved.

Using the Fixed Password



Fixed Password Encryption

File Encryption must encrypt the following file before continuing. Provide the password used to decrypt the file.

File name: **C:\USERS\ADMINISTRATOR\Google Drive\Sample.txt**

Password:

Confirm:

This screen automatically closes in 144 seconds.

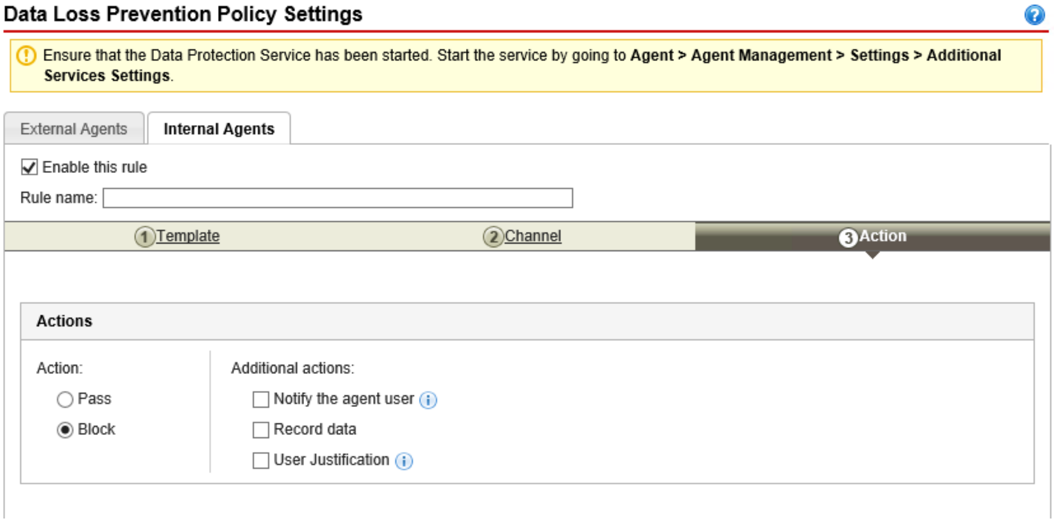
Note: Do not attempt to access the file contents on the USB device or cloud storage folder while connected to the File Encryption endpoint. Click for more details...

© 2015 Trend Micro, Inc. all rights reserved.

NOTES 🗎

- The target endpoint must have Endpoint Encryption installed and the user must log in to Endpoint Encryption in order to encrypt data. DLP can automatically encrypt files before allowing a user to pass them to another location.
- Encrypted files located on USB devices are subject to DLP scanning when users attempt to decrypt the files. Decrypting files containing sensitive data on a USB device triggers the USB encryption protocol resulting in the system requiring that the sensitive data be encrypted (again). To prevent OfficeScan from attempting to "re-encrypt" the data, move the encrypted files to a local drive before attempting to access the data.
- DLP blocks attempts to upload files to cloud storage when using a web client. Encrypt the files manually before uploading using a web client.

BLOCK ACTION AND ITS ADDITIONAL ACTIONS



Data Loss Prevention Policy Settings

Ensure that the Data Protection Service has been started. Start the service by going to **Agent > Agent Management > Settings > Additional Services Settings**.

☑ Enable this rule

Rule name:

Actions

Action:

○ Pass

● Block

Additional actions:

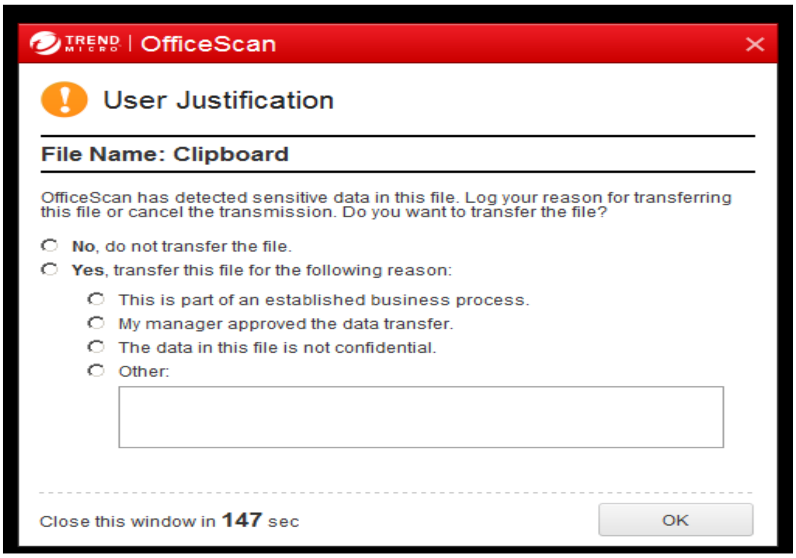
□ Notify the agent user

□ Record data

□ User Justification

Data Loss Prevention prompts the user before performing the *Block* action. User can select to override the *Block* action by providing an explanation as to why the sensitive data is safe to pass.

For example, a given target may meet multiple policy conditions during a scan. If any policy with *Block* action is defined, the target is blocked even if it meets other policies with *Pass* action defined.



User Justification

File Name: Clipboard

OfficeScan has detected sensitive data in this file. Log your reason for transferring this file or cancel the transmission. Do you want to transfer the file?

○ **No**, do not transfer the file.

○ **Yes**, transfer this file for the following reason:

○ This is part of an established business process.

○ My manager approved the data transfer.

○ The data in this file is not confidential.

○ Other:

Close this window in **147** sec

The four description items of the user justification UI can be customized and deployed to the OSCE agent. On the server side, the four items will be saved into `Ofcscan.ini` of the section [Global Setting].

```
[Global Setting]
lpUserJustificationItem0=This is part of an established business process.
DlpUserJustificationItem1=My manager approved the data transfer.
DlpUserJustificationItem2=The data in this file is not confidential.
DlpUserJustificationItem3=
```

3.5 > Investigating and Restoring Forensic Data

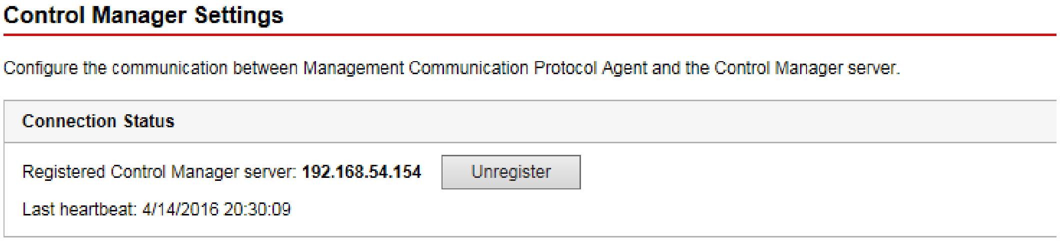
To investigate the forensic data blocked by OfficeScan, a Control Manager 6.0 server is required. Only users who have appropriate permission in Control Manager Server have access to forensic data.

Setup

Follow the Control Manager *Administration Guide* to set up a Control Manager server if there is no Control Manager server available in your environment.

Register OfficeScan 11.0 to the Control Manager server. Go to **Administration** > **Settings** > **Control Manager**.

A successful OfficeScan registration should display a similar page:



Control Manager Settings

Configure the communication between Management Communication Protocol Agent and the Control Manager server.

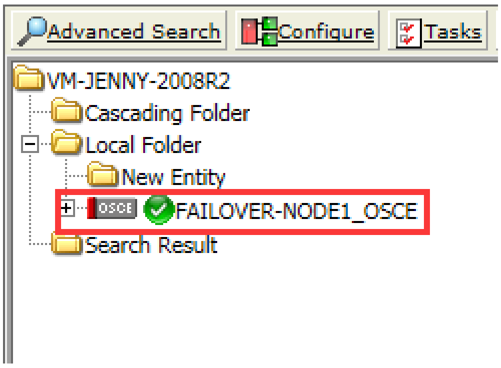
Connection Status

Registered Control Manager server: **192.168.54.154**

Last heartbeat: 4/14/2016 20:30:09

1. On the Control Manager web console, go to **Directories** > **Products**.
2. Expand the Local Folder and then click **New Entity**.

   The registered OfficeScan server should be displayed under the product tree.

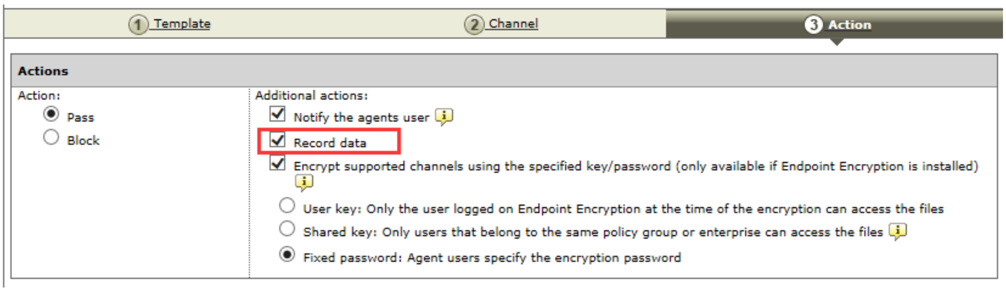


3. Enable recording of forensic data on OfficeScan:

   a. Create a DLP policy.

      For more information, see *Creating a Data Loss Prevention Policy* on the OfficeScan Administrator's Guide.

   b. On the Action tab, make sure [Record data] is checked.



Actions

Action:

● Pass

○ Block

Additional actions:

☑ Notify the agents user

☑ Record data

☑ Encrypt supported channels using the specified key/password (only available if Endpoint Encryption is installed)

○ User key: Only the user logged on Endpoint Encryption at the time of the encryption can access the files

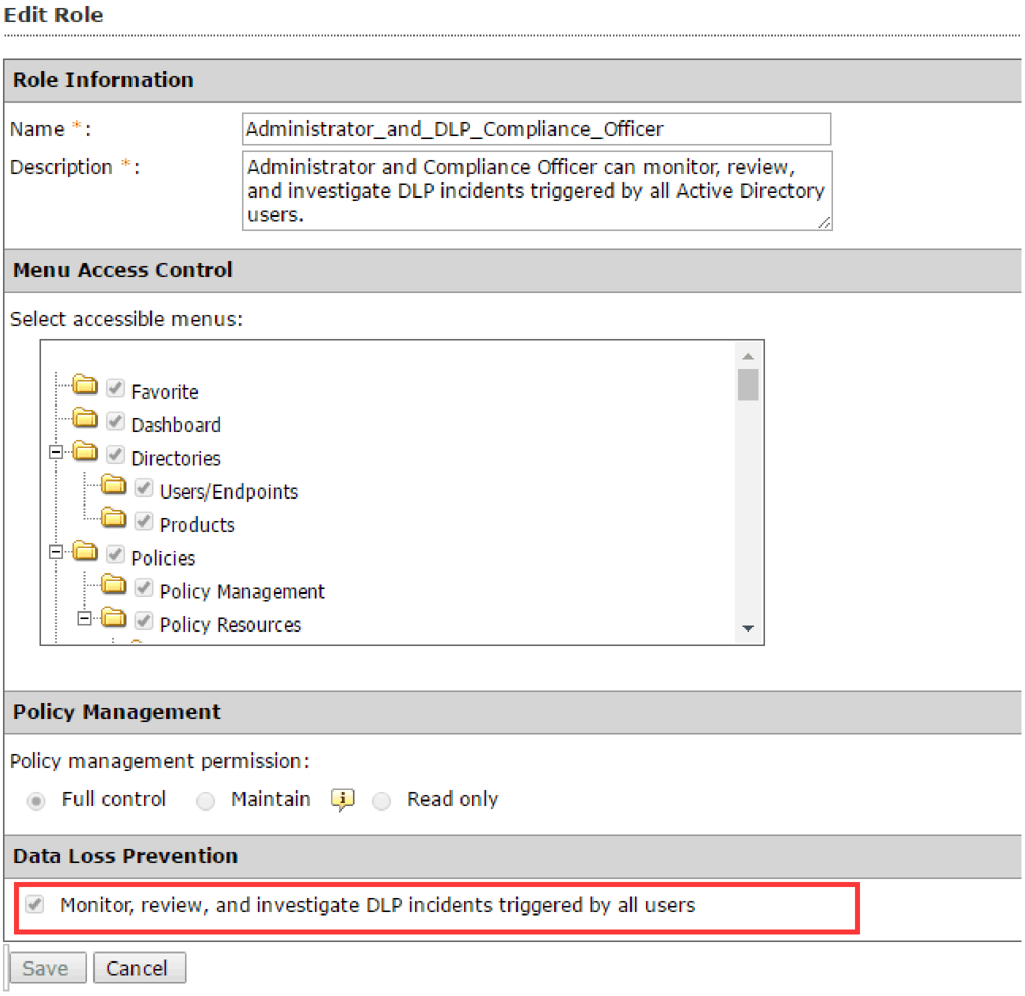
○ Shared key: Only users that belong to the same policy group or enterprise can access the files

● Fixed password: Agent users specify the encryption password

Modifying User Roles

1. On the Control Manager web console, go to **Administration** > **Account Management** > **User Roles**.
2. Select the user role that you want to modify.

   The Edit Role screen appears.
3. Under Data Loss Protection, select **Monitor, review, and investigate DLP incidents triggered by all users**.



Edit Role

Role Information

Name *: Administrator_and_DLP_Compliance_Officer

Description *: Administrator and Compliance Officer can monitor, review, and investigate DLP incidents triggered by all Active Directory users.

Menu Access Control

Select accessible menus:

- ☑ Favorite
- ☑ Dashboard
- ☑ Directories
  - ☑ Users/Endpoints
  - ☑ Products
- ☑ Policies
  - ☑ Policy Management
  - ☑ Policy Resources

Policy Management

Policy management permission:

● Full control ○ Maintain ○ Read only

Data Loss Prevention

☑ Monitor, review, and investigate DLP incidents triggered by all users

Tip ✓ You can also create user accounts on an Active Directory. For more information, see http://docs.trendmicro.com/en-us/enterprise/control-manager-60-service-pack-1/dlp_investigation_abt/dlp_inv_admin_tasks/dlp_roles_abt.aspx.

Checking forensic data

1. Log on with an account that has DLP review permission.

   For more information on modifying user roles, see previous task.

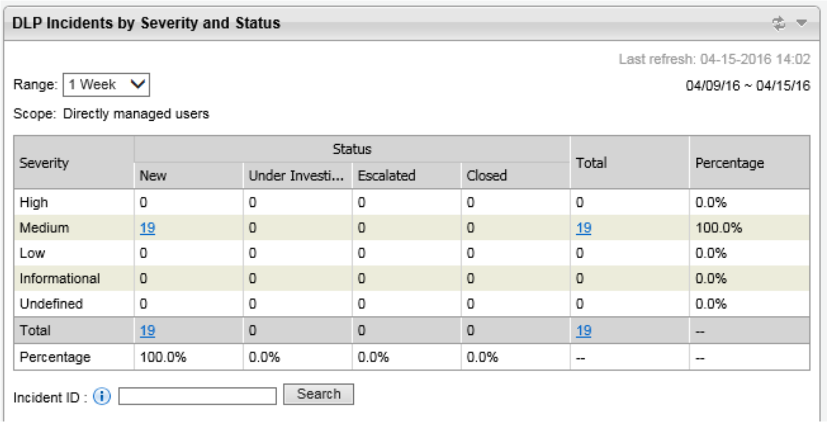
2. Perform any of the following steps to view the forensic data:

   - On the server, locate the following folder:

     `<Server installation folder>\PCCSRV\Private\DLPForensicData`

   - On the Control Manager web console, go to **Dashboard** > **DLP Incident Investigation**.

     a. Check the DLP Incidents by Severity and Status and the DLP Incidents by User widgets.



DLP Incidents by Severity and Status

Last refresh: 04-15-2016 14:02

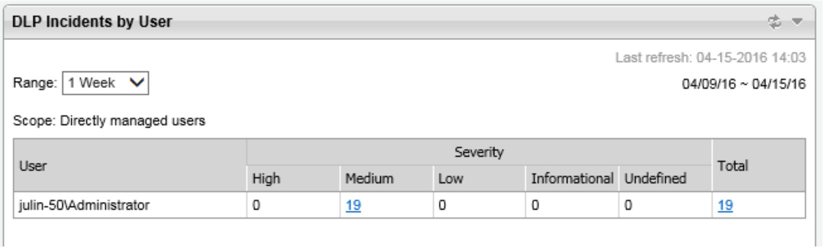
Range: 1 Week

04/09/16 ~ 04/15/16

Scope: Directly managed users

Severity	Status				Total	Percentage
	New	Under Investi...	Escalated	Closed		
High	0	0	0	0	0	0.0%
Medium	19	0	0	0	19	100.0%
Low	0	0	0	0	0	0.0%
Informational	0	0	0	0	0	0.0%
Undefined	0	0	0	0	0	0.0%
Total	19	0	0	0	19	--
Percentage	100.0%	0.0%	0.0%	0.0%	--	--

Incident ID :



DLP Incidents by User

Last refresh: 04-15-2016 14:03

Range: 1 Week

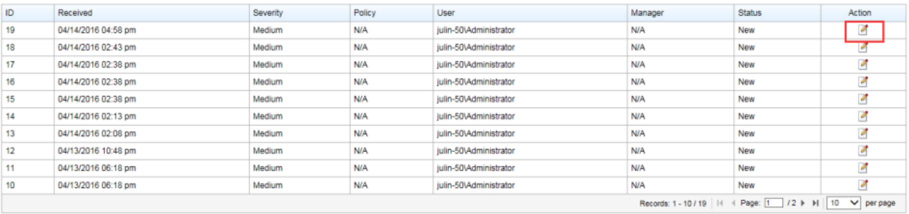
04/09/16 ~ 04/15/16

Scope: Directly managed users

User	Severity					Total
	High	Medium	Low	Informational	Undefined	
julin-50\Administrator	0	19	0	0	0	19

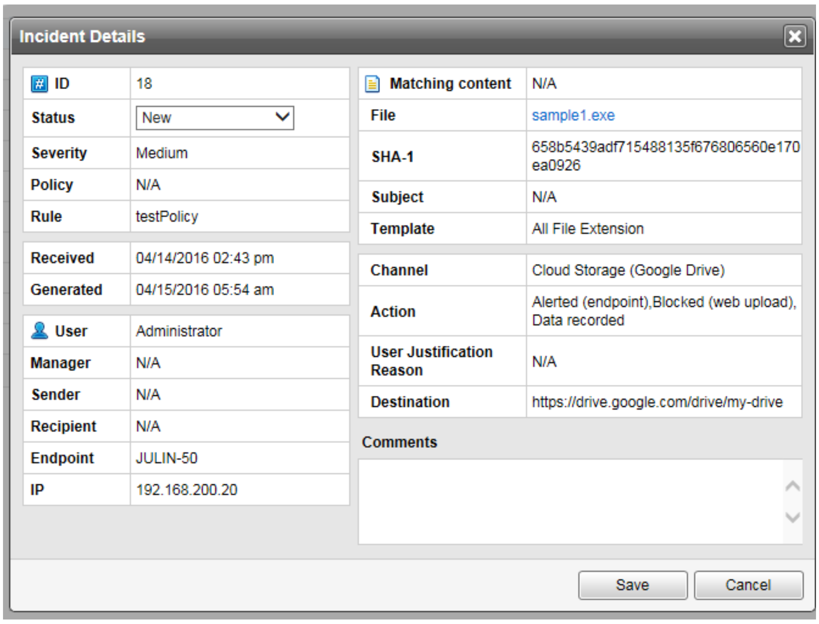
     b. Click the incident numbers to view the incident summary log.

     c. On the Logs screen, click the **Action** icon beside the log information to view the details of the incidents and download the blocked file.



ID	Received	Severity	Policy	User	Manager	Status	Action
19	04/14/2016 04:58 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
18	04/14/2016 02:43 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
17	04/14/2016 02:38 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
16	04/14/2016 02:38 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
15	04/14/2016 02:38 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
14	04/14/2016 02:13 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
13	04/14/2016 02:08 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
12	04/13/2016 10:48 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
11	04/13/2016 06:18 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝
10	04/13/2016 06:18 pm	Medium	N/A	julin-50\Administrator	N/A	New	📝

Records: 1 - 10 / 19 Page: 1 / 2 10 per page



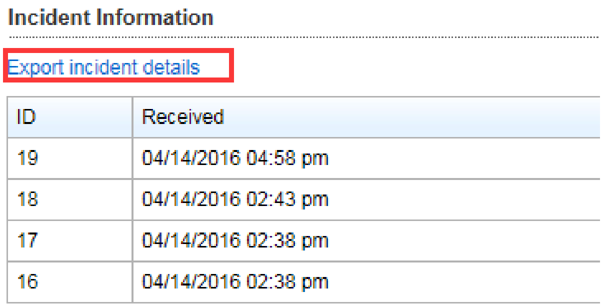
Incident Details

ID	18
Status	New
Severity	Medium
Policy	N/A
Rule	testPolicy
Received	04/14/2016 02:43 pm
Generated	04/15/2016 05:54 am
User	Administrator
Manager	N/A
Sender	N/A
Recipient	N/A
Endpoint	JULIN-50
IP	192.168.200.20

Matching content	N/A
File	sample1.exe
SHA-1	658b5439adf715488135f676806560e170ea0926
Subject	N/A
Template	All File Extension
Channel	Cloud Storage (Google Drive)
Action	Alerted (endpoint),Blocked (web upload), Data recorded
User Justification Reason	N/A
Destination	https://drive.google.com/drive/my-drive

Comments

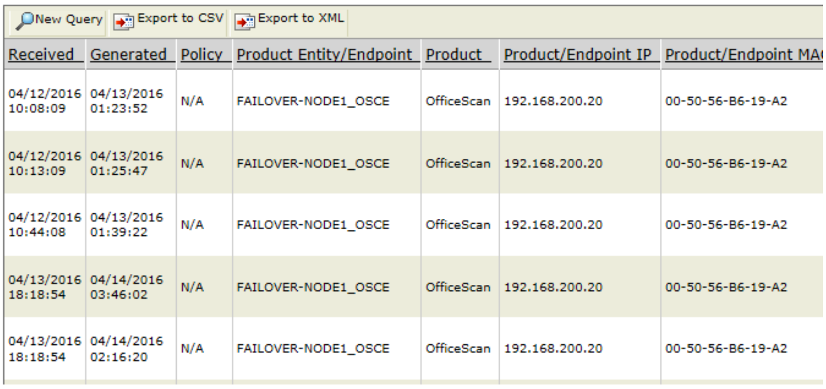
d. On the Incident Information screen, click **Export incident details** to generate a copy of the log.



Incident Information

Export incident details

ID	Received
19	04/14/2016 04:58 pm
18	04/14/2016 02:43 pm
17	04/14/2016 02:38 pm
16	04/14/2016 02:38 pm



Received	Generated	Policy	Product Entity/Endpoint	Product	Product/Endpoint IP	Product/Endpoint MA
04/12/2016 10:08:09	04/13/2016 01:23:52	N/A	FAILOVER-NODE1_OSCE	OfficeScan	192.168.200.20	00-50-56-B6-19-A2
04/12/2016 10:13:09	04/13/2016 01:25:47	N/A	FAILOVER-NODE1_OSCE	OfficeScan	192.168.200.20	00-50-56-B6-19-A2
04/12/2016 10:44:08	04/13/2016 01:39:22	N/A	FAILOVER-NODE1_OSCE	OfficeScan	192.168.200.20	00-50-56-B6-19-A2
04/13/2016 18:18:54	04/14/2016 03:46:02	N/A	FAILOVER-NODE1_OSCE	OfficeScan	192.168.200.20	00-50-56-B6-19-A2
04/13/2016 18:18:54	04/14/2016 02:16:20	N/A	FAILOVER-NODE1_OSCE	OfficeScan	192.168.200.20	00-50-56-B6-19-A2

3.6 > Using the Widgets on the OfficeScan Dashboard

The Dashboard appears when you open the OfficeScan web console or when you click **Dashboard** on the main menu.

Each web console user account has a completely independent dashboard. Any changes made to a user account's dashboard do not affect the dashboards of the other user accounts.

If a dashboard contains OfficeScan agent data, the data that displays depends on the agent domain permissions for the user account. For example, if you grant a user account permission to manage domains A and B, the user account's dashboard only shows data from agents belonging to domains A and B.

OfficeScan server provides the following two iDLP widgets. The two widgets are available only if you activate OfficeScan Data Protection.

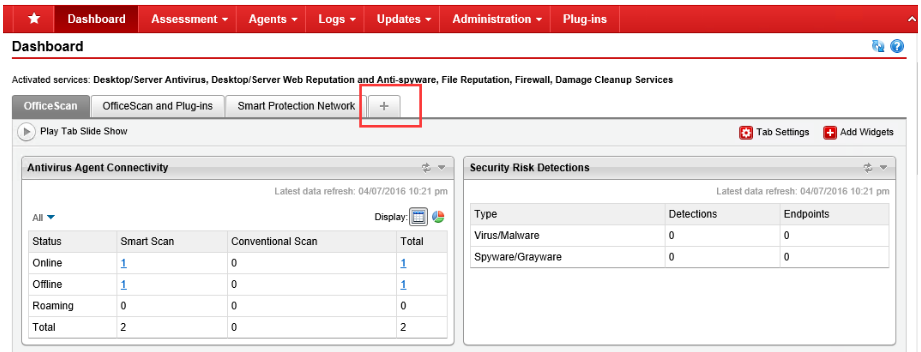
- Top Data Loss Preventions Incidents Widget – This widget is available only if you activate OfficeScan Data Protection. It shows the number of digital asset transmissions, regardless of the action (Block or Pass).

NOTE 🗎 The widget shows a maximum of 10 users, channels, templates, or computers.

- Data Loss Prevention Incidents Over Time Widget **–** This widget plots the number of digital asset transmissions over a period of time. Transmissions include those that are blocked or passed (allowed).

By default, the OfficeScan Server dashboard does not display the two widgets. To display the iDLP widgets, perform the following steps:

1. On the OfficeScan dashboard, click **+.**



Dashboard

Activated services: Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, Firewall, Damage Cleanup Services

Antivirus Agent Connectivity

Latest data refresh: 04/07/2016 10:21 pm

Status	Smart Scan	Conventional Scan	Total
Online	1	0	1
Offline	1	0	1
Roaming	0	0	0
Total	2	0	2

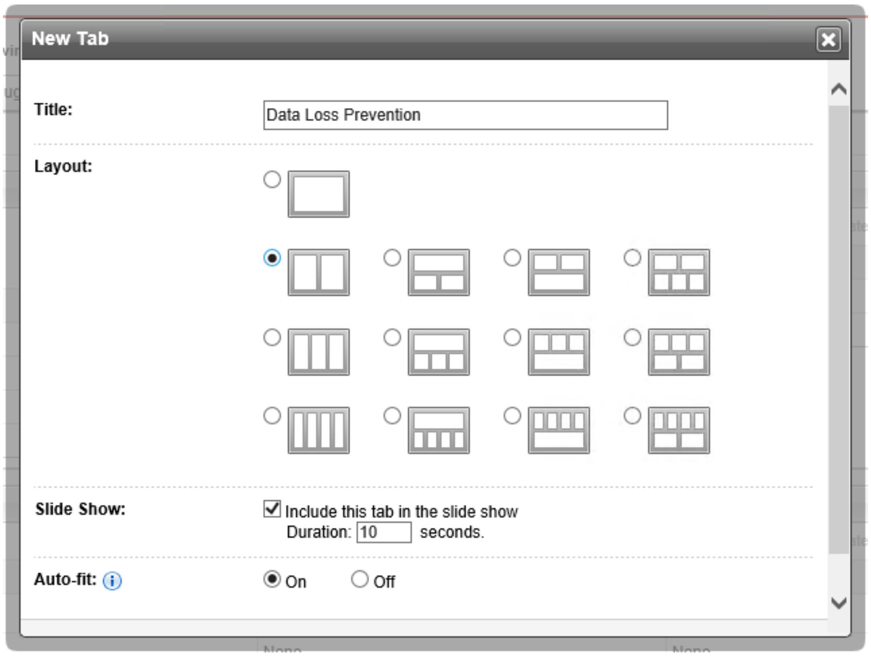
Security Risk Detections

Latest data refresh: 04/07/2016 10:21 pm

Type	Detections	Endpoints
Virus/Malware	0	0
Spyware/Grayware	0	0

2. On the New Tab screen, provide the following details.

   - Title – Type a title for the new tab.
   - Layout – Select a layout for the Dashboard tab.
   - Slide Show – Choose to enable the slideshow option.
   - Auto-fit – Enable or disable to automatically adjust the height of a single widget to match the highest column. This feature is only available if there is only one widget in a column.


New Tab

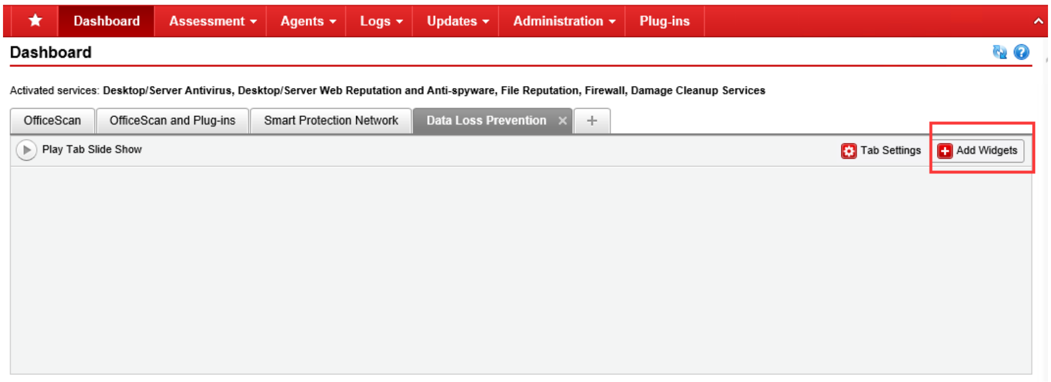
Title: Data Loss Prevention

Layout:

Slide Show: ☑ Include this tab in the slide show
Duration: 10 seconds.

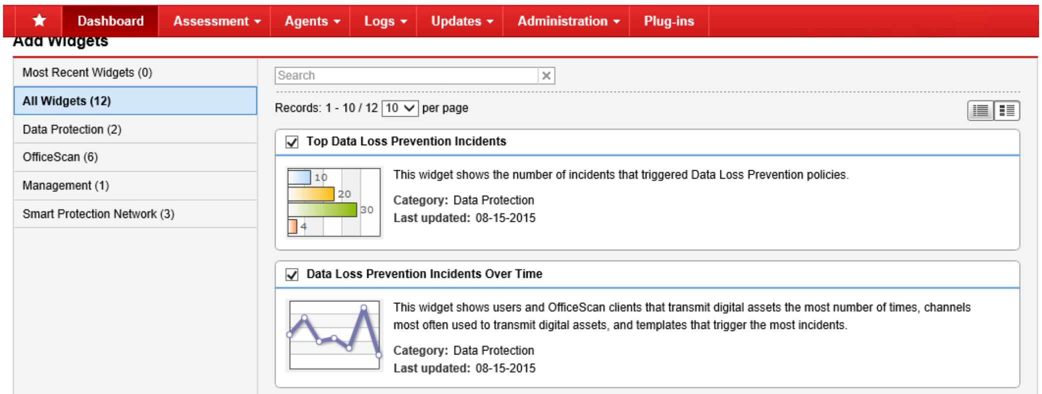
Auto-fit: ● On ○ Off

3. On the newly created tab, click **Add Widgets**.



Activated services: Desktop/Server Antivirus, Desktop/Server Web Reputation and Anti-spyware, File Reputation, Firewall, Damage Cleanup Services

4. On the Add Widgets screen, select **Top Data Loss Protection Incidents** and **Data Loss Prevention Incidents Over Time**.



☑ Top Data Loss Prevention Incidents

This widget shows the number of incidents that triggered Data Loss Prevention policies.

Category: Data Protection
Last updated: 08-15-2015

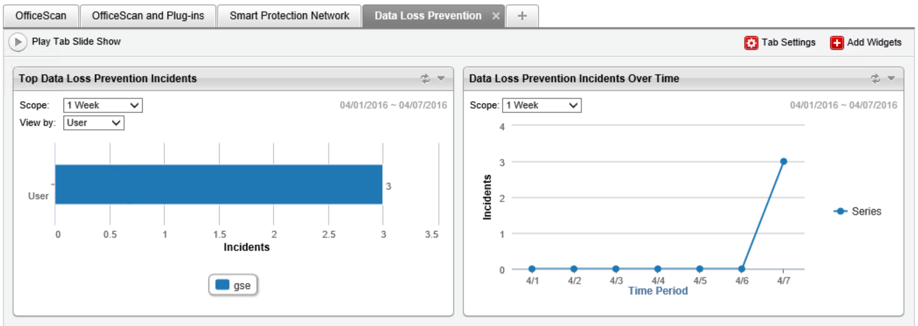
☑ Data Loss Prevention Incidents Over Time

This widget shows users and OfficeScan clients that transmit digital assets the most number of times, channels most often used to transmit digital assets, and templates that trigger the most incidents.

Category: Data Protection
Last updated: 08-15-2015

5. Click **Save**.

The two widgets appear on the Dashboard.



Viewing Widget Information

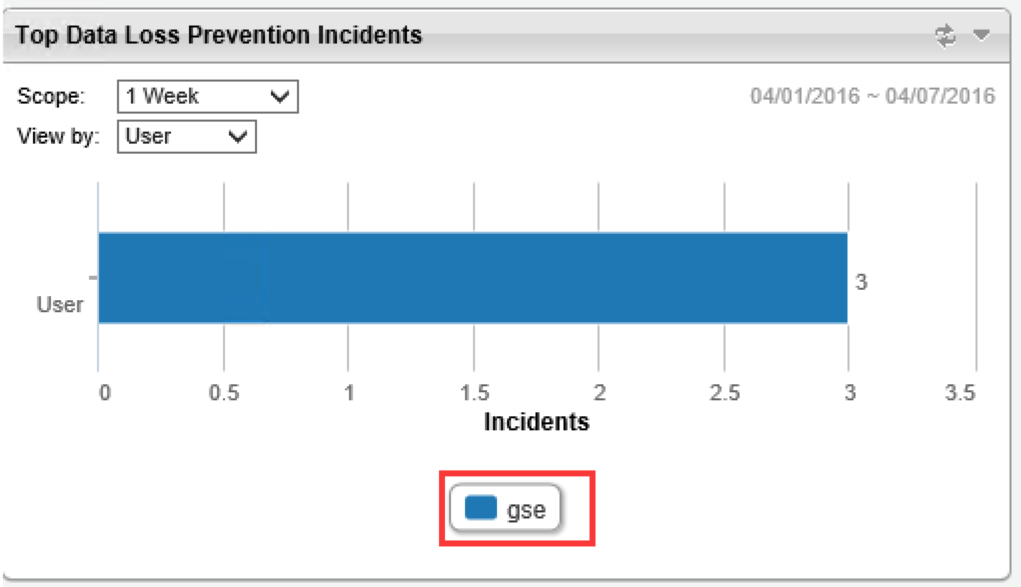
On the Top Data Loss Prevention Incidents widget:

1. Select a time period for the detections. Choose from:
   - Last 24 hours – detections in the last 24 hours, including the current hour
   - 1 Week – detections in the last 7 days, including the current day
   - 2 Weeks – detections in the last 14 days, including the current day
   - 1 Month – detections in the last 30 days, including the current day
2. After selecting the time period, choose from:
   - User – users that transmitted digital assets the most number of times

- Channel – channels most often used to transmit digital assets
- Template – digital asset templates that triggered the most detections
- Computer – computers that transmitted digital assets the most number of times

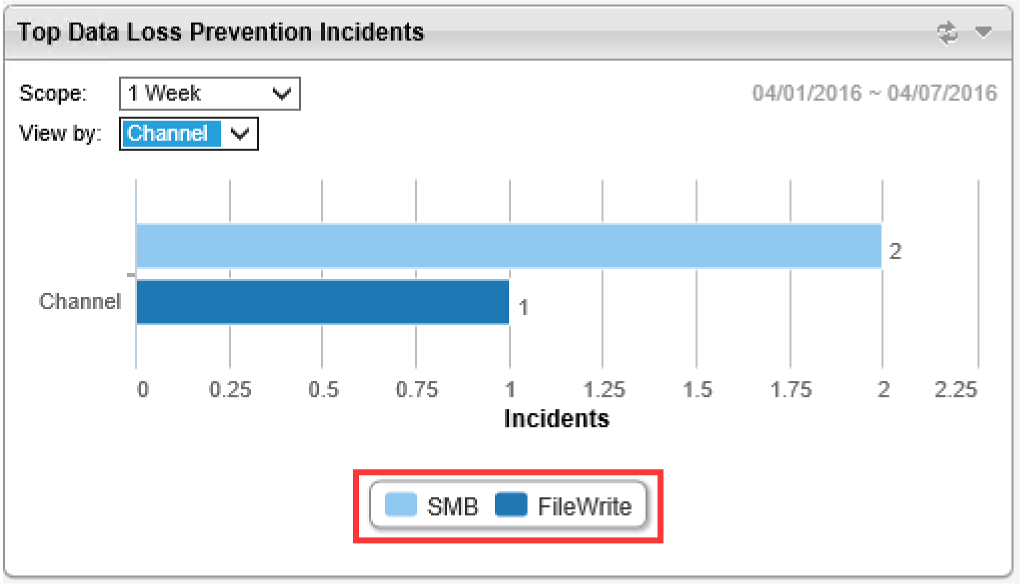
In the example screens below, here are the key findings:

- The user "gse" transmitted digital assets the most number of times in one week.



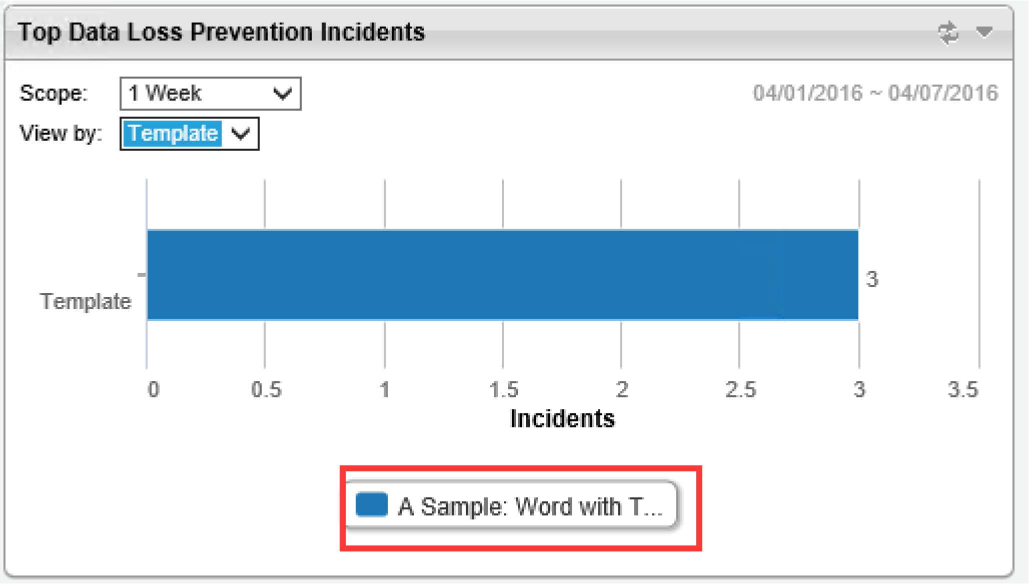
Scope: 1 Week
View by: User

- Channels most often used to transmit digital assets were from *SMB* and *FileWrite*.

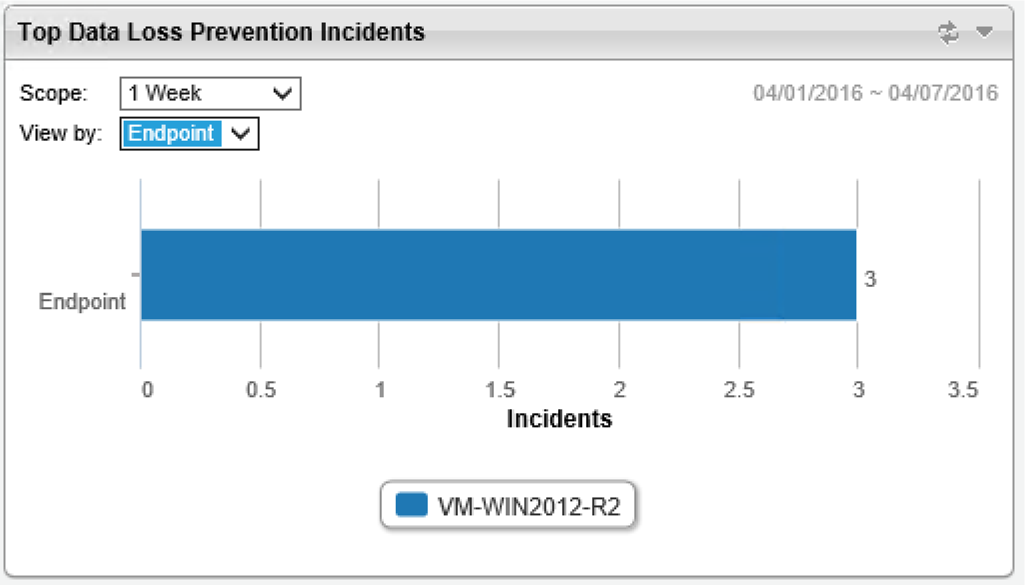


Scope: 1 Week
View by: Channel

- The digital asset template that triggered the most number of detections was "A Sample: Word with Trend Micro".

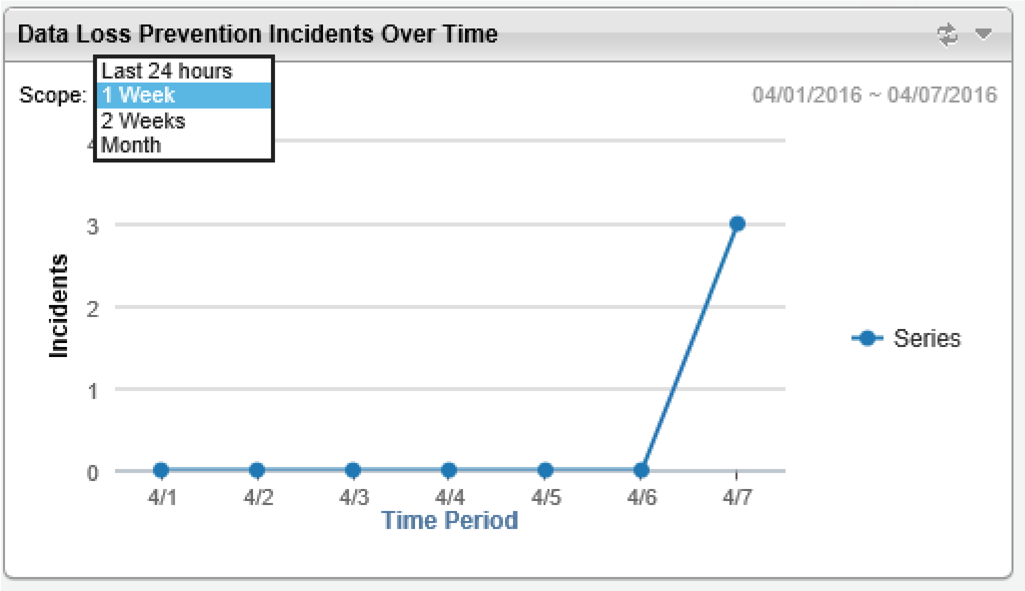


- The computer that transmitted digital assets the most number of times was "VM-WIN2012-R2".



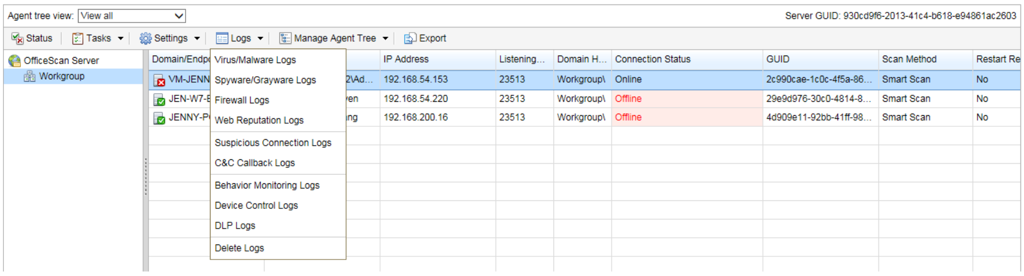
On the Data Loss Prevention Incidents Over Time widget, select a time period for the detections. Choose from:

- Last 24 Hours – detections in the last 24 hours, including the current hour
- 1 Week – detections in the last 7 days, including the current day
- 2 Weeks – detections in the last 14 days, including the current day
- 1 Month – detections in the last 30 days, including the current day



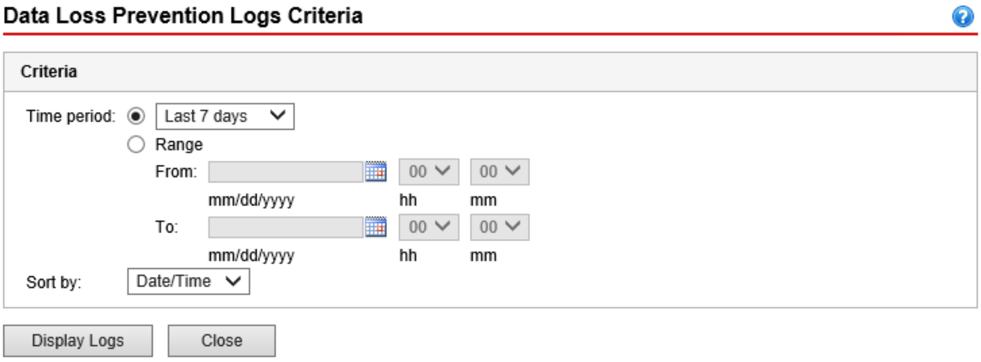
3.7 > Viewing DLP Logs

1. On the OfficeScan web console, go to **Logs** > **Agents** > **Security Risks**.
2. Locate the domain or agent and then right-click to display the menu.
3. Go to **View Logs** > **DLP Logs**.



Domain/Endp		IP Address	Listening...	Domain H...	Connection Status	GUID	Scan Method	Restart Re
VM-JENN	2\Ad...	192.168.54.153	23513	Workgroup\	Online	2c990cae-1c0c-4f5a-86...	Smart Scan	No
JEN-W7-E	ven	192.168.54.220	23513	Workgroup\	Offline	29e9d976-30c0-4814-8...	Smart Scan	No
JENNY-P	ng	192.168.200.16	23513	Workgroup\	Offline	4d909e11-92bb-41ff-98...	Smart Scan	No

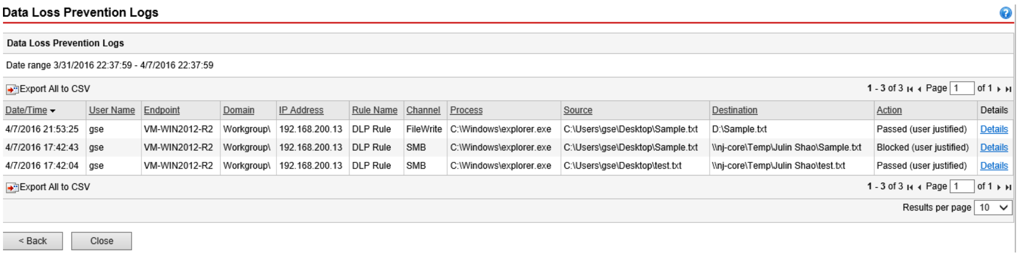
4. Select the time period.



Time period: ● Last 7 days
○ Range
From: mm/dd/yyyy 00 hh 00 mm
To: mm/dd/yyyy 00 hh 00 mm
Sort by: Date/Time

5. Click **Display Logs**.

   DLP log entries appear.



Data Loss Prevention Logs

Data Loss Prevention Logs

Date range 3/31/2016 22:37:59 - 4/7/2016 22:37:59

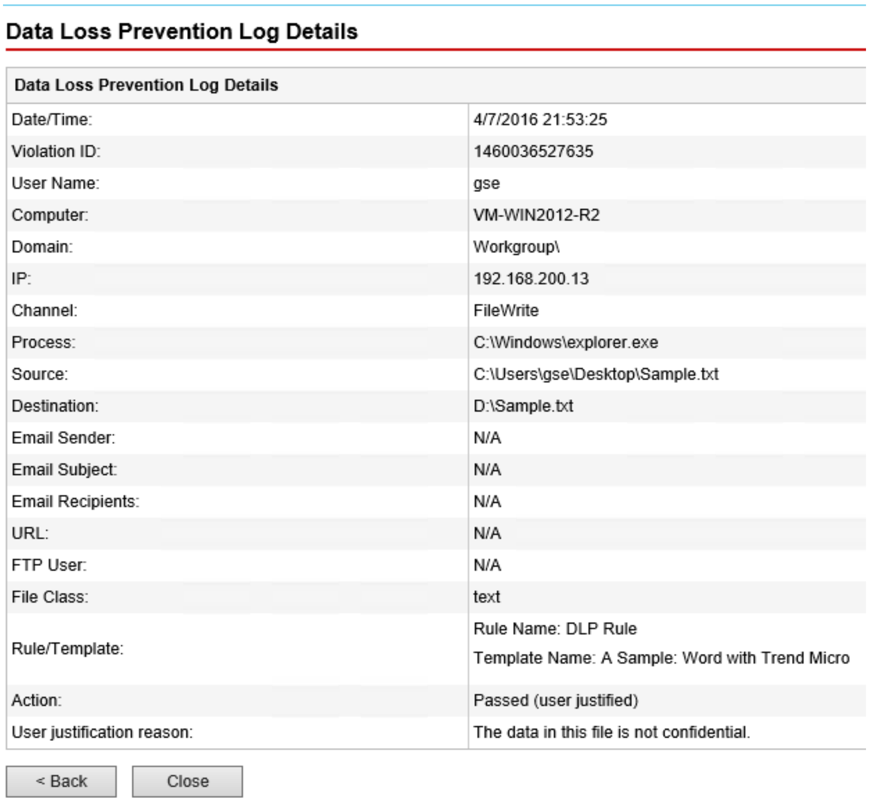
Export All to CSV 1 - 3 of 3 Page 1 of 1

Date/Time	User Name	Endpoint	Domain	IP Address	Rule Name	Channel	Process	Source	Destination	Action	Details
4/7/2016 21:53:25	gse	VM-WIN2012-R2	Workgroup\	192.168.200.13	DLP Rule	FileWrite	C:\Windows\explorer.exe	C:\Users\gse\Desktop\Sample.txt	D:\Sample.txt	Passed (user justified)	Details
4/7/2016 17:42:43	gse	VM-WIN2012-R2	Workgroup\	192.168.200.13	DLP Rule	SMB	C:\Windows\explorer.exe	C:\Users\gse\Desktop\Sample.txt	\\nj-core\Temp\Julin Shao\Sample.txt	Blocked (user justified)	Details
4/7/2016 17:42:04	gse	VM-WIN2012-R2	Workgroup\	192.168.200.13	DLP Rule	SMB	C:\Windows\explorer.exe	C:\Users\gse\Desktop\test.txt	\\nj-core\Temp\Julin Shao\test.txt	Passed (user justified)	Details

Export All to CSV 1 - 3 of 3 Page 1 of 1

Results per page 10

6. To view the detailed information for each log, click **Details**.

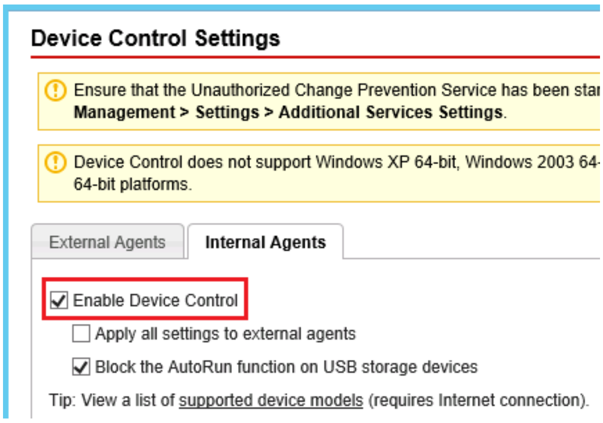


Data Loss Prevention Log Details

Data Loss Prevention Log Details	
Date/Time:	4/7/2016 21:53:25
Violation ID:	1460036527635
User Name:	gse
Computer:	VM-WIN2012-R2
Domain:	Workgroup\
IP:	192.168.200.13
Channel:	FileWrite
Process:	C:\Windows\explorer.exe
Source:	C:\Users\gse\Desktop\Sample.txt
Destination:	D:\Sample.txt
Email Sender:	N/A
Email Subject:	N/A
Email Recipients:	N/A
URL:	N/A
FTP User:	N/A
File Class:	text
Rule/Template:	Rule Name: DLP Rule Template Name: A Sample: Word with Trend Micro
Action:	Passed (user justified)
User justification reason:	The data in this file is not confidential.

3.8 > Device Control

Device Control regulates access to external storage devices and network resources. Device Control helps prevent the propagation of malware on removable drives and network shares and, combined with file scanning, helps guard against security risks.



Device Control Settings

Ensure that the Unauthorized Change Prevention Service has been star
Management > Settings > Additional Services Settings.

Device Control does not support Windows XP 64-bit, Windows 2003 64-
64-bit platforms.

☑ Enable Device Control

□ Apply all settings to external agents

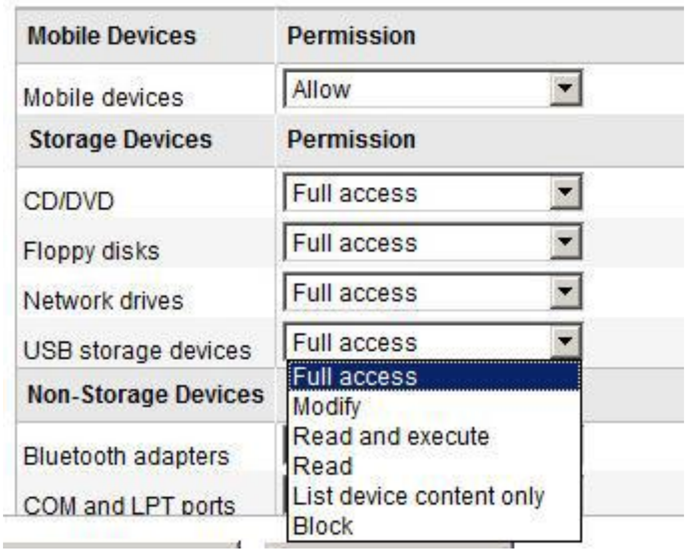
☑ Block the AutoRun function on USB storage devices

Tip: View a list of supported device models (requires Internet connection).

Notification messages are displayed on the endpoints when device control violations occur. Administrators can modify the default notification message.

In OfficeScan 11.0, the Device Control function integrates both Unauthorized Change Prevention Service and DLP features to manage storage devices. Device Access Control and DLP Device Control perform different roles.

For example, in the figure below, different privileges can be set on USB storage devices. Unauthorized Change Prevention Service handles the following privileges: modify, read and execute, read, and list device content only. The block privilege is handled by DLP Device Control.



Mobile Devices	Permission
Mobile devices	Allow
Storage Devices	**Permission**
CD/DVD	Full access
Floppy disks	Full access
Network drives	Full access
USB storage devices	Full access
Non-Storage Devices	
Bluetooth adapters	
COM and LPT ports	

Furthermore, DLP Device Control supports one more device type: mobile devices. This includes smartphones and pads, and software for synchronizing apps such as iTunes and HTC Sync.

Using Device Control

Device Control supports several kinds of devices. The next sections describe how to manage a USB device in the following scenarios:

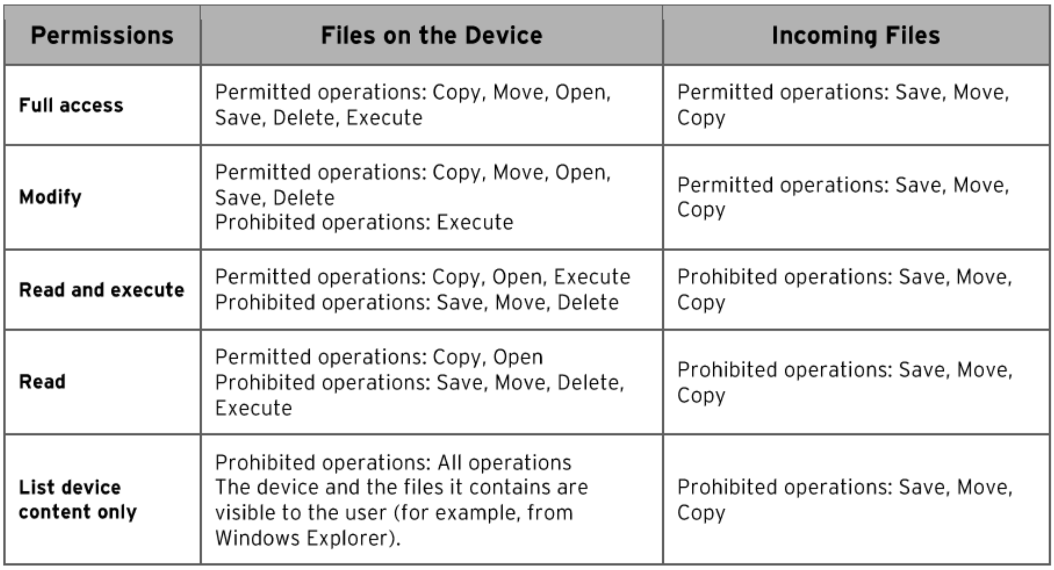
- Only Unauthorized Change Prevention Service is enabled
- Both Unauthorized Change Prevention Service and DLP Device Control are enabled
- Only DLP Device Control is enabled

3.8.1 Managing your USB device using Unauthorized Change Prevention Service

To activate this feature, Unauthorized Change Prevention Service (**Agents** > **Agent Management** > **Settings** > **Additional Service Settings**) and Device Control (**Settings** > **Device Control Settings**) must be enabled on the OfficeScan agent. OfficeScan only monitors USB storage devices when the DLP module is not activated.

When the **Block the auto-run function on USB storage devices** option is enabled on the Device Control Settings screen, OfficeScan prohibits USB storage devices from automatically running. It does not permit the USB storage to execute `autorun.inf` and display the contents of the storage device. This prevents some viruses that use `autorun.inf` from infecting the system.

You can assign any of the following permissions to a USB storage device.



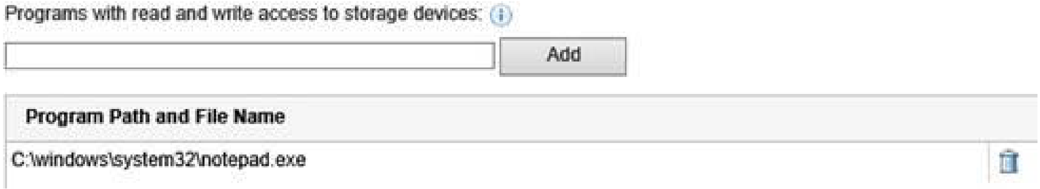
Permissions	Files on the Device	Incoming Files
Full access	Permitted operations: Copy, Move, Open, Save, Delete, Execute	Permitted operations: Save, Move, Copy
Modify	Permitted operations: Copy, Move, Open, Save, Delete Prohibited operations: Execute	Permitted operations: Save, Move, Copy
Read and execute	Permitted operations: Copy, Open, Execute Prohibited operations: Save, Move, Delete	Prohibited operations: Save, Move, Copy
Read	Permitted operations: Copy, Open Prohibited operations: Save, Move, Delete, Execute	Prohibited operations: Save, Move, Copy
List device content only	Prohibited operations: All operations The device and the files it contains are visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

For more information, see *Permissions for Storage Devices* in the OfficeScan Online Help.

To exempt specific programs and certificate providers from this feature, configure the following program lists.

Program List	Description
Programs with read and write access to devices	This list contains local programs and programs on storage devices that have read and write access to the devices. An example of a local program is Microsoft Word (winword.exe), which is usually found in C:\Program Files\Microsoft Office\Office. If the permission for USB storage devices is "List device content only" but "C:\Program Files \Microsoft Office\Office\winword.exe" is included in this list: • A user will have read and write access to any file on the USB storage device that is accessed from Microsoft Word. • A user can save, move, or copy a Microsoft Word file to the USB storage device.
Programs on devices that are allowed to execute	This list contains programs on storage devices that users or the system can execute. For example, if you want to allow users to install software from a CD, add the installation program path and name, such as "E:\Installer\Setup.exe", to this list.

Place local programs on storage devices into the "Programs with read and write access to storage devices" list to give them read and write access permission. For example, add "c:\windows\system32\notepad.exe" into "Programs with read and write access to storage devices" list to allow users to open and modify the programs.

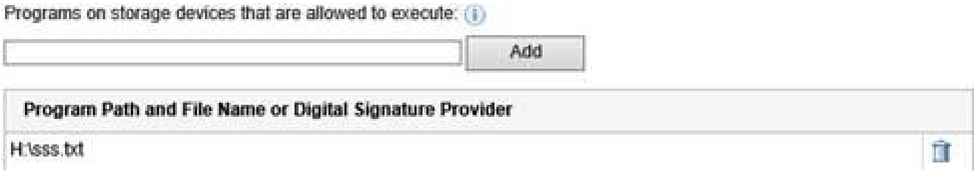


Programs with read and write access to storage devices:

Program Path and File Name
C:\windows\system32\notepad.exe

For more information on how users can add the file path, see *Advanced Permissions for Storage Devices* and *Specifying a Program Path and Name* in the OfficeScan Online Help.

Place programs on storage devices into the "Programs on storage devices that are allowed to execute" list to allow users or systems to execute the programs.



Programs on storage devices that are allowed to execute:

Program Path and File Name or Digital Signature Provider
H:\sss.txt

NOTE 🗎 The antivirus feature in OfficeScan complements Device Control. For example, if Device Control allows a file to open from a regulated device but OfficeScan detects that the file is infected, a scan action will still be performed on the file to eliminate the malware.

Select whether to display a notification message on the client computer when OfficeScan detects unauthorized device access.

If you selected domain(s) or client(s) on the client tree, click **Save** to apply the settings to the domain(s) or client(s). If you selected the root icon, choose from the following options:

- Apply to All Clients – Applies settings to all existing clients and to any new client added to an existing/future domain. Future domains are domains not yet created at the time you configure the settings.
- Apply to Future Domains Only – Applies settings only to clients added to future domains. This option will not apply settings to new clients added to an existing domain.

3.8.2 Managing USB devices using Device Control with Data Protection Activated

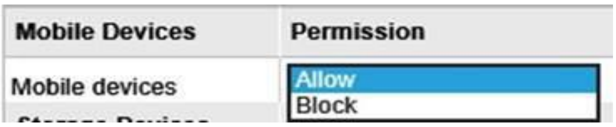
To enable this feature, the user must first install and activate OfficeScan Data Protection and then enable the Unauthorized Change Prevention Service and Device Control for the OfficScan agent.

When OfficeScan Data Protection is activated, there options on the Device Control Settings screen change. Block permission is managed by iDLP.

Permissions	Files on the Device	Incoming Files
Block (available after installing Data Protection)	Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

With Data Protection (iDLP) installed, OfficeScan offers more functionality for USB access. Apart from the Device Control feature, iDLP adds the following options.

- Allow or block access to mobile devices – This setting controls access to mobile devices using synchronization apps such as iTunes and HTC Sync.

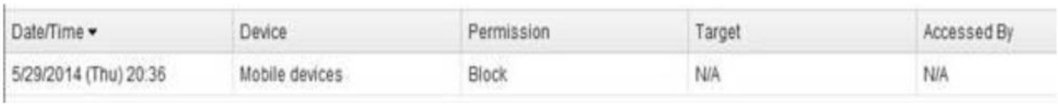


Mobile Devices	Permission
Mobile devices	Allow Block

OS support list	Synchronous application list
Android, iOS	iTunes, htcsync, HTC sync manager, Samsung kies, 豌豆荚， HiSuite, 91Mobile
Windows phone	Windows phone (desktop), Windows phone(metro), Nokia PC Suite, Zune
Blackberry	Blackberry Device manager
Symbian OS	

To view the detailed list of supported mobile devices, go to **Agents** > **Agent Management** > **Device Control Settings** and then click **supported device models**.

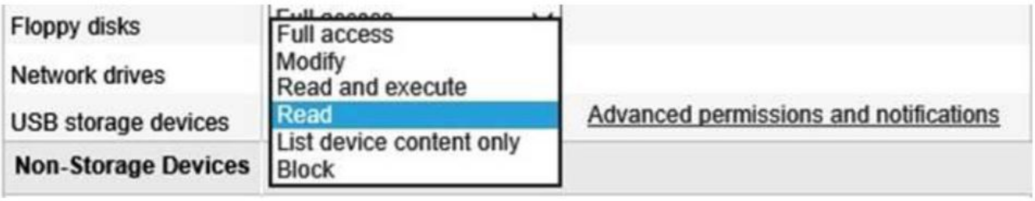
- Allow or block access to non-storage devices – This setting allows or blocks access to non-storage devices. There are no granular or advanced permissions for these devices.



Date/Time ▾	Device	Permission	Target	Accessed By
5/29/2014 (Thu) 20:36	Mobile devices	Block	N/A	N/A

Device Type	Device Description	Permission
Non-storage Devices	COM and LPT ports	Block/Allow
	IEEE 1394 interface	Block/Allow
	Imaging Devices	Block/Allow
	Infrared devices	Block/Allow
	Modems	Block/Allow
	PCMCIA card	Block/Allow
	Print screen key	Block/Allow
	Bluetooth adapter	Block/Allow
	Wireless NICs	Block/Allow

- Allow or block the access to USB storage devices



Floppy disks

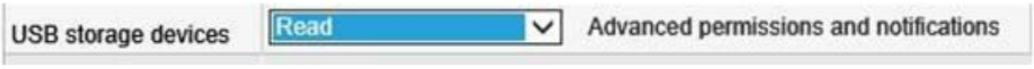
Network drives

USB storage devices

Non-Storage Devices

The *Read* and *Block* permissions are controlled by iDLP. Device Control allows users to block access to all USB storage devices, except those that have been added to the list of approved devices.

To modify the whitelist, select **Read** and then click **Advanced permissions and notifications**.



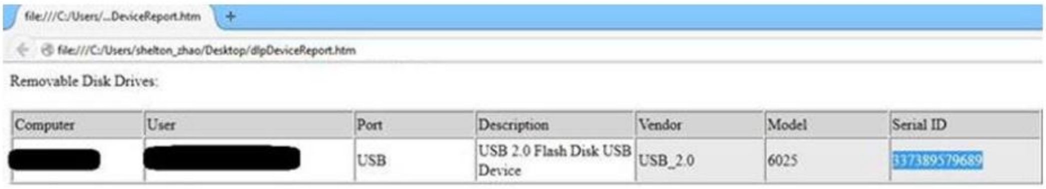
USB storage devices | Read | Advanced permissions and notifications

The user can allow access to a specific device by adding its vendor, model, and serial ID information to iDLP whitelist. If a device is in the whitelist, iDLP allows access to the device.

Trend Micro also provides a Device List Tool that scans an endpoint for external devices and then displays device information in a browser window. Users can then use the information when configuring device settings for Data Loss Prevention and Device Control.

Users can find the `listDeviceInfo.exe` file in the following folder location:

`<Server installation folder>\PCCSRV\Admin\Utility\ListDeviceInfo`.



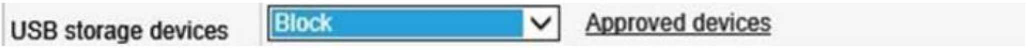
file:///C:/Users/...DeviceReport.htm
file:///C:/Users/shelton_zhao/Desktop/dlpDeviceReport.htm

Removable Disk Drives:

Computer	User	Port	Description	Vendor	Model	Serial ID
[redacted]	[redacted]	USB	USB 2.0 Flash Disk USB Device	USB_2.0	6025	337389579689

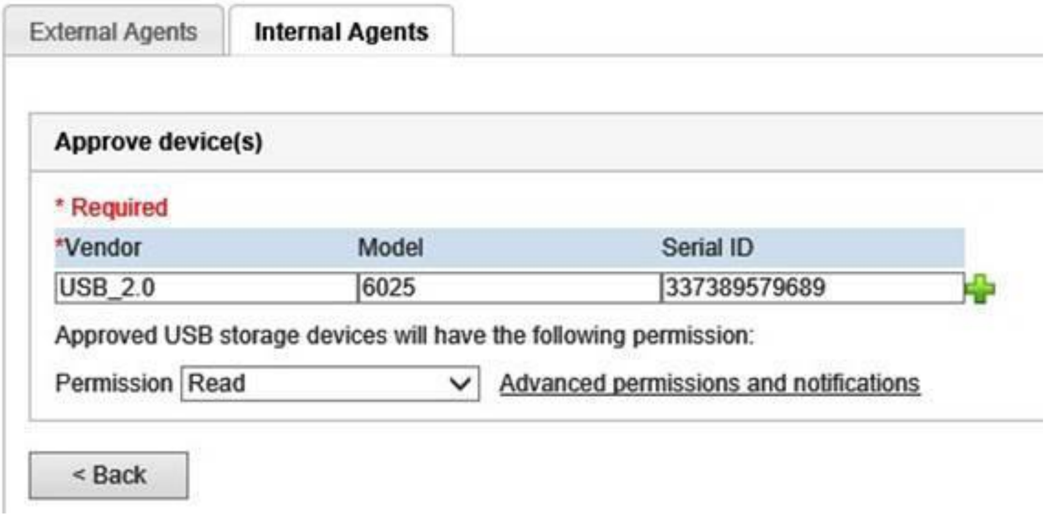
To add a device, the vendor information is required. However, if the system cannot read the device vendor information, type "*" and then add the other information generated by the Device List Tool. Adding devices to the Program Lists is also recommended.

Alternatively, users can select **Block** and then add specific USB storage devices into the whitelist by clicking **Approved devices**.



USB storage devices | Block | Approved devices

After adding a device to the list, users can click **Advanced permissions and notifications** and then add devices to the Program Lists.



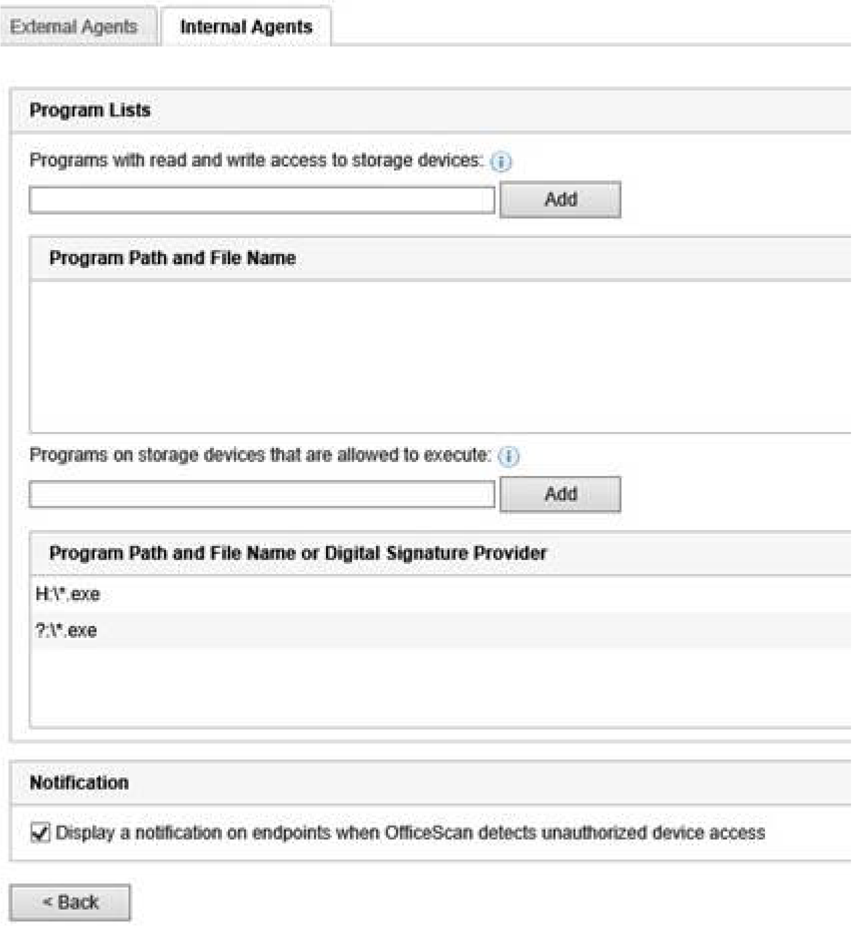
Approve device(s)

* Required

*Vendor	Model	Serial ID
USB_2.0	6025	337389579689

Approved USB storage devices will have the following permission:

Permission: Read | Advanced permissions and notifications



External Agents | Internal Agents

Program Lists

Programs with read and write access to storage devices:

Program Path and File Name

Programs on storage devices that are allowed to execute:

Program Path and File Name or Digital Signature Provider
H:\*.exe
?:*.exe

Notification

☑ Display a notification on endpoints when OfficeScan detects unauthorized device access

NOTE The advanced permissions and notifications are not available if Full Access is selected.

3.8.3 Managing USB devices using Device Control with Unauthorized Change Prevention Service Disabled and Data Protection Activated

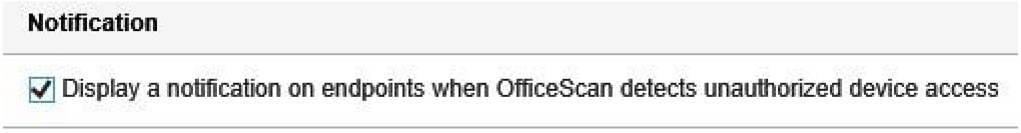
When the Unauthorized Change Prevention Service is disabled and Device Control is enabled, only the iDLP features are available.

- For USB storage devices, the following permissions are available: *Full access*, *Read*, and *Block*.
- When *Read* is selected, the advanced permissions and notifications are all available.
- When *Block* is selected, users can add approved devices but only the *Full access* permission may be assigned to the approved devices.
- The Program Lists are unavailable.

Device Type	Device Description	Permission
Mobile devices	Phones and tablets with/without sync app	Block/Allow
USB storage devices	Storage device	Block/Allow/Read
Non-storage devices	COM and LPT ports	Block/Allow
	IEEE 1394 interface	Block/Allow
	Imaging Devices	Block/Allow
	Infrared devices	Block/Allow
	Modems	Block/Allow
	PCMCIA card	Block/Allow
	Print screen key	Block/Allow
	Bluetooth adapter	Block/Allow
	Wireless NICs	Block/Allow

3.8.4 Using Device Control Notifications

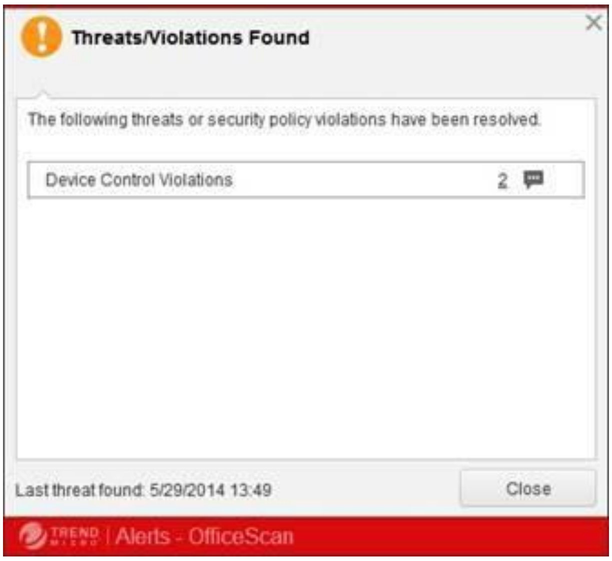
Notification messages display on endpoints when Device Control violations occur if the Device Control notifications are enabled.



Notification

☑ Display a notification on endpoints when OfficeScan detects unauthorized device access

When a violation occurs, users would see a message similar to the following image:



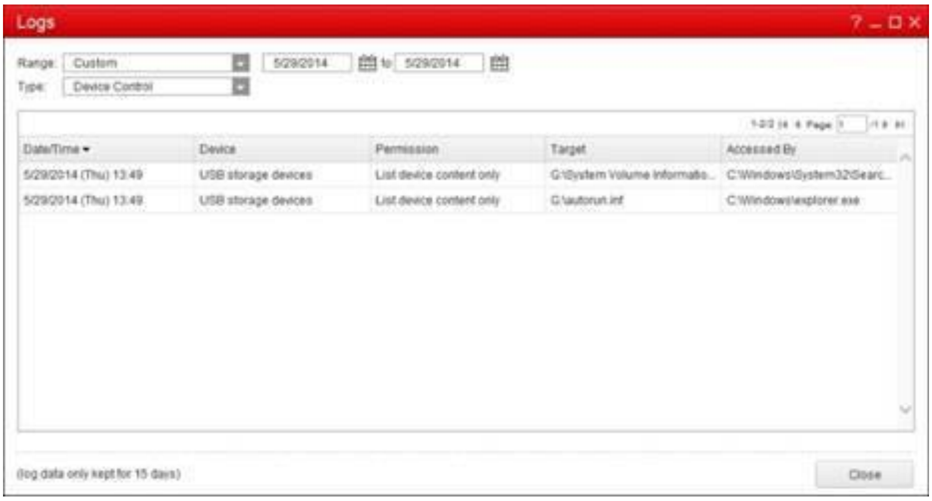
Threats/Violations Found

The following threats or security policy violations have been resolved.

Device Control Violations 2

Last threat found: 5/29/2014 13:49

USB access violation logs will also be available:



Range: Custom 5/29/2014 to 5/29/2014

Type: Device Control

Date/Time ▾	Device	Permission	Target	Accessed By
5/29/2014 (Thu) 13:49	USB storage devices	List device content only	G:\System Volume Informatio...	C:\Windows\System32\Searc...
5/29/2014 (Thu) 13:49	USB storage devices	List device content only	G:\autorun.inf	C:\Windows\explorer.exe

(log data only kept for 15 days)