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.

Trend Micro, the Trend Micro t-ball logo, OfficeScan, Damage Cleanup Services, ScanMail, and TrendLabs are service marks, trademarks or registered trademarks of Trend Micro, Incorporated.

BigFix®, Fixlet® and "Fix it before it fails"® are registered trademarks of BigFix, Inc. iprevention, Powered by BigFix, Relevance Engine, and related BigFix logos are trademarks of BigFix, Inc.

All other product or company names may be trademarks or registered trademarks of their respective owners.

Protected by U.S. Patent No. 5,623,600; 5,889,943; 5,951,698; 6,119,165

Copyright © 2011 Trend Micro Incorporated. All rights reserved.

Document Part No. APEM05258_111107

Release Date: November 2011

Related Documents

Use this Administrator’s Guide to upgrade, install and/or configure Trend Micro Data Protection Services in conjunction with Trend Micro Core Protection Module.

For related information, see:

- **Core Protection Module 10.6 - Administrator’s Guide**: Contains deployment strategies, installation instructions, and common configuration tasks.
Feedback

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

IMPORTANT NOTICE AND LIMITATION

Your use of the Trend Micro Core Protection Module - Data Protection Services is limited to supporting the Trend Micro Core Protection Module and other BigFix Products purchased from Trend Micro only as expressly described in and permitted by this user guide.

You are only authorized and licensed to use the software distribution capabilities of the Trend Micro Core Protection Module - Data Protection Services to distribute the Trend Micro Core Protection Module and other BigFix Products purchased from Trend Micro, but you are not authorized or licensed to use the Trend Micro Core Protection Module to distribute any other Trend Micro, BigFix, or any third party software.

You are authorized and licensed to use the Trend Micro Core Protection Module - Data Protection Services only to customize the Fixlets that are provided with the Trend Micro Core Protection Module and other BigFix Products purchased from Trend Micro, but you are not authorized to create completely new Fixlets unrelated to such software purchased from Trend Micro.

However, you may at any time purchase an upgrade from Trend Micro that permits you to use the full and complete software distribution capabilities of the Trend Micro Core Protection Module with any software application (any Trend Micro, BigFix, or third party software) and to create new Fixlets that are unrelated to the software purchased from Trend Micro.
Contents

**Introducing Data Protection** ........................................... 1

About Data Protection ...................................................... 1
About Data Loss Prevention ............................................... 2
DLP Settings Wizard .......................................................... 2
Device Control ............................................................... 3
Device Control Wizard ....................................................... 4
Installing the Data Protection Module ................................. 5
Adding the Data Protection Site .......................................... 6
Configuring Client Notifications ........................................ 6

**DLP Data Identifiers** ...................................................... 7

Data Identifier Types ...................................................... 7
Expressions ................................................................. 8
Predefined Expressions .................................................... 8
Viewing Settings for Predefined Expressions ...................... 8
Customized Expressions ................................................... 9
Criteria for Customized Expression .................................. 9
Creating a Customized Expression .................................... 11
Importing Customized Expressions ................................... 11

File Attributes ............................................................. 12
Creating a File Attribute List .......................................... 12
Importing a File Attribute List ....................................... 13

Keywords ................................................................. 14
Predefined Keyword Lists ............................................... 14
Customized Keyword Lists ............................................... 14
Customized Keyword List Criteria .................................. 15
Creating a Keyword List ................................................ 16
Importing a Keyword List ............................................... 17
## Device Control

- Permissions for Storage Devices
- Advanced Permissions for Storage Devices
- Specifying a Digital Signature Provider
- Specifying a Program Path and Name
- Permissions for Non-storage Devices
- Managing Access to External Devices
- Configuring Advanced Permissions
- Configuring an Approved List of USB Devices

## Data Protection Analyses and Reports

- Data Protection Analyses
- Data Protection - Endpoint Information Analysis
- Data Protection - Detected Data Loss Prevention Violation Information Analysis
- Data Protection - Data Loss Prevention Policy Information Analysis
- Data Protection - Detected Device Control Violation Information Analysis
- Data Protection - Device Control for Non-Storage Devices Information Analysis
- Data Protection - Device Control for Storage Devices Information Analysis
- Data Loss Prevention Report
- Device Control Detections Report

## Data Protection Reference Tables

- Predefined Expression List
- Supported File Types
- Predefined Keyword Lists
- How Keyword Lists Work
- Number of Keywords Condition
- Distance Condition
- Keyword List Descriptions
- Predefined DLP Template List
- Wildcard Usage in Device Control
Introducing Data Protection

This chapter introduces the Data Protection features available in Core Protection Module and how to install the services.

- “About Data Protection” on page 1
- “About Data Loss Prevention” on page 2
- “DLP Settings Wizard” on page 3
- “Device Control” on page 4
- “Device Control Wizard” on page 5
- “Installing the Data Protection Module” on page 6
- “Adding the Data Protection Site” on page 6
- “Configuring Client Notifications” on page 7

About Data Protection

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 data identifiers—to outside 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
- Result in unnecessary costs to cover for remediation and to pay fines for violating compliance regulations
- Lead to lost business opportunities and revenue when intellectual property is stolen

With the prevalence and damaging effects of data breaches, organizations now see the protection of sensitive information as a critical component of their security infrastructure.
About Data Loss Prevention

Data Loss Prevention safeguards an organization’s sensitive data against accidental or deliberate leakage. Data Loss Prevention allows you to:

- Identify the sensitive information, through use of data identifiers, to protect
- Create policies that limit or prevent the transmission of data identifiers through common transmission channels, such as email and external devices
- Enforce compliance to established privacy standards

Before you can monitor sensitive information 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 security violation occurs?

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

If you already defined your sensitive information and security policies, you can begin to define data identifiers and company policies.

Data Loss Prevention protects your organization through use of:

- DLP Data Identifier Management (see “DLP Data Identifiers” on page 8)
- DLP Template Management (see “Data Loss Prevention Templates” on page 18)
- DLP Policy Management (see “Data Loss Prevention Policies” on page 22)

DLP Settings Wizard

Use the DLP Settings Wizard to create, modify, and manage your Data Loss Prevention data identifiers, templates, and policies.

The DLP Settings Wizard Overview screen provides a tree view to help you plan your DLP policies from beginning to end. Start creating your policies by clicking either the hyperlinks at the top of the Overview screen or the buttons located in the tree view.
To create a customized Data Loss Prevention policy, perform the following steps:

1) Create the necessary data identifiers to include in your policy. The three types of data identifiers available are:
   - Expressions (see “Expressions” on page 8)
   - File Attributes (see “File Attributes” on page 13)
   - Keywords (see “Keywords” on page 15)

2) Create a Data Loss Prevention template using your customized data identifiers, or select from the predefined data identifiers provided with Data Protections services (see “Data Loss Prevention Templates” on page 18).

3) Create and deploy a policy using your customized templates, or select from the predefined compliance templates provided with Data Protection services (see “Data Loss Prevention Policies” on page 22).

**Figure 1:** DLP Settings Wizard

Device Control regulates access to external storage devices and network resources connected to computers. Device Control helps prevent data loss and leakage and, combined with file scanning, helps guard against security risks.
You can configure Device Control policies for internal and external clients. CPM administrators typically configure a stricter policy for external clients.

You can enforce specific policies to client groups or individual clients. You can also enforce a single policy to all clients.

After you deploy the policies, clients use the location criteria you have set in the Location Property Wizard (see the Core Protection Module Administrator’s Guide, Chapter 9 for more details) to determine their location and the policy to apply. Clients switch policies each time the location changes.

Important:

- Device Control only supports 32-bit platforms.
- For a list of supported device models, see:

**Device Control Wizard**

Use the Device Control Wizard to manage and deploy device access permissions on your endpoints.

The wizard provides multi-layered permissions to storage devices that allows you to customize the level of access granted to a device, and the access to specific programs on the device (see “Permissions for Storage Devices” on page 35).

Manage permissions to non-storage devices by allowing or blocking access them. Device Control manages the following non-storage devices:

- COM and LPT ports
- IEEE 1394 interface
- Imaging devices
- Infrared devices
- Modems
- PCMCIA cards
- Print screen key

For more information about Device Control, see “Device Control” on page 35.
INTRODUCING DATA PROTECTION
INSTALLING THE DATA PROTECTION MODULE

Figure 2: Device Control Wizard

Installing the Data Protection Module

Before you can begin protecting your endpoints from data leakage, you must first install the Data Protection module. The Data Protection module provides DLP policy and Device Control features.

NOTE: Data Protection Services are not supported on 64-bit platforms. Endpoints with Trend Micro Data Loss Prevention installed must uninstall the program before installing the Data Protection Services.

TASK

1. Navigate to Endpoint Protection > Core Protection Module > Deployment > Install.
2. In the upper right pane, click Data Protection - Install Data Protection Services.
3. Click Take Action.
4. In the Target tab, select the endpoints to which to install the Data Protection Services.
5. Click OK. At the prompt, type your private key password and click OK.
6. In the Action | Summary window that opens, monitor the "Status" of the Action to confirm that it is "Evaluating", "Running", and then "Completed".
Adding the Data Protection Site

Install the Trend Micro Data Protection site from the console by adding its masthead (*Trend Micro Data Protection.efxm*) to the list of managed sites.

**TASK**
1. Copy the *Trend Micro Data Protection.efxm* file to the CPM server.
2. Double-click the file.
3. Click Yes to subscribe to the Trend Micro Data Protection Site.
4. At the prompt, type your private key password and click **OK**.
5. Select the applicable computers to deploy the new Activation Code to. Select **All computers** to deploy the new code to all endpoints.
6. Click **Save Changes**. At the prompt, type your private key password and click **OK**.
7. Close any open windows to return to the ESP Console view.

Configuring Client Notifications

Once Data Protection detects a DLP policy violation or Device Control violation, CPM performs the administrator-defined action associated with the violation that occurred. Administrators can configure a customized message to inform users that CPM performed an action on their endpoint.

For example, if a user attempts to access a USB device on their endpoint and the administrator has configured Device Control to block access to USB devices, configure a message such as, “A Device Control violation has been detected. Access to the device has been denied.” This message informs users that their current action is in violation of a policy and that their computer is functioning properly.

Administrators can configure separate notifications for Device Control and Data Identifier Transmissions.

**TASK**
1. Navigate to **Endpoint Protection > Configuration > Client Notifications > Client Notification Settings**.
2. Modify the message that displays on endpoints for **Device Control Violations** and **Data Identifier Transmissions**, or accept the default messages.
3. Click **Create Configuration Task**. The Create Task window appears.
4. Click **OK**, type your Private Key Password, and click **OK**. A Task window appears.
5. Click the hyperlink in the Actions window. The Take Action window opens.
6. Select all Applicable Computers and click **OK**. When prompted, type your private key password and click **OK**.
7. In the Action | Summary window that opens, monitor the "Status" and "Count" of the Action to confirm that it is "Running" and then "Completed."

---

## DLP Data Identifiers

This chapter describes the different DLP data identifier types and how to configure customized data identifiers for use in templates.

- "Data Identifier Types” on page 8
- "Expressions” on page 8
- “Creating a Customized Expression” on page 11
- “File Attributes” on page 13
- “Creating a File Attribute List” on page 13
- "Keywords” on page 15
- “Creating a Keyword List” on page 17

### Data Identifier Types

Data identifiers are files and data that an organization must protect against unauthorized transmission. You can define data identifiers using the following:

- **Expressions**: Data that has a certain structure. For details, see “Expressions” on page 8.
- **File attributes**: File properties such as file type and file size. For details, see “File Attributes” on page 13.
• **Keywords:** A list of special words or phrases. For details, see “Keywords” on page 15.

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

### 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 9 and “Customized Expressions” on page 9.

### Predefined Expressions

CPM comes with a set of predefined expressions. These expressions cannot be modified, copied, exported, or deleted.

CPM verifies these expressions using pattern matching and mathematical equations. After CPM matches potentially sensitive data with an expression, the data may also undergo additional verification checks.

For a complete list of predefined expressions, see “Predefined Expression List” on page 48.

### Viewing Settings for Predefined Expressions

**NOTE:** Predefined expressions cannot be modified, copied, exported, or deleted.

**TASK**

1. Navigate to **Endpoint Protection > Configuration > Data Protection > DLP Settings Wizard > Data Identifier Management**.

2. Click the **Expression** tab.

3. Click the expression name.

4. View settings in the screen that opens.
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 CPM 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.

There are several criteria that you can choose from when creating expressions. An expression must satisfy your chosen criteria before CPM subjects it to a DLP policy. For details about the different criteria options, see “Criteria for Customized Expression” on page 10.

Criteria for Customized Expression

Table 1: Criteria Options for Customized Expressions

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
</table>
| None     | None | All - Names from US Census Bureau  
- Expression:
  [^\w]\([A-Z][a-z]\{1,12\}\{\s?,\s?\|\s\|\s([A-Z])\}\.\s\{A-Z}\{a-z}\{1,12\}\)\[^\w|
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Rule</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<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:</td>
</tr>
<tr>
<td></td>
<td>within the minimum and maximum limits.</td>
<td>•[^d]([0123678][d][8])[^d]</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Characters: 0123456789</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Minimum characters: 9</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Maximum characters: 9</td>
</tr>
<tr>
<td>Suffix</td>
<td>Suffix refers to the last segment of an expression. A suffix</td>
<td>All - Home Address</td>
</tr>
<tr>
<td></td>
<td>must include the characters you have specified and contain a</td>
<td>• Expression:</td>
</tr>
</tbody>
</table>
|                                | certain number of characters.                                       | • \D\(\d+\s[a-z.]+\s[a-z.]+\s[0,2]
|                                | In addition, the number of characters in the expression must be    | • [0-9a-z.\s.\s][0,30] \s[0,2]
|                                | within the minimum and maximum limits.                              | • \s\d\(\s\d\(4\)\)\d\-\d\-
|                                |                                                                     | • Suffix characters: 0123456789-                                      |
|                                |                                                                     | • Number of characters: 5                                               |
|                                |                                                                     | • Minimum characters in the expression: 25                             |
|                                |                                                                     | • Maximum characters in the expression: 80                             |
| Single-character separator    | An expression must have two segments separated by a character.      | All - Email Address                                                   |
|                                | The character must be 1 byte in length.                            | • Expression:                                                          |
|                                | In addition, the number of characters left of the separator must   | •[^w\.]\([w\.]\)[1,20]@[a-z0-9]\[2,20]\[\a-z\]2,5[a-z.]\([0,10]\)\-
|                                | be within the minimum and maximum limits.                         | • Separator: @                                                         |
|                                | The number of characters right of the separator must not           | • Minimum characters to the left: 3                                   |
|                                | exceed the maximum limit.                                          | • Maximum characters to the left: 15                                   |
|                                |                                                                     | • Maximum characters to the right: 30                                  |
Creating a Customized Expression

**TASK**

1. Navigate to **Endpoint Protection > Configuration > Data Protection** > **DLP Settings Wizard > Data Identifier Management**.
2. Click the **Expression** tab.
3. Click **Add**. A new screen displays.
4. Type a name for the expression. The name must not exceed 64 bytes in length and cannot contain the following characters:
   - > < * ^ | & ? /
5. Type a description that does not exceed 256 bytes in length.
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. Choose one of the following criteria and configure additional settings for the chosen criteria (see “Criteria for Customized Expression” on page 10):
   - None
   - Specific characters
   - Suffix
   - Single-character separator
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 detect any data wastes system resources and may impact performance.*

---

**Importing Customized Expressions**

Use this option if you have a properly-formatted .xml file containing the expressions. You can generate the file by exporting the expressions from either the CPM server you are currently accessing or from another CPM server.
1. Navigate to **Endpoint Protection > Configuration > Data Protection > DLP Settings Wizard > Data Identifier Management**.

2. Click the **Expression** tab.

3. Click **Import** and then locate the `.xml` file containing the expressions.

4. Click **Open**. A message appears, informing you if the import was successful. If an expression to be imported already exists in the list, it will be skipped.

---

**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 example, a software development company may want to limit the sharing of the company’s software installer to the R&D department, whose members are responsible for the development and testing of the software. In this case, the CPM administrator can create a policy that blocks the transmission of executable files that are 10 to 40MB in size to all departments except R&D.

By themselves, file attributes are poor identifiers of sensitive files. Continuing the example in this topic, third-party software installers shared by other departments will most likely be blocked. Trend Micro therefore recommends combining file attributes with other DLP data identifiers for a more targeted detection of sensitive files.

For a complete list of supported file types see “Supported File Types” on page 53.

---

**Creating a File Attribute List**

1. Navigate to **Endpoint Protection > Configurations > Data Protection > DLP Settings Wizard > Data Identifier Management**.

2. Click the **File Attribute** tab.

3. Click **Add**. A new screen displays.

4. Type a name for the file attribute list. The name must not exceed 64 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. CPM 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.scmd
     - *.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.

---

**Importing a File Attribute List**

Use this option if you have a properly-formatted .xml file containing the file attribute lists. You can generate the file by exporting the file attribute lists from either the CPM server you are currently accessing or from another CPM server.

**TASK**

1. Navigate to Endpoint Protection > Configurations > Data Protection > DLP Settings Wizard > Data Identifier Management.
2. Click the File Attribute tab.
3. Click Import and then locate the .xml file containing the file attribute lists.
4. Click Open. A message appears, informing you if the import was successful. If a file attribute list to be imported already exists and is older than the existing copy, it will be skipped.
Keywords

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. If you want to prevent the transmission of medical certificate files, you can use these keywords in a DLP policy and then configure CPM to block files containing these keywords.

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 codes, such as "END-IF", "END-READ", and "AT END".

You can use predefined and customized keyword lists. For details, see “Predefined Keyword Lists” on page 15 and “Customized Keyword Lists” on page 15.

Predefined Keyword Lists

CPM comes with a set of predefined keyword lists. These keyword lists cannot be modified, copied, exported, or deleted.

For details about the predefined lists in CPM, see “Predefined Keyword Lists” on page 55.

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 CPM subjects it to a DLP policy. Choose one of the following criteria for each keyword list:

- Any keyword
- All keywords
- All keywords within <x> characters
- Combined score for keywords exceeds threshold

For details regarding the criteria rules, see “Customized Keyword List Criteria” on page 16.
### Customized Keyword List Criteria

**Table 2: Criteria for a Keyword List**

<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 WEB, DISK, and USB and the number of characters you specified is 20. If CPM detects all keywords in the order DISK, WEB, and USB, the number of characters from the “D” (in DISK) to the “W” (in WEB) and from the “W” to the “U” (in USB) must be 20 characters or less.  
  - The following data matches the criteria: DISK####WEB############USB  
  - The following data does not match the criteria: DISK**********WEB****USB(23 characters between “D” and “W”)  
  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. |
| Combined score for keywords exceeds threshold | 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 “salary increase” 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. |
Creating a Keyword List

**TASK**

1. Navigate to **Endpoint Protection > Configurations > Data Protection > DLP Settings Wizard > Data Identifier Management.**
2. Click the **Keyword** tab.
3. Click **Add.** A new screen displays.
4. Type a name for the keyword list. The name must not exceed 64 bytes in length and cannot contain the following characters: > < * ^ | & ? /
5. Type a description that does not exceed 256 bytes in length.
6. 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**
7. To manually add keywords to the list:
   a. Type a keyword that is 3 to 40 bytes in length and specify whether it is case-sensitive.
   b. Click **Add.**
8. To add keywords by using the "import" option:
   
   **NOTE:** Use this option if you have a properly-formatted .csv file containing the keywords. You can generate the file by exporting the keywords from either the CPM server you are currently accessing or from another CPM server. For details about exporting keywords, see step 9.
   a. Click **Import** and then locate the .csv file containing the keywords.
   b. 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.
9. To delete keywords, select the keywords and click **Delete.**
10. To export keywords:
    
    **NOTE:** Use the "export" feature to back up the keywords or to import them to another CPM server. All keywords in the keyword list will be exported. It is not possible to export individual keywords.
    a. Click **Export.**
    b. Save the resulting .csv file to your preferred location.
11. Click **Save.**
Importing a Keyword List

Use this option if you have a properly-formatted .xml file containing the keyword lists. You can generate the file by exporting the keyword lists from either the CPM server you are currently accessing or from another CPM server.

**TASK**

1. Navigate to **Endpoint Protection > Configurations > Data Protection > DLP Settings Wizard > Data Identifier Management**.
2. Click the **Keyword** tab.
3. Click **Import** and then locate the .xml file containing the keyword lists.
4. Click **Open**. A message appears, informing you if the import was successful. If a keyword list to be imported already exists and is older than the existing copy, it will be skipped.

Data Loss Prevention Templates

This chapter introduces the available predefined templates and details how to create customized templates for use in Data Loss Prevention policies.

- “Data Loss Prevention Templates” on page 18
- “Predefined DLP Templates” on page 19
- “Customized DLP Templates” on page 19
- “Creating a Template” on page 20

Data Loss Prevention Templates

A DLP template combines DLP 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 DLP policy.

For example, a file must be a Microsoft Word file (file attribute) AND must contain certain 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 through printing so that
DATA LOSS PREVENTION TEMPLATES
PREDEFINED DLP TEMPLATES

the printed 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 DLP data identifiers. You can also use predefined templates. For details, see “Customized DLP Templates” on page 19 and “Predefined DLP Templates” on page 19.

NOTE: It is not possible to delete a template that is being used in a DLP policy. Remove the template from the policy before deleting it.

Predefined DLP Templates

CPM comes with the following set of predefined templates that you can use to comply with various regulatory standards. These templates cannot be modified, copied, exported, 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

For a detailed list on the purposes of these templates, and examples of data being protected, see “Predefined DLP Template List” on page 58.

Customized DLP 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.

For more information and examples on how condition statements and logical operators work, see “Condition Statements and Logical Operators” on page 19.

Condition Statements and Logical Operators

CPM 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.
See the examples in the following table.

**Table 3: Sample Condition Statements**

<table>
<thead>
<tr>
<th>Condition Statement</th>
<th>Interpretation and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>[Data Identifier 1] And [Data Identifier 2] Except [Data Identifier 3]</td>
<td>A file must satisfy [Data Identifier 1] and [Data Identifier 2] but not [Data Identifier 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>[Data Identifier 1] Or [Data Identifier 2]</td>
<td>A file must satisfy [Data Identifier 1] or [Data Identifier 2]. For example: A file must be [an Adobe PDF document] or [a Microsoft Word document].</td>
</tr>
<tr>
<td>Except [Data Identifier 1]</td>
<td>A file must not satisfy [Data Identifier 1]. For example: A file must not be [a multimedia file].</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.

**Creating a Template**

**TASK**

1. Navigate to **Endpoint Protection > Configurations > Data Protection > DLP Settings Wizard > Template Management**.
2. Click **Add**. A new screen displays.
3. Type a name for the template. The name must not exceed 64 bytes in length and cannot contain the following characters: > < * ^ | & ? \ /
4. Type a description that does not exceed 256 bytes in length.
5. Select data identifiers and then click the "add" icon. When selecting definitions:
   - Select multiple entries by pressing and holding the CTRL key and then selecting the data identifiers.
   - Use the search feature if you have a specific definition in mind. You can type the full or partial name of the data identifier.
   - Each template can contain a maximum of 30 data identifiers.

6. To create a new expression, click **Expressions** and then click **Add new expression**. In the screen that appears, configure settings for the expression.

7. To create a new file attribute list, click **File attributes** and then click **Add new file attribute**. In the screen that appears, configure settings for the file attribute list.

8. To create a new keyword list, click **Keywords** and then click **Add new keyword**. In the screen that appears, configure settings for the keyword list.

9. If you selected an expression, type the number of occurrences, which is the number of times an expression must occur before CPM subjects it to a DLP policy.

10. Choose a logical operator for each definition.
    
    **NOTE:** Use logical operators carefully when configuring condition statements. Incorrect usage leads to an erroneous condition statement that will likely produce unexpected results. For examples of correct usage, see “Condition Statements and Logical Operators” on page 19.

11. To remove a data identifier from the list of selected identifiers, click the trash bin icon.

12. Below **Preview**, check the condition statement and make changes if this is not your intended statement.

13. Click **Save**.

---

**Importing Templates**

Use this option if you have a properly-formatted `.xml` file containing the templates. You can generate the file by exporting the templates from either the CPM server you are currently accessing or from another CPM server.

**TASK**

1. Navigate to **Endpoint Protection > Configurations > Data Protection > DLP Settings Wizard > Template Management.**
2. Click **Import** and then locate the .xml file containing the templates.

3. Click **Open**. A message appears, informing you if the import was successful. If a template to be imported already exists and is older than the existing copy, it will be skipped.

---

### Data Loss Prevention Policies

This chapter explains how to configure and deploy Data Loss Prevention policies on endpoints.

- “Data Loss Prevention Policies” on page 22
- “DLP Channels” on page 23
- “Data Loss Prevention Actions” on page 32
- “Configuring Data Loss Prevention Policies” on page 33

#### Data Loss Prevention Policies

CPM evaluates a file or data against a set of rules defined in DLP policies. Policies determine files or data that must be protected from unauthorized transmission and the action that CPM performs when it detects transmission.

**NOTE:** *Data transmissions between the CPM server and its clients are not monitored.*

You can configure policies for internal and external clients. CPM administrators typically configure a stricter policy for external clients.

You can enforce specific policies to client groups or individual clients. You can also enforce a single policy to all clients.

After you deploy the policies, clients use the location criteria you have set in the Location Property Wizard (see the *Core Protection Module Administrator’s Guide*, Chapter 9 for more details) to determine their location and the policy to apply. Clients switch policies each time the location changes.
Policy Configuration

Define DLP policies by configuring the following settings:

**Table 4: Settings that Define a DLP Policy**

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Identifiers</td>
<td>CPM uses data identifiers to identify sensitive information. Data identifiers include expressions, file attributes, and keywords.</td>
</tr>
<tr>
<td>Template</td>
<td>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 will be subject to a DLP policy. CPM comes with a set of predefined templates and allows you to create customized templates. A DLP policy can contain one or several templates. CPM uses the first-match rule when checking templates. This means that if a file or data matches the data identifiers on a template, CPM will no longer check the other templates.</td>
</tr>
<tr>
<td>Channel</td>
<td>Channels are entities that transmit sensitive information. CPM supports popular transmission channels, such as email, removable storage devices, and instant messaging applications.</td>
</tr>
<tr>
<td>Action</td>
<td>CPM performs one or several actions when it detects an attempt to transmit sensitive information through any of the channels.</td>
</tr>
</tbody>
</table>

DLP Channels

Users can transmit sensitive information through various channels. CPM can monitor the following channels:

- **Network channels**: Sensitive information is transmitted using network protocols, such as HTTP and FTP.
- **System and application channels**: Sensitive information is transmitted using a local computer’s applications and peripherals.

Network Channels

CPM can monitor data transmission through the following network channels:

- Email clients
- FTP
• HTTP and HTTPS
• IM Applications
• SMB protocol
• Webmail

To determine data transmissions to monitor, CPM checks the transmission scope, which you need to configure. Depending on the scope that you selected, CPM will monitor all data transmissions or only transmissions outside the Local Area Network (LAN). For details about transmission scope, see “Transmission Scope and Targets for Network Channels” on page 27.

Email Clients

CPM monitors email transmitted through various email clients. CPM checks the email’s subject, body, and attachments for data identifiers. For a list of supported email clients, see:


Monitoring occurs when a user attempts to send the email. If the email contains data identifiers, CPM will either allow or block the email.

You can define monitored and non-monitored internal email domains.

• Monitored email domains: When CPM detects email transmitted to a monitored domain, it checks the action for the policy. Depending on the action, the transmission is allowed or blocked.

  NOTE: If you select email clients as a monitored channel, an email must match a policy for it to be monitored. In contrast, an email sent to monitored email domains is automatically monitored, even if it does not match a policy.

• Non-monitored email domains: CPM immediately allows the transmission of emails sent to non-monitored domains.

  NOTE: Data transmissions to non-monitored email domains and to monitored email domains where “Monitor” is the action are similar in that the transmission is allowed. The only difference is that for non-monitored email domains, CPM does not log the transmission, whereas for monitored email domains, the transmission is always logged.

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
For email messages sent through the SMTP protocol, CPM checks if the target SMTP server is on the following lists:

1) Monitored targets
2) Non-monitored targets

NOTE: For details about monitored and non-monitored targets, see “Defining Monitored and Non-monitored Targets” on page 28.

3) Monitored email domains
4) Non-monitored email domains

This means that if an email is sent to an SMTP server on the monitored targets list, the email is monitored. If the SMTP server is not on the monitored targets list, CPM checks the other lists.

For emails sent through other protocols, CPM only checks the following lists:

1) Monitored email domains
2) Non-monitored email domains

FTP

When CPM detects that an FTP client is attempting to upload files to an FTP server, it checks for the presence of data identifiers in the files. No file has been uploaded at this point. Depending on the DLP policy, CPM will allow or block the upload.

When you configure a policy that blocks file uploads, remember the following:

• When CPM blocks an upload, some FTP clients will try to re-upload the files. In this case, CPM terminates the FTP client to prevent the re-upload. Users do not receive a notification after the FTP client terminates. Inform them of this situation when you roll out your DLP policies.

• If a file to be uploaded will overwrite a file on the FTP server, the file on the FTP server may be deleted.

For a list of supported FTP clients, see:

HTTP and HTTPS

CPM monitors data to be transmitted through HTTP and HTTPS. For HTTPS, CPM checks the data before it is encrypted and transmitted.

For a list of supported web browsers and applications, see:
IM Applications

CPM monitors messages and files that users send through instant messaging (IM) applications. Messages and files that users receive are not monitored.

For a list of supported IM applications, see:

When CPM blocks a message or file sent through AOL Instant Messenger, MSN, Windows Messenger, or Windows Live Messenger, it also terminates the application. If CPM does not do this, the application will become unresponsive and users will be forced to terminate the application anyway. Users do not receive a notification after the application terminates. Inform them of this situation when you roll out your DLP policies.

SMB Protocol

CPM monitors data transmissions through the Server Message Block (SMB) protocol, which facilitates shared file access. When another user attempts to copy or read a user’s shared file, CPM checks if the file is or contains a data identifier and then allows or blocks the operation.

NOTE: The Device Control action has a higher priority than the DLP action. For example, if Device Control does not allow files on mapped network drives to be moved, transmission of sensitive data does not proceed even if DLP allows it. For details on Device Control actions, see “Permissions for Storage Devices” on page 35.

For a list of applications that CPM monitors for shared file access, see:

Webmail

Web-based email services transmit data through HTTP. If CPM detects outgoing data from supported services, it checks the data for the presence of data identifiers.

For a list of supported web-based email services, see:
Transmission Scope and Targets for Network Channels

Transmission scope and targets define data transmissions on network channels that CPM must monitor. For transmissions that should be monitored, CPM checks for the presence of data identifiers before allowing or blocking the transmission. For transmissions that should not be monitored, CPM does not check for the presence of data identifiers and immediately allows the transmission.

Transmission Scope: All Transmissions

CPM monitors data transmitted outside the host computer.

NOTE: Trend Micro recommends choosing this scope for external clients.

If you do not want to monitor data transmissions to certain targets outside the host computer, define the following:

• **Non-monitored targets**: CPM does not monitor data transmitted to these targets.

  NOTE: Data transmissions to non-monitored targets and to monitored targets where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored targets, CPM does not log the transmission, whereas for monitored targets, the transmission is always logged.

• **Monitored targets**: These are specific targets within the non-monitored targets that should be monitored. Monitored targets are:
  
  – Optional if you defined non-monitored targets.
  
  – Not configurable if you did not define non-monitored targets.

For example:

The following IP addresses are assigned to your company’s Legal Department:

• 10.201.168.1 to 10.201.168.25

You are creating a policy that monitors the transmission of Employment Certificates to all employees except the Legal Department’s full time staff. To do this, you would select **All transmissions** as the transmission scope and then:

**Option 1:**

1) Add 10.201.168.1-10.201.168.25 to the non-monitored targets.

2) Add the IP addresses of the Legal Department’s part-time staff to the monitored targets. Assume that there are 3 IP addresses, 10.201.168.21-10.201.168.23.

**Option 2:**
Add the IP addresses of the Legal Department’s full time staff to the non-monitored targets:

- 10.201.168.1-10.201.168.20
- 10.201.168.24-10.201.168.25

For guidelines on defining monitored and non-monitored targets, see “Defining Monitored and Non-monitored Targets” on page 28.

**Transmission Scope: Only Transmissions Outside the Local Area Network**

CPM monitors data transmitted to any target outside the Local Area Network (LAN).

*NOTE:* Trend Micro recommends choosing this scope for internal clients.

"Network" refers to the company or local network. This includes the current network (IP address of the endpoint and netmask) and the following standard private IP addresses:

- Class A: 10.0.0.0 to 10.255.255.255
- Class B: 172.16.0.0 to 172.31.255.255
- Class C: 192.168.0.0 to 192.168.255.255

If you select this transmission scope, you can define the following:

- **Non-monitored targets:** Define targets outside the LAN that you consider safe and therefore should not be monitored.

*NOTE:* Data transmissions to non-monitored targets and to monitored targets where "Monitor" is the action are similar in that the transmission is allowed. The only difference is that for non-monitored targets, CPM does not log the transmission, whereas for monitored targets, the transmission is always logged.

- **Monitored targets:** Define targets within the LAN that you want to monitor.

For guidelines on defining monitored and non-monitored targets, see “Defining Monitored and Non-monitored Targets” on page 28.

**Defining Monitored and Non-monitored Targets**

Follow these guidelines when defining monitored and non-monitored targets:

1) Define each target by:

- IP address or address range
• Host name
• FQDN
• Network address and subnet mask, such as 10.1.1.1/32

NOTE: For the subnet mask, CPM only supports a classless inter-domain routing (CIDR) type port. That means that you can only type a number like 32 instead of 255.255.255.0.

2) 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.

3) You can also include port ranges. To include all ports, ignore the port range.

Below are some 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

4) Separate targets with commas.

Resolving Conflicts

If settings for transmission scope, monitored targets, and non-monitored targets conflict, CPM recognizes the following priorities, in order of highest priority to lowest:
• Monitored targets
• Non-monitored targets
• Transmission scope

System and Application Channels

CPM can monitor the following system and application channels:
• Data recorders (CD/DVD)
• Peer-to-peer applications
• Printer
DATA LOSS PREVENTION POLICIES

DLP CHANNELS

• Removable storage
• Synchronization software (ActiveSync)
• Windows clipboard

Data Recorders (CD/DVD)

CPM monitors data recorded to a CD or DVD. For a list of supported data recording devices and software, see:


When CPM detects a "burn" command initiated on any of the supported devices or software and the action is Pass, data recording proceeds. If the action is Block, CPM checks if any of the files to be recorded is or contains a data identifier. If CPM detects at least one data identifier, all files—including those that are not, or do not contain, data identifiers—will not be recorded. CPM may also prevent the CD or DVD from ejecting. If this issue occurs, instruct users to restart the software process or reset the device.

CPM implements additional CD/DVD recording rules:

• To reduce false positives, CPM does not monitor the following files:

  .bud  .dll  .gif  .gpd  .htm  .ico  .ini
  .jpg  .lnk  .sys  .ttf  .url  .xml

• Two file types used by Roxio data recorders (*.png and *.skn) are not monitored to increase performance.

• CPM does not monitor files in the following directories:

  */autoexec.bat  */Windows
  ../Application Data  ../Cookies
  ../Local Settings  ../ProgramData
  ../Program Files  ../Users/*/AppData
  ../WINNT

• ISO images created by the devices and software are not monitored.
Peer-to-Peer Applications

CPM monitors files that users share through peer-to-peer applications.

For a list of supported peer-to-peer applications, see:

Printer

CPM monitors printer operations initiated from various applications.

CPM does not block printer operations on new files that have not been saved because printing information has only been stored in the memory at this point.

For a list of supported applications that can initiate printer operations, see:

Removable Storage

CPM monitors data transmissions to or within removable storage devices.

Activities related to data transmission include:

- Creation of a file within the device
- Copying of a file from the host machine to the device
- Closing of a modified file within the device
- Modifying of file information (such as the file’s extension) within the device

When a file to be transmitted contains a data identifier, CPM either blocks or allows the transmission.

**NOTE:** The Device Control action has a higher priority than the DLP action. For example, If Device Control does not allow copying of files to a removable storage device, transmission of sensitive information does not proceed even if DLP allows it. For details on Device Control actions, see “Permissions for Storage Devices” on page 35.

For a list of supported removable storage devices and applications that facilitate data transmission activities, see:


The handling of file transmission to a removable storage device is a straightforward process. For example, a user who creates a file from Microsoft Word may want to save the file to an SD card (it does not matter which file type the user
saves the file as). If the file contains a data identifier that should not be transmitted, CPM prevents the file from being saved.

For file transmission within the device, CPM first backs up the file (if its size is 75MB or less) to %WINDIR%\system32\dgagent\temp before processing it. CPM removes the backup file if it allowed the file transmission. If CPM blocked the transmission, it is possible that the file may have been deleted in the process. In this case, CPM will copy the backup file to the folder containing the original file.

CPM allows you to define non-monitored devices. CPM always allows data transmissions to or within these devices. Identify devices by their vendors and optionally provide the device models and serial IDs.

**Synchronization Software (ActiveSync)**

CPM monitors data transmitted to a mobile device through synchronization software.

For a list of supported synchronization software, see:


If the data has a source IP address of 127.0.0.1 and is sent through either port 990 or 5678 (the ports used for synchronization), CPM checks if the data is a data identifier before allowing or blocking its transmission.

When CPM blocks a file transmitted on port 990, a file of the same name containing malformed characters may still be created at the destination folder on the mobile device. This is because parts of the file have been copied to the device before CPM blocked the transmission.

**Data Loss Prevention Actions**

When CPM detects the transmission of data identifiers, it checks the DLP policy for the detected data identifiers and performs the action configured for the policy.

The following table lists the Data Loss Prevention actions.

**Table 5:** Data Loss Prevention Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Actions</td>
<td></td>
</tr>
</tbody>
</table>
Decompression Rules

Files contained in compressed files can be scanned for sensitive information. To determine the files to scan, CPM subjects a compressed file to the following rules:

- Total number of embedded layers in compressed file exceeds __ (1-20)
- Total number of files in compressed file exceeds __ (1-2000)

Configuring Data Loss Prevention Policies

You can start to create Data Loss Prevention policies after you have configured data identifiers and organized them in templates.

In addition to data identifiers and templates, you need to configure channels and actions when creating a policy.

**TASK**

1. Navigate to **Endpoint Protection > Core Protection Module > Configuration > Data Protection > DLP Settings Wizard > Policy Management**.
2. Click Add. A new screen appears.

3. Type a name for the template. The name must not exceed 64 bytes in length and cannot contain the following characters: > < * ^ | & ? \ /

4. Search for and select an available template. Click Add > to include the template to the policy.

5. Select the network channels to monitor. For more information on network channels, see “Network Channels” on page 23.
   - Click Exceptions next to Email clients to configure Non-monitored Email Domains.
   - Configure the Transmission Scope to include Only transmissions outside the Local Area Network to improve scan performance.
   - Expand the Exceptions section to configure specific Non-monitored Targets. Identify non-monitored endpoints by IP address, host name, FQDN, or network address and subnet mask.

6. Select the system and application channels to monitor. For more information on system and application channels, see “System and Application Channels” on page 29.
   - Click Exceptions next to Removable storage to configure Non-monitored Devices. Add non-monitored removable storage devices, identifying them by their vendors. The device model and serial ID are optional.

7. Select the action that CPM takes upon identifying a policy violation. For more information on the available actions, see “Data Loss Prevention Actions” on page 32.

8. Modify the default Decompression Settings as necessary. For more information on decompression settings, see “Decompression Rules” on page 33.

9. Click Create Fixlet and Save.

10. Type your Private Key Password and click OK.

11. Below Actions, click the hyperlink to open the Take Action window.

12. In the Target tab, click All computers with the property values selected in the tree below and then choose a property that will include all the computers you want to deploy this Action to.

13. When finished identifying the computers you want to include in the exception, click OK. At the prompt, type your private key password and click OK.

14. The Action | Summary window that opens, monitor the "Status" of the Action to confirm that it is "Running" and then "Completed".
Device Control

This chapter outlines the Device Control permission types and how to manage endpoint access to external devices.

- “Permissions for Storage Devices” on page 35
- “Advanced Permissions for Storage Devices” on page 36
- “Managing Access to External Devices” on page 38

Permissions for Storage Devices

Device Control permissions for storage devices are used when you:

- Allow access to USB storage devices, CD/DVD, floppy disks, and network drives. You can grant full access to these devices or limit the level of access.
- Configure the list of approved USB storage devices. Device Control allows you to block access to all USB storage devices, except those that have been added to the list of approved devices. You can grant full access to the approved devices or limit the level of access.

The following table lists the permissions:

**Table 6: Device Control Permissions for Storage Devices**

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Files on the Device</th>
<th>Incoming Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full access</td>
<td>Permitted operations: Copy, Move, Open, Save, Delete, Execute</td>
<td>Permitted operations: Save, Move, Copy This means that a file can be saved, moved, and copied to the device.</td>
</tr>
<tr>
<td>Modify</td>
<td>Permitted operations: Copy, Move, Open, Save, Delete Prohibited operations: Execute</td>
<td>Permitted operations: Save, Move, Copy</td>
</tr>
<tr>
<td>Read and execute</td>
<td>Permitted operations: Copy, Open, Execute Prohibited operations: Save, Move, Delete</td>
<td>Prohibited operations: Save, Move, Copy</td>
</tr>
</tbody>
</table>
The file-based scanning function in CPM complements and may override the device permissions. For example, if the permission allows a file to be opened but CPM detects that the file is infected with malware, a specific scan action will be performed on the file to eliminate the malware. If the scan action is Clean, the file opens after it is cleaned. However, if the scan action is Delete, the file is deleted.

### Advanced Permissions for Storage Devices

Advanced permissions apply when you grant limited permissions to storage devices. The permission can be any of the following:

- Modify
- Read and execute
- Read
- List device content only

You can keep the permissions limited but grant advanced permissions to certain programs on the storage devices and on the local computer.

To define programs, configure the following program lists:

<table>
<thead>
<tr>
<th>Permissions</th>
<th>Files on the Device</th>
<th>Incoming Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read</td>
<td>Permitted operations: Copy, Open Prohibited operations: Save, Move, Delete, Execute</td>
<td>Prohibited operations: Save, Move, Copy</td>
</tr>
<tr>
<td>List device content only</td>
<td>Prohibited operations: All operations The device and the files it contains are visible to the user (for example, from Windows Explorer).</td>
<td>Prohibited operations: Save, Move, Copy</td>
</tr>
<tr>
<td>Block</td>
<td>Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Windows Explorer).</td>
<td>Prohibited operations: Save, Move, Copy</td>
</tr>
</tbody>
</table>
Table 7: Program Lists

<table>
<thead>
<tr>
<th>Program List</th>
<th>Description</th>
<th>Valid Inputs</th>
</tr>
</thead>
</table>
| 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. | Program path and name  
For details, see "Specifying a Program Path and Name" on page 38. |
| 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. | Program path and name or Digital Signature Provider  
For details, see "Specifying a Program Path and Name" on page 38 or "Specifying a Digital Signature Provider" on page 37. |

There are instances when you need to add a program to both lists. Consider the data lock feature in a USB storage device, which, if enabled, prompts users for a valid user name and password before the device can be unlocked. The data lock feature uses a program on the device called "Password.exe", which must be allowed to execute so that users can unlock the device successfully. "Password.exe" must also have read and write access to the device so that users can change the user name or password.

Each program list on the user interface can contain up to 200 programs.

**Specifying a Digital Signature Provider**

Specify a Digital Signature Provider if you trust programs issued by the provider. For example, type Microsoft Corporation or Trend Micro, Inc. You can obtain the Digital Signature Provider by checking the properties of a program (for example, by right-clicking the program and selecting **Properties**).
Specifying a Program Path and Name

A program path and name should have a maximum of 259 characters and must only contain alphanumeric characters (A-Z, a-z, 0-9). It is not possible to specify only the program name.

You can use wildcards in place of drive letters and program names. Use a question mark (?) to represent single-character data, such as a drive letter. Use an asterisk (*) to represent multi-character data, such as a program name.

For more information on the correct usage of wildcards, see “Wildcard Usage in Device Control” on page 59.

NOTE: Wildcards cannot be used to represent folder names. The exact name of a folder must be specified.

Permissions for Non-storage Devices

You can allow or block access to non-storage devices. There are no granular or advanced permissions for these devices.

Managing Access to External Devices

<table>
<thead>
<tr>
<th>TASK</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Navigate to <strong>Endpoint Protection &gt; Core Protection Module &gt; Configuration &gt; Device Control &gt; Device Control Settings</strong>.</td>
</tr>
<tr>
<td>2. Select <strong>Enable Device Control</strong>.</td>
</tr>
<tr>
<td>3. Choose to allow or block the AutoRun function (autorun.inf) on USB storage devices.</td>
</tr>
<tr>
<td>4. Configure settings for storage devices.</td>
</tr>
<tr>
<td>a Select a permission for each storage device. For details about permissions, see “Permissions for Storage Devices” on page 35.</td>
</tr>
<tr>
<td>b Configure advanced permissions and notifications if the permission for a storage device is any of the following: <strong>Modify</strong>, <strong>Read and execute</strong>, <strong>Read</strong>, or <strong>List device content only</strong>. See “Configuring Advanced Permissions” on page 1.</td>
</tr>
<tr>
<td>c If the permission for USB storage devices is <strong>Block</strong>, configure a list of approved devices. Users can access these devices and you can control the level of access using permissions. See “Configuring an Approved List of USB Devices” on page 2.</td>
</tr>
<tr>
<td>5. For each non-storage device, select <strong>Allow</strong> or <strong>Block</strong>.</td>
</tr>
</tbody>
</table>
6. Click **Create a Task to deploy the settings**.
7. Click **OK**. At the prompt, type your private key password and click **OK**.
8. Below Actions, click the hyperlink to open the Take Action window.
9. In the Target tab, click **Specific computers selected in the list below** and then choose the computers you want to deploy this Action to.
10. When finished identifying the computers you want to include in the exception, click **OK**. At the prompt, type your private key password and click **OK**.
11. The Action | Summary window that opens, monitor the "Status" of the Action to confirm that it is "Running" and then "Completed".

---

**Configuring Advanced Permissions**

Although you can configure advanced permissions and notifications for a specific storage device on the user interface, the permissions and notifications are actually applied to all storage devices. This means that when you click **Advanced permissions and notifications** for CD/DVD, you are actually defining permissions and notifications for all storage devices.

**NOTE:** For details about advanced permissions and how to correctly define programs with advanced permissions, see “Advanced Permissions for Storage Devices” on page 36.

---

**TASK**

1. Click **Advanced permissions and notifications**. A new screen opens.
2. Below **Programs with read and write access to storage devices**, type a program path and file name and then click **Add**. Digital Signature Provider is not accepted.
3. Below **Programs on storage devices that are allowed to execute**, type the program path and name or the Digital Signature Provider and then click **Add**.
4. Select **Display a notification message on the client computer when Core Protection Module detects unauthorized device access**.
5. Click **OK**.
Configuring an Approved List of USB Devices

**TASK**

1. Click **Approved devices**.
2. Click **Add new devices**.
3. Type the device vendor.
4. Type the device model and serial ID.
5. Select the permission for the device. For details about permissions, see “Permissions for Storage Devices” on page 35.
6. To add more devices, click the + icon.
7. Click **OK**.

**NOTE:** Use the Device List Tool to query devices connected to endpoints. The tool provides the device vendor, model, and serial ID for each device. For details, see http://docs.trendmicro.com/en-us/enterprise/core-protection-module.aspx.

Data Protection Analyses and Reports

This chapter highlights the available Data Protection analyses and the information that the analyses display.

- “Data Protection Analyses” on page 41
- “Data Protection - Endpoint Information Analysis” on page 41
- “Data Protection - Detected Data Loss Prevention Violation Information Analysis” on page 42
- “Data Protection - Data Loss Prevention Policy Information Analysis” on page 43
- “Data Protection - Detected Device Control Violation Information Analysis” on page 44
- “Data Protection - Device Control for Non-Storage Devices Information Analysis” on page 44
- “Data Protection - Device Control for Storage Devices Information Analysis” on page 45
- “Data Loss Prevention Report” on page 47
Data Protection Analyses

Data Protection allows you to view detailed information about an endpoint or group of endpoints protected by DLP policies and Device Control Tasks. The following table outlines the different Data Protection analyses available in CPM.

Table 8: Available Analyses by Module

<table>
<thead>
<tr>
<th>Module</th>
<th>Available Analyses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection</td>
<td>• Data Protection - Endpoint Information</td>
</tr>
<tr>
<td>Data Loss Prevention</td>
<td>• Data Protection - Detected Data Loss Prevention Violation Information</td>
</tr>
<tr>
<td></td>
<td>• Data Protection - Data Loss Prevention Policy Information</td>
</tr>
<tr>
<td>Device Control</td>
<td>• Data Protection - Detected Device Control Violation Information</td>
</tr>
<tr>
<td></td>
<td>• Data Protection - Device Control for Non-Storage Devices Information</td>
</tr>
<tr>
<td></td>
<td>• Data Protection - Device Control for Storage Devices Information</td>
</tr>
</tbody>
</table>

Data Protection - Endpoint Information Analysis

This analysis contains details about the current Data Protection configuration of endpoints in your deployment.

To view this analysis:

1) Navigate to Endpoint Protection > Core Protection Module > Analyses > Data Protection > Data Protection - Endpoint Information.
2) Click the Applicable Computers tab. Double-click an endpoint to examine its analysis.
3) Scroll down to view the Data Protection - Endpoint Information pane.

The following table details the information available in this analysis.
Table 9: Data Protection - Endpoint Information Analysis

<table>
<thead>
<tr>
<th>Item</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Core Service Status</td>
<td>The following values indicate the current core service status:</td>
</tr>
<tr>
<td></td>
<td>• 0 = No agent</td>
</tr>
<tr>
<td></td>
<td>• 1 = Running</td>
</tr>
<tr>
<td></td>
<td>• 2 = Stopped</td>
</tr>
<tr>
<td></td>
<td>• 3 = Trend Micro Data Leakage Prevention is installed.</td>
</tr>
<tr>
<td></td>
<td>• 4 = Reboot needed</td>
</tr>
<tr>
<td></td>
<td>• 5 = x64 not supported</td>
</tr>
<tr>
<td></td>
<td>• 6 = Cannot install</td>
</tr>
<tr>
<td>Core Service Version</td>
<td>The current version of Data Protection.</td>
</tr>
<tr>
<td>Device Control Enabled</td>
<td>True/False</td>
</tr>
<tr>
<td>Data Loss Prevention Enabled</td>
<td>True/False</td>
</tr>
<tr>
<td>Service Running Status</td>
<td>True/False</td>
</tr>
</tbody>
</table>

Data Protection - Detected Data Loss Prevention Violation Information Analysis

This analysis contains details about the detected number of Data Loss Prevention violations on the selected endpoint.

To view this analysis:

1) Navigate to Endpoint Protection > Core Protection Module > Analyses > Data Protection > Data Protection - Detected Data Loss Prevention Violation Information.

2) Click the Applicable Computers tab. Double-click an endpoint to examine its analysis.

3) Scroll down to view the Data Protection - Detected Data Loss Prevention Violation Information pane.

The following table details the information available in this analysis.

Table 10: Data Protection - Detected Data Loss Prevention Violation Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Detected Data Loss Prevention Violation</td>
<td>The log content regarding policy violations detected by DLP policies on the selected endpoint.</td>
</tr>
</tbody>
</table>
NOTE: Change the Maximum Data Loss Prevention Violation Report Count by navigating to **Endpoint Protection > Core Protection Module > Common Tasks** and select **Data Protection - Set Maximum Data Loss Prevention Count**. The valid values are between 0 - 2147483647.

### Data Protection - Data Loss Prevention Policy Information Analysis

This analysis contains details about the current DLP policy associated with the selected endpoint.

To view this analysis:

1) Navigate to **Endpoint Protection > Core Protection Module > Analyses > Data Protection > Data Protection - Data Loss Prevention Policy Information**.

2) Click the **Applicable Computers** tab. Double-click an endpoint to examine its analysis.

3) Scroll down to view the **Data Protection - Data Loss Prevention Information** pane.

The following table details the information available in this analysis.

**Table 11: Data Protection - Data Loss Prevention Policy Information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Channel</td>
<td>Displays the current channels that the DLP policy monitors.</td>
</tr>
<tr>
<td>Email Exception</td>
<td>Displays any email exceptions in the current policy.</td>
</tr>
<tr>
<td>IP Exception</td>
<td>Displays any IP exceptions in the current policy.</td>
</tr>
<tr>
<td>Maximum Compression Layer</td>
<td>Displays the maximum number of compressed layers that the policy scans within a compressed file.</td>
</tr>
<tr>
<td>Policy Name</td>
<td>The name of the policy associated with the selected endpoint.</td>
</tr>
<tr>
<td>Policy Timestamp</td>
<td>The time that the policy was created. Calculated using the number of seconds passed since January 1, 1970.</td>
</tr>
</tbody>
</table>
This analysis contains details about the detected number of Device Control violations on the selected endpoint.

To view this analysis:

1) Navigate to Endpoint Protection > Core Protection Module > Analyses > Data Protection > Data Protection - Detected Device Control Violation Information.

2) Click the Applicable Computers tab. Double-click an endpoint to examine its analysis.

3) Scroll down to view the Data Protection - Detected Device Control Violation Information pane.

The following table details the information available in this analysis.

<table>
<thead>
<tr>
<th>Item</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template List</td>
<td>Displays the templates that the policy implements.</td>
</tr>
<tr>
<td>USB Exception</td>
<td>Displays any USB exceptions in the current policy.</td>
</tr>
</tbody>
</table>

**Data Protection - Device Control for Non-Storage Devices Information Analysis**

This analysis contains details about the current Device Control permissions for non-storage devices on the selected endpoint.

**NOTE:** Change the Maximum Device Control Violation Report Count by navigating to Endpoint Protection > Core Protection Module > Common Tasks and select Data Protection - Set Maximum Device Control Violation Report Count. The valid values are between 0 - 2147483647.
To view this analysis:

1) **Navigate to Endpoint Protection > Core Protection Module > Analyses > Data Protection > Data Protection - Device Control for Non-Storage Devices Information.**

2) Click the **Applicable Computers** tab. Double-click an endpoint to examine its analysis.

3) Scroll down to view the **Data Protection - Device Control for Non-Storage Devices Information** pane.

The following table details the information available in this analysis.

**Table 13: Data Protection - Device Control for Non-Storage Devices Information**

<table>
<thead>
<tr>
<th>Item</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>COM and LPT ports permission</td>
<td>Allow/Block</td>
</tr>
<tr>
<td>IEEE 1394 interface permission</td>
<td>Allow/Block</td>
</tr>
<tr>
<td>Imaging devices permission</td>
<td>Allow/Block</td>
</tr>
<tr>
<td>Infrared devices permission</td>
<td>Allow/Block</td>
</tr>
<tr>
<td>Modems permission</td>
<td>Allow/Block</td>
</tr>
<tr>
<td>PCMCIA cards permission</td>
<td>Allow/Block</td>
</tr>
<tr>
<td>Print screen key permission</td>
<td>Allow/Block</td>
</tr>
</tbody>
</table>

---

**Data Protection - Device Control for Storage Devices Information Analysis**

This analysis contains details about the current Device Control permissions for storage devices on the selected endpoint.

To view this analysis:

1) **Navigate to Endpoint Protection > Core Protection Module > Analyses > Data Protection > Data Protection - Device Control for Storage Devices Information.**

2) Click the **Applicable Computers** tab. Double-click an endpoint to examine its analysis.

3) Scroll down to view the **Data Protection - Device Control for Storage Devices Information** pane.

The following table details the information available in this analysis.
Table 14: Data Protection - Device Control for Storage Devices Information

<table>
<thead>
<tr>
<th>Item</th>
<th>Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved USB devices (Vendor, Model, Serial ID)</td>
<td>Allow/Block</td>
</tr>
<tr>
<td>Approved USB devices permission</td>
<td>Full access, Modify, Read and execute, Read, List device content only, Block</td>
</tr>
<tr>
<td>Block AutoRun on USB devices</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>CD/DVD permission</td>
<td>Full access, Modify, Read and execute, Read, List device content only, Block</td>
</tr>
<tr>
<td>Exception program 1 on devices</td>
<td>Displays the first exception program on devices.</td>
</tr>
<tr>
<td>Exception program 1 on endpoints</td>
<td>Displays the first exception program on the endpoint.</td>
</tr>
<tr>
<td>Exception program 2 on devices</td>
<td>Displays the second exception program on devices.</td>
</tr>
<tr>
<td>Exception program 2 on endpoints</td>
<td>Displays the second exception program on the endpoint.</td>
</tr>
<tr>
<td>Exception program 3 on devices</td>
<td>Displays the third exception program on devices.</td>
</tr>
<tr>
<td>Exception program 3 on endpoints</td>
<td>Displays the third exception program on the endpoint.</td>
</tr>
<tr>
<td>Exception program 4 on devices</td>
<td>Displays the fourth exception program on devices.</td>
</tr>
<tr>
<td>Exception program 4 on endpoints</td>
<td>Displays the fourth exception program on the endpoint.</td>
</tr>
<tr>
<td>Exception program 5 on devices</td>
<td>Displays the fifth exception program on devices.</td>
</tr>
<tr>
<td>Exception program 5 on endpoints</td>
<td>Displays the fifth exception program on the endpoint.</td>
</tr>
<tr>
<td>Floppy disks permission</td>
<td>Full access, Modify, Read and execute, Read, List device content only, Block</td>
</tr>
<tr>
<td>Network devices permission</td>
<td>Full access, Modify, Read and execute, Read, List device content only, Block</td>
</tr>
<tr>
<td>Notification enabled</td>
<td>Enabled/Disabled</td>
</tr>
<tr>
<td>Number of approved devices when blocking USB storage</td>
<td>Displays the number of approved devices when blocking USB storage.</td>
</tr>
</tbody>
</table>
Data Loss Prevention Report

The DLP Detections report lists the most recent DLP policy violations detected by CPM.

Access this report by navigating to Endpoint Protection > Core Protection Module > Reports > Threat Detection and clicking the DLP Detections tab.

This report provides the following information.

- **Date/Time**: The date and time that the violation occurred.
- **Computer**: The computer from which the violation originated.
- **Process**: The system process where CPM detected the violation.
- **Policy**: The DLP policy which triggered the violation.
- **Channel**: The channel where the violation occurred.
- **Action**: The action that CPM performed on the violation.
- **Template**: The template which triggered the violation.
- **User Name**: The name of the user logged onto the computer from which the violation originated.
- **Description**: Details concerning the information that triggered the violation.

### Device Control Detections Report

The Device Control Detections report lists the most recent Device Control violations detected by CPM.

Access this report by navigating to Endpoint Protection > Core Protection Module > Reports > Threat Detection and clicking the Device Control Detections tab.
This report provides the following information.

- **Date/Time**: The date and time that the violation occurred.
- **Computer**: The computer from which the violation originated.
- **Accessed By**: The name of the user logged onto the computer from which the violation originated.
- **Target**: The location on the device that the user tried to access.
- **Device**: The device that the user tried to access.
- **Permission**: The permission level granted to the device.

### Predefined Expression List

The following table lists the predefined expressions and the additional verification tasks that CPM performs, if any.

**Table 15: Predefined Expression List Details**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Additional Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>All - Credit Card Number</td>
<td>Credit Card Number</td>
<td>CPM checks the prefix and further verifies it with the Luhn checksum, a widely used algorithm for validating identification numbers.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Additional Verification</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>All - Email Address</td>
<td>Email Address</td>
<td>None</td>
</tr>
<tr>
<td>All - Home Address</td>
<td>Home addresses in the United States of America and the United Kingdom</td>
<td>None</td>
</tr>
<tr>
<td>All - IBAN (International Bank Account Number)</td>
<td>International Bank Account Number</td>
<td>CPM verifies the International Bank Account Number, which has several different formats depending on the country of origin. The first two letters define the country code. CPM also verifies the format for the specific country code.</td>
</tr>
<tr>
<td>All - Names from US Census Bureau</td>
<td>Names from US Census Bureau</td>
<td>CPM verifies first and last names from the US Census Bureau, up to the year 1990.</td>
</tr>
<tr>
<td>All - Swift BIC</td>
<td>SWIFT Business Identifier Codes</td>
<td>CPM verifies the Society for Worldwide Interbank Financial Telecommunication (SWIFT) Bank Identifier Code (BIC). Swift-BIC is also known as the BIC code, SWIFT ID, or SWIFT code. It consists of a bank code, a country code, and a location code. verifies the country code against a list of country codes that are considered significant to the business. Some country codes are not included in the list.</td>
</tr>
<tr>
<td>Austria - SSN (Sozialversicherungsnummer)</td>
<td>Austrian Social Security Number</td>
<td>CPM verifies the social security number used in Austria and the expression's own checksum.</td>
</tr>
<tr>
<td>Canada - Quebec RAMQ</td>
<td>Quebec Healthcare Medical Number</td>
<td>CPM verifies the health insurance card number used in Quebec, Canada and the expression's own checksum.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Additional Verification</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>------------------------------------</td>
<td>-----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Canada - SSN (Social Insurance Number)</td>
<td>Canadian Social Insurance Number</td>
<td>CPM verifies the prefix and the Luhn checksum, a widely used algorithm for validating identification numbers.</td>
</tr>
<tr>
<td>China - National ID Number</td>
<td>China National ID Number</td>
<td>CPM verifies the national ID card number used in the People’s Republic of China. CPM checks the birth date embedded in the ID number and the expression’s own checksum.</td>
</tr>
<tr>
<td>Date - Full (day/month/year)</td>
<td>Date format commonly used in the United Kingdom</td>
<td>CPM validates dates in the Day-Month-Year format. CPM checks the range of the month and day for the specified month and if the year is earlier than 2051.</td>
</tr>
<tr>
<td>Date - Full (month/day/year)</td>
<td>Date with day, month, and year, such as a birth date</td>
<td>CPM validates dates in the Month-Day-Year format. CPM checks the range of the month and day for the specified month and if the year is earlier than 2051.</td>
</tr>
<tr>
<td>Date - Full (year/month/day)</td>
<td>Date format defined by the International Organization for Standardization</td>
<td>CPM validates dates in the Year-Month-Day format. CPM checks the range of the month and day for the specified month and if the year is earlier than 2051.</td>
</tr>
<tr>
<td>Date - Partial (month/year)</td>
<td>Date with only the month and year</td>
<td>None</td>
</tr>
<tr>
<td>Denmark - Personal ID Number</td>
<td>Danish Personal ID Number</td>
<td>CPM verifies the personal identification number used in Denmark and the expression’s own checksum.</td>
</tr>
<tr>
<td>Dominican Republic - Personal ID Number</td>
<td>Dominican Republic Personal ID Number</td>
<td>CPM verifies the personal identification number used in the Dominican Republic and the expression’s own checksum.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Additional Verification</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Finland - Personal ID Number</td>
<td>Finnish Personal ID Number</td>
<td>CPM verifies the personal identification number used in Finland and the expression's own checksum.</td>
</tr>
<tr>
<td>France - INSEE Code</td>
<td>France INSEE Code</td>
<td>CPM verifies the INSEE code and the expression's own checksum. The INSEE code is a numerical indexing code used by the French National Institute for Statistics and Economic Studies (INSEE). INSEE identifies various entities and is used as the National Identification Numbers for individuals.</td>
</tr>
<tr>
<td>France - National Insurance Number</td>
<td>French National Insurance Number</td>
<td>None</td>
</tr>
<tr>
<td>Germany - Electronic Taxpayer ID</td>
<td>German Electronic Taxpayer ID Number</td>
<td>CPM verifies the German Tax ID (eTIN) by checking both the birth month and day defined in the eTIN. CPM also verifies the expression's checksum.</td>
</tr>
<tr>
<td>Ireland - PPSN</td>
<td>Irish Personal Public Service Number</td>
<td>CPM verifies the Irish Personal Public Service Number and the expression's checksum.</td>
</tr>
<tr>
<td>Ireland - VAT</td>
<td>Irish Value Added Tax</td>
<td>None</td>
</tr>
<tr>
<td>Norway - Birth Number</td>
<td>Norwegian Birth Number</td>
<td>CPM verifies the birth date and the 3-digit personal number embedded in the data. CPM also verifies the expression's two checksums.</td>
</tr>
<tr>
<td>Poland - Document ID Number</td>
<td>Polish document ID number</td>
<td>CPM verifies the document ID number used in Poland and the expression's own checksum.</td>
</tr>
<tr>
<td>Poland - National ID Number</td>
<td>Polish ID Number</td>
<td>CPM verifies the PESEL and the expression's own checksum. PESEL is the national identification number used in Poland.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Additional Verification</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>South Korea - Registration Number</td>
<td>Republic of Korea (South Korea) Registration Number</td>
<td>CPM verifies the registration number of a citizen from the Republic of Korea and the birth date included in the data and gender digit.</td>
</tr>
<tr>
<td>Spain - Fiscal Identification Number</td>
<td>Spanish Fiscal Identification Number</td>
<td>CPM verifies the Spanish Fiscal Identification Number and the expression's own checksum.</td>
</tr>
<tr>
<td>Spain - National Identity Card Number</td>
<td>Spanish National Identity Card Number</td>
<td>None</td>
</tr>
<tr>
<td>Spain - SSN (Social Security Number)</td>
<td>Spanish Social Security Number</td>
<td>None</td>
</tr>
<tr>
<td>Taiwan - National ID Number</td>
<td>Taiwan National ID Number</td>
<td>CPM verifies the national ID card number used in Taiwan, the gender digit, and the expression's own checksum.</td>
</tr>
<tr>
<td>Taiwan - SKH Medical Record Number</td>
<td>Shin Kong Wu Ho-Su Memorial Hospital Medical Record Number</td>
<td>verifies the medical record number used in the Shin Kong Wu Ho-Su Memorial Hospital and the expression's own checksum.</td>
</tr>
<tr>
<td>Taiwan - VGH Medical Record Number</td>
<td>Taiwan Veterans General Hospital Medical Record Number</td>
<td>CPM verifies the medical record number used in the Taiwan Veterans General Hospital and the expression's own checksum.</td>
</tr>
<tr>
<td>Turkey - Identification Number</td>
<td>Turkish Republic ID Number</td>
<td>CPM verifies the national ID number used in the Turkish Republic and the expression's own checksum.</td>
</tr>
<tr>
<td>UK - National Health System Number</td>
<td>UK National Health System Number</td>
<td>None</td>
</tr>
<tr>
<td>UK - National Insurance Number</td>
<td>UK National Insurance Number</td>
<td>CPM verifies the national health service number used in the United Kingdom and the expression's own checksum.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Additional Verification</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>--------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>US - ABA Routing Number</td>
<td>ABA Routing Number</td>
<td>CPM verifies the first two digits of the data and the expression's own checksum.</td>
</tr>
<tr>
<td>US - California ID or DL Number</td>
<td>California ID Number or Driver's License Number</td>
<td>None</td>
</tr>
<tr>
<td>US - Dollar Amount</td>
<td>US dollar amount</td>
<td>None</td>
</tr>
<tr>
<td>US - HIC (Health Insurance Claim)</td>
<td>Health Insurance Claim</td>
<td>CPM verifies a valid Health Insurance Claim (HIC) suffix letter. The HIC number has one or two suffix letters.</td>
</tr>
<tr>
<td>US - NPI (National Provider Identifier)</td>
<td>National Provider Identifier in the United States</td>
<td>CPM verifies the National Provider Identifier (NPI). The NPI has its own checksum based on the Luhn algorithm, which is widely used for validating identification numbers. CPM also verifies the expression's checksum.</td>
</tr>
<tr>
<td>US - Phone Number</td>
<td>Telephone number</td>
<td>CPM checks the area code against a dictionary of collected US area codes.</td>
</tr>
<tr>
<td>US - SSN (Social Security Number)</td>
<td>United States Social Security Number</td>
<td>CPM validates a 9-digit number by checking its area code and group number and then matching it against invalid SSNs identified by the U.S. Social Security Administration (SSA).</td>
</tr>
</tbody>
</table>

**Supported File Types**

Choose from the following true file types when defining file attributes:
**Table 16: Supported File Types**

<table>
<thead>
<tr>
<th>File Type Group</th>
<th>File Types</th>
</tr>
</thead>
</table>
| **Documents and Encoding Methods** | • Adobe™ PDF - Non-encrypted (.pdf)  
• HTML (.htm)  
• Ichitaro (.jtd)  
• Lotus™ Ami Pro (.sam)  
• Microsoft Word for Windows - Non-encrypted (.doc, .dot, .docx, .dotx, .docm, .dotm)  
• Microsoft Write (.wri)  
• RTF (.rtf)  
• WordPerfect™ (.wp, .wpd)  
• WordStar (.wsd)  
• XML (.xml)  
• Xerox™ DocuWorks (.xdw, .xbd) |
| **Graphics** | • AutoCAD™ (.dxf)  
• AutoDesk™ (.dwg)  
• Bitmap (.bmp)  
• CATIA™ (.CATDrawing, .CATPart, .CATProduct)  
• DICOM (.dcm)  
• EPS (.eps)  
• GIF (.gif)  
• Graphic Data System (.gds)  
• JPEG (.jpg)  
• PNG (.png)  
• PostScript (.ps)  
• Siemens™ NX Unigraphics (.prt)  
• SolidWorks (.abc, .slddrw, .slprt, .sldasm)  
• TIFF (.tif) |
| **Multimedia Files** | • Adobe Flash™ (.swf)  
• Apple™ QuickTime™ (.mov)  
• AVI (.avi)  
• Microsoft Wave (.wav)  
• MIDI (.mid)  
• MPEG (.mpeg) |
| **Compressed Files** | • ARJ (.ari)  
• bzip2 (.bz2)  
• compress (.Z)  
• GZ (.gz)  
• LHA (.lzh)  
• Microsoft Compiled HTML Help (.chm)  
• Microsoft Outlook™ (.msg)  
• Microsoft Outlook (.pst)  
• Microsoft Outlook Express (.dbx)  
• MIME (.eml)  
• PAK/ARC (.arc)  
• PGP Keyring (.pgp)  
• RAR (.rar)  
• TAR (.tar)  
• Zipped File (.zip) |
| **Databases** | • dBase” (.dbf)  
• KIRI Database (.tbl)  
• Microsoft Access™ (.mdb, .accdb)  
• SAS System Data Set (.sas7bdat) |
| **Spreadsheets** | • Lotus 1-2-3 (.123, .wk1, .wk3, .wk4, .wke, .wks)  
• Microsoft Excel™ - Non-encrypted (.xls, .xlw, .xlsx, .xltx, .xlsb, .xltm, .xslm, .xlc, .xlam)  
• Quattro™ (.qpw, .wb3, .wb2, .wb1, .wq1) |
Predefined Keyword Lists

CPM comes with a set of predefined keyword lists. These keyword lists cannot be modified, copied, exported, or deleted. Each list has its own built-in conditions that determine if the template should trigger a policy violation.

How Keyword Lists Work

Number of Keywords Condition

Each keyword list contains a condition that requires a certain number of keywords be present in a document before the list will trigger a violation.

The number of keywords condition contains the following values:

- **All**: All of the keywords in the list must be present in the document.
- **Any**: Any one of the keywords in the list must be present in the document.
- **Specific number**: There must be at least the specified number of keywords in the document. If there are more keywords in the document than the number specified, a violation will trigger.
**Distance Condition**

Some of the lists contain a “distance” condition to determine if a violation is present. “Distance” refers to the amount of characters between the first character of one keyword and the first character of another keyword. Consider the following entry:

**First Name: John** _ Last Name: Smith_

The **Forms - First Name, Last Name** list has a “distance” condition of fifty (50) and the commonly used form fields of “First Name” and “Last Name”. In the example above, a violation will trigger as the number of characters between the “F” in First Name and the “L” in Last Name is equal to eighteen (18).

For an example of an entry that would not trigger a violation, consider the following:

The **first name of our new employee from Switzerland is John. His last name is Smith.**

In this example, the number of characters between the “f” in “first name” and the “l” in “last name” is sixty-one (61). This exceeds the distance threshold and does not trigger a violation.

---

**Keyword List Descriptions**

The following table describes the content that each of the keyword lists detect and the conditions necessary to trigger a policy violation.

**Table 17: Overview of the Keyword Lists**

<table>
<thead>
<tr>
<th>List Name</th>
<th>Description</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adult</td>
<td>The Adult list detects a wide variety of sensitive words commonly associated with the adult entertainment industry and pornographic websites.</td>
<td>Specific number: 4</td>
</tr>
<tr>
<td>Common medical terms</td>
<td>The Common medical terms list detects a wide variety of terms used by hospitals, clinics, and other health care providers.</td>
<td>Specific number: 5</td>
</tr>
<tr>
<td>Forms - (First), (Middle), Name</td>
<td>The Forms - (First), (Middle), Name list detects documents such as forms that contain private information. This list detects the common use of the &quot;(First)&quot;, &quot;(Middle)&quot;, and &quot;Last Name&quot; fields.</td>
<td>• All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Distance: 50</td>
</tr>
<tr>
<td>List Name</td>
<td>Description</td>
<td>Conditions</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>Forms - Date of birth</td>
<td>The Forms - Date of birth list detects documents such as forms that contain private information. This list detects the common use of the &quot;Birth Date&quot;, &quot;Birthdate&quot;, or &quot;Date of Birth&quot; fields.</td>
<td>Any</td>
</tr>
<tr>
<td>Forms - Expiration date</td>
<td>The Forms - Expiration date list detects documents such as labels or contracts that contain a date of expiration. This list detects the common use of terms that state information about when an item (such as a credit card) expires.</td>
<td>Any</td>
</tr>
<tr>
<td>Forms - First Name, Last Name</td>
<td>The Forms - First Name, Last Name list detects documents such as forms that contain private information. This list detects the common use of the &quot;First Name&quot; and &quot;Last Name&quot; fields.</td>
<td>• All</td>
</tr>
<tr>
<td>Forms - Place of birth</td>
<td>The Forms - Place of birth list detects documents such as forms that contain private information. This list detects the common use of terms that state information about a person's birthplace.</td>
<td>• All</td>
</tr>
<tr>
<td>Forms - Street, City, State</td>
<td>The Forms - Street, City, State detects documents such as forms that contain private information. This list detects the common use of the &quot;State&quot;, &quot;City&quot;, and &quot;Street&quot; fields.</td>
<td>• All</td>
</tr>
<tr>
<td>HCFA (CMS) 1500 Form (Health Care Financing Agency) (Centers for Medicare and Medicaid Services)</td>
<td>This list detects the HCFA-1500 and the CMS-1500 forms. These are documents used in the United States for health insurance claims.</td>
<td>• All</td>
</tr>
<tr>
<td>Racism</td>
<td>The Racism list detects a wide variety of sensitive words that may be offensive to specific ethnic groups.</td>
<td>Specific number: 4</td>
</tr>
<tr>
<td>Source code - C#</td>
<td>The Source code - C# list detects a large number of common source code functions/commands used in C#.</td>
<td>• All</td>
</tr>
<tr>
<td>Source code - C/C++</td>
<td>The Source code - C/C++ list detects a large number of common source code functions/commands used in C/C++.</td>
<td>• All</td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>List Name</th>
<th>Description</th>
<th>Conditions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source code - COBOL</td>
<td>The Source code - COBOL list detects a large number of common source code</td>
<td>Specific number: 10</td>
</tr>
<tr>
<td></td>
<td>functions/commands used in COBOL.</td>
<td></td>
</tr>
<tr>
<td>Source code - Java</td>
<td>The Source code - Java list detects a large number of common source code</td>
<td>Specific number: 10</td>
</tr>
<tr>
<td></td>
<td>functions/commands used in Java.</td>
<td>Case-sensitive</td>
</tr>
<tr>
<td>Source code - Perl</td>
<td>The Source code - Perl list detects a large number of common source code</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td>functions/commands used in Perl.</td>
<td>Case-sensitive</td>
</tr>
<tr>
<td>Source code - VB</td>
<td>The Source code - VB list detects a large number of common source code</td>
<td>Specific number: 10</td>
</tr>
<tr>
<td></td>
<td>functions/commands used in Visual Basic.</td>
<td></td>
</tr>
<tr>
<td>UB-04 Form (Uniform Bill-04 Form)</td>
<td>The UB-04 Form list detects the billing document used in the United States at hospitals, nursing homes, hospices, home health agencies, and other institutional providers.</td>
<td>All</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Case-sensitive</td>
</tr>
<tr>
<td>Weapons</td>
<td>The Weapons list detects a wide variety of words that describe implements of</td>
<td>Specific number: 4</td>
</tr>
<tr>
<td></td>
<td>violence.</td>
<td></td>
</tr>
</tbody>
</table>

**Predefined DLP Template List**

**Table 18:** Predefined Templates

<table>
<thead>
<tr>
<th>Template</th>
<th>Purpose</th>
<th>Samples of Data Protected</th>
</tr>
</thead>
<tbody>
<tr>
<td>GLBA (Gramm-Leach-Billey Act)</td>
<td>• Created for financial institutions such as banks and securities/insurance companies&lt;br&gt;• Directs the disclosure of a customer’s personal and financial information</td>
<td>• Credit card number&lt;br&gt;• ABA routing number (bank code)&lt;br&gt;• Social security number&lt;br&gt;• Birth date</td>
</tr>
<tr>
<td>Template</td>
<td>Purpose</td>
<td>Samples of Data Protected</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
</tbody>
</table>
| HIPAA (Health Insurance Portability and Accountability Act) | • Created for agencies that maintain medical records, such as health care providers or HMOs  
• Maintains and protects the privacy of health information | • Social security number  
• Credit card number  
• Health insurance claim number  
• Common medical terms |
| PCI-DSS (Payment Card Industry Data Security Standard) | • Created for companies that process credit card payments  
• Aims to help credit card companies prevent fraud | • Credit card number  
• Name  
• Partial date  
• Expiration date |
| SB-1386 (US Senate Bill 1386) | • Created for people or agencies conducting business that involves California residents’ personal information  
• Requires the “notification to California residents of security breaches to their non-encrypted information” | • Social security number  
• Credit card number  
• California ID number  
• California driver’s license number |
| US PII (United States Personally Identifiable Information) | Protects the personal identifiable information (PII) of people from the United States | • Social security number  
• Credit card number  
• Name  
• Home address  
• Phone number  
• Email address  
• Birth place  
• Birth date |

**Wildcard Usage in Device Control**

Wildcards are used correctly in the following examples:

**Table 19: Correct Usage of Wildcards**

<table>
<thead>
<tr>
<th>Example</th>
<th>Matched Data</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>?:\Password.exe</code></td>
<td>The “Password.exe” file located directly under any drive</td>
</tr>
</tbody>
</table>
Wildcards are used incorrectly in the following examples:

**Table 20:** Incorrect Usage of Wildcards

<table>
<thead>
<tr>
<th>Example</th>
<th>Matched Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>C:\Program Files\Microsoft*.exe</td>
<td>Any file in C:\Program Files that has a file extension</td>
</tr>
<tr>
<td>C:\Program Files*.*</td>
<td>Any file in C:\Program Files that has a file extension</td>
</tr>
<tr>
<td>C:\Program Files\a?c.exe</td>
<td>Any .exe file in C:\Program Files that has 3 characters starting with the letter &quot;a&quot; and ending with the letter &quot;c&quot;</td>
</tr>
<tr>
<td>C:*</td>
<td>Any file located directly under the C:\ drive, with or without file extensions</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Example</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>??:\Buffalo\Password.exe</td>
<td>?? represents two characters and drive letters only have a single alphabetic character.</td>
</tr>
<tr>
<td>*:\Buffalo\Password.exe</td>
<td>* represents multi-character data and drive letters only have a single alphabetic character.</td>
</tr>
<tr>
<td>C:\Password.exe</td>
<td>Wildcards cannot be used to represent folder names. The exact name of a folder must be specified.</td>
</tr>
<tr>
<td>C:?:Password.exe</td>
<td>Wildcards cannot be used to represent folder names. The exact name of a folder must be specified.</td>
</tr>
</tbody>
</table>
Index

A
actions
  Data Loss Prevention 31
Activation Code 6
ActiveSync 31
advanced permissions
  configuring 38
  storage devices 35–36
analyses 40–44
  device control violation information 43
  non-storage devices information 43
  policy information 42
  storage devices information 44

C
client notifications 6
compressed files
  decompression rules 32
condition statements 18
criteria
  customized expressions 9
  keywords 14
customized expressions 9, 11
  creating 11
  criteria 9
  importing 11
customized keywords 14
  creating 16
  criteria 15
  importing 17
customized policy
  procedure overview 3
customized templates 18
  creating 19
  importing 20

D
data identifiers 7
  expressions 7
  file attributes 7
  keywords 7
Data Loss Prevention 2, 6–7, 21, 46
  actions 31
  analyses 40
    violation information 41
  analysis 42
  channels 22
  client notification 6
  data identifiers 7
  decompression rules 32
  expressions 8–9, 11, 47
  file attributes 12–13, 11
  keywords 14–17, 55–56
  network channels 22–28
  policy 3, 21, 32
  report 46
  system and application channels 28–31
  templates 17–20, 58
  wizard 2
Data Loss Prevention Policy Information Analysis 42
data protection 1, 5–6
  Activation Code 6
  analyses 40, 42–44
    endpoint information 40
  client notifications 6
  installing 5
  license 6
  renewing 6
Data Protection - Detected Data Loss Prevention Information Analysis 41
decompression rules 32
device control 3–4, 6, 34–39, 46, 59
  advanced permissions 38
    configuring 38
  analyses 40
  analysis 43–44
  approved list 39
  client notification 6
  Digital Signature Provider 36
  external devices 37
  managing access 37
  non-storage devices 4, 37
  permissions 34–37
    program path and name 37
  report 46
  requirements 3
  storage devices 34–36
  USB devices 39
  wildcards 59
  wizard 4
Device Control Detections report 46
Device Control for Non-Storage Devices Information Analysis 43
Device Control for Storage Devices Information Analysis 44
Device Control Violation Information Analysis 43
Device Control Wizard 4
Digital Signature Provider 36
specifying 36
DLP Detections report 46
DLP Settings Wizard 2
DSP 36

E
email domains 23
Endpoint Information Analysis 40
expressions 7–8
  customized 9, 11
criteria 9
predefined 8, 47
external devices
  managing access 37

F
file attributes 7, 12–13, 54
  creating 12–13
importing 13
supported file types 54
wildcards 13
FTP 24

G
GLBA 58

H
HIPAA 59
HTTP and HTTPS 24

I
IM applications 25

K
keywords 7, 14
  customized 14–17
predefined 14, 55–56

L
license 6
logical operators 18

M
monitored email domains 23
monitored targets 26–27

N
network channels 22–28
  email clients 23
FTP 24
HTTP and HTTPS 24
IM applications 25
monitored targets 27–28
non-monitored targets 27–28
SMB protocol 25
transmission scope 28
  all transmissions 26
conflicts 28
  external transmissions 27
transmission scope and targets 26
webmail 25
non-monitored email domains 23
non-monitored targets 26–27
non-storage devices
analysis 43
permissions 37

P
PCI-DSS 59
PCRE 9
Perle Compatible Regular Expressions 9
permissions
  advanced 38
non-storage devices 37
program path and name 37
storage devices 34
policy 21, 32
  configuring 32
procedure overview 3
predefined expressions 8, 47
viewing 8
predefined keywords 55
distance 56
list descriptions 56
number of keywords 55
predefined templates 18, 58

R
reports 46
  Device Control Detections 46
DLP Detections 46
SB-1386 59
SMB protocol 25
storage devices
  advanced permissions 35–36
  analysis 44
  permissions 34
supported file types 54
system and application channels 22, 28–31
  CD/DVD 29
  peer-to-peer (P2P) 30
  printer 30
  removable storage 30
  synchronization software 31
templates 17–20, 58
  condition statements 18
  customized 18–20
  logical operators 18
  predefined 18, 58
US PII 59
USB devices
  approved list 39
  configuring 39
webmail 25
wildcards 13
  device control 59
  file attributes 13