COPYRIGHT
© 2016 Intel Corporation

TRADEMARK ATTRIBUTIONS
Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee and the McAfee logo, McAfee Active Protection, McAfee DeepSAFE, ePolicy Orchestrator, McAfee ePO, McAfee EMM, McAfee Evader, Foundscore, Foundstone, Global Threat Intelligence, McAfee LiveSafe, Policy Lab, McAfee QuickClean, Safe Eyes, McAfee SECURE, McAfee Shredder, SiteAdvisor, McAfee Stinger, McAfee TechMaster, McAfee Total Protection, TrustedSource, VirusScan are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO McAfee OR THE PLACE OF PURCHASE FOR A FULL REFUND.
# Contents

- **Preface**
  - About this guide ................................ 9
  - Audience .................................. 9
  - Conventions ................................. 9
  - Find product documentation ................. 10

- **1 Introduction to McAfee DLP Endpoint**
  - McAfee DLP Endpoint and Device Control — Controlling endpoint content and removable media ..................... 11
    - Classify .................................. 13
    - Track ................................... 13
    - Protect ................................... 14
    - Monitor ................................... 15
  - Product modules and how they interact ......................... 15
  - How the client software works ................................ 18
    - McAfee DLP Endpoint on the Microsoft Windows platform .................. 18
    - McAfee DLP Endpoint on the OS X platform .......................... 19

- **2 Deployment options and scenarios**
  - Planning your deployment ................................ 23
  - McAfee DLP Endpoint and Device Control options .................. 24
  - Deploying McAfee DLP Endpoint in Citrix environments ............... 25
  - System requirements ................................ 25

- **3 Install the McAfee DLP Endpoint or Device Control software**
  - Install and license the McAfee DLP extension ...................... 27
    - Applying backward compatibility ................................ 29
    - Convert policies and migrate data ................................ 30
  - Install the McAfee DLP Endpoint and Device Control client software ............. 31

- **4 Deploying the client software and policies**
  - Deploy McAfee DLP Endpoint client with McAfee ePO ................... 33
    - Verify the installation ................................ 34
  - Deploy policies with McAfee ePO ................................ 34
    - Assign a policy or client configuration .......................... 35
    - Refresh the policy ................................ 35

- **5 Configuring system components**
  - Policy Catalog .................................. 39
  - Configuring McAfee DLP in the Policy Catalog ......................... 39
    - Import or export the McAfee DLP Endpoint configuration ............ 40

## Deployment and installation

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>9</td>
</tr>
<tr>
<td>About this guide</td>
<td>9</td>
</tr>
<tr>
<td>Audience</td>
<td>9</td>
</tr>
<tr>
<td>Conventions</td>
<td>9</td>
</tr>
<tr>
<td>Find product documentation</td>
<td>10</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>11</td>
</tr>
<tr>
<td>Introduction to McAfee DLP Endpoint</td>
<td>11</td>
</tr>
<tr>
<td>McAfee DLP Endpoint and Device Control — Controlling endpoint content and removable media</td>
<td>11</td>
</tr>
<tr>
<td>Classify</td>
<td>13</td>
</tr>
<tr>
<td>Track</td>
<td>13</td>
</tr>
<tr>
<td>Protect</td>
<td>14</td>
</tr>
<tr>
<td>Monitor</td>
<td>15</td>
</tr>
<tr>
<td>Product modules and how they interact</td>
<td>15</td>
</tr>
<tr>
<td>How the client software works</td>
<td>18</td>
</tr>
<tr>
<td>McAfee DLP Endpoint on the Microsoft Windows platform</td>
<td>18</td>
</tr>
<tr>
<td>McAfee DLP Endpoint on the OS X platform</td>
<td>19</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>23</td>
</tr>
<tr>
<td>Deployment options and scenarios</td>
<td>23</td>
</tr>
<tr>
<td>Planning your deployment</td>
<td>23</td>
</tr>
<tr>
<td>McAfee DLP Endpoint and Device Control options</td>
<td>24</td>
</tr>
<tr>
<td>Deploying McAfee DLP Endpoint in Citrix environments</td>
<td>25</td>
</tr>
<tr>
<td>System requirements</td>
<td>25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>27</td>
</tr>
<tr>
<td>Install the McAfee DLP Endpoint or Device Control software</td>
<td>27</td>
</tr>
<tr>
<td>Install and license the McAfee DLP extension</td>
<td>27</td>
</tr>
<tr>
<td>Applying backward compatibility</td>
<td>29</td>
</tr>
<tr>
<td>Convert policies and migrate data</td>
<td>30</td>
</tr>
<tr>
<td>Install the McAfee DLP Endpoint and Device Control client software</td>
<td>31</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>33</td>
</tr>
<tr>
<td>Deploying the client software and policies</td>
<td>33</td>
</tr>
<tr>
<td>Deploy McAfee DLP Endpoint client with McAfee ePO</td>
<td>33</td>
</tr>
<tr>
<td>Verify the installation</td>
<td>34</td>
</tr>
<tr>
<td>Deploy policies with McAfee ePO</td>
<td>34</td>
</tr>
<tr>
<td>Assign a policy or client configuration</td>
<td>35</td>
</tr>
<tr>
<td>Refresh the policy</td>
<td>35</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>39</td>
</tr>
<tr>
<td>Configuring system components</td>
<td>39</td>
</tr>
<tr>
<td>Policy Catalog</td>
<td>39</td>
</tr>
<tr>
<td>Configuring McAfee DLP in the Policy Catalog</td>
<td>39</td>
</tr>
<tr>
<td>Import or export the McAfee DLP Endpoint configuration</td>
<td>40</td>
</tr>
</tbody>
</table>
6 Protecting removable media

- Protecting devices ........................................ 54
- Managing devices with device classes ...................... 54
- Define a device class .................................... 55
  - Obtain a GUID ........................................... 55
  - Create a device class ..................................... 55
- Organizing devices with device definitions .................. 56
  - Working with device definitions ......................... 57
  - Device properties ..................................... 60
- Device control rules ...................................... 63
  - Create a removable storage device rule .................. 64
  - Create a plug-and-play device rule ....................... 65
  - Create a removable storage file access device rule ..... 66
  - Create a fixed hard drive device rule .................... 66
  - Create a Citrix device rule .............................. 67
  - Create a TrueCrypt device rule ......................... 67
- Removable storage file access rules ......................... 68

7 Classifying sensitive content ............................. 69

- Components of the Classification module .................... 69
- Using classifications .................................... 70
  - Classify by file destination ................................ 71
  - Classifying by file location ............................... 72
  - Text extraction ........................................... 72
  - How McAfee DLP Endpoint categorizes applications ......... 73
- Classification definitions and criteria ....................... 73
  - Dictionary definitions .................................. 75
  - Advanced pattern definitions .............................. 76
  - Classifying content with document properties or file information 76
  - Application templates .................................. 77
- Manual classification .................................... 78
  - Embedded tags ........................................... 79
- Registered documents ..................................... 80
  - Whitelisted text ........................................ 80
- Create and configure classifications ......................... 81
  - Create a classification .................................. 81
  - Create classification criteria ............................ 81
  - Upload registered documents .............................. 82
  - Upload files to whitelist text ............................. 82
- Configure classification components for McAfee DLP Endpoint 83
  - Create content fingerprinting criteria .................... 83
Use case: Allow a specified user group to send credit information ........................................... 123
Use case: Classify attachments as NEED-TO-SHARE based on their destination ......................... 125

10 Scanning data with McAfee DLP Endpoint discovery .............................................................. 129
  Protecting files with discovery rules ............................................................................................ 129
  How discovery scanning works .................................................................................................... 130
  Find content with the Endpoint Discovery crawler ..................................................................... 130
    Create and define a discovery rule ......................................................................................... 131
    Create a scheduler definition ............................................................................................... 131
    Set up a scan ......................................................................................................................... 132
  Use case: Restore quarantined files or email items ................................................................... 133

Monitoring and reporting

11 Incidents and operational events ................................................................................................. 137
  Monitoring and reporting events ............................................................................................... 137
  DLP Incident Manager ............................................................................................................. 138
    How the Incident Manager works .......................................................................................... 138
    Working with incidents ......................................................................................................... 140
  View incidents .......................................................................................................................... 140
    Sort and filter incidents ........................................................................................................ 141
    Configure column views ....................................................................................................... 141
    Configure incident filters ...................................................................................................... 142
    View incident details ............................................................................................................. 143
  Manage incidents ..................................................................................................................... 144
    Update a single incident ....................................................................................................... 145
    Update multiple incidents ..................................................................................................... 145
  Manage labels ............................................................................................................................ 147
  Working with cases ................................................................................................................... 148
  Manage cases ............................................................................................................................ 148
    Create cases .......................................................................................................................... 148
    View case information .......................................................................................................... 148
    Assign incidents to a case ..................................................................................................... 149
    Move or remove incidents from a case .................................................................................. 149
  Update cases ............................................................................................................................. 150
  Add or remove labels to a case ................................................................................................. 151
  Delete cases .............................................................................................................................. 151

12 Collecting and managing data .................................................................................................... 153
  Edit server tasks ....................................................................................................................... 153
    Create a Purge events task ..................................................................................................... 154
    Create an Automatic mail Notification task ....................................................................... 155
    Create a Set Reviewer task ................................................................................................... 155
  Monitor task results ................................................................................................................. 156
  Creating reports ........................................................................................................................ 156
    Report types .......................................................................................................................... 156
    Report options ....................................................................................................................... 157
    Predefined dashboards ........................................................................................................ 157
    Create a data rollup server task ............................................................................................ 159

Maintenance and troubleshooting

13 McAfee DLP Endpoint Diagnostics ............................................................................................ 163
  Diagnostic Tool ........................................................................................................................ 163
    Checking the agent status ..................................................................................................... 164
    Run the Diagnostic Tool ....................................................................................................... 164
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tuning policies</td>
<td>165</td>
</tr>
<tr>
<td>Index</td>
<td>167</td>
</tr>
</tbody>
</table>
Preface

This guide provides the information you need to work with your McAfee product.

Contents
- About this guide
- Find product documentation

About this guide

This information describes the guide’s target audience, the typographical conventions and icons used in this guide, and how the guide is organized.

Audience

McAfee documentation is carefully researched and written for the target audience.
The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company’s security program.
- **Security officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company’s intellectual property.

Conventions

This guide uses these typographical conventions and icons.

- **Italic** Title of a book, chapter, or topic; a new term; emphasis
- **Bold** Text that is emphasized
- **Monospace** Commands and other text that the user types; a code sample; a displayed message
- **Narrow Bold** Words from the product interface like options, menus, buttons, and dialog boxes
- **Hypertext blue** A link to a topic or to an external website

- **Note:** Extra information to emphasize a point, remind the reader of something, or provide an alternative method
- **Tip:** Best practice information
- **Caution:** Important advice to protect your computer system, software installation, network, business, or data
- **Warning:** Critical advice to prevent bodily harm when using a hardware product
Find product documentation

On the ServicePortal, you can find information about a released product, including product documentation, technical articles, and more.

**Task**
1. Go to the ServicePortal at https://support.mcafee.com and click the Knowledge Center tab.
2. In the Knowledge Base pane under Content Source, click Product Documentation.
3. Select a product and version, then click Search to display a list of documents.
Introduction to McAfee DLP Endpoint

Data loss is when confidential or private information leaves the enterprise as a result of unauthorized communication through channels such as applications, physical devices, or network protocols. Data loss prevention software enforces predefined information security policies to prevent such losses.

Data to be protected can be usefully categorized according to three vectors — data-in-use, data-in-motion, and data-at-rest.

Table 1-1 Data vector descriptions

<table>
<thead>
<tr>
<th>Data vector</th>
<th>Description</th>
<th>Associated products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data-in-use</td>
<td>Data-in-use applies to the actions of users on endpoint devices. Examples are copying data and files to removable media, printing files to a local printer, and taking screen captures.</td>
<td>McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint)</td>
</tr>
</tbody>
</table>
| Data-in-motion  | Data-in-motion applies to live traffic on your network. Traffic is analyzed, categorized, and stored in the McAfee® Data Loss Prevention (McAfee DLP) (McAfee DLP) database. | • McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor)  
• McAfee® Data Loss Prevention Prevent (McAfee DLP Prevent) |
| Data-at-rest    | Data-at-rest applies to data residing in databases, file shares, and repositories. McAfee DLP can scan, track, and perform remedial actions on data at rest. | • McAfee® Data Loss Prevention Discover (McAfee DLP Discover)  
• McAfee DLP Endpoint discovery |

Contents

- McAfee DLP Endpoint and Device Control — Controlling endpoint content and removable media
- Product modules and how they interact
- How the client software works

McAfee DLP Endpoint and Device Control — Controlling endpoint content and removable media

McAfee DLP Endpoint inspects enterprise users’ actions on sensitive content on their computers.

McAfee Device Control prevents unauthorized use of removable media devices. McAfee DLP Endpoint includes all Device Control functionality, and, in addition, protects against data loss through a broad set of potential data-loss channels.

Key features

McAfee Device Control:
• Controls what data can be copied to removable devices, or controls the devices themselves. It can block devices completely, make them read-only, or block applications run from removable drives.
• Provides protection for USB drives, smartphones, Bluetooth devices, and other removable media

McAfee DLP Endpoint protects against data loss from:
• Cloud applications
• Email
• Printers
• Screen captures
• Clipboard software
• Web posts
• Network shares

The McAfee DLP classification engine (also used by McAfee DLP Discover) applies definitions and classification criteria that define the content to be protected, and where and when the protection is applied.

The McAfee DLP Endpoint discovery crawler runs on the local endpoint, searching local file system and email storage files and applying policies to protect sensitive content.

**How it works**

McAfee DLP Endpoint safeguards sensitive enterprise information:
• Applies policies that consist of definitions, classifications, rule sets, and endpoint client configurations
• Monitors the policies and blocks actions on sensitive content, as needed
• Encrypts sensitive content before allowing the action
• Creates reports for review and control of the process, and can store sensitive content as evidence

![Diagram of McAfee DLP protection process](image.png)

**Figure 1-1 The McAfee DLP protection process**
**Classify**

To protect sensitive content, start by defining and classifying sensitive information to be protected. Content is classified by defining *classifications* and *classification criteria*. Classification criteria defines the conditions on how data is classified. Methods to define criteria include:

- **Advanced patterns** — Regular expressions combined with validation algorithms, used to match patterns such as credit card numbers.

- **Dictionaries** — Lists of specific words or terms, such as medical terms for detecting possible HIPAA violations.

- **True file types** — Document properties, file information, or the application that created the file.

- **Source or destination location** — URLs, network shares, or the application or user that created or received the content.

McAfee DLP Endpoint supports third-party classification software. You can classify email using Boldon James Email Classifier. You can classify email or other files using Titus classification clients — Titus Message Classification, Titus Classification for Desktop, and Titus Classification Suite. To implement Titus support, the Titus SDK must be installed on the endpoint computers.

**Track**

McAfee DLP Endpoint can track content based on its origin using two techniques – registered documents and tagging criteria.

Using these techniques, you can, for example, specify that all files downloaded from the engineering SharePoint site are tracked and classified as Intellectual Property.

**Registered documents**

The registered documents feature is based on pre-scanning all files in specified repositories (such as the engineering SharePoint) and creating signatures of fragments of each file in these repositories. These signatures are then distributed to all managed endpoints. The McAfee DLP Endpoint client is then able to track any paragraph copied from one of these documents and classify it according to the classification of the registered document signature.

Registered documents use extensive memory which might affect performance, as each document that the McAfee DLP Endpoint client inspects is compared to all registered document signatures to identify its origin.

**Best practice:** To minimize the number of signatures and the performance implications of this technique, use registered documents to track only the most sensitive documents.

**Content fingerprinting**

Content fingerprinting is a content tracking technique unique to the McAfee DLP Endpoint product. The administrator creates a set of content fingerprinting criteria that define the file location and the classification to place on files from that location. McAfee DLP Endpoint client tracks any file that is opened from the locations defined in the content fingerprinting criteria and creates fingerprint signatures of these files in real time when the files are accessed. It then uses these signatures to track the files or fragments of the files. Content fingerprinting criteria can be defined by location (UNC path or URL) or the application used to access the file.

**Support for persistent fingerprint information**

Content fingerprint signatures are stored in a file's extended file attributes (EA) or alternate data streams (ADS). When such files are accessed, McAfee DLP Endpoint software tracks data transformations and maintains the classification of the sensitive content persistently, regardless of
how it is being used. For example, if a user opens a fingerprinted Word document, copies a few paragraphs of it into a text file, and attaches the text file to an email message, the outgoing message has the same signatures as the original document.

For file systems that do not support EA or ADS, McAfee DLP Endpoint software stores signature information as a metafile on the disk. The metafiles are stored in a hidden folder named ODB$, which the McAfee DLP Endpoint client software creates automatically.

Signatures and content fingerprinting criteria are not supported in McAfee Device Control.

**Protect**

Create rules to identify sensitive data and take appropriate action.

Rules are made up of conditions, exceptions, and actions. Conditions contain multiple parameters — such as classifications — to define the data or user action to identify. Exceptions specify parameters to exclude from triggering the rule. Actions specify how the rule behaves when a rule is triggered, such as blocking user access, encrypting a file, and creating an incident.

**Data Protection rules**

Data protection rules are used by McAfee DLP Endpoint and Device Control to prevent unauthorized distribution of classified data. When a user tries to copy or attach classified data, McAfee DLP intercepts the attempt and uses the data protection rules to determine what action to take. For example, McAfee DLP Endpoint can halt the attempt and display a dialog to the end user. The user inputs the justification for the attempt, and processing continues.

McAfee Device Control uses only removable storage data protection rules.

**Device Control rules**

Device Control rules monitor and potentially block the system from loading physical devices such as removable storage devices, Bluetooth, Wi-Fi, and other plug-and-play devices. Device Control rules consist of device definitions and reaction specifications, and can be assigned to specific end-user groups by filtering the rule with end-user group definitions.

**Discovery rules**

Discovery rules are used by McAfee DLP Endpoint and McAfee DLP Discover for file and data scanning.

Endpoint Discovery is a crawler that runs on managed computers. It scans the local endpoint file system and the local email (cached) inbox and PST files. Local file system and email storage discovery rules define whether the content is to be quarantined, tagged, or encrypted. These rules can also define whether the classified file or email is reported as an incident, and whether to store the file or email as evidence included in the incident.

File system scans are not supported on server operating systems.

McAfee DLP Discover scans repositories and can move or copy files, apply Rights Management policies to files, and create incidents.

**Rule sets**

Rules are organized into rule sets. A rule set can contain any combination of rule types.
Policies

Policies contain active rule sets and are deployed from McAfee ePO to the McAfee DLP Endpoint client software or Discovery server. McAfee DLP Endpoint policies also contain policy assignment information and definitions.

Monitor

Review incidents for policy violations that have occurred.

Monitoring functions include:

- **Incident management** — Incidents are sent to the McAfee ePO Event Parser and stored in a database. Incidents contain the details about the violation, and can optionally include evidence information. You can view incidents and evidence as they are received in the DLP Incident Manager console.

- **Case management** — Group related incidents into cases for further review in the DLP Case Management console.

- **Operational events** — View errors and administrative events in the DLP Operations console.

- **Evidence collection** — For rules that are configured to collect evidence, a copy of the data or file is saved and linked to the specific incident. This information can help determine the severity or exposure of the event. Evidence is encrypted using the AES algorithm before being saved.

- **Hit highlighting** — Evidence can be saved with highlighting of the text that caused the incident. Highlighted evidence is stored as a separate encrypted HTML file.

- **Reports** — McAfee DLP Endpoint can create reports, charts, and trends for display in McAfee ePO dashboards.

Product modules and how they interact

McAfee DLP Endpoint consists of five modules. In addition, it uses the McAfee ePO Policy Catalog, Server Tasks, Server Settings, and Permission Sets.

McAfee DLP version 10.0 has a reorganized workflow with increased granularity.

Policy Catalog

The McAfee ePO Policy Catalog stores the policies that are deployed to the endpoint computers. The Data Loss Prevention 10.0 policies are displayed when you select that option from the Product drop-down list.

McAfee DLP policies have the following components:

- **DLP Policy** — Contains tabs for Active Rule Sets, Endpoint Discovery scans, Settings, and Policy Validation. Discovery rules in the rule sets can be applied to either endpoint or network discovery scans when both McAfee DLP Endpoint and McAfee DLP Discover are installed in McAfee ePO.

- **Windows Client Configuration** — Contains information for Microsoft Windows end-user computers.

- **Mac OS X Client Configuration** — Contains information for OS X end-user computers.

- **Server Configuration** — Contains settings for McAfee DLP Discover servers.
Table 1-2 Client configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced configuration</td>
<td>• <strong>Windows client:</strong> Endpoint and access protection settings</td>
</tr>
<tr>
<td></td>
<td>• <strong>OS X client:</strong> Stop agent bypass when updating</td>
</tr>
<tr>
<td>Clipboard Protection</td>
<td>Enables the Microsoft Office clipboard; used to add whitelisted</td>
</tr>
<tr>
<td></td>
<td>processes.</td>
</tr>
<tr>
<td>Content Tracking</td>
<td>Text extractor settings and whitelisted processes for application file access protection rules.</td>
</tr>
<tr>
<td>Corporate connectivity</td>
<td>Used to configure corporate and VPN servers for data protection options.</td>
</tr>
<tr>
<td>Debugging and Logging</td>
<td>• <strong>Windows client:</strong> Set up logging and memory dumps for troubleshooting, print log checkbox.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OS X client:</strong> Print log checkbox.</td>
</tr>
<tr>
<td>Discovery (Endpoint)</td>
<td>Sets scan performance parameters and prefix for quarantined emails.</td>
</tr>
<tr>
<td>Email Protection</td>
<td>Settings for email protection rules and third party software integration.</td>
</tr>
<tr>
<td>Evidence Copy Service</td>
<td>Settings for evidence storage share, file size, and evidence age.</td>
</tr>
<tr>
<td>Operational Mode and Modules</td>
<td>• <strong>Windows client:</strong> Sets operation mode for Device Control or McAfee DLP Endpoint; activates add-ins and handlers.</td>
</tr>
<tr>
<td></td>
<td>• <strong>OS X client:</strong> Sets operation mode for Device Control or McAfee DLP Endpoint for Mac; modules supported are device blocking and reporting service.</td>
</tr>
<tr>
<td>Printing Protection</td>
<td>Used to add whitelisted processes.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Settings for quarantine folder.</td>
</tr>
<tr>
<td>Removable Storage Protection</td>
<td>Sets deletion mode for removable storage.</td>
</tr>
<tr>
<td>Screen Capture Protection</td>
<td>Adds screen capture application support.</td>
</tr>
<tr>
<td>User Interface Components</td>
<td>Defines the endpoint user interface.</td>
</tr>
<tr>
<td>Web Post Protection</td>
<td>Sets HTTP GET request behavior, Google Chrome version support, timeout strategy, and whitelisted URLs.</td>
</tr>
</tbody>
</table>

Classifications

The Classification module stores *content classification criteria*, *content fingerprinting criteria*, and the definitions used to configure them. The module is also used to set up *registered documents* repositories, user authorization for manual tagging, and *whitelisted text*.

Classifications are required for configuring data protection and endpoint discovery rules, and for McAfee DLP Discover classification and remediation scans.

DLP Policy Manager

The DLP Policy Manager module defines the rule sets, policy assignments, and definitions that make up a DLP policy.

DLP *rule sets* define data protection, device control, and discovery rules. Each rule in a rule set can include any or all three types of rules. You can include multiple rules in a rule set, and assign multiple rule sets to a DLP policy.
**Incident Manager and Operations**

The DLP Incident Manager module displays security events from policy violations. A Details page for each entry displays evidence specified in the client configuration, rules and classifications applied, and other details. The DLP Operations module displays administrative events such as deployments or policy updates.

**Case Management**

The DLP Case Management module allows administrators to collaborate toward the resolution of related incidents.

In many situations, an incident is not an isolated event. You might see multiple incidents in the DLP Incident Manager that share common properties or are related to each other. You can assign these related incidents to a case. Multiple administrators can monitor and manage a case depending on their roles in the organization.

**Workflow**

Use the following workflow to create policies and deploy them to endpoint computers.

1. Create classification and tagging criteria and the definitions required to define them. (You can create definitions as needed for defining criteria.)

2. Create data protection, device, and discovery rules and the definitions required to define them.
   
   | Data protection and discovery rules include assigning a classification as part of defining the rule. |

3. Assign rule sets to DLP policies. Create discovery scan definitions in the DLP policies.

4. Assign and deploy the policies in the System Tree.

---

**Figure 1-2 Workflow**

![Workflow Diagram]

---

*McAfee Data Loss Prevention Endpoint 10.0.0  Product Guide*
How the client software works

The McAfee DLP Endpoint client software is deployed as a McAfee Agent plug-in, and enforces the policies defined in the McAfee DLP policy. The McAfee DLP Endpoint client software audits user activities to monitor, control, and prevent unauthorized users from copying or transferring sensitive data. It then generates events recorded by the McAfee ePO Event Parser.

Event Parser

Events generated by the McAfee DLP Endpoint client software are sent to the McAfee ePO Event Parser, and recorded in tables in the McAfee ePO database. Events are stored in the database for further analysis and used by other system components.

Online/offline operation

You can apply different device and protection rules, depending on whether the managed computer is online (connected to the enterprise network) or offline (disconnected from the network). Some rules also allow you to differentiate between computers within the network and those connected to the network by VPN.

McAfee DLP Endpoint on the Microsoft Windows platform

Windows-based computers can be protected with either McAfee Device Control or McAfee DLP Endpoint. The McAfee DLP Endpoint client software uses advanced discovery technology, text pattern recognition, and predefined dictionaries. It identifies sensitive content, and incorporates device management and encryption for added layers of control.

Information Rights Management (IRM) software protects sensitive files using encryption and management of access permissions. McAfee DLP Endpoint supports Microsoft Rights Management Service (RMS) and Seclore FileSecure as complementary methods of data protection. A typical use is to prevent copying files that are not IRM protected.

Classification software verifies that emails and other files are consistently classified and protectively labeled. McAfee DLP Endpoint integrates with Titus Message Classification and Boldon James Email Classifier for Microsoft Outlook to create email protection rules based on the applied classifications. It integrates with other Titus classification clients through the Titus SDK to create other protection rules based on the applied Titus classifications.

Screen reader support

Job Access With Sound (JAWS), the widely used screen reader software for the visually impaired, is supported on endpoint computers. The following McAfee DLP Endpoint features are supported:

- **End-user notification popup** — If the popup dialog is set to close manually (in DLP Policy Manager), dialog text is read allowing a visually impaired person to navigate the buttons and links.

- **End-user justification dialog** — The combo box is accessible with the tab key, and justification can be selected with arrow keys.

- **End-user console Notification History tab** — When the tab is selected, JAWS reads, "Notification history tab selected." There is no actionable content. All information in the right pane is read.

- **End-user console Discovery tab** — When the tab is selected, JAWS reads, "Discovery tab selected." There is no actionable content. All information in the right pane is read.
• **End-user console Tasks tab** — When the tab is selected, JAWS reads, "Tasks tab selected." All steps are accessible with the tab key, and appropriate instructions are read.

• **End-user console About tab** — When the tab is selected, JAWS reads, "About tab selected." There is no actionable content. All information in the right pane is read.

**Multiple user sessions**

The McAfee DLP Endpoint client software supports Fast User Switching (FUS) with multiple user sessions on those versions of the Windows operating system that support FUS. Virtual desktop support can also lead to multiple users sessions on a single host computer.

**Endpoint console**

The endpoint console was designed to share information with the user and to facilitate self-remediation of problems. It is configured on the Client Configuration | User Interface Service tab.

On Windows-based computers, the console is activated from the icon in the System Tray by selecting Manage Features | DLP Endpoint Console. Fully configured, it has four tabbed pages:

• **Notifications History** — Displays events, including details of aggregated events.

• **Discovery** — Displays details of discovery scans.

• **Tasks** — Generates ID codes and enter release codes for agent bypass and quarantine.

• **About** — Displays information about agent status, active policy, configuration, and computer assignment group, including revision ID numbers.

**McAfee DLP Endpoint on the OS X platform**

McAfee DLP Endpoint for Mac prevents unauthorized use of removable devices and provides protection for sensitive content on the endpoint computer and network shares.

McAfee DLP Endpoint for Mac supports removable storage and plug-and-play device rules. It also supports the following data protection rules:

• Network share protection rules

• Removable storage protection rules

• Application file access protection rules

You can identify sensitive content with classifications, as on Windows-based computers, but registered documents and tagging are not supported. Manual classifications are recognized, but there is no option to set them or see them in the user interface. Text extraction is supported, as are evidence encryption and business justification definitions.
**Endpoint console**

On Mac endpoints, the console is activated from the McAfee menulet on the status bar. The Dashboard is integrated with other installed McAfee software such as McAfee® VirusScan® for Mac, and displays an overview of the status of all installed McAfee software. The Event Log page displays recent McAfee software events. Click an entry to view the details.

![McAfee Endpoint Security for Mac Event Log](image)

*Figure 1-3 McAfee DLP Endpoint for Mac endpoint display*

To activate the agent bypass screen, select Preferences from the menulet.
Deployment and installation

Determine the deployment option that best suits your environment, then install the software and deploy the McAfee DLP Endpoint clients to the enterprise computers.

---

Chapter 2  Deployment options and scenarios
Chapter 3  Install the McAfee DLP Endpoint or Device Control software
Chapter 4  Deploying the client software and policies
Deployment options and scenarios

Classifying corporate information into different data loss prevention categories is a key step in deploying and administering McAfee Data Loss Prevention Endpoint software.

Contents

- Planning your deployment
- System requirements

Planning your deployment

The ideal schema depends on your enterprise goals and needs, and is unique for each installation. Choosing between the two DLP options — McAfee Device Control and full McAfee DLP Endpoint — is the first step in determining how those needs are met.

Best practice: Deploying to a sample group

Because it might be hard to determine in advance exactly what your unique needs are, deploy initially to a sample group of 15–20 users for a trial period of about a month. During this trial, no data is classified, and a policy is created to monitor, not block, transactions. The monitoring data helps the security officers make good decisions about where and how to classify corporate data. The policies created from this information are then tested on a larger test group or, for large companies, on a series of successively larger groups, before being deployed to the whole enterprise.

Installation

McAfee DLP policy design and monitoring software is installed in McAfee ePO. In a simple installation, one McAfee ePO server with Microsoft SQL Server is used, but for larger enterprises multiple server installations or cluster environments are possible.

McAfee DLP Endpoint client software can be deployed to Microsoft Windows servers, workstations, and laptops in either Device Control or full McAfee DLP Endpoint versions.
McAfee DLP Endpoint and Device Control options

The recommended installation for a simple McAfee DLP Endpoint implementation is on a single McAfee ePO server.

For recommendations on whether to use a separate server for the McAfee ePO database in more complex installations, see the McAfee ePolicy Orchestrator Hardware Sizing and Bandwidth Usage Guide.

Figure 2-1   McAfee DLP Endpoint components and relationships

The recommended architecture includes:

- **McAfee ePO server** — Hosts the embedded McAfee DLP Endpoint, Incident Manager, and Operations consoles, and communicates with McAfee Agent software on the endpoint computers.
- **McAfee ePO Event Parser** — Communicates with the McAfee Agent and stores event information in a database.
- **DLP Event Parser** — Collects McAfee DLP Endpoint events from the McAfee ePO Event Parser and stores them in DLP tables in the SQL database.
- **ePO database** — Communicates with the McAfee ePO Policy Distributor to distribute policies, and with the DLP Event Parser to collect events and evidence.
- **Administrator workstation** — Accesses McAfee ePO and the McAfee DLP Endpoint policy console in a browser.
- **Managed endpoint** — Applies the security policies using the following software:
  - **McAfee DLP Endpoint client** — A McAfee Agent plug-in that provides the McAfee DLP Endpoint policies and processes.
  - **McAfee Agent** — Provides the communication channel between the McAfee ePO server and the McAfee DLP Endpoint client software.
Deploying McAfee DLP Endpoint in Citrix environments

McAfee DLP Endpoint for Windows can be installed on Citrix controllers for XenApp and XenDesktop. Using McAfee DLP Endpoint for Windows in Citrix environments has the following requirements:

- Citrix XenApp 6.5 FP2, or 7.8
- Citrix XenDesktop 7.0, 7.5, or 7.8

Deploy McAfee Agent and McAfee DLP Endpoint client to the Citrix controllers, as to any endpoint. Deploy a McAfee DLP Endpoint for Windows client policy to the Citrix controllers.

McAfee DLP Endpoint client does not need to be deployed to the endpoints to work with Citrix. Citrix Receiver 4.4.1000 is all that is required. When the Windows endpoint connects to the Citrix controller and opens files or emails, rules are enforced.

How it works

Protection rules in Citrix have the following differences from McAfee DLP Endpoint installed on an enterprise computer:

- Citrix Device Rules are not supported when using a separate controller server with XenApp 7.8.
- Screen capture protection rules are not supported. This is because the screen capture is activated from the endpoint computer where the rule cannot take effect. For screen capture protection, install McAfee DLP Endpoint client on the endpoint computer.
- Clipboard protection rules are supported, but without popup notifications or events. This is because the attempted copy action takes place on the Citrix controller, where rules are supported, but the attempted paste action takes place on the endpoint, and cannot activate the popup or generate an event.

These limitations do not apply if you use RDP to connect to the Citrix controller.

System requirements

Each McAfee DLP product has its own set of requirements.

For a list of system requirements for McAfee DLP Endpoint, see the McAfee Data Loss Prevention Endpoint Release Notes.
Install the McAfee DLP Endpoint or Device Control software

The McAfee DLP Endpoint console is fully integrated in McAfee ePO. McAfee DLP Endpoint clients are deployed by McAfee ePO to the enterprise computers.

Contents
- Install and license the McAfee DLP extension
- Install the McAfee DLP Endpoint and Device Control client software

Install and license the McAfee DLP extension

The extension provides the user interface for configuring McAfee DLP in McAfee ePO.

Before you begin
- Download the McAfee DLP extension from the McAfee download site.
  You can also navigate in McAfee ePO to Menu | Software | Software Manager to view, download, and install the software.
- Verify that the McAfee ePO server name is listed under Trusted Sites in the Internet Explorer security settings.

You must enter at least one license key — more if you have multiple McAfee DLP products. The licenses you enter determines which configuration options in McAfee ePO are available to you.

You can enter a license for either McAfee DLP Endpoint or Device Control in the McAfee DLP Endpoint field. Replacing one type of license with another changes the configuration.

You can enter keys for these products:
- McAfee DLP Endpoint or Device Control
- McAfee DLP Discover
- McAfee DLP (network) version 9.3.4
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Software | Extensions**, then click **Install Extension**.

2. Browse to the extension .zip file and click **OK**.

   The installation dialog box displays the file parameters to verify that you are installing the correct extension.

3. Click **OK**. The extension is installed.

4. Install licenses and components to customize the installation.

   Installing the license activates the related McAfee ePO components and McAfee ePO Policy Catalog policies. The product license you have determines the McAfee DLP features available to you.

   a. Select **Menu | Data Protection | DLP Settings**.

   b. For each license that you want to add: In the **License Keys | Key** field, enter the license, then click **Add**.

5. In the **Default Evidence Storage** field, enter the path.

   The evidence storage path must be a network path, that is \\[server]\\[share]. This step is required to save the settings and activate the software.

6. (Optional) Edit the remaining settings on the page.

   The remaining settings have defaults. You can either accept the defaults and save the page, or edit them as required.

   a. Set the shared password.

   ![Best practice: For improved security, change the password.](image)

   b. Set the backward compatibility.

      For compatibility with older clients, select 9.4.0.0 or 9.4.200.0 compatibility. This setting limits the possibility of using new features.

      Two modes of compatibility are available: strict and non-strict. In strict mode, policies with backward compatibility errors cannot be applied. In non-strict mode, the policy owner, or a user with Administrator permissions, can choose to apply policies with backward compatibility errors.

   c. Set the Challenge-Response key length.

      The options are 8-character and 16-character keys.

   d. Set System Tree permissions.

      System Tree access permission can be used to filter information for incidents, events, queries, and dashboards.

   e. Select the **Incident Management** event product display option.

   f. Select the **Case Management** email options.

   g. Set the customized event time zone.

      Customized event time zone allows an administrator to order events according to his/her local time zone. The setting is the offset from UTC time.
7 Click Save.

8 To back up the configuration, click the Backup & Restore tab, then click Backup to file.

McAfee DLP modules appear in Menu | Data Protection according to the license.

Tasks

- **Applying backward compatibility on page 29**
  You can create backward-compatible policies to deploy to computers running older clients. This allow you to use the new extension with older client versions, providing large enterprises with an orderly upgrade path.

- **Convert policies and migrate data on page 30**
  Upgrading to McAfee DLP 10.0 from versions earlier than 9.4.100 requires migrating or converting incidents, operational events, or policies. McAfee ePO server tasks are used for the conversion/migration.

See also

- Applying backward compatibility on page 29
- Creating evidence folders on page 47

Applying backward compatibility

You can create backward-compatible policies to deploy to computers running older clients. This allow you to use the new extension with older client versions, providing large enterprises with an orderly upgrade path.

Backward compatibility is supported for McAfee DLP 9.4.0 and later policies. The options appear on the DLP Settings page (Menu | Data Protection | DLP Settings). Backward compatibility is not supported for McAfee DLP 9.3 policies. Policies from versions earlier than 9.4.0 must be migrated to the 9.4 schema.

Selecting the 9.4.0.0 compatibility option with non-strict mode can lead to errors in the policy when selecting rule options that are not supported in that version. If strict mode is in force, such policies fail when you try to apply them to the McAfee ePO database. If non-strict mode is in force, and there are compatibility errors in the policy, a warning window appears when you try to apply the policy.

Selecting the checkbox applies the policy with errors. The errors are displayed in the Policy Catalog on the active DLP Policy | Policy Validation page. The Details column on the page includes a description of what can happen if you apply the rule with the error to endpoint clients that don't support the feature. You can edit the rule from this page to correct the error.

Example – Device descriptions

Device definitions in McAfee DLP version 9.4.200 and 10.0 can have an optional parameter named Device Description that was not available in earlier versions. Using a device description to define a device definition, and including that definition in a Device Control rule, creates a rule set that cannot be enforced on 9.4.0 clients. If you accept the policy despite the warning, the error is displayed on the Policy Validation page. The Details field explains that the error "matches and performs reactions for devices you did not intend to match..." You can click Edit to repair the error.
Convert policies and migrate data

Upgrading to McAfee DLP 10.0 from versions earlier than 9.4.100 requires migrating or converting incidents, operational events, or policies. McAfee ePO server tasks are used for the conversion/migration.

**Before you begin**

This task describes upgrading from McAfee DLP Endpoint 9.3.x.

You can upgrade from McAfee DLP Endpoint 9.4.0 directly. You can set backward compatibility to support 9.4.0 clients, but must run the DLP Incident Events conversion from 9.4 to 9.4.1 and above server task if you want to display older incidents and operational events in the version 10.0 DLP Incident Manager or DLP Operations consoles.

Upgrade the McAfee DLP Endpoint extension to version 9.3.600 (9.3 Patch 6) or later, then install the McAfee DLP 9.4.100 or later extension in McAfee ePO.

The policy conversion task only converts rules that are enabled and applied to the database. To verify the status of rules you want to convert, review your McAfee DLP Endpoint 9.3 policy before conversion.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Automation | Server Tasks.

2. Select DLP Policy Conversion, then click Actions | Run.

   The Server Task Log page opens, allowing you to verify that the task is running. The converted policy is compatible with version 9.4.100 and later policies.

   The task fails if it has run previously. If you make changes to the McAfee DLP 9.3 policy and want to rerun the conversion, edit the server task by deselecting the option Do not run policy conversion if rule set [9.3] Policy Conversion Rule Set exists on the Actions page. The previous rule set is deleted and replaced.

3. Return to the Server Tasks page, select DLP Incident Migration, then click Actions | Edit.

   DLP Operational Events Migration is performed in the same way.

4. Select Schedule status | Enabled, then click Next twice.

   The migration is pre-programmed, so you can skip the Actions page.

5. Select a schedule type and occurrence.

   **Best practice:** Schedule the migration tasks for weekends or other non-work hours due to the load they place on the processor.

   a. Set the start date and end date to define a time period, and schedule the task for every hour.

   b. Schedule repeating the task according to the size of incident database you are migrating.

      Incidents are migrated in chunks of 200,000.

6. Click Next to review the settings, then click Save.

---

See also

Convert policies and migrate data on page 30
Install the McAfee DLP Endpoint and Device Control client software

Use McAfee ePO to deploy the client software to endpoint computers.
Clean install of McAfee DLP Endpoint 10.0 client software does not require restarting the endpoint computer. If you are upgrading the client from an earlier version, however, you must restart the endpoint computer after installation.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Software | Master Repository**.
2. In the Master Repository, click **Check In Package**.
3. Select package type **Product or Update (.ZIP)**. Click **Browse**.
   - For Microsoft Windows client, browse to ...\HDLP_Agent_10_0_0_xxx.zip. For Mac client, browse to ...\DlpAgentInstaller.zip.
4. Click **Next**.
5. Review the details on the Check in Package page, then click Save.
   - The package is added to the **Master Repository**.
Install the McAfee DLP Endpoint or Device Control software
Install the McAfee DLP Endpoint and Device Control client software
Deploying the client software and policies

McAfee DLP policies are enforced by the McAfee Agent on endpoint computers. The first step is deployment of the McAfee DLP Endpoint client software, a McAfee Agent plug-in, to the endpoints.

**Best practice:** Use McAfee ePO for client deployment. Manual deployment is possible in cases where McAfee ePO deployment is not possible.

**Contents**
- Deploy McAfee DLP Endpoint client with McAfee ePO
- Verify the installation
- Deploy policies with McAfee ePO

**Deploy McAfee DLP Endpoint client with McAfee ePO**

Before policies can be applied, McAfee DLP Endpoint client must be deployed to the endpoint computers by McAfee ePO.

**Before you begin**
A current version of McAfee Agent must be installed in McAfee ePO and deployed to the target computers before McAfee DLP Endpoint is deployed. See the **McAfee Data Loss Prevention Endpoint Release Notes** for the supported McAfee Agent versions for Microsoft Windows and Mac OS X endpoint computers.

Consult the McAfee ePO documentation on how to verify the version, and how to install it if necessary.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | System Tree**.
2. In the **System Tree**, select the level at which to deploy McAfee DLP Endpoint.

**Leaving the level at My Organization** deploys to all workstations managed by McAfee ePO.

If you select a level under **My Organization**, the right pane displays the available workstations. You can also deploy McAfee DLP Endpoint to individual workstations.
3 Open the **Client Task Builder** wizard: click the **Assigned Client Tasks** tab. Select **Actions | New Client Task Assignment**. The **Client Task Builder** wizard opens.

4 Fill in the Task Builder fields:
- In the **Product** field, select **McAfee Agent**.
- In the **Task Type** field, select **Product Deployment**.

5 Click **Create New Task**.

6 In the **Products and Components** field, select **Data Loss Prevention 9.4**. The **Action** field automatically resets to **Install**. Click **Save**.

7 Change the **Schedule type** to **Run immediately**. Click **Next**.

8 Review the task summary. When you are satisfied that it is correct, click **Save**. The task is scheduled for the next time the McAfee Agent updates the policy. To force the installation to take place immediately, issue an agent wake-up call.

9 After McAfee DLP Endpoint has been deployed, restart the managed computers.

**Verify the installation**

After installing McAfee DLP Endpoint software, verify the installation in the **DLP Operations** console.

**Task**

1 In McAfee ePO, select **Menu | Data Protection | DLP Operations**. Click an event to view the details.

![Figure 4-1  DLP Operations details pane](image)

2 Verify the McAfee DLP Endpoint client software installation from the McAfee Agent system tray icon on the endpoint computer by selecting **About**. Scroll through the information for McAfee DLP Endpoint.

**Deploy policies with McAfee ePO**

McAfee DLP Endpoint policies contain rule sets, classifications, definitions, and client and server configurations.

McAfee DLP Endpoint works with these policies:
- DLP policy
- Client configuration
Each of these policies is assigned the revision number 1 when it is created, and the number is incremented each time the policy is changed. The revision number is important for supporting troubleshooting processes, to ensure that policy changes are actually applied to the endpoint computers. It is also used when requesting a client bypass or uninstall key. The DLP Endpoint console on the client computer displays the current policy revision numbers.

Before applying a policy, verify that:

- All settings are configured correctly.
- All rules are enabled.
- End User Groups (where required) are assigned to each rule.

**Assign a policy or client configuration**

Policies applied to McAfee ePO must be assigned and deployed to managed computers in order to be used.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | System Tree**.
2. Locate the directory containing the computers that will be assigned a policy, and select them.
3. Select **Actions | Agent | Wake Up Agents**.
4. Select **Agent Wake-Up Call**, and set **Randomization** to 0 minutes. Click **OK**.
5. When the agent wake-up call is completed, you are returned to the System Tree. Reselect the computers that will be assigned a policy, and click **Actions | Agent | Set Policy & Inheritance**.
6. On the **Assign Policy** page:
   a. From the drop-down **Product** list, select **Data Loss Prevention [version]**.
   b. From the drop-down **Category** list, select the policy you want to assign: **DLP Policy**, **Windows Client Configuration**, or **Mac OS X Client Configuration**.
   c. From the drop-down **Policy** list, select the policy to assign.
7. Click the **Break inheritance** option, then click **Save**.

**Refresh the policy**

The system policy deployment relies on the McAfee ePO server, and the policy refresh on the managed computer is performed in accordance with the McAfee Agent settings. You can, however, refresh in McAfee ePO without waiting for the scheduled refresh.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | System Tree, then select the computer or computers to be refreshed.
2. Click More Actions | Wake Up Agents.
3. Select the wake-up call type, and set Randomization to 0 minutes. Click OK.

---

Policies are updated on a scheduled basis by the McAfee ePO server. Users of managed computers do not refresh policies manually unless specifically instructed to do so.
Configuration and use

Configure the software for optimized use in the enterprise environment based on management decisions of what content to protect, and how best to protect it.

Chapter 5       Configuring system components
Chapter 6       Protecting removable media
Chapter 7       Classifying sensitive content
Chapter 8       Working with policies
Chapter 9       Protecting sensitive content
Chapter 10      Scanning data with McAfee DLP Endpoint discovery
Configuring system components

System components can be customized to best fit the needs of your enterprise. By configuring the agent and system options, you can optimize the system to safeguard sensitive enterprise information efficiently.

Contents
- Policy Catalog
- Configuring McAfee DLP in the Policy Catalog
- Protecting files with rights management
- Documenting events with evidence
- Controlling assignments with users and permission sets
- Configure manual classification

Policy Catalog

The McAfee ePO Policy Catalog can display the following McAfee DLP policy configurations:

- **DLP Policy** — Contains the Active Rule Sets assigned to the policy, scheduled Endpoint Discovery scans, Settings for application strategy, device class overrides, and privileged users, and Policy Validation.

- **Server Configuration** — Contains the McAfee DLP Discover configuration. Allows you to set the evidence copy service and logging options, Rights Management and SharePoint settings, and text extractor options.

  The server configuration displays only if a McAfee DLP Discover license is registered.

- **Client Configurations** — Separate configurations for Windows and OS X computers contain the configuration settings for the McAfee DLP Endpoint clients. The settings determine how clients apply McAfee DLP policies on the endpoint computers.

Configuring McAfee DLP in the Policy Catalog

McAfee DLP uses the McAfee ePO Policy Catalog to store policies and client configurations.

McAfee DLP creates policies in the McAfee ePO Policy Catalog:

- DLP Policy
- Server configuration
- Client configuration

The DLP Policy consists of Active Rule Sets, the Endpoint Discovery configuration, Settings, and Policy Validation.
The Server Configuration policy is where you enable the Evidence Copy Service for McAfee Data Loss Prevention Discover, and enter the path to the evidence storage share. It is also where you set the Logging parameters — logger output type and log level.

The client configuration policies contains settings that determine how the endpoint computers work with policies.

### Import or export the McAfee DLP Endpoint configuration

Endpoint policy configurations can be saved in HTML format for backup or to transfer policies to other McAfee ePO servers.

- **Do not use this procedure to save DLP Policy configurations.** While the Export option does save the file, Import fails to import it. To save DLP Policies, use the Backup & Restore page in DLP Settings.

#### Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Policy Catalog | Product | Data Loss Prevention.

2. Do one of the following:

   - To export, click Export. In the Export window, right-click the file link and select Save Link As to save the policy as an XML file.

   ![The Export button exports all policies. You can export an individual policy by selecting Export in the Actions column in the policy name row.]

   - To import a saved policy, click Import. In the Import Policies window, browse to a saved policy, click Open, then OK.

   The import window opens, displaying the policies you are about to import and whether there is a naming conflict. You can deselect any conflicting policies and not import them. If you choose to import a policy with a name conflict, it overwrites the existing policy and assumes its assignments.

### Client configuration

The McAfee DLP Endpoint client software for McAfee Agent resides on enterprise computers and executes the defined policy. The software also monitors user activities involving sensitive content. Client configuration is stored in the policy, which is deployed to managed computers.

- The Policy Catalog comes with McAfee default policies for Windows and OS X endpoint configurations and DLP policy. Click Duplicate (in the Actions column) to create an editable copy as a base for your policy.

The client configuration is stored in the policy, which is deployed to managed computers by McAfee ePO. If the configuration is updated, you must redeploy the policy.

### Client Service WatchDog

To maintain normal operation of McAfee DLP Endpoint software even in the event of malicious interference, McAfee DLP Endpoint runs a protective service called the Client Service WatchDog. This service monitors the McAfee DLP Endpoint software, and restarts it if it stops running for any reason. The service is enabled by default. If you want to verify that it is running, look in the Microsoft Windows Task Manager processes for the service named fcagswd.exe.

- The Client Service WatchDog is not supported on McAfee DLP Endpoint for Mac.
Client configuration settings

Client configuration settings determine how the endpoint software operates. Most of the client configuration settings have reasonable defaults that can be used for initial setup and testing without alteration.

![Best practice: To verify that the client configuration settings continue to meet your requirements, review them at regular intervals.]

The following table lists some of the more important settings to verify.

### Table 5-1  Endpoint configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Configuration</td>
<td>Microsoft Windows client: Run DLP client in Safe Mode</td>
<td>Disabled by default. When enabled, McAfee DLP Endpoint is fully functional when the computer is started in Safe Mode. A recovery mechanism exists in case the McAfee DLP Endpoint client causes a boot failure.</td>
</tr>
<tr>
<td>Content Tracking</td>
<td>Use the following fallback ANSI code page</td>
<td>If no language is set, the fallback is the default language of the endpoint computer.</td>
</tr>
<tr>
<td></td>
<td>Whitelisted Processes</td>
<td>Add processes and extensions to whitelist.</td>
</tr>
<tr>
<td>Corporate connectivity</td>
<td>Corporate Network Detection</td>
<td>You can apply different prevent actions to endpoint computers in the corporate network or outside the network. For some rules, you can apply different prevent actions when connected by VPN. To use the VPN option, or to determine network connectivity by corporate server rather than by connection to McAfee ePO, set the server IP address in the relevant section.</td>
</tr>
<tr>
<td></td>
<td>Corporate VPN Detection</td>
<td></td>
</tr>
<tr>
<td>Email Protection</td>
<td>Email Caching</td>
<td>Stores tag signatures from emails to disk to eliminate re-parsing emails.</td>
</tr>
<tr>
<td></td>
<td>Email Handling API</td>
<td>Outgoing email is handled by either Outlook Object Model (OOM) or Messaging Application Programming Interface (MAPI). OOM is the default API, but some configurations require MAPI.</td>
</tr>
<tr>
<td></td>
<td>Outlook 3rd party add-in integration</td>
<td>Two third-party classification applications are supported: Titus and Boldon James.</td>
</tr>
<tr>
<td></td>
<td>Email Timeout Strategy</td>
<td>Sets the maximum time to analyze an email and the action if the time is exceeded.</td>
</tr>
<tr>
<td>Evidence Copy Service</td>
<td>Evidence Storage share UNC</td>
<td>Replace the example text with the evidence storage share.</td>
</tr>
<tr>
<td></td>
<td>Client Settings</td>
<td>You can change the way hit highlighting is displayed by setting classification matches to all matches or abbreviated results.</td>
</tr>
<tr>
<td>Operational Mode and Modules</td>
<td>Operational Mode</td>
<td>Set Device Control or full McAfee DLP Endpoint mode. Reset this parameter if you upgrade or downgrade licensing.</td>
</tr>
<tr>
<td>Data Protection Modules</td>
<td>Activate required modules</td>
<td></td>
</tr>
<tr>
<td>Web Post Protection (Windows client only)</td>
<td>Web protection evaluation</td>
<td>Select inputs for web request evaluation when matching web protection rules. These settings allow blocking requests sent by AJAX to a different URL from the one displayed in the address bar. At least one option must be selected.</td>
</tr>
<tr>
<td></td>
<td>Process HTTP GET requests</td>
<td>GET requests are disabled by default because they are resource-intensive. Use this option with caution.</td>
</tr>
</tbody>
</table>
### Table 5-1 Endpoint configuration (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported Chrome versions</td>
<td>If you use Google Chrome, click <strong>Browse</strong> to add the current list of supported versions. The list is an XML file that you download from McAfee Support.</td>
<td></td>
</tr>
<tr>
<td>Web Timeout strategy</td>
<td>Sets the web post analysis timeout, action to perform if timeout is exceeded, and optional user message.</td>
<td></td>
</tr>
<tr>
<td>Whitelisted URLs</td>
<td>Lists URLs excluded from web post protection rules.</td>
<td></td>
</tr>
</tbody>
</table>

### Support for client configuration parameters

McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac are configured in separate client policies.

### Table 5-2 Debugging and Logging page

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Operating system support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative events reported by the clients</td>
<td>The filter settings that apply to both McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac are:</td>
</tr>
<tr>
<td></td>
<td>• Client Enters Bypass Mode</td>
</tr>
<tr>
<td></td>
<td>• Client Leaves Bypass Mode</td>
</tr>
<tr>
<td></td>
<td>• Client Installed</td>
</tr>
<tr>
<td></td>
<td>All other settings apply to McAfee DLP Endpoint for Windows only.</td>
</tr>
<tr>
<td>Logging</td>
<td>Supported on both McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac.</td>
</tr>
</tbody>
</table>

### Table 5-3 User Interface Components page

<table>
<thead>
<tr>
<th>Section</th>
<th>Parameter</th>
<th>Operating system support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client User Interface</td>
<td>Show DLP Console (all options)</td>
<td>McAfee DLP Endpoint for Windows only</td>
</tr>
<tr>
<td></td>
<td>Enable end-user notification popup</td>
<td>McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac</td>
</tr>
<tr>
<td></td>
<td>Show request justification dialog</td>
<td>McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac</td>
</tr>
<tr>
<td>Challenge and Response</td>
<td>All options</td>
<td>McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac</td>
</tr>
<tr>
<td>Release code lockout policy</td>
<td>All options</td>
<td>McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac</td>
</tr>
<tr>
<td>Client Banner Image</td>
<td>All options</td>
<td>McAfee DLP Endpoint for Windows only</td>
</tr>
</tbody>
</table>

### Protecting files with rights management

McAfee DLP Endpoint and McAfee DLP Discover can integrate with rights management (RM) servers to apply protections to files that match rule classifications.

> With McAfee DLP Endpoint version 10.0, you must install Active Directory Rights Management Services Client 2.1 build 1.0.2004.0 on each endpoint computer using RM services. The **Apply RM** command does not work without this version of the RM client.

You can apply an RM policy reaction to these data protection and discovery rules:
• Cloud protection
• Endpoint file system

**Information**

RM policies cannot be used with Device Control rules.

McAfee DLP can recognize RM protected files by adding a file encryption property to either content classification or content fingerprinting criteria. These files can be included or excluded from the classification.

**How McAfee DLP works with rights management**

McAfee DLP follows a workflow to apply RM policies to files.

**RM workflow**

1. Create and apply a data protection or a discovery rule with a reaction to apply RM policy. The reaction requires an RM server and an RM policy entry.

2. When a file triggers the rule, McAfee DLP sends the file to the RM server.

3. The RM server applies protections based on the specified policy, such as encrypting the file, limiting the users allowed to access or decrypt the file, and limiting the conditions in which the file can be accessed.

4. The RM server sends the file back to the source with the applied protections.

5. If you’ve configured a classification for the file, McAfee DLP can monitor the file.

When the McAfee DLP software applying the file system discovery rule finds a file to protect, it uses the template GUID as a unique identifier to locate the template and apply protection.

**Limitations**

McAfee DLP Endpoint software does not inspect RM protected files for content. When a classification is applied to a file that is RM protected, only content fingerprint criteria (location, application, or web application) are maintained. If a user modifies the file, all fingerprint signatures are lost when the file is saved.

**Supported RM servers**

McAfee DLP Endpoint supports Microsoft Windows Rights Management Services (Microsoft RMS) and Seclore FileSecure™ information rights management (IRM). McAfee DLP Discover supports Microsoft RMS.

**Microsoft RMS**

McAfee DLP supports Microsoft RMS on Windows Server 2003 and Active Directory RMS (AD-RMS) on Windows Servers 2008 and 2012. You can apply Windows Rights Management Services protection to:

<table>
<thead>
<tr>
<th>Document type</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Excel</td>
<td></td>
</tr>
<tr>
<td>Microsoft PowerPoint</td>
<td></td>
</tr>
<tr>
<td>SharePoint</td>
<td>2007</td>
</tr>
<tr>
<td>Exchange Server</td>
<td></td>
</tr>
</tbody>
</table>
With Microsoft RMS, McAfee DLP can inspect the content of protected files if the current user has view permissions.


**Seclore IRM**

McAfee DLP Endpoint supports Seclore FileSecure RM, which supports over 140 file formats including most commonly used document formats:

- Microsoft Office documents
- Open Office documents
- PDF
- Text and text-based formats, including CSV, XML, and HTML
- Image formats, including JPEG, BMP, GIF and so forth
- Engineering design formats, including DWG, DXF, and DWF

The McAfee DLP Endpoint client works with the FileSecure desktop client to provide online and offline integration.

For more information on Seclore IRM, go to http://seclore.com/seclorefilesecure_overview.html.

**Define a Rights Management server**

McAfee DLP Endpoint supports two Rights Management (RM) systems: Microsoft Windows Rights Management Services (RMS) and Seclore FileSecure™. To use these systems, configure the server providing the RM policies in McAfee ePO.

**Before you begin**

- Set up the RM servers and create users and policies. Obtain the URL and password for all servers – policy template, certification, and licensing. For Seclore, you need the *Hot Folder Cabinet ID* and *passphrase*, and information on advanced licenses, if any.
- Verify that you have permission to view, create, and edit Microsoft RMS and Seclore servers. In McAfee ePO, select **Menu | User Management | Permission Sets**, and verify that you belong to a group that has the required permissions in **Registered Servers**.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Registered Servers**.
2. Click **New Server**.
   
   The **Registered Servers** description page opens.
3. From the **Server type** drop-down list, select the type of server you want to configure: **Microsoft RMS Server** or **Seclore Server**.
4. Type a name for the server configuration, then click **Next**.
5 Enter the required details. When you have entered the required fields, click Test Connectivity to verify the data entered.

- RMS settings also include a DLP enforcement settings section. The Local path to RMS template field is optional, but the URL fields for certification and licensing are required unless you choose the AD auto-service discovery option.

- Seclore requires HotFolder Cabinet information, but additional license information is optional.

6 Click Save when you have completed the configuration.

---

**Documenting events with evidence**

Evidence is a copy of the file or email that caused a security event to be posted to the DLP Incident Manager.

**Using evidence and evidence storage**

Most rules allow the option of storing evidence. When this option is selected, an encrypted copy of the content that was blocked or monitored is stored in the predefined evidence folder on the endpoint computer.

When the McAfee DLP passes information to the server, the folder is purged and the evidence is stored in the server evidence folder. You can specify the maximum size and age of local evidence storage when the computer is offline.

**Prerequisites for evidence storage**

Enabling evidence storage is the default condition for McAfee DLP. If you do not want to save evidence, you can improve performance by disabling the evidence service. The following are either required or set as defaults when setting up the software:

- **Evidence storage folder** — Creating an evidence storage folder and specifying the UNC path to the folder are requirements for applying a policy to McAfee ePO. Specify the path in the Policy Catalog on the Evidence Copy Service page of the configuration policy.

- **Evidence copy service** — The evidence copy service for McAfee DLP is enabled on the Operational Mode and Modules page of the client configuration policy. Reporting Service, under which it is a subentry, must also be enabled for evidence collection. For McAfee DLP Discover, the service is activated in the server configuration policy.

**Evidence storage and memory**

The number of evidence files stored per event has implications for storage volume, event parser performance, and the screen rendering (and thus user experience) of the DLP Incident Manager and DLP Operations pages. To handle different evidence requirements, McAfee DLP software does the following:

- The maximum number of evidence files to store per event is set on the Evidence Copy Service page of the client configuration policy. The default is 1,000.

- When many evidence files are linked to one event, only the first 100 file names are stored in the database and displayed in the DLP Incident Manager details page. The remaining evidence files (up to the set maximum) are stored in the evidence storage share, but are not associated with the event. Reports and queries that filter evidence based on file name have access only to these first 100 file names.

- The DLP Incident Manager field Total Match Count displays the total evidence count.
Hit highlighting

The hit highlighting option helps administrators identify exactly which sensitive content caused an event. When selected, it stores an encrypted HTML evidence file with extracted text.

The evidence file is made up of snippets, where a snippet for content classifications or content fingerprints typically contains the sensitive text, with 100 characters preceding it and 100 characters after it (for context) organized by the content classification or content fingerprint that triggered the event, and including a count of the number of events per content classification or content fingerprint. If there are multiple hits within 100 characters of the previous hit, those hits are highlighted, and the highlighted text together with the next 100 characters are added to the snippet. If the hit is in the header or footer of a document, the snippet contains the highlighted text without the 100 character prefix or suffix.

Display options are set on the Evidence Copy Service page of the client configuration policy in the Classification matches file field:

- Create abbreviated results (default)
- Create all matches
- Disabled — Disables the hit highlighting feature

Abbreviated results can contain up to 20 snippets. An all matches hit highlight file can contain an unlimited number of snippets, but there is a limit on the number of hits per classification. For Advanced Pattern and Keyword classifications, the limit is 100 hits. For Dictionary classifications, the limit is 250 hits per dictionary entry. If there are multiple classifications in a hit highlight file, the classification names and the match counts are displayed at the beginning of the file, before the snippets.

Rules allowing evidence storage

These rules have the option of storing evidence.

Table 5-4 Evidence saved by rules

<table>
<thead>
<tr>
<th>Rule</th>
<th>What is saved</th>
<th>Product</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application File Access Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>Clipboard Protection Rule</td>
<td>Copy of the clipboard</td>
<td></td>
</tr>
<tr>
<td>Cloud Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>Email Protection Rule</td>
<td>Copy of the email</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>Network Share Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>Printer Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>Removable Storage Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>Screen Capture Protection Rule</td>
<td>JPEG of the screen</td>
<td>McAfee DLP Discover</td>
</tr>
<tr>
<td>Web Post Protection Rule</td>
<td>Copy of the web post</td>
<td></td>
</tr>
<tr>
<td>File System Discovery Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>Email Storage Discovery Rule</td>
<td>Copy of the .msg file</td>
<td>McAfee DLP Discover</td>
</tr>
<tr>
<td>Box Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Discover</td>
</tr>
<tr>
<td>File Server (CIFS) Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
<tr>
<td>SharePoint Protection Rule</td>
<td>Copy of the file</td>
<td>McAfee DLP Endpoint</td>
</tr>
</tbody>
</table>
Creating evidence folders

Evidence folders contain information used by all McAfee DLP software products for creating policies and for reporting. Depending on your McAfee DLP installation, certain folders and network shares must be created, and their properties and security settings must be configured appropriately.

Evidence folder paths are set in different locations in the various McAfee DLP products. When more than one McAfee DLP product is installed in McAfee ePO, the UNC paths for the evidence folders are synchronized. The folders do not need to be on the same computer as the McAfee DLP Database server, but it is usually convenient to put them there.

- **Evidence folder** — Certain rules allow for storing evidence, so you must designate, in advance, a place to put it. If, for example, a file is blocked, a copy of the file is placed in the evidence folder.
- **Copy and move folders** — Used by McAfee DLP Discover to remediate files.

The evidence storage path must be a network share, that is, it must include the server name.

We suggest the following folder paths, folder names, and share names, but you can create others as appropriate for your environment.

- \c:\dlp_resources\`
- \c:\dlp_resources\evidence
- \c:\dlp_resources\copy
- \c:\dlp_resources\move

Controlling assignments with users and permission sets

McAfee DLP uses McAfee ePO Users and Permission Sets to assign different parts of the McAfee DLP administration to different users or groups.

- **Best practice**: Create specific McAfee DLP permission sets, users, and groups.
- **Best practice**: Create different roles by assigning different administrator and reviewer permissions for the different McAfee DLP modules in McAfee ePO.

System Tree filtering permissions support

McAfee DLP Endpoint supports McAfee ePO System Tree filtering permissions in the DLP Incident Manager and DLP Operations. When System Tree filtering is enabled, McAfee ePO operators can only see incidents from computers in their permitted part of the System Tree. Group Administrators do not have any permissions in the McAfee ePO System Tree by default. Regardless of permissions assigned in the Data Loss Prevention permission set, they cannot see any incidents in DLP Incident Manager or DLP Operations. System Tree filtering is disabled by default, but can be enabled in DLP Settings.

- **Best practice**: For customers who have been using Group Administrators in Data Loss Prevention permission sets, give Group Administrators
  - View "System Tree" tab permission (under Systems)
  - System Tree access permissions at the appropriate level

Sensitive data redaction and the McAfee ePO permission sets

To meet the legal demand in some markets to protect confidential information in all circumstances, McAfee DLP Endpoint software offers a data redaction feature. Fields in the DLP Incident Manager and DLP Operations consoles with confidential information can be redacted to prevent unauthorized viewing. Links to sensitive evidence are hidden. The feature is designed with a "double key" release. Thus, to use the feature, you must create two permission sets: one to view the incidents and events...
and another to view the redacted fields (supervisor permission). Both roles can be assigned to the same user.

See also
Install and license the McAfee DLP extension on page 27

Create end-user definitions
McAfee DLP accesses Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) servers to create end-user definitions.

End-user groups are used for administrator assignments and permissions, and in protection and device rules. They can consist of users, user groups, or organizational units (OU), thus allowing the administrator to choose an appropriate model. Enterprises organized on an OU model can continue using that model, while others can use groups or individual users where required.

LDAP objects can be identified by name or security ID (SID). SIDs are more secure, and permissions can be maintained even if accounts are renamed. On the other hand, they are stored in hexadecimal, and have to be decoded to convert them to a readable format.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager.
2 Click the Definitions tab.
3 Select Source/Destination | End-User Group, then Actions | New.
4 In the New End-User Group page, enter a unique name and optional description.
5 Select the method of identifying objects (SID or name).
6 Click one of the Add... buttons (Add Users, Add Groups, Add OU).
   The selection window opens displaying the selected type of information.
   The display might take a few seconds if the list is long. If no information appears, select Container and children from the Preset drop-down menu.
7 Select names and click OK to add them to the definition.
   Repeat the operation as required to add additional users, groups, or organizational users.
8 Click Save.

Assigning McAfee DLP permission sets
McAfee DLP permission sets assign permissions to view and save policies, and view redacted fields. They are also used to assign role-based access control (RBAC).

Installing the McAfee DLP server software adds the McAfee ePO permission set Data Loss Prevention. If a previous version of McAfee DLP is installed on the same McAfee ePO server, that permission set also appears.

The permission set cover all sections of the management console. There are three levels of permissions:

• Use — The user can see only names of objects (definitions, classifications, and so forth), not details.

   For policies, the minimum permission is no permission.
• **View and use** — The user can view details of objects, but cannot change them.

• **Full permission** — The user can create and change objects.

You can set permissions for different sections of the management console, giving administrators and reviewers different permissions as required. The sections are grouped by logical hierarchy, for example, selecting **Classifications** automatically selects **Definitions** because configuring classification criteria requires using definitions.

- Policy Catalog
- DLP Policy Manager
- Classifications
- Definitions

- DLP Policy Manager
- Classifications
- Definitions

- Classifications
- Definitions

Incident Management, Operational Events, and Case Management can be selected separately.

Permissions for Data Loss Prevention Actions have been moved to the Help Desk Actions permission set. These permissions allow administrators to generate client bypass and uninstall keys, release from quarantine keys, and master keys.

In addition to the default permission for the section, you can set an override for each object. The override can either increase or decrease the permission level. For example, in the DLP Policy Manager permissions, all rule sets existing when the permission set is created are listed. You can set a different override for each one. When new rule sets are created, they receive the default permission level.

![Figure 5-1  McAfee DLP permission sets](image)

**Create a McAfee DLP permission set**

Permission sets are used to define different administrative and reviewer roles in McAfee DLP software.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | User Management | Permission Sets**.

2. Select a predefined permission set or click **New** to create a permission set.
   a. Type a name for the set and select users.
   b. Click **Save**.
3 Select a permission set, then click **Edit** in the **Data Loss Prevention** section.

   a In the left pane, select a data protection module.
   
   Incident Management, Operational Events, and Case Management can be selected separately. Other options automatically create predefined groups.

   b Edit the options and override permissions as required.

   Policy Catalog has no options to edit. If you are assigning Policy Catalog to a permission set, you can edit the sub-modules in the Policy Catalog group.

   c Click **Save**.

**Tasks**

- **Use case: DLP administrator permissions on page 50**
  
  You can separate administrator tasks as required — for example, to create a policy administrator with no event review responsibilities.

- **Use case: Limit DLP Incident Manager viewing with redaction permissions on page 50**
  
  To protect confidential information, and to meet legal demands in some markets, McAfee DLP Endpoint offers a data redaction feature.

**Use case: DLP administrator permissions**

You can separate administrator tasks as required — for example, to create a policy administrator with no event review responsibilities.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select **Menu | Permission Sets**.

2 Click **New** to create a permission set.

   a Type a name for the set and select users.

   To edit a policy, the user must be the policy owner or a member of the global administrator permission set.

   b Click **Save**.

3 In the **Data Loss Prevention** permissions set, select **Policy Catalog**.

   DLP Policy Manager, Classifications, and Definitions are selected automatically.

4 In each of the three submodules, verify that the user has full permissions and full access.

   Full permissions is the default setting.

   The administrator can now create and change policies, rules, classifications, and definitions.

**Use case: Limit DLP Incident Manager viewing with redaction permissions**

To protect confidential information, and to meet legal demands in some markets, McAfee DLP Endpoint offers a data redaction feature.

When using data redaction, specific fields in the DLP Incident Manager and DLP Operations displays containing confidential information are encrypted to prevent unauthorized viewing, and links to evidence are hidden.

   The fields **computer name** and **user name** are predefined as private.
This example shows how to set up the DLP Incident Manager permissions for a redaction reviewer — a single administrator who cannot view actual incidents, but can reveal encrypted fields when required for another reviewer viewing the incident.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | User Management | Permission Sets**

2. Create permission sets for regular reviewers and for the redaction reviewer.
   a. Click **New** (or **Actions | New**).
   b. Enter a name for the group such as DLPE Incident Reviewer or Redaction Reviewer.
      
      You can assign different types of incidents to different reviewer groups. You must create the groups in **Permission Sets** before you can assign incidents to them.
   c. Assign users to the group, either from available McAfee ePO users or by mapping Active Directory users or groups to the permission set. Click **Save**.

   The group appears in the left panel **Permission Sets** list.

3. Select a standard reviewer permission set, then click **Edit** in the **Data Loss Prevention** section.
   a. In the left pane, select **Incident Management**.
   b. In the **Incidents Reviewer** section, select **User can view incidents assigned to the following permission sets**, click the choose icon, and select the relevant permission set or sets.
   c. In the **Incidents Data Redaction** section, deselect the default **Supervisor permission**, and select the **Obfuscate sensitive incidents data** option.

      Selecting this option activates the redaction feature. Leaving it deselected displays all data fields in clear text.
   d. In the **Incident Tasks** section, select or deselect tasks as required.
   e. Click **Save**.

4. Select the redaction reviewer permission set, then click **Edit** in the **Data Loss Prevention** section.
   a. In the left pane, select **Incident Management**.
   b. In the **Incidents Reviewer** section, select **User can view all incidents**.

      In this example, we assume a single redaction reviewer for all incidents. You can also assign different redaction reviewers for different sets of incidents.
   c. In the **Incidents Data Redaction** section, select both the **Supervisor permission** and the **Obfuscate sensitive incidents data** option.
   d. In the **Incident Tasks** section, deselect all tasks.

      Redaction reviewers do not normally have other reviewer tasks. This is optional according to your specific requirements.
   e. Click **Save**.
Configure manual classification

Manual classification has several options that specify how the feature works, and what messages are displayed.

Manual classification allows end-users to add classifications to files from the Windows Explorer right-click menu. For Microsoft Office applications and Outlook, manual classifications can be applied when saving files or sending emails.

Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO select Menu | Data Protection | Classification.
2. Click Manual Classification.
3. From the View drop-down list, select General Settings.
4. Select or deselect options to optimize to your enterprise requirements.
5. (Optional) Select additional information to add to the email by clicking and selecting a notification definition or creating one.

The notifications support the Locales feature for all supported languages.

See also

Manual classification on page 78
Customizing end-user messages on page 110
Embedded tags on page 79
Protecting removable media

McAfee® Device Control protects enterprises from the risk associated with unauthorized transfer of sensitive content whenever storage devices are used.

Device Control can monitor or block devices attached to enterprise-managed computers, allowing you to monitor and control their use in the distribution of sensitive information. Devices such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or plug-and-play devices can all be controlled.

McAfee Device Control is a component of McAfee DLP Endpoint that is sold as a separate product. While the term Device Control is used throughout this section, all features and descriptions apply to McAfee DLP Endpoint as well. Implementation of Device Control rules on Microsoft Windows and OS X computers is similar, but not identical. The table below identifies some of the differences.

### Table 6-1 Device Control terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Applies to operating systems:</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device class</td>
<td>Windows</td>
<td>A collection of devices that have similar characteristics and can be managed in a similar manner. Device classes have the status Managed, Unmanaged, or Whitelisted.</td>
</tr>
<tr>
<td>Device definition</td>
<td>Windows, OS X</td>
<td>A list of device properties used to identify or group devices.</td>
</tr>
<tr>
<td>Device property</td>
<td>Windows, OS X</td>
<td>A property such as bus type, vendor ID, or product ID that can be used to define a device.</td>
</tr>
<tr>
<td>Device rule</td>
<td>Windows, OS X</td>
<td>Defines the action taken when a user attempts to use a device that has a matching device definition in the policy. The rule is applied to the hardware, either at the device driver level or the file system level. Device rules can be assigned to specific end-users.</td>
</tr>
<tr>
<td>Managed device</td>
<td>Windows</td>
<td>A device class status indicating that the devices in that class are managed by Device Control.</td>
</tr>
<tr>
<td>Removable storage device rule</td>
<td>Windows, OS X</td>
<td>Used to block or monitor a device, or set it as read-only.</td>
</tr>
<tr>
<td>Removable storage protection rule</td>
<td>Windows, OS X</td>
<td>Defines the action taken when a user attempts to copy content labeled as sensitive to a managed device.</td>
</tr>
<tr>
<td>Unmanaged device</td>
<td>Windows</td>
<td>A device class status indicating that the devices in that class are not managed by Device Control.</td>
</tr>
<tr>
<td>Whitelisted device</td>
<td>Windows</td>
<td>A device class status indicating that the devices in that class cannot be managed by Device Control because attempts to manage them can affect the managed computer, system health, or efficiency.</td>
</tr>
</tbody>
</table>
Protecting devices

USB drives, small external hard drives, smartphones, and other removable devices can be used to remove sensitive data from the enterprise.

USB drives are an easy, cheap, and almost-untraceable method of downloading large amounts of data. They are often considered the "weapon of choice" for unauthorized data transfer. Device Control software monitors and controls USB drives and other external devices, including smartphones, Bluetooth devices, plug-and-play devices, audio players, and non-system hard disks. Device Control runs on most Microsoft Windows and OS X operating systems, including servers. See the system requirements page in this guide for details.

McAfee Device Control protection is built in three layers:

- **Device classes** — Collections of devices that have similar characteristics and can be managed in a similar manner. Device classes apply only to plug-and-play device definitions and rules, and are not applicable to OS X operating systems.
- **Device definitions** — Identify and group devices according to their common properties.
- **Device rules** — Control the behavior of devices.

A device rule consists of a list of the device definitions included or excluded from the rule, and the actions taken when use of the device triggers the rule. In addition, it can specify end-users included or excluded from the rule. They can optionally include an application definition to filter the rule according to the source of the sensitive content.

**Removable storage protection rules**

In addition to device rules, Device Control includes one data protection rule type. Removable storage protection rules include one or more classifications to define the sensitive content that triggers the rule. They can optionally include an application definition or web browser URL, and can include or exclude end users.

> Web browser URLs are not supported on McAfee DLP Endpoint for Mac.

Managing devices with device classes

A device class is a collection of devices that have similar characteristics and that can be managed in a similar manner.

Device classes name and identify the devices used by the system. Each device class definition includes a name and one or more globally unique identifiers (GUIDs). For example, the Intel® PRO/1000 PL Network Connection and Dell wireless 1490 Dual Band WLAN Mini-Card are two devices that belong to the Network Adapter device class.

> Device classes are not applicable to OS X devices.
How device classes are organized

The DLP Policy Manager lists predefined (built-in) device classes on the Definitions tab under Device Control. Device classes are categorized by status:

- **Managed** devices are specific plug-and-play or removable storage devices that are managed by McAfee DLP Endpoint.
- **Unmanaged** devices are not managed by Device Control in the default configuration.
- **Whitelisted** devices are devices that Device Control does not try to control, such as battery devices or processors.

To avoid potential system or operating system malfunction, the device classes cannot be edited, but they can be duplicated and changed to add user-defined classes to the list.

**Best practice:** Do not add a device class to the list without first testing the consequences. In the Policy Catalog, use the DLP policy | Device Classes | Settings tab to create temporary device class overrides to device class status and filter type settings.

Overrides can be used for testing user-defined changes before creating a permanent class, as well as troubleshooting device control problems.

Device Control uses device definitions and plug-and-play device control rules to control the behavior of managed device classes and specific devices belonging to a managed device class. Removable storage device rules, on the other hand, do not require a managed device class. The reason is related to the different way the two types of device rules use device classes:

- Plug-and-play device rules are triggered when the hardware device is plugged into the computer. Since the reaction is to a device driver, the device class must be managed for the device to be recognized.
- Removable storage device rules are triggered when a new file system is mounted. When this occurs, the Device Control client associates the drive letter with the specific hardware device and checks the device properties. Since the reaction is to a file system operation (that is, when the file system is mounted) the device class does not need to be managed.

**See also**

Create a device class on page 56

Define a device class

If a suitable device class does not exist on the predefined list, or is not created automatically when new hardware is installed, you can create a new device class in the McAfee DLP Endpoint Policy Manager console.

**Obtain a GUID**

Device class definitions require a name and one or more globally unique identifiers (GUIDs).

Some hardware devices install their own new device class. To control the behavior of plug-and-play hardware devices that define their own device class, you must first add a new device class to the Managed status in the Device Classes list.

A device class is defined by two properties: a name and a GUID. The name of a new device is displayed in the device manager, but the GUID is displayed only in the Windows Registry and there is no easy way to obtain it. To ease the retrieval of new device names and GUIDs, the Device Control client reports a New Device Class Found event to the DLP Incident Manager when a hardware device that does not belong to a recognized device class is plugged into the host computer.
Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select (Menu | Data Protection | DLP Incident Manager | Incident List).

2 Click Edit next to the Filter drop-down list to edit the filter criteria.

3 In the Available Properties list (left pane), select Incident Type.

4 Verify that the Comparison drop-down list value is Equals.

5 From the Values drop-down list, select Device New Class Found.

6 Click Update Filter.

The Incident List displays the new device classes found on all endpoint computers.

7 To view the name and GUID of a specific device, double-click the item to display the incident details.

Create a device class
Create a device class if a suitable device class does not exist on the predefined list or is not created automatically when new hardware is installed.

Before you begin
Obtain the device GUID before beginning this task.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Definitions.

2 In the left pane, select Device Control | Device Class.

3 Do one of the following:
   • Select Actions | New.
   • Locate a similar device class on the built-in device class list, then click Duplicate in the Actions column. Click Edit for the duplicated device class.

4 Enter a unique Name and optional Description.

5 Verify the Status and Filter Type required.

6 Enter the GUID, then click Add.

   The GUID must be in the correct format. You are prompted if you enter it incorrectly.

7 Click Save.

See also
Managing devices with device classes on page 54
Organizing devices with device definitions on page 57
Organizing devices with device definitions

A device definition is a list of device properties such as bus type, device class, vendor ID and product ID.

The role of device definitions is to identify and group devices according to their common device properties. Some device properties can be applied to any device definition, others are exclusive to a specific device type or types.

Available device definitions types are:

- **Fixed hard drive devices** attach to the computer and are not marked by the operating system as removable storage. Device Control can control fixed hard drives other than the boot drive.

- **Plug-and-play devices** are added to the managed computer without any configuration or manual installation of DLLs and drivers. Plug-and-play devices include most Microsoft Windows devices. Apple OS X devices are supported for USB only.

- **Removable storage devices** are external devices containing a file system that appear on the managed computer as drives. Removable storage device definitions support either Microsoft Windows or Apple OS X operating systems.

- **Whitelisted plug-and-play devices** do not interact with device management properly and might cause the system to stop responding or cause other serious problems. Supported for Microsoft Windows devices only.

Whitelisted plug-and-play device definitions are added automatically to the excluded list in every plug-and-play device control rule. They are never managed, even if the parent device class is managed.

Removable storage device definitions are more flexible and include additional properties related to the removable storage devices.

**Best practice:** Use the removable storage device definitions and rules to control devices that can be classified as either, such as USB mass storage devices.

See also
Create a device class on page 56

Working with device definitions

Multiple parameters are added to device definitions as either logical OR (by default) or logical AND. Multiple parameter types are always added as logical AND.

For example, the following parameter selection:
Creates this definition:

- Bus Type is one of: Firewire (IEEE 1394) OR USB
- AND Device Class is one of Memory Devices OR Windows Portable Devices

**Create a device definition**

Device definitions specify the properties of a device to trigger the rule.

**Best practice:** Create whitelisted plug-and-play definitions for devices that do not cleanly handle management, which could cause the system to stop responding or create other serious problems. No action will be taken on these devices even when a rule is triggered.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager | Definitions**.
2. In the left pane, select **Device Control | Device Definitions**.
3. Select **Actions | New**, then select the type of definition.
4. Enter a unique **Name** and optional **Description**.
5. Select the **Applies to** option for Microsoft Windows or OS X devices.

   The Available Properties list changes to match properties for the operating system selected.

6. Select properties for the device.

   - To add a property, click >.
   - To remove a property, click <.
   - To add additional values for the property, click +.
     Values are added as logical **OR** by default. Click the and/or button to change it to **AND**.
   - To remove properties, click -.

7. Click **Save**.

**Create a whitelisted plug-and-play definition**

The purpose of whitelisted plug-and-play devices is to deal with those devices that do not handle device management well. If not whitelisted, they might cause the system to stop responding or cause other serious problems. Whitelisted plug-and-play definitions are not supported on McAfee DLP Endpoint for Mac.

Whitelisted plug-and-play devices are added to plug-and-play device rules on the **Exceptions** tab. They are never managed, even if their parent device class is managed.

**Best practice:** To avoid compatibility problems, add devices that do not handle device management well to the whitelisted device list.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu** | **Data Protection** | **DLP Policy Manager** | **Definitions**.

2. In the left pane, select **Device Control** | **Device Definitions**, then select **Actions** | **New** | **Whitelisted Plug and Play Device Definition**.

3. Enter a unique **Name** and optional **Description**.

4. Select properties for the device.
   - To add a property, click >.
   - To remove a property, click <.
   - To add additional values for the property, click +.
     Values are added as logical OR by default. Click the and/or button to change it to AND.
   - To remove properties, click −.

5. Click **Save**.

---

**Create a removable storage device definition**
A removable storage device is an external device containing a file system that appears on the managed computer as a drive. Removable storage device definitions are more flexible than plug-and-play device definitions, and include additional properties related to the devices.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu** | **Data Protection** | **DLP Policy Manager** | **Definitions**.

2. In the left pane, select **Device Control** | **Device Definitions**, then select **Actions** | **New** | **Removable Storage Device Definition**.

3. Enter a unique **Name** and optional **Description**.

4. Select the **Applies to** option for Microsoft Windows or OS X devices.
   The **Available Properties** list changes to match properties for the operating system selected.

5. Select properties for the device.
   - To add a property, click >.
   - To remove a property, click <.
   - To add additional values for the property, click +.
     Values are added as logical OR by default. Click the and/or button to change it to AND.
   - To remove properties, click −.

6. Click **Save**.
Create a serial number and user pair definition
You can create exceptions for Plug and Play and removable storage device rules based on paired device serial numbers and user identities. By linking the device to the logged on user, you create a higher level of security.

Before you begin
Obtain the device serial numbers for the devices you are adding to the definition.

Serial number and user pair definitions are not supported on McAfee DLP Endpoint for Mac.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Definitions.
2 In the left pane, select Device Control | Serial Number & End User Pair.
3 Select Actions | New.
4 Enter a unique Name and optional Description.
5 Enter the required information in the text boxes at the bottom of the page, then click Add. Repeat as required to add additional serial number and end-user pairs.
   For User Type | Everyone, leave the End-User field blank. If you are specifying a user, use the format user@name.domain.
6 Click Save.

See also
Device properties on page 60

Device properties
Device properties specify device characteristics such as the device name, bus type, or file system type.

The table provides device property definitions, which definition types use the property, and which operating system they apply to.
### Table 6-2  Types of device properties

<table>
<thead>
<tr>
<th>Property name</th>
<th>Device definition</th>
<th>Applies to operating systems:</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus Type</td>
<td>All</td>
<td>• Windows — Bluetooth, Firewire (IEEE1394), IDE/SATA, PCI, PCMIA, SCSI, USB • Mac OS X — Firewire (IEEE1394), IDE/SATA, SD, Thunderbolt, USB</td>
<td>Selects the device BUS type from the available list. For plug and play device rules, McAfee DLP Endpoint for Mac only supports USB bus type.</td>
</tr>
<tr>
<td>CD/DVD Drives</td>
<td>Removable storage</td>
<td>• Windows • Mac OS X</td>
<td>Select to indicate any CD or DVD drive.</td>
</tr>
<tr>
<td>Content encrypted by Endpoint Encryption</td>
<td>Removable storage</td>
<td>Windows</td>
<td>Devices protected with Endpoint Encryption.</td>
</tr>
<tr>
<td>Device Class</td>
<td>Plug and play</td>
<td>Windows</td>
<td>Selects the device class from the available managed list.</td>
</tr>
<tr>
<td>Device Compatible IDs</td>
<td>All</td>
<td>Windows</td>
<td>A list of physical device descriptions. Effective especially with device types other than USB and PCI, which are more easily identified using PCI VendorID/DeviceID or USB PID/VID.</td>
</tr>
<tr>
<td>Device Instance ID</td>
<td>All</td>
<td>Windows</td>
<td>A Windows-generated string that uniquely identifies the device in the system. Example: USB\VID_0930&amp;PID_6533\5&amp;26450FC&amp;0&amp;6.</td>
</tr>
<tr>
<td>Device Friendly Name</td>
<td>All</td>
<td>• Windows • Mac OS X</td>
<td>The name attached to a hardware device, representing its physical address.</td>
</tr>
<tr>
<td>Property name</td>
<td>Device definition</td>
<td>Applies to operating systems:</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| File System Type             | • Fixed hard disk                 | • Windows — CDFS, exFAT, FAT16, FAT32, NTFS, UDFS                                                 | The type of file system.  
• For hard disks, select one of exFAT, FAT16, FAT32, or NTFS.  
• For removable storage devices, any of the above plus CDFS or UDFS.                                                                                                                                  |
|                              | • Removable storage               | • Mac OS X — CDFS, exFAT, FAT16, FAT32, HFS/HFS+, NTFS, UDFS                                    |                                                                                                                                                                                                          |
|                              |                                   | Mac OS X supports FAT only on disks other than the boot disk.  
Mac OS X supports NTFS as read-only.                                                                                                                                                                       |
| File System Access           | Removable storage                 | • Windows                                                                                      | The access to the file system: read only or read-write.                                                                                                                                                   |
|                              |                                   | • Mac OS X                                                                                     |                                                                                                                                                                                                          |
| File System Volume Label     | • Fixed hard disk                 | • Windows                                                                                      | The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.                                                                                                                     |
|                              | • Removable storage               | • Mac OS X                                                                                     |                                                                                                                                                                                                          |
| File System Volume Serial Number | Fixed hard disk                | Windows                                                                                       | A 32-bit number generated automatically when a file system is created on the device. It can be viewed by running the command-line command dir x:, where x: is the drive letter.                                  |
|                              | • Removable storage               |                                                                                               |                                                                                                                                                                                                          |
| PCI VendorID / DeviceID      | All                               | Windows                                                                                       | The PCI VendorID and DeviceID are embedded in the PCI device. These parameters can be obtained from the Hardware ID string of physical devices.                                                          |
|                              |                                   |                                                                                               | Example:  
PCI\VEN_8086&DEV_2580&SUBSYS_00000000 &REV_04                                                                                                                                                    |
| TrueCrypt devices            | Removable storage                 | Windows                                                                                       | Select to specify a TrueCrypt device.                                                                                                                                                                    |
| USB Class Code               | Plug and play                     | Windows                                                                                       | Identifies a physical USB device by its general function. Select the class code from the available list.                                                                                                  |
### Table 6-2  Types of device properties (continued)

<table>
<thead>
<tr>
<th>Property name</th>
<th>Device definition</th>
<th>Applies to operating systems:</th>
<th>Description</th>
</tr>
</thead>
</table>
| USB Device Serial Number    | • Plug and play                    | • Windows                           | A unique alphanumeric string assigned by the USB device manufacturer, typically for removable storage devices. The serial number is the last part of the instance ID.  
**Example:**  
USB\VID_3538&PID_0042\00000000002CD8  
A valid serial number must have a minimum of 5 alphanumeric characters and must not contain ampersands (&). If the last part of the instance ID does not follow these requirements, it is not a serial number. |
|                             | • Removable storage                | • Mac OS X                          |                                                                                                                                             |
| USB Vendor ID / Product ID  | • Plug and play                    | • Windows                           | The USB VendorID and ProductID are embedded in the USB device. These parameters can be obtained from the Hardware ID string of physical devices.  
**Example:**  
USB\Vid_3538&Pid_0042  |
|                             | • Removable storage                | • Mac OS X                          |                                                                                                                                             |

### Device control rules

Device control rules define the action taken when particular devices are used.

<table>
<thead>
<tr>
<th>Device control rule</th>
<th>Description</th>
<th>Supported on</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removable Storage Device Rule</td>
<td>Used to block or monitor removable storage devices, or set as read-only. The user can be notified of the action taken.</td>
<td>McAfee DLP Endpoint for Windows, McAfee DLP Endpoint for Mac</td>
</tr>
<tr>
<td>Plug-and-play Device Rule</td>
<td>Used to block or monitor plug-and-play devices. The user can be notified of the action taken.</td>
<td>McAfee DLP Endpoint for Windows, McAfee DLP Endpoint for Mac (USB devices only)</td>
</tr>
<tr>
<td>Removable Storage File Access Rule</td>
<td>Used to block executables on plug-in devices from running.</td>
<td>McAfee DLP Endpoint for Windows</td>
</tr>
<tr>
<td>Fixed Hard Drive Rule</td>
<td>Used to block or monitor fixed hard drives, or set as read-only. The user can be notified of the action taken. Fixed hard drive device rules do not protect the boot or system partition.</td>
<td>McAfee DLP Endpoint for Windows</td>
</tr>
<tr>
<td>Citrix XenApp Device Rule</td>
<td>Used to block Citrix devices mapped to shared desktop sessions.</td>
<td>McAfee DLP Endpoint for Windows</td>
</tr>
<tr>
<td>TrueCrypt Device Rule</td>
<td>Used to protect TrueCrypt devices. Can be used to block, monitor, or set to read-only. The user can be notified of the action taken.</td>
<td>McAfee DLP Endpoint for Windows</td>
</tr>
</tbody>
</table>
Create a removable storage device rule

Removable storage devices appear on the managed computer as drives. Use removable storage device rules to block use of removable devices, or to set them to read-only. They are supported on both McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac.

Removable storage device rules do not require a managed device class due to the difference in how the two types of device rules use device classes:

- Plug-and-play device rules are triggered when the hardware device is plugged into the computer. Since the reaction is to a device driver, the device class must be managed for the device to be recognized.

- Removable storage device rules are triggered when a new file system is mounted. When file system mount occurs, the McAfee DLP Endpoint software associates the drive letter with the specific hardware device and checks the device properties. Since the reaction is to a file system operation, not a device driver, the device class does not need to be managed.

Device rules have an Enforce on parameter that applies the rule to either Windows or OS X or both. Device definitions used in device rules have an Applies to parameter that specifies either Windows devices or Mac OSX devices. When selecting device definitions, match the operating system in the definition and the rule. The McAfee DLP Endpoint clients for both operating systems ignore properties that do not apply to that system. But you cannot save a rule that, for example, enforces on Windows only but contains Mac OS X device definitions.

Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Rule Sets.
2. Select Actions | New Rule Set, or edit an existing rule set.
3. Click the rule set name to open the rule set for editing. Click the Device Control tab.
5. Enter a unique Rule Name.
6. (Optional) Change the status and select a severity.
7. Deselect the McAfee DLP Endpoint for Windows or McAfee DLP Endpoint for Mac OS X checkbox if the rule applies to only one operating system.
8. On the Condition tab, select one or more removable storage device definitions. Optional: assign end-user groups and a Process Name to the rule.
9. (Optional) On the Exceptions tab, select a whitelisted definition and fill in the required fields. You can add multiple exceptions by adding more than one whitelisted definition.
10. On the Reaction tab, select a Prevent Action. Optional: add a User Notification, and Report Incident. If you don’t select Report Incident there is no record of the incident in the DLP Incident Manager.
11. (Optional) Select a different Prevent Action when the end-user is working outside the corporate network.
12. Click Save.
Create a plug-and-play device rule

Use plug-and-play device rules to block or monitor plug-and-play devices. They are supported on both McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac. On OS X computers, support is for USB devices only.

A plug-and-play device is a device that can be added to the managed computer without any configuration or manual installation of DLLs and drivers. For plug-and-play device rules to control Microsoft Windows hardware devices, the device classes specified in device definitions used by the rule must be set to Managed status.

Device rules have an Enforce on parameter that applies the rule to either Windows or OS X or both. Device definitions used in device rules have an Applies to parameter that specifies either Windows devices or Mac OS X devices. When selecting device definitions, match the operating system in the definition and the rule. The McAfee DLP Endpoint clients for both operating systems ignore properties that do not apply to that system. But you cannot save a rule that, for example, enforces on Windows only but contains Mac OS X device definitions.

Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Rule Sets.
2. Select Actions | New Rule Set, or edit an existing rule set.
3. To open the rule set for editing, click the rule set name. Click the Device Control tab.
5. Enter a unique rule name.
6. (Optional) Change the status and select a severity.
7. Deselect the McAfee DLP Endpoint for Windows or McAfee DLP Endpoint for Mac OS X checkbox if the rule applies to only one operating system.
8. On the Condition tab, select one or more plug-and-play device definitions.
9. (Optional) Assign end-user groups to the rule.
10. (Optional) On the Exceptions tab, select a whitelisted definition and fill in the required fields. You can add multiple exceptions by adding more than one whitelisted definition.
   If you don’t select Report Incident, there is no record of the incident in the DLP Incident Manager.
12. (Optional) Select a different Prevent Action when the end user is working outside the corporate network, or is connected by VPN.
13. Click Save.

See also

Use case: Block and charge an iPhone with a plug-and-play device rule on page 120
Create a removable storage file access device rule

Use removable storage file access rules to block executables on plug-in devices from running.

Task

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Rule Sets.
2 Select Actions | New Rule Set, or edit an existing rule set.
3 Click the rule set name to open the rule set for editing. Click the Device Control tab.
5 Enter a unique Rule Name.
6 (Optional) Change the status and select a severity.
7 On the Condition tab, select one or more removable storage device definitions. (Optional) assign end-user groups to the rule.
8 (Optional) Change the default True File Type or File Extension definitions according to your requirements.
9 (Optional) On the Exceptions tab, select Whitelisted File Names, and fill in the required fields.
   The File Name exception is for applications that must be allowed to run. An example is encryption applications on encrypted drives.
10 On the Reaction tab, select a Prevent Action. (Optional) add a User Notification, and Report Incident.
    If you don’t select Report Incident there is no record of the incident in the DLP Incident Manager.
11 (Optional) Select a different Prevent Action when the end-user is working outside the corporate network.
12 Click Save.

See also

Removable storage file access rules on page 68

Create a fixed hard drive device rule

Use fixed hard drive device rules to control hard drives attached to the computer and not marked by the operating system as removable storage. They are supported on McAfee DLP Endpoint for Windows only.

Fixed hard drive rules include a drive definition with an action to block or make read-only, an end-user definition, and optional user notification. They do not protect the boot or system partition.

Task

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Rule Sets.
2 Select Actions | New Rule Set, or edit an existing rule set.
3 Click the rule set name to open the rule set for editing. Click the Device Control tab.
4 Select Actions | New Rule | Fixed Hard Drive Rule.
5 Enter a unique Rule Name.
6 (Optional) change the status and select a severity.

7 On the Condition tab, select one or more fixed hard drive device definitions. (Optional) assign end-user groups to the rule.

8 (Optional) On the Exceptions tab, select a whitelisted definition and fill in the required fields. You can add multiple exceptions by adding more than one whitelisted definition.

9 On the Reaction tab, select a Prevent Action. Optional: add a User Notification, and Report Incident. If you don’t select Report Incident there is no record of the incident in the DLP Incident Manager.

10 (Optional) Select a different Prevent Action when the end-user is working outside the corporate network.

11 Click Save.

Create a Citrix device rule

Use Citrix device rules to block Citrix devices mapped to shared desktop sessions. Citrix XenApp device rules are supported on Windows-based computers only. McAfee DLP Endpoint software can block Citrix devices mapped to shared desktop sessions. Floppy disk, fixed, CD, removable, and network drives can all be blocked, as well as printers and clipboard redirection. You can assign the rule to specific end users.

Task

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Rule Sets.

2 Select Actions | New Rule Set, or edit an existing rule set.

3 Click the rule set name to open the rule set for editing. Click the Device Control tab.


5 Enter a unique Rule Name.

6 (Optional) Change the status and select a severity.

7 On the Condition tab, select one or more resources.

8 (Optional) Assign end-user groups to the rule.

9 (Optional) On the Exceptions tab, fill in the required fields for whitelisted users.

10 Click Save.

The selected resources are blocked.

The only Prevent Action for Citrix rules is Block. You do not need to set the action on the Reaction pane.

Create a TrueCrypt device rule

Use TrueCrypt device rules to block or monitor TrueCrypt virtual encryption devices, or set them to read-only. They are supported on McAfee DLP Endpoint for Windows only.

TrueCrypt device rules are a subset of removable storage device rules. TrueCrypt encrypted virtual devices can be protected with TrueCrypt device rules or with removable storage protection rules.
• Use a device rule if you want to block or monitor a TrueCrypt volume, or make it read-only.
• Use a protection rule if you want content-aware protection of TrueCrypt volumes.

McAfee DLP Endpoint client software treats all TrueCrypt mounts as removable storage, even when the TrueCrypt application is writing to the local disk.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager | Rule Sets**.
2. Select **Actions | New Rule Set**, or edit an existing rule set.
3. Click the rule set name to open the rule set for editing. Click the **Device Control** tab.
4. Select **Actions | New Rule | TrueCrypt Device Rule**.
5. Enter a unique **Rule Name**.
6. (Optional) Change the status and select a severity.
7. (Optional) On the **Condition** tab, assign end-user groups to the rule.
8. (Optional) On the **Exceptions** tab, fill in the required fields for whitelisted users.
9. On the **Reaction** tab, select a **Prevent Action**. (Optional) add a **User Notification**, and **Report Incident**.
   If you don’t select **Report Incident** there is no record of the incident in the DLP Incident Manager.
10. (Optional) Select a different **Prevent Action** when the end-user is working outside the corporate network.
11. Click **Save**.

**Removable storage file access rules**
Removable storage file access rules are used to block executables on plug-in devices from running. They are supported on Microsoft Windows computers only.

Removable storage file access rules block removable storage devices from running applications. You can specify included and excluded devices in the rule. Because some executables, such as encryption applications on encrypted devices, must be allowed to run, the rule includes a **File Name | is none of** parameter to exempt named files from the blocking rule.

File access rules use true file type and extension to determine which files to block. True file type identifies the file by its internally registered data type, providing accurate identification even if the extension was changed. By default, the rule blocks compressed files (.zip, .gz, .jar, .rar, and .cab) and executables (.bat, .bin, .cgi, .com, .cmd, .dll, .exe, .class, .sys, and .msi). You can customize the file extension definitions to add any file type required.

File access rules also block executable files from being copied to removable storage devices because the file filter driver cannot differentiate between opening and creating an executable.
Classifying sensitive content

Classifications identify and track sensitive content and files.

Contents
- Components of the Classification module
- Using classifications
- Classification definitions and criteria
- Manual classification
- Registered documents
- Whitelisted text
- Create and configure classifications
- Configure classification components for McAfee DLP Endpoint
- Create classification definitions
- Use case: Integrate Titus Client with third-party tags
- Use case: Integrate Boldon James Email Classifier with classification criteria

Components of the Classification module

McAfee DLP uses two mechanisms to classify sensitive content: content classifications and content fingerprinting, and two modes: automatic and manual classification.

Automatic classifications are defined in McAfee DLP and distributed by McAfee ePO in the policies deployed to endpoint computers. They are then applied to content according to the criteria that define them. Manual classifications are applied by authorized users to files and emails on their endpoint computers.

Content classifications include data and file conditions that define sensitive content. The classification criteria are compared to the content when a data protection, endpoint discovery, or McAfee DLP Discover rule is triggered.

Content fingerprints are defined by application (that is, the application that created the file or the web application that opened the file) or by location. They can also include data and file conditions. They are applied to content when it is used, even if no rule is triggered.

The Classification module in McAfee DLP stores content classification and fingerprinting criteria, and the definitions used to configure them. It is also the place for setting up registered documents repositories, user authorization for manual classification and fingerprinting, and whitelisted text.

Content classification criteria are supported on McAfee DLP Endpoint for Windows, McAfee DLP Endpoint for Mac, and on McAfee DLP Discover. Content fingerprinting, registered documents, and whitelisted text are supported only on McAfee DLP Endpoint for Windows. McAfee DLP Endpoint for Mac and McAfee DLP Discover can recognize manual classifications, but cannot set or view them.

The module provides these features:
• **Manual Classification** — Configures the end-user groups allowed to manually classify or fingerprint content

• **Definitions** — Defines the content, properties, and location of files for classification

• **Classification** — Creates classifications and defines content classification and fingerprinting criteria

• **Register Documents** — Uploads files containing known sensitive content

• **Whitelisted Text** — Uploads files containing text for whitelisting

---

### Using classifications

Classifications identify and track sensitive content by applying content fingerprints or classification criteria to files and content.

McAfee DLP identifies and tracks sensitive content with user-defined classifications. All McAfee DLP products support classification criteria. McAfee DLP Endpoint for Windows also supports content fingerprints. Content fingerprints label the sensitive information, and the label stays with the content even if it is copied into another document or saved to a different format.

#### Content classification criteria

Classification criteria identify sensitive text patterns, dictionaries, keywords, or combinations of these. Combinations can be simply multiple named properties, or properties with a defined relationship known as proximity. They can also specify file conditions such as the file type, document properties, file encryption, or location in the file (header/body/footer).

#### Content fingerprint criteria

Content fingerprint criteria are applied to files or content based on one of these options:

- **Application-based** — The application that created or changed the file.
- **Location-based** — The network share or the removable storage definition of where the file is stored.
- **Web-based** — The web addresses that opened or downloaded the files.

All data and file conditions available to classification criteria are also available to content fingerprint criteria, allowing fingerprints to combine the functionality of both criteria types.

Content fingerprint signatures are stored in a file's extended file attributes (EA) or alternate data streams (ADS) and are applied to a file when the file is saved. If a user copies or moves fingerprinted content to another file, the fingerprint criteria are applied to that file. If the fingerprinted content is removed from the file, the content fingerprint signatures are also removed.

McAfee DLP Endpoint applies content fingerprint criteria to files after a policy is applied regardless of whether the classification is used in a protection rule or not.

### Applying criteria

Criteria are applied to a file in one of these ways:

- McAfee DLP Endpoint applies criteria when:
  - The file matches a configured classification.
  - The file or sensitive content is moved or copied to a new location.
  - A file is matched during a discovery scan.
• A user with permission manually adds criteria to a file.

See also
Create classification criteria on page 81
Create content fingerprinting criteria on page 83
Assign manual classification permissions on page 84

Classify by file destination
In addition to classifying content by its originating location, you can classify and control where content is being sent. In data loss prevention parlance, this is known as data-in-motion.
File protection rules controlling destinations include:
• Cloud Protection rules
• Email Protection rules
• Network Communication Protection rules (outgoing)
• Printer Protection rules
• Removable Storage Protection rules
• Web Post Protection rules

Working with email
McAfee DLP Endpoint protects sensitive data in email headers, body, or attachments when emails are sent. Email storage discovery detects emails with sensitive data in OST or PST files and either tags or quarantines them.
McAfee DLP Endpoint protects sensitive content in email by classifying and tagging content and blocking emails with sensitive content from being sent. The email protection policy can specify different rules for different users and email destinations, or for emails protected with encryption or Rights Management.

See also
Email protection rules on page 104

Define network parameters
Network definitions serve as filter criteria in network protection rules.
• Network Addresses monitor network connections between an external source and a managed computer. The definition can be a single address, a range, or a subnet. You can include and exclude defined network addresses in network communication protection rules.
• Network Port definitions in network communication protection rules allow you to exclude specific services as defined by their network ports. A list of common services and their ports is built in. You can edit the items on the list, or create your own definitions.
• Network Share definitions specify shared network folders in network share protection rules. You can include or exclude defined shares.

Working with printers
Printer protection rules manage both local and network printers, and either block or monitor the printing of confidential material.
Printer protection rules in McAfee DLP Endpoint 9.4 support advanced mode and V4 printers. Defined printers and end-users can be included or excluded from a rule. Image printers and PDF printers can be included in the rule.
Printer protection rules can include application definitions. You can define whitelisted processes that are exempted from printer protection rules in the Policy Catalog | Data Loss Prevention 9.4 | Client Configuration | Printing Protection setting.

**Controlling information uploaded to websites**

Web addresses are used in web post protection rules. You can use web address definitions to block tagged data from being posted to defined web destinations (websites or specific pages in a website), or use them to prevent tagged data from being posted to websites that are not defined. Typically, the web address definitions define any internal websites as well as external websites where posting tagged data is allowed.

**Classifying by file location**

Sensitive content can be defined by where it is located (stored) or by where it is used (file extension or application).

McAfee DLP Endpoint uses several methods to locate and classify sensitive content. *Data-at-rest* is the term used to describe file locations. It classifies content by asking questions like "where is it in the network?" or "which folder is it in?" *Data-in-use* is the term used to define content by how or where it is used. It classifies content by asking questions like "which application called it?" or "what is the file extension?"

McAfee DLP Endpoint Discovery rules find your data-at-rest. They can search for content in endpoint computer files or email storage (PST, mapped PST, and OST) files. Depending on the properties, applications, or locations in the rule classification, the rule can search specified storage locations and apply encryption, quarantine, or RM policies. Alternately, the files can be tagged or classified to control how they are used.

**Text extraction**

The text extractor parses the file content when files are opened or copied and compares it to text patterns and dictionary definitions in the classification rules. When a match occurs, the criteria are applied to the content.

McAfee DLP supports accented characters. When an ASCII text file contains a mix of accented characters, such as French and Spanish, as well as some regular Latin characters, the text extractor might not correctly identify the character set. This issue occurs in all text extraction programs. There is no known method or technique to identify the ANSI code page in this case. When the text extractor cannot identify the code page, text patterns and content fingerprint signatures are not recognized. The document cannot be properly classified, and the correct blocking or monitoring action cannot be taken. To work around this issue, McAfee DLP uses a fallback code page. The fallback is either the default language of the computer or a different language set by the administrator.

**Text extraction with McAfee DLP Endpoint**

Text extraction is supported on Microsoft Windows and Apple OS X computers.

The text extractor can run multiple processes depending on the number of cores in the processor.

- A single core processor runs only one process.
- Dual-core processors run up to two processes.
- Multi-core processors run up to three simultaneous processes.

If multiple users are logged on, each user has their own set of processes. Thus, the number of text extractors depends on the number of cores and the number of user sessions. The multiple processes can be viewed in the Windows Task Manager. Maximum memory usage for the text extractor is configurable. The default is 75 MB.
How McAfee DLP Endpoint categorizes applications

Before you create classifications or rule sets using applications, you should understand how McAfee DLP Endpoint categorizes them, and the effect this has on system performance.

This categorization is not supported on McAfee DLP Endpoint for Mac.

McAfee DLP Endpoint software divides applications into four categories called strategies. These affect how the software works with different applications. You can change the strategy to achieve a balance between security and the computer's operating efficiency.

The strategies, in order of decreasing security, are:

- **Editor** — Any application that can modify file content. This includes "classic" editors like Microsoft Word and Microsoft Excel, as well as browsers, graphics software, accounting software, and so forth. Most applications are editors.

- **Explorer** — An application that copies or moves files without changing them, such as Microsoft Windows Explorer or certain shell applications.

- **Trusted** — An application that needs unrestricted access to files for scanning purposes. Examples are McAfee VirusScan Enterprise, backup software, and desktop search software such as Google Desktop.

- **Archiver** — An application that can reprocess files. Examples are compression software such as WinZip, and encryption applications such as McAfee Endpoint Encryption software or PGP.

How to work with DLP strategies

Change the strategy as necessary to optimize performance. For example, the high level of observation that an editor application receives is not consistent with the constant indexing of a desktop search application. The performance penalty is high, and the risk of a data leak from such an application is low. Therefore, you should use the trusted strategy with these applications.

You can override the default strategy on the DLP Policy | Settings | Application Strategy page. Create and remove overrides as necessary to experiment with fine-tuning the policy.

You can also create more than one template for an application and assign it more than one strategy. Use the different templates in different classifications and rules to achieve different results in different contexts. You must be careful, however, in assigning such templates within rule sets to avoid conflicts. McAfee DLP Endpoint resolves potential conflicts according to the following hierarchy: archiver > trusted > explorer > editor. That is, editor has the lowest ranking. If an application is an editor in one template and anything else in another template in the same rule set, McAfee DLP Endpoint does not treat the application as an editor.

Classification definitions and criteria

Classification definitions and criteria contain one or more conditions describing the content or file properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Applies to:</th>
<th>Definition</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Pattern</td>
<td>Definitions, criteria</td>
<td>Regular expressions or phrases used to match data such as dates or credit card numbers.</td>
<td>All products</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Definitions, criteria</td>
<td>Collections of related keywords and phrases such as profanity or medical terminology.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 7-1 Available conditions (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Applies to</th>
<th>Definition</th>
<th>Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyword</td>
<td>Criteria</td>
<td>A string value. You can add multiple keywords to content classification or content fingerprinting criteria. The default Boolean for multiple keywords is OR, but can be changed to AND.</td>
<td></td>
</tr>
<tr>
<td>Proximity</td>
<td>Criteria</td>
<td>Defines a conjunction between two properties based on their location to each other. Advanced patterns, dictionaries, or keywords can be used for either property. The Closeness parameter is defined as &quot;less than x characters,&quot; where the default is 1. You can also specify a Match count parameter to determine the minimum number of matches to trigger a hit.</td>
<td></td>
</tr>
</tbody>
</table>
| Document Properties | Definitions, criteria | Contains these options:  
- Any Property  
- Author  
- Category  
- Comments  
- Company  
- Keywords  
- Last saved by  
- Manager Name  
- Security  
- Subject  
- Template  
- Title  
Any Property is a user-defined property. |          |
| File Encryption | Criteria | Contains these options:  
- Not encrypted*  
- McAfee Encrypted Self-Extractor  
- McAfee Endpoint Encryption  
- Microsoft Rights Management encryption*  
- Seclore Rights Management encryption  
- Unsupported encryption types or password protected file* | McAfee DLP Endpoint for Windows (All options)  
McAfee DLP Discover (Options marked with *) |
| File Extension | Definitions, criteria | Groups of supported file types such as MP3 and PDF. | All products |
| File Information | Definitions, criteria | Contains these options:  
- Date Accessed  
- Date Created  
- Date Modified  
- File Extension  
- File Name  
- File Owner  
- File Size | All products |
### Dictionary definitions

A **dictionary** is a collection of keywords or key phrases where each entry is assigned a score. Content classification and content fingerprinting criteria use specified dictionaries to classify a document if a defined threshold (total score) is exceeded — that is, if enough words from the dictionary appear in the document.

The difference between a **dictionary** and a string in a **keyword** definition is the assigned score.

- A keyword classification always tags the document if the phrase is present.
- A dictionary classification gives you more flexibility because you can set a threshold, which makes the classification relative.

The assigned scores can be negative or positive, which allows you to look for words or phrases in the presence of other words or phrases.

McAfee DLP software includes several built-in dictionaries with terms commonly used in health, banking, finance, and other industries. In addition, you can create your own dictionaries. Dictionaries can be created (and edited) manually or by copying and pasting from other documents.
Limitations
There are some limitations to using dictionaries. Dictionaries are saved in Unicode (UTF-8) and can be written in any language. The following descriptions apply to dictionaries written in English. The descriptions generally apply to other languages, but there might be unforeseen problems in certain languages.

Dictionary matching has these characteristics:

• It is only case sensitive when you create case-sensitive dictionary entries. Built-in dictionaries, created before this feature was available, are not case-sensitive.
• It can optionally match substrings or whole phrases.
• It matches phrases including spaces.

If substring matching is specified, use caution when entering short words because of the potential for false positives. For example, a dictionary entry of "cat" would flag "cataracts" and "duplicate." To prevent these false positives, use the whole phrase matching option, or use statistically improbable phrases (SIPs) to give the best results. Similar entries are another source of false positives. For example, in some HIPAA disease lists, both "celiac" and "celiac disease" appear as separate entries. If the second term appears in a document and substring matching is specified, it produces two hits (one for each entry) and skews the total score.

See also
Create or import a dictionary definition on page 87

Advanced pattern definitions
Advanced patterns use regular expressions (regex) that allow complex pattern matching, such as in social security numbers or credit card numbers. Definitions use the Google RE2 regular expression syntax.

Advanced pattern definitions include a score (required), as with dictionary definitions. They can also include an optional validator — an algorithm used to test regular expressions. Use of the proper validator can significantly reduce false positives. The definition can include an optional Ignored Expressions section to further reduce false positives. The ignored expressions can be regex expressions or keywords. You can import multiple keywords to speed up creating the expressions.

Advanced patterns indicate sensitive text. Sensitive text patterns are redacted in hit highlighted evidence.

If both an matched pattern and an ignored pattern are specified, the ignored pattern has priority. This allows you to specify a general rule and add exceptions to it without rewriting the general rule.

See also
Create an advanced pattern on page 88

Classifying content with document properties or file information
Document property definitions classify content by predefined metadata values. File information definitions classify content by file metadata.

Document properties
Document properties can be retrieved from any Microsoft Office document or PDF, and can be used in classification definitions. Partial matching is supported using the Contains comparison.

There are three types of document properties:
• **Predefined properties** — Standard properties such as *author* and *title*.

• **Custom properties** — Custom properties added to the document metadata are allowed by some applications such as Microsoft Word. A custom property can also reference a standard document property that is not on the predefined properties list, but cannot duplicate a property that is on the list.

• **Any property** — Allows defining a property by value alone. This feature is useful in cases where the keyword has been entered in the wrong property parameter or when the property name is unknown. For example, adding the value *Secret* to the *Any property* parameter classifies all documents that have the word *Secret* in at least one property.

**File information**

File information definitions are used in data protection and discovery rules, and in classifications, to increase granularity. File information includes date created, date modified, file owner, and file size. The date properties have both exact (before, after, between) and relative (in last X days, weeks, years) date options. *File Type (extensions only)* is a predefined, extensible list of file extensions.

**Application templates**

An application template controls specific applications using properties such as product or vendor name, executable file name, or window title.

An application template can be defined for a single application, or a group of similar applications. There are built-in (predefined) templates for a number of common applications such as Windows Explorer, web browsers, encryption applications, and email clients.

The application template definition includes a field with a checkbox for operating system. Analyzing memory mapped files is a Windows-only feature, and is disabled automatically when you select OS X applications.

Application templates for Microsoft Windows can use any of the following parameters:

• **Command line** — Allows command line arguments, for example: `java-jar`, that can control previously uncontrollable applications.

• **Executable directory** — The directory where the executable is located. One use of this parameter is to control U3 applications.

• **Executable file hash** — The application display name, with an identifying SHA2 hash.

• **Executable file name** — Normally the same as the display name (minus the SHA2 hash), but could be different if the file is renamed.

• **Original executable file name** — Identical to the executable file name, unless the file has been renamed.

• **Product name** — The generic name of the product, for example, Microsoft Office 2012, if listed in the executable file's properties.

• **Vendor name** — The company name, if listed in the executable file's properties.

• **Window title** — A dynamic value that changes at runtime to include the active file name.

All parameters except the SHA2 application name and the executable directory accept substring matches.

Application templates for OS X can use any of the following parameters:

• **Command line**

• **Executable directory**
Manual classification

End users can manually apply or remove content classification or fingerprinting criteria to files. By default, end users do not have permission to view, add, or remove classifications. You can, however, assign specific classifications to specific user groups, or to Everyone. The assigned users can then apply the classification to files as they work. If the McAfee DLP Endpoint client encounters a manually classified file in, for example, an email attachment, it will take appropriate action based on the classification. Manual classification can also allow you to maintain your organization’s classification policy even in special cases of sensitive or unique information that the system does not process automatically.

McAfee DLP Endpoint for Windows users can manually classify files. McAfee DLP Endpoint for Mac users can recognized manually classified files, but have no option to set or view manual classifications.

When setting up permission for manual classification, you have the option of allowing content classifications, content fingerprints, or both to be applied manually.

Support for manual classification

McAfee DLP offers two types of support for manual classifications: Microsoft Office support and supported file types.

Microsoft Office applications (Word, Excel, and PowerPoint) and Microsoft Outlook are supported at the file creation level. End-users can choose to classify files, or you can set options to force users to classify Office files, when they are saved, and Outlook emails when they are sent.
Other supported file types, as well as Microsoft Office files, can be classified from Windows Explorer using the right-click menu.

**Embedded tagging**

There is a difference between automatically and manually applied content classifications. Automatic content classifications compare the content for a match each time a rule containing the classification is triggered. They do not change the file. Manual content classifications embed a physical tag in the file. For email, they embed an x-header in emails, and can add markup text to the header or footer to indicate the classification.

Manually applied content fingerprints work the same way as those applied automatically: the signatures are stored in the file’s extended file attributes or alternate data streams.

**See also**

*Assign manual classification permissions on page 84*

**Embedded tags**

Tags embedded when using manual classification allow 3rd-party applications to integrate with McAfee DLP tagged documents.

The following table lists the supported file types, tag name, and the technology applied.

<table>
<thead>
<tr>
<th>True file type</th>
<th>Technology</th>
<th>Embedded tag name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Doc</td>
<td>Doc-properties</td>
<td>DLP_CLASSIFICATION</td>
</tr>
<tr>
<td>DOCS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RTF</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDF</td>
<td>XMP</td>
<td></td>
</tr>
<tr>
<td>JPEG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The internal labels are:

- **Classification**: `DLPManualClassification`
- **Classifier**: `DLPManualClassificationClassifier`
- **Date**: `DLPManualClassificationDate`

and the XMP supported file types are:

- AIFF (aif)
- ASF (wma, wmv)
- AVCHD (m2ts, mts, m2t)
- FLV (flv)
- InDesign (indd, indt)
- JPEG (jpg, jpeg)
- MP3 (mp3)
- MPEG2 (mpg, mpeg, mp2, mod, m2v, mpa, mpv, m2p, m2a, m2t, mpe, vob, ms-pvr, dvr-ms)
- MPEG4 (mov, mp4, m4v, m4a, f4v)
- P2
- PDF (pdf)
- PNG (png)
- POST-SCRIPT (ps, eps)
- PSD (psd)
- RIFF (avi)
- SONY-HDV
- TIFF (tif, tiff, dng)
- UCF (ucf, xfl, pdfxml, mars, idml, idap, icap)
- WAVE (wav)
- XDCAM
- XDCAMEX

**See also**

*Manual classification on page 78*

*Customizing end-user messages on page 110*
**Registered documents**

The registered documents feature is an extension of location-based content fingerprinting. It gives administrators another way to define sensitive information, to protect it from being distributed in unauthorized ways.

Registered documents are predefined as sensitive, for example sales estimate spreadsheets for the upcoming quarter. McAfee DLP software categorizes and fingerprints the contents of these files. The signatures created are language-agnostic, that is, the process works for all languages. When you create a package, the signatures are loaded to the McAfee ePO database to be distributed to all endpoint workstations. The McAfee DLP Endpoint client on the managed computers controls the distribution of documents containing registered content fragments.

To use **registered documents**, you upload files on the Register Documents tab of the Classification module, assigning them to a classification as you upload them. The endpoint client ignores classifications that don't apply. For example, registered document packages classified with file properties are ignored when email is being parsed for sensitive content.

There are two viewing options: Statistics and Classifications. The statistics view displays totals for number of files, file size, number of signatures, and so forth, in the left pane, and statistics per file in the right pane. Use this data to remove less important packages if the signature limit is approached. The classifications view displays uploaded files per classification. Information about last package creation and changes to the file list are displayed in the upper right.

When you create a package, the software processes all files on the list, and loads the fingerprints to the McAfee ePO database for distribution. When you add or delete documents, you must create a new package. The software makes no attempt to calculate whether some of the files have already been fingerprinted. It always processes the entire list.

**See also**  
*Upload registered documents on page 82*  

---

**Whitelisted text**

McAfee DLP ignores whitelisted text when processing file content.

You can upload files containing text to McAfee ePO for whitelisting. Whitelisted text will not cause content to be classified, even if parts of it match content classification or content fingerprinting criteria. Use whitelisting for text that commonly appears in files, such as boilerplates, legal disclaimers, and copyright information.

- Files for whitelisting must contain at least 400 characters.
- If a file contains both classified and whitelisted data, it is not ignored by the system. All relevant content classification and content fingerprinting criteria associated with the content remain in effect.

**See also**  
*Upload files to whitelist text on page 82*
Create and configure classifications

Create classifications and criteria for use in rules or scans.

Tasks

- Create a classification on page 81
  Data protection and discovery rules require classification definitions in their configuration.
- Create classification criteria on page 81
  Apply classification criteria to files based on file content and properties.
- Upload registered documents on page 82
  Select and classify documents to distribute to the endpoint computers.
- Upload files to whitelist text on page 82
  Upload files containing commonly used text for whitelisting.

Create a classification

Data protection and discovery rules require classification definitions in their configuration.

Task

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Click New Classification.
3 Enter a name and optional description.
4 Click OK.
5 Add end user groups to manual classification, or registered documents to the classification, by clicking Edit for the respective component.
6 Add content classification criteria or content fingerprinting criteria with the Actions control.

Create classification criteria

Apply classification criteria to files based on file content and properties.

You build content classification criteria from data and file Definitions. If a required definition does not exist, you can create it as you define the criteria.

Task

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Select the classification to add the criteria to, then select Actions | New Content Classification Criteria.
3 Enter the name.
4 Select one or more properties and configure the comparison and value entries.
   • To remove a property, click <.
   • For some properties, click ... to select an existing property or to create a new one.
- To add additional values to a property, click +.
- To remove values, click –.

5 Click Save.

See also
Using classifications on page 70

Upload registered documents
Select and classify documents to distribute to the endpoint computers.

- McAfee DLP Discover does not support registered documents.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Click the Register Documents tab.
3 Click File Upload.
4 Browse to the file, select whether or not to overwrite a file if the file name exists, and select a classification.


5 Click OK.

The file is uploaded and processed, and statistics are displayed on the page.

When you have completed the file list, click Create Package. A signature package of all registered documents and all whitelisted documents is loaded to the McAfee ePO database for distribution to the endpoint computers.

You can create a package of just registered or whitelisted documents by leaving one list blank. When files are deleted, remove them from the list and create a new package to apply the changes.

See also
Registered documents on page 80

Upload files to whitelist text
Upload files containing commonly used text for whitelisting.

- McAfee DLP Discover does not support whitelisted text.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Click the Whitelisted Text tab.
3 Click File Upload.
Configure classification components for McAfee DLP Endpoint

McAfee DLP Endpoint supports manual classification and applying content fingerprinting criteria.

Tasks

- Create content fingerprinting criteria on page 83
  Apply fingerprinting criteria to files based on the application or file location.
- Use case: Application-based fingerprinting on page 84
  You can classify content as sensitive according to the application that produced it.
- Assign manual classification permissions on page 84
  Configure users allowed to manually classify files.
- Use case: Manual classification on page 85
  Workers whose jobs require routine creation of files containing sensitive data can be
  assigned manual classification permission. They can classify the files as they create them
  as part of their normal workflow.

Create content fingerprinting criteria

Apply fingerprinting criteria to files based on the application or file location.

Task

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Select the classification to add the criteria to.
3 Select Actions | New Content Fingerprinting Criteria, then select the type of fingerprinting criteria.
4 Enter the name and specify additional information based on the type of fingerprinting criteria.
   - Application — Click ... to select one or more applications.
   - Location — Click ... to select one or more network shares. If needed, specify the type of
     removable media.
   - Web application — Click ... to select one or more URL lists.
4 (Optional) Select one or more properties and configure the comparison and value entries.
   - To remove a property, click <.
   - For some properties, click ... to select an existing property or to create a new one.
   - To add additional values to a property, click +.
   - To remove values, click –.
5 Click Save.

See also

Using classifications on page 70
Use case: Application-based fingerprinting

You can classify content as sensitive according to the application that produced it.

In some cases, content can be classified as sensitive by the application that produces it. An example is top-secret military maps. These are JPEG files, typically produced by a specific US Air Force GIS application. By selecting this application in the fingerprinting criteria definition, all JPEG files produced by the application are tagged as sensitive. JPEG files produced by other applications are not tagged.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 On the Definitions tab, select Application Template, then select Actions | New.
3 Enter a name, for example GIS Application, and optional description. Using one or more properties from the Available Properties list, define the GIS application. Click Save.
4 On the Classification tab, click New Classification, and enter a name, for example, GIS application, and optional definition. Click OK.
5 Select Actions | New Content Fingerprinting Criteria | Application.

The applications fingerprinting criteria page opens.

6 In the Name field, enter a name for the tag, for example GIS tag.
7 In the Applications field, select the GIS application created in step 1.
8 From the Available Properties | File Conditions list, select True File Type. In the Value field, select Graphic files [built-in].

The built-in definition includes JPEG, as well as other graphic file types. By selecting an application as well as a file type, only JPEG files produced by the application are included in the classification.

9 Click Save, then select Actions | Save Classification.

The classification is ready to be used in protection rules.

Assign manual classification permissions
Configure users allowed to manually classify files.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Click the Manual Classification tab.
3 From the View drop-down list, select either Group by classifications or Group by end-user groups.

You can assign classifications to end-user groups or end-user groups to classifications, which ever is more convenient. The View list controls the display.

4 If you are grouping by classifications:
   a Select a classification from the displayed list.
   b In the Classifications section, select the classification type.

   Reduce the list by typing a string in the Filter list text box if the list is very long.
c Select Actions | Select End-User Groups.

d In the Choose from existing values window, select user groups or click New Item to create a new group. Click OK.

5 If you are grouping by end-user groups:
   a Select a user group from the displayed list.
   b Select Actions | Select Classifications.
   c In the Choose from existing values window, select classifications. Click OK.

### Use case: Manual classification

Workers whose jobs require routine creation of files containing sensitive data can be assigned manual classification permission. They can classify the files as they create them as part of their normal workflow.

In this example, a health-care provider knows that all patient records must be considered confidential under HIPAA rules. Workers creating or editing patient records are given manual classification permissions.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Create a user group or groups for workers who create or edit patient records.
   a In McAfee ePO, open the Classification module (Menu | Data Protection | Classification).
   c Select Actions | New, replace the default name with a meaningful name such as PHI User Group, and add users or groups to the definition.
   d Click Save.

2 Create a PHI (Protected Health Information) classification.
   a In the Classification module, on the Classification tab, select [Sample] PHI [built-in] in the left pane, then select Actions | Duplicate Classification.
      An editable copy of the sample classification appears.
   b Edit the Name, Description, and Classification Criteria fields as required.
   c In the Manual Classification field, click Edit.
   d In the Additional Actions section, select the classification type.
      By default, Manual classification only is selected.
   e Select Actions | Select End-User Groups.
   f In the Choose from existing values window, select the group or groups you created previously, then click OK.
   g Go back to the Classification tab and select Actions | Save Classification.

Workers who are members of the assigned groups can now classify the patient records as they are created by right-clicking on the file, selecting Data Protection, and selecting the appropriate option.

Only options selected (step 2.d.) appear in the menu.
Create classification definitions

You can use predefined classification definitions or create new definitions. Predefined definitions cannot be modified or deleted.

Tasks

• *Create a general classification definition on page 87*
  Create and configure definitions for use in classifications and rules.

• *Create or import a dictionary definition on page 87*
  A dictionary is a collection of keywords or key phrases where each entry is assigned a score. Scores allow for more granular rule definitions.

• *Create an advanced pattern on page 88*
  Advanced patterns are used to define classifications. An advanced pattern definition can consist of a single expression or a combination of expressions and false positive definitions.

• *Create a network port range on page 89*
  Network port ranges serve as filter criteria in network communication protection rules.

• *Create a network address range on page 89*
  Network address ranges serve as filter criteria in network communication protection rules.

• *Create an email address definition on page 89*
  Email address definitions are predefined email domains or specific email addresses that can be referenced in email protection rules.

• *Create a network printer definition on page 90*
  Use network printer definitions to create granular printer protection rules. Defined printers can be included or excluded from rules.

• *Create a URL list definition on page 90*
  URL list definitions are used to define web post protection rules. They are added to rules as *Web address (URL)* conditions.
See also
*Classification definitions and criteria on page 73*

**Create a general classification definition**
Create and configure definitions for use in classifications and rules.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | Classification**.
2. Select the type of definition to configure, the select **Actions | New**.
3. Enter a name and configure the options and properties for the definition.
   - The available options and properties vary depending on the type of definition.
4. Click **Save**.

**Create or import a dictionary definition**
A dictionary is a collection of keywords or key phrases where each entry is assigned a score. Scores allow for more granular rule definitions.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | Classification**.
2. Click the **Definitions** tab.
3. In the left pane, select **Dictionary**.
4. Select **Actions | New**.
5. Enter a name and optional description.
6. Add entries to the dictionary.
   - **To import entries:**
     a. Click **Import Entries**.
     b. Enter words or phrases, or cut and paste from another document.
        - The text window is limited to 20,000 lines of 50 characters per line.
     c. Click **OK**.
        - All entries are assigned a default score of 1.
     d. If needed, updated the default score of 1 by clicking **Edit** for the entry.
     e. Select the **Start With**, **End With**, and **Case Sensitive** columns as needed.
        - **Start With** and **End With** provide substring matching.
To manually create entries:

a Enter the phrase and score.

b Select the Start With, End With, and Case Sensitive columns as needed.

c Click Add.

7 Click Save.

**Create an advanced pattern**

Advanced patterns are used to define classifications. An advanced pattern definition can consist of a single expression or a combination of expressions and false positive definitions.

Advanced patterns are defined using regular expressions (regex). A discussion of regex is beyond the scope of this document. There are a number of regex tutorials on the Internet where you can learn more about this subject.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | Classification.

2 Select the Definitions tab, then select Advanced pattern in the left pane.

   The available patterns appear in the right pane.

   To view only the user-defined advanced patterns, deselect the Include Built-in items checkbox. User-defined patterns are the only patterns that can be edited.

3 Select Actions | New.

   The New Advanced pattern definition page appears.

4 Enter a name and optional description.

5 Under Matched Expressions, do the following:

   a Enter an expression in the text box. Add an optional description.

   b Select a validator from the drop-down list.

      McAfee recommends using a validator when possible to minimize false positives, but it is not required. If you don't want to specify a validator, or if validation is not appropriate for the expression, select No Validation.

   c Enter a number in the Score field.

      This number indicates the weight of the expression in threshold matching. This field is required.

   d Click Add.

6 Under False Positive, do the following:

   a Enter an expression in the text box.

   If you have text patterns stored in an external document, you can copy-paste them into the definition with Import Entries.
b In the **Type** field, select **RegEx** from the drop-down list if the string is a regular expression, or **Keyword** if it is text.

c Click **Add**.

7 Click **Save**

**Create a network port range**

Network port ranges serve as filter criteria in network communication protection rules.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager | Definitions**.

2 In the left pane select **Network Port**, then click **Actions | New**.

   ![You can also edit the built-in definitions.](image)

3 Enter a unique name and optional description.

4 Enter the port numbers, separated by commas, and optional description. Click **Add**.

5 When you have added all required ports, click **Save**.

**Create a network address range**

Network address ranges serve as filter criteria in network communication protection rules.

**Task**

For each required definition, perform steps 1–4: For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager | Definitions**.

2 In the left pane select **Network Address (IP address)**, then click **Actions | New**.

3 Enter a unique name for the definition and an optional description.

4 Enter an address, a range, or a subnet in the text box. Click **Add**.

   Correctly formatted examples are displayed on the page.

5 When you have entered all required definitions, click **Save**.

**Create an email address definition**

Email address definitions are predefined email domains or specific email addresses that can be referenced in email protection rules.

To get granularity in email protection rules, you include some email addresses and exclude others. Make sure to create both types of definitions.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager | Definitions**.

2 In the left pane, select **Email Address**, then **Actions | New**.
3 Enter a Name and optional Description.

4 Select an Operator from the drop-down list.
   Operators are:
   - Domain name is
   - Email address is
   - Display name is
   - Display name contains

5 Enter a value, then click Add.

6 Click Save when you have finished adding email addresses.

**Create a network printer definition**

Use network printer definitions to create granular printer protection rules. Defined printers can be included or excluded from rules.

**Before you begin**
Obtain the UNC path of the printer in the network.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Definitions.
2 In the left panel, select Network Printer, then select Actions | New.
3 Enter a unique Name and optional Description.
4 Enter the UNC path.
   All other fields are optional.
5 Click Save.

**Create a URL list definition**

URL list definitions are used to define web post protection rules. They are added to rules as Web address (URL) conditions.

**Task**
For each URL required, perform steps 1–4. For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager | Definitions.
2 In the left pane, select URL List, then select Actions | New.
3 Enter a unique Name and optional Definition.
4 Do one of the following:
   - Enter the Protocol, Host, Port, and Path information in the text boxes, then click Add.
   - Paste a URL in the Paste URL text box, then click Parse, then click Add.
The URL fields are filled in by the software.

5 When all required URLs are added to the definition, click Save.

---

**Use case: Integrate Titus Client with third-party tags**

Content classification or content fingerprinting criteria can include multiple Titus tag name/tag value pairs.

---

**Before you begin**

1. In the Policy Catalog, open the current Client Configuration. Select **Settings | Operational Modes and Modules**. Verify that **Outlook Add-ins | Activate 3rd Party Add-in Integration** is selected.

2. In **Settings | Email Protection**, in the **Outlook 3rd Party Add-in Integration** section, select Titus from the **Vendor Name** drop-down list.

---

McAfee DLP Endpoint calls the Titus API to identify tagged files and determine the tags. Classifications created with third party tags can be applied to all protection and discovery rules that inspect files.

---

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | Classification**.

2. Click **New Classification**.

3. Type a unique name and an optional description.

4. Click **Actions**, then select either **New Content Classification Criteria** or **New Content Fingerprinting Criteria**.

5. Select the **Third Party tags** property.

6. Enter the Titus field name and a value. Select the value definition from the drop-down list. The value string entered can be defined as:
   - equals one of
   - equals all of
   - contains one of
   - contains all of

7. (Optional) Click + and add another name / value pair.

8. Click Save.
Use case: Integrate Boldon James Email Classifier with classification criteria

Create classification criteria to integrate Boldon James Email Classifier.

Boldon James Email Classifier is an email solution that labels and classifies emails. McAfee DLP Endpoint software can integrate with Email Classifier and block emails based on assigned classifications. You can choose what string Email Classifier sends to McAfee DLP Endpoint when you set up the Email Classifier software. Use this string to define the classification criteria.

Task

For details about product features, usage, and best practices, click ? or Help.

1 Set up Boldon James compatibility in McAfee DLP Endpoint:
   a Using the Boldon James Classifier Administration console, open Classifier Application Settings | Outlook Settings. Set McAfee Host DLP scan to Enabled and set McAfee Host DLP marking to refer to a marking format that contains the classification value together with static text unique to the DLP marking. A string based on this marking format will be passed to McAfee DLP Endpoint containing the classification criteria.
   b In the Policy Catalog, open the current Client Configuration. Select Settings | Operational Modes and Modules. Verify that Outlook Add-ins | Activate 3rd Party Add-in Integration is selected.
   c In Settings | Email Protection, in the Outlook 3rd Party Add-in Integration section, select Boldon James from the Vendor Name drop-down list.

2 Create a Boldon James classification.
   For each required classification, perform the following steps:
   a In McAfee ePO, select Menu | Data Protection | Classification.
   b Click the Classification tab, then click New Classification.
   c Type a unique name and an optional description.
   d Click Actions | New Content Classification Criteria.
   e Select the Keyword property. In the Value field, enter the string built from the marking format that you selected in the Classifier Administration setup to send to McAfee DLP Endpoint.

3 In McAfee ePO, select Menu | Data Protection | DLP Rule Sets.

4 On the Rule Sets tab, do one of the following.
   • Select Actions | New Rule Set.
   • Select an existing rule set.

5 Select Actions | New Rule | Email Protection.
   An Email Protection definition form appears.

6 Enter a unique rule name.
7 On the **Condition** tab, select **Body** from the drop-down list, then select the appropriate Boldon James classification. Select appropriate **End-User**, **Email Envelope**, and **Recipients** options.

The McAfee DLP Endpoint client considers the Boldon James classification to be part of the email body. Limiting the definition to scan only the body makes the rule more efficient.

8 On the **Reaction** tab, select the appropriate **Prevent Action**, **User Notification**, **Report Incident**, and **Severity** parameters. Set the **Status** to **Enabled**, then click **Save**.
Classifying sensitive content
Use case: Integrate Boldon James Email Classifier with classification criteria
Working with policies

McAfee DLP Endpoint stores policies and configurations in the McAfee ePO Policy Catalog. DLP Policies in the McAfee ePO Policy Catalog consist of rule sets (protection rules) and their associated classifications and definitions. They can also include endpoint discovery scan configurations and server settings.

You create rules and rule sets in the DLP Policy Manager. Rule sets can contain multiple Data Protection, Device Control, and Discovery rules. The rules in a rule set are logical OR, that is, the rule set applies if the inspected content matches any of the rules. Within a rule, some parameters are logical AND or NOT, and some parameter combinations are either AND, OR, or NOT, as specified by the administrator.

Workflow

The steps to managing policies are:

1. Create and save the rule sets on the DLP Policy Manager | Rule Sets page.
2. Most rules require classifications. Define the classifications in the Classification console.
3. Assign the rule set to a DLP Policy on the DLP Policy Manager | Policy Assignment page.
4. Create or edit definitions.
5. Apply the policies to McAfee ePO on the Policy Catalog | DLP Policy | Active Rule Sets page.

On the Active Rule Sets page, you can create new policies by duplicating a default or other existing policy. You can also assign rule sets by selecting Actions | Activate Rule Set.

Contents

- Create and assign policies
- Using multiple policies
- How definitions work
- Edit a DLP policy
- Policy validation

Create and assign policies

McAfee DLP supports multiple policies and multiple client configurations. Policies and client configurations are applied to the McAfee ePO database, and assigned for deployment to the endpoint computers.

Use this workflow to create policies, apply them to McAfee ePO, and assign them for deployment.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Policy | Policy Catalog**.
2. From the **Product** drop-down list, select **Data Loss Prevention 10**. (Optional) Simplify the list by selecting a **Category**.
3. Click **Duplicate** (in the **Actions** column) for an existing policy or client configuration. Edit the name and click **OK**.
   
   Duplicating and editing a default policy or configuration, or an existing working one, is how you create working policies and client configurations.
4. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.
5. In the **Policy Manager**, select **Actions | New Rule Set**. Click the rule set to open it and add rules.

   You can create multiple rule sets, based on your requirements. Each rule set can contain multiple rules.
6. When you have defined your rule set, click the **Policy Assignment** tab.

   The tab displays the details of all assigned rule sets.
7. Click **Actions**, and do one of the following:
   - Select **Assign Rule Sets to a policy**.
   - Select **Assign a Rule Set to policies**.

   The rule set or sets are assigned to the policy or policies selected.
8. Click **Apply Selected Policies**. When you have verified your selection in the **Policy selection** window, click **Apply Policy**.

   The policies are applied to the McAfee ePO database.
9. In McAfee ePO, select **Menu | System | System Tree**.

   To view assignments, click the **Assigned Policies** tab.
10. On the **Assigned Client Tasks** tab, select **Actions | New Client Task Assignment**, and follow the steps to deploy the policy to the endpoints.

**See also**
- Rule sets on page 101
- Create a rule set on page 114

---

**Using multiple policies**

Use multiple policies to override common settings and definitions.

Some settings and definitions can affect endpoint system behavior. For example, changing a device class from unmanaged to managed causes the McAfee DLP Endpoint client to monitor and attempt to control devices belonging to that class. If some endpoint computers use devices that have compatibility issues with the McAfee DLP Endpoint device driver, their performance can be seriously compromised.
McAfee DLP solves this problem by offering multiple policies. Administrators can override device class and application template settings per policy, and set different settings and definitions for different systems in the organizations. You can assign different policies with policy assignment rules or user assignment groups. By default, the My Default DLP Policy is assigned to the root of the System Tree.

How definitions work

Definitions are used to configure rules, classification criteria, and discovery scans. McAfee DLP definitions are stored in a definitions catalog. Once defined, they are available to all McAfee DLP features. While all definitions are user-configurable, some definitions are also predefined.

View Built-in definitions by selecting the checkbox.

Table 8-1  Definitions available by McAfee DLP feature

<table>
<thead>
<tr>
<th>Classifications</th>
<th>Rule Sets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td></td>
</tr>
<tr>
<td>Advanced Pattern*</td>
<td>File Extension*</td>
</tr>
<tr>
<td>Dictionary*</td>
<td></td>
</tr>
<tr>
<td>Document Properties</td>
<td></td>
</tr>
<tr>
<td>File Extension*</td>
<td></td>
</tr>
<tr>
<td>File Information</td>
<td></td>
</tr>
<tr>
<td>True File Type*</td>
<td></td>
</tr>
<tr>
<td>Device Control</td>
<td></td>
</tr>
<tr>
<td>Device Class</td>
<td>Device Definitions</td>
</tr>
<tr>
<td>Notification</td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td>User Notification</td>
</tr>
<tr>
<td>Other</td>
<td></td>
</tr>
<tr>
<td>Scheduler</td>
<td></td>
</tr>
<tr>
<td>Source/Destination</td>
<td></td>
</tr>
<tr>
<td>Application Template</td>
<td></td>
</tr>
<tr>
<td>Email Address</td>
<td></td>
</tr>
<tr>
<td>End-User Group</td>
<td></td>
</tr>
<tr>
<td>Local Folder</td>
<td></td>
</tr>
<tr>
<td>Network Address (IP address)</td>
<td></td>
</tr>
<tr>
<td>Network Port</td>
<td></td>
</tr>
<tr>
<td>Network Printer</td>
<td></td>
</tr>
<tr>
<td>Network Share</td>
<td></td>
</tr>
<tr>
<td>Process Name</td>
<td></td>
</tr>
<tr>
<td>URL List</td>
<td></td>
</tr>
<tr>
<td>Windows Title</td>
<td></td>
</tr>
</tbody>
</table>

* Indicates that predefined (Built-in) definitions are available

Edit a DLP policy

DLP policy configuration consists of rule sets, policy assignments, and definitions.
Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | DLP Policy Manager. Create at least one rule set to assign to the DLP policy.
   
   See Create a rule set in this manual for details.

2. In McAfee ePO, select Menu | Policy Catalog | Product: Data Loss Prevention <version>. Open a DLP Policy configuration.

   Select a DLP Policy label in the Category column, and click in the Name column.

3. Select the Active Rule Sets tab.

   If any rule sets have been assigned to the policy, they appear listed on the page.

4. To assign new rule sets to the policy:
   
   a. Select Menu | DLP Policy Manager | Policy Assignment.

   b. Select Actions | Assign Rule Sets to a policy.

   Alternately, you can assign a rule set to multiple policies from the Actions menu.

   c. In the selection window, select a policy from the drop-down list and select the rule sets to assign with the checkboxes. Click OK.

   The selected rule sets are applied to the policy.

5. To remove rule sets from the policy:

   a. Select Actions | Assign Rule Sets to a policy.

   b. Deselect the boxes in the selection window for the rule sets to remove from the policy. Click OK.

   Selected rule sets are removed from the policy.

6. Select the Endpoint Discovery tab.

7. Select Actions | New Endpoint Scan, and select the type of scan you want to run: Local Email or Local File System.

   A scan setup page appears. On the page you select a Schedule definition, and select Rules to apply, as well as other scan details. Click Save when you have filled in all required details.

8. Select the Settings tab. On this page you can set the following options.

   • Default application strategy, and override application strategy for selected applications.

   • Device class overrides and filter types.

   • Add privileged users or user groups.

9. When you have completed all edits, click Apply Policy.

   The changes are applied to the McAfee ePO database.
Policy validation

The Policy validation page displays errors and provides a short-cut to fixing the problems. McAfee DLP validates policies before applying them to the McAfee ePO database. If there are errors, application is blocked and the errors are listed on the Policy Catalog | DLP Policy | Policy validation page, with a Severity rating. An Edit link facilitates editing the rules to correct the errors.
Protecting sensitive content

McAfee DLP protects sensitive content with a combination of McAfee DLP Endpoint and McAfee DLP Discover policies.

McAfee ePO deploys the McAfee DLP policies to the endpoint computers or Discover servers. The McAfee DLP Endpoint client software, server software, or appliance applies the policies to protect the sensitive content.

Contents

- Rule sets
- Rules
  - Data protection rules
  - Device control rules
  - Discovery rules
- Whitelists
  - Customizing end-user messages
  - Reactions available for rule types
- Create and configure rules and rule sets
- Rule use cases

Rule sets

Rule sets define McAfee DLP policies. Rule sets can contain a combination of data protection, device control, and discovery rules.

The Rule Sets page displays a list of defined rule sets and the status of each. The display includes the number of incidents logged for each rule set, how many rules have been defined, and how many enabled. Colored icons indicate the types of rules enabled. The ToolTip displayed when mousing over icons shows the type of rule and number of enabled rules.

Figure 9-1  Rule Sets page showing ToolTip information

In Rule set 1, six data protection rules, two discovery rules, and one device control rule have been defined. Only three of the data protection rules are enabled. The ToolTip shows two of these are clipboard rules. The third, represented by the blue icon on the right side of the column, is an application file access protection rule. To view which rules are defined but disabled, open the rule for editing.
See also

Protecting files with discovery rules on page 129
Create a rule on page 114

Rules

Rules define the action taken when an attempt is made to transfer or transmit sensitive data. Rule sets can contain three types of rules: data protection, device control, and discovery. A rule has three parts, Condition, Exceptions, and Reaction. Each part is defined on a separate tab in the rule definition. Rules can be enabled or disabled, and are assigned a Severity, selected from a drop-down list.

Condition

The condition defines what triggers the rule. For data protection and discovery rules, the condition always includes a Classification, and can include other conditions. For example, a cloud protection rule contains fields to define the end user and cloud service in addition to the classification. For device control rules, the condition always specifies the end user, and can include other conditions such as the device definition. Device control rules do not include classifications.

Exceptions

Exceptions define parameters excluded from the rule. For example, a cloud protection rule can allow specified users and classifications to upload data to the specified cloud services, while blocking those users and classifications defined in the condition section of the rule. Exceptions have a separate setting to enable or disable them, allowing you to turn the exception on or off when testing rules. Creating an exception definition is optional.

Exception definitions for data protection and discovery rules are similar to condition definitions. The parameters available for exclusion are a subset of the parameters available for defining the condition. For device control rules, the exception is defined by selecting whitelisted definitions from a list. The available whitelisted definitions depend on the type of device rule.

Reaction

The reaction defines what happens when the rule triggers. The actions available vary with the type of rule, but the default for all rules is No Action. When selected together with the Report Incident option, you can monitor the frequency of rule violations. This procedure is useful for tuning the rule to the correct level to catch data leaks without creating false positives.

The reaction also defines whether the rule is applied outside the enterprise and, for some rules, when connected to the enterprise by VPN.

Data protection rules

Data protection rules monitor and control user content and activity.
McAfee DLP Endpoint for Windows supports all data protection rules.

McAfee DLP Endpoint for Mac supports application file access, network share, and removable storage protection rules.
Application File Access Protection rules

Protection rules for file access monitor files based on the application or applications that created them. They are supported on Microsoft Windows and OS X computers. On McAfee DLP Endpoint for Mac, only OS X-supported applications and browsers are supported.

Select an application or URL definition to limit the rule to specific applications.

URL definitions are not supported on McAfee DLP Endpoint for Mac

Application file access protection rules communicate with the McAfee® Data Exchange Layer (DXL) in McAfee® Threat Intelligence Exchange (TIE). You can use information from TIE to define the rule according to TIE reputation. When selecting an application, the drop-down list allows you to choose a TIE reputation instead of an application or browser URL.

In order to use TIE reputation in rules, DXL client must be installed on the endpoint computer.

Use classification definitions to limit the rule to specific content fingerprinting or content classification criteria. You can also limit the rule to local users or to specified user groups.

Actions

Available actions are Block, User Notification, Report Incident, and Store Original File. Storing evidence is optional when reporting an incident. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network.

When the Classification field is set to is any data (ALL), the Block action is not allowed. Attempting to save the rule with these conditions generates a warning.

Client configuration

Whitelisted processes and specific extensions can be added to the client configuration on the Application File Access Protection page.

See also

Use case: Prevent burning sensitive information to disk on page 121

Cloud protection rules

Cloud protection rules manage files uploaded to cloud applications. They are supported on McAfee DLP Endpoint for Windows only.

Cloud applications are increasingly used to back up and share files. Most cloud applications create a special folder on the disk drive that synchronizes with the cloud server. McAfee DLP Endpoint intercepts file creation in the cloud application folder, scans the files, and applies the relevant policies. If the policy allows synchronizing the file to the cloud application folder, and the file is later changed, it is rescanned and the policy reapplied. If the changed file violates a policy, it cannot be synchronized to the cloud.

The McAfee DLP Endpoint Cloud Protection Rule supports

- Box
- Dropbox
- GoogleDrive
- iCloud
- OneDrive (personal)
- OneDrive for business (groove.exe)
- Syncplicity

To improve scanning speed, you can specify the top-level subfolders included or excluded in the rule.
Use classification definitions to limit the rule to specific content fingerprinting or content classification criteria. You can also limit the rule to local users or to specified user groups, and by the top-level subfolder name.

**Actions**

Available actions are **Block**, **Request Justification**, **Apply RM Policy**, and **Encrypt**. The **User Notification** can be specified, and incident reporting, with or without storage of the original file, is available. Different actions can be applied when the computer is disconnected from the corporate network.

**Client configuration**

To support the cloud protection rule, **Cloud Protection Handlers** are selected in the **Policy Catalog** on the **Client Configuration | Operational Mode and Modules** page. The handler and all supported applications are selected by default. You can deselect individual applications for more granular control.

**Email protection rules**

Email protection rules monitor or block email sent to specific destinations or users. They are supported on McAfee DLP Endpoint for Windows.

Email protection rules can block emails to specified recipients. The **Email Envelope** field can specify that the email is protected by RMS permissions, PGP encryption, digital signature, or S/MIME encryption. This option is typically used to define exceptions.

Use classification definitions to limit the rule to specific content fingerprinting or content classification criteria. The classifications can define the whole email, or just the subject, the body, or the attachments. You can also limit the rule to local users or to specified user groups.

**Actions**

Available McAfee DLP Endpoint actions are **Block**, **Request Justification**, **User Notification**, **Report Incident**, and **Store original email**. Storing evidence is optional when reporting an incident. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network.

**Client configuration**

If you are using Lotus Notes, activate the Lotus Notes plug-in on the **Operational Mode and Modules** page. If you are using Microsoft Outlook, activate the required add-ins.

In systems where both Microsoft Exchange and Lotus Notes are available, email rules do not work if the outgoing mail server (SMTP) name is not configured for both.

To use Microsoft Outlook third party add-ins (Boldon James or Titus), select the add-in on the **Email Protection** page. The McAfee DLP Outlook add-in sets itself to bypass mode when the third party add-in is installed and active. Other settings on the **Email Protection** page control timeout strategy, caching, API, and user notification.

**Best practice:** For improved performance, disable unused handlers.
Network communication protection rules

Network communication protection rules monitor or block incoming or outgoing data on your network. They are supported on McAfee DLP Endpoint for Windows only.

Network communication protection rules control network traffic based on specified network addresses (required) and ports (optional). You can also specify incoming or outgoing connections, or both. You can add one network address definition and one port definition, but definitions can contain multiple addresses or ports.

Use classification definitions to limit the rule to specific content fingerprinting criteria. You can also limit the rule to local users or to specified user groups, and by specifying the application creating the connection.

Network communication protection rules do not check content classification criteria. Use content fingerprinting criteria when defining classifications used with network communication protection rules.

Actions

Network communication protection rule actions include Block, Report Incident, and Notify User. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network, or when the computer is connected to the corporate network using VPN.

Client configuration

The Network Communication Driver is activated (by default) on the Operational Mode and Modules page.

Network share protection rules

Network share protection rules control sensitive content stored on network shares. They are supported on Microsoft Windows and OS X computers.

Network share protection rules can apply to all network shares or to specified shares. One share definition can be included in the rule, and the definition can contain multiple shares. An included classification (required) defines what sensitive content is protected.

Use classification definitions to limit the rule to specific content fingerprinting or content classification criteria. You can also limit the rule to local users or to specified user groups, by specific network shares, or by the application copying the file.

Actions

Network share protection rule actions include Encrypt, Request justification, Report Incident, Store Original File, and Notify User.

Encrypt action is not supported on McAfee DLP Endpoint for Mac.

Storing evidence is optional when reporting an incident. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network. Encryption options are McAfee File and Removable Media Protection (FRP) and StormShield Data Security encryption software.
**Printer protection rules**

Printer protection rules monitor or block files from being printed. They are supported on McAfee DLP Endpoint for Windows only.

Use classifications to limit the rule. You can also limit the rule by specifying users, printers, or applications printing the file. The printer definition can specify local printers, network printers, named network printers, or image printers.

*Image printers, which had a separate rule in earlier versions, are now included in the general printer rule.*

**Actions**

Printer protection rule actions include Block, Request justification, Notify User, Report Incident, and Store Original File. Storing evidence is optional when reporting an incident. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network, or when the computer is connected to the corporate network using VPN.

**Client configuration**

Whitelisted processes are listed on the Printer Protection page. Printer protection rules ignore files printed from whitelisted processes.

Printer application add-ins, selected on the Operational Mode and Modules page, can improve printer performance when using certain common applications. The add-ins are only installed when a printer protection rule is enabled on the managed computer.

**Removable storage protection rules**

Removable storage protection rules monitor or block data from being written to removable storage devices. They are supported on McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac. On McAfee DLP Endpoint for Mac, CD and DVD devices are not supported.

Removable storage protection rules can control CD and DVD devices, removable storage devices, or both. Limit the rule with content fingerprinting or content classification criteria in classifications (required). You can also define the rule with specified users, applications, or web URLs.

*Removable storage protection rules for McAfee DLP Endpoint for Mac only support control of removable storage devices. They do not support CD/DVD devices.*

Use classifications to limit the rule. You can also limit the rule by specifying users, or the applications copying the file.

**Actions**

Removable storage protection rule actions include Block, Request justification, Encrypt, Notify User, Report Incident, and Store Original File. Storing evidence is optional when reporting an incident. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network.

*Encryption is not supported on McAfee DLP Endpoint for Mac.*

**Client configuration**

Set the deletion mode on the Removable Storage Protection page. Normal mode deletes the file; aggressive mode makes the deleted file unrecoverable.
Activate advanced options on the Operational Mode and Modules page. Options are:

- Protect TrueCrypt disk mounts
- Portable devices handler
- Advanced file copy protection

**Portable devices handler**

Media Transfer Protocol (MTP) is used for transferring files and associated metadata from computers to mobile devices such as smartphones. MTP devices are not traditional removable devices because the device implements the file system, not the computer it is connected to. When the client is configured for MTP devices, the removable storage protection rule allows it to intercept MTP transfers and apply security policies. Only USB connections are currently supported.

The handler works with all data transfers made by Windows Explorer. It does not work with iOS devices, which use iTunes to manage the data transfers. One alternative strategy with iOS devices is to use a removable storage device rule to set the devices to read-only.

**Protecting TrueCrypt devices with removable storage protection rules**

TrueCrypt encrypted virtual devices can be protected with TrueCrypt device rules, or with removable storage protection rules. TrueCrypt protection is not supported on McAfee DLP Endpoint for Mac.

- Use a device rule if you want to block or monitor a TrueCrypt volume, or make it read-only.
- Use a protection rule if you want content-aware protection of TrueCrypt volumes.

Signatures are lost when content fingerprinted content is copied to TrueCrypt volumes because TrueCrypt volumes do not support extended file attributes. Use document properties, file encryption, or file type groups definitions in the classification definition to identify the content.

**Advanced file copy protection**

Advanced file copy protection intercepts Windows Explorer copy operations and allows the McAfee DLP Endpoint client to inspect the file at source before copying it to the removable device. It is enabled by default, and should only be disabled for troubleshooting.

There are use cases where advanced copy protection does not apply. For example, a file opened by an application and saved to a removable device with Save As reverts to normal copy protection. The file is copied to the device, then inspected. If sensitive content is found, the file is immediately deleted.

**Screen capture protection rules**

Screen capture protection rules control data copied and pasted from a screen. They are supported on McAfee DLP Endpoint for Windows only.

Use classification definitions to limit the rule to specific content fingerprinting criteria. You can also limit the rule to local users or to specified user groups, or by applications visible on the screen.

Screen capture protection rules do not check content classification criteria. Use content fingerprinting criteria when defining classifications used with screen capture rules.

**Actions**

Screen capture protection rule actions include Block, Notify User, Report Incident, and Store Original File. Storing evidence is optional when reporting an incident. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network.
Client configuration

Applications protected by screen capture protection rules are listed on the Screen Capture Protection page. The list is pre-populated with common screen capture applications, and you can add, edit, or delete applications.

The screen capture service is activated on the Operational Mode and Modules page. You can enable the application handler and the Print Screen key handler separately. By default, both are enabled. Disabling the application handler, or the screen capture service, disables all the applications listed on the Screen Capture Protection page.

Web post protection rules

Web post protection rules monitor or block data from being posted to websites, including web-based email sites. They are supported on McAfee DLP Endpoint for Windows.

Web post protection rules are defined by adding web addresses to the rule.

Use classification definitions to limit the rule to specific content fingerprinting or content classification criteria. You can also limit the rule to local users or to specified user groups.

Actions

Web post protection rule actions include Block, Request Justification, Notify User, Report Incident, and Store Original File. Storing evidence is optional when reporting an incident. Selecting user notification activates the user notification pop-up on the endpoint computer. Different actions can be applied when the computer is disconnected from the corporate network.

Client configuration

Enable browsers for web protection on the Operational Mode and Modules page. Microsoft Internet Explorer, Microsoft Edge, Mozilla Firefox, and Google Chrome are supported.

The Web Post Protection page contains options for other web post settings.

Table 9-1  Option definitions

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web protection evaluation</td>
<td>Settings to select inputs for web request evaluation. Used if HTTP/S requests could be sent by AJAX to a URL different from that displayed in the address bar.</td>
</tr>
<tr>
<td>Process HTTP GET requests</td>
<td>Enable or disable processing HTTP GET requests. GET requests are disabled by default because they are resource-intensive. Use this option with caution.</td>
</tr>
<tr>
<td>Supported Chrome versions</td>
<td>This list is required due to the frequency of Chrome updates. It is populated by downloading a current list from McAfee Support and using Browse to install the XML file.</td>
</tr>
<tr>
<td>Web Timeout Strategy</td>
<td>Sets a maximum time for analyzing web posts, and the action to be taken if the time is exceeded. The options are block or allow. You can also select user notification.</td>
</tr>
<tr>
<td>Whitelisted URLs</td>
<td>Lists URLs that are excluded from web post protection rules.</td>
</tr>
</tbody>
</table>
Device control rules

Device control rules define the action taken when particular devices are used. Device control rules can monitor or block devices attached to enterprise-managed computers. McAfee DLP Endpoint for Windows supports the following types of rules:

- Removable storage
- Plug-and-play
- Fixed hard drive
- Citrix XenApp
- TrueCrypt
- Removable storage file access

McAfee DLP Endpoint for Mac supports the following types of rules:

- Removable storage
- Plug-and-play (USB devices only)

Device control rules are described in detail in the Protecting removable media section.

See also
Protecting removable media on page 4

Discovery rules

McAfee DLP Endpoint and McAfee DLP Discover use discovery rules to scan files and repositories.

Table 9-2  Data vector descriptions

<table>
<thead>
<tr>
<th>Product</th>
<th>Discovery rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee DLP Endpoint</td>
<td>Local Email (OST, PST)</td>
</tr>
<tr>
<td></td>
<td>Local File System</td>
</tr>
<tr>
<td>McAfee DLP Discover</td>
<td>Box Protection</td>
</tr>
<tr>
<td></td>
<td>File Server (CIFS) Protection</td>
</tr>
<tr>
<td></td>
<td>SharePoint Protection</td>
</tr>
</tbody>
</table>

Whitelists

Whitelists are collections of items that you want the system to ignore. You can whitelist content, devices, processes, and user groups.

Whitelists in data protection rules

You can specify whitelisted processes for clipboard and printing protection rules in the Policy Catalog Windows client configuration on their respective pages. You can specify whitelisted URLs on the Web Protection page. Because these whitelists are applied at the client, they work with all clipboard, printing, and web post protection rules. Clipboard and printing protection rules ignore content produced by whitelisted processes. Web post protection rules are not enforced on whitelisted URLs.

You can specify whitelisted processes for text extraction on the Content Tracking page. Depending on the definition, the text extractor does not analyze files or content fingerprinting opened by the specified application, or does not create dynamic fingerprints for web upload. The definition can specify specific folders and extensions, allowing granular control what is whitelisted. If no folder is named, the process is not monitored by application file access rules.
Whitelists in device rules

You can create whitelisted plug-and-play definitions in the Device Definitions in the DLP Policy Manager.

Some plug-and-play devices do not handle device management well. Attempting to manage them might cause the system to stop responding or cause other serious problems. Whitelisted plug-and-play devices are automatically excluded when a policy is applied.

Whitelisted plug-and-play definitions are not applicable on OS X operating systems.

The Exceptions tab in device control rules is defined by whitelists that are specific to the rule that contains them. The whitelists exclude the specified definitions from the rule.

- **Users** — Used in all device rules
- **Device definitions** — Used in all device rules except Citrix and TrueCrypt
- **Processes** — Used in plug-and-play and removable storage rules
- **Serial number and user pairs** — Used in plug-and-play and removable storage rules
- **File names** — Used in removable storage file access rules to exempt files such as anti-virus applications

Customizing end-user messages

Two types of messages are used to communicate with end users: notifications and user justification messages.

Notification and justification definitions can specify *Locales* (languages), and add placeholders that are replaced by their real values. When locales are defined, the messages and option buttons (for business justifications) appear in the default language of the endpoint computer. The following locales are supported:

- English (US)
- English (UK)
- French
- German
- Spanish
- Japanese
- Korean
- Russian
- Chinese (simplified)
- Chinese (traditional)

English (US) is the standard default locale, but any supported locale can be set as the default in the definition. The default locale is used when other defined locales are not available as the endpoint computer default language.

User notification

User notifications are pop up messages that notify the user of a policy violation.

When a rule triggers multiple events, the pop-up message states: *There are new DLP events in your DLP console*, rather than displaying multiple messages.

User notification messages are defined in *DLP Policy Manager | Definitions | Notifications*. 
Business justification

Business justification is a form of policy bypass. When Request Justification is specified as the prevent action in a rule, the user can enter the justification to continue without being blocked.

Business justification messages are defined in DLP Policy Manager | Definitions | Justification.

Placeholders

Placeholders are a way of entering variable text in messages, based on what triggered the end-user message. The available placeholders are:

- `%c` for classifications
- `%r` for rule-set name
- `%v` for vector (email protection, web protection, and so forth)
- `%a` for action
- `%s` for string value (file name, device name, and so forth)

See also

Create a justification definition on page 117
Create a notification definition on page 118

Reactions available for rule types

The available reactions for a rule vary depending on the rule type.

- Data protection rules are available for McAfee DLP Endpoint.
- Device control rules are available for McAfee DLP Endpoint and Device Control.
- Some discovery rules are available for McAfee DLP Endpoint, some are available for McAfee DLP Discover.

<table>
<thead>
<tr>
<th>Reaction</th>
<th>Applies to rules:</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Action</td>
<td>All</td>
<td>Allows the action.</td>
</tr>
<tr>
<td>Block</td>
<td>Data Protection, Device Control</td>
<td>Blocks the action.</td>
</tr>
<tr>
<td>Copy</td>
<td>Discovery</td>
<td>Copies the file to the specified UNC location.</td>
</tr>
<tr>
<td>Encrypt</td>
<td>Data Protection, Discovery</td>
<td>Encrypts the file. Encryption options are FRP or StormShield Data Security encryption software.</td>
</tr>
<tr>
<td>Move</td>
<td>Discovery</td>
<td>Moves the file to the specified UNC location. Allows creation of a placeholder file (optional) to notify the user that the file has been moved.</td>
</tr>
<tr>
<td>Read-only</td>
<td>Device Control</td>
<td>Forces read-only access.</td>
</tr>
</tbody>
</table>
Table 9-3 Available reactions (continued)

<table>
<thead>
<tr>
<th>Reaction</th>
<th>Applies to rules:</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request justification</td>
<td>Data Protection</td>
<td>Produces a pop-up on the end user computer. The user selects a justification (with optional user input) or selects an optional action.</td>
</tr>
<tr>
<td>Apply RM Policy</td>
<td>• Data Protection • Discovery Not supported on McAfee DLP Endpoint for Mac.</td>
<td>Applies a rights management (RM) policy to the file.</td>
</tr>
<tr>
<td>Quarantine</td>
<td>Discovery</td>
<td>Quarantines the file.</td>
</tr>
<tr>
<td>Tag</td>
<td>Discovery</td>
<td>Tags the file.</td>
</tr>
<tr>
<td>Show file in DLP Endpoint console</td>
<td>Discovery</td>
<td>Displays Filename and Path in the endpoint console. Filename is a link to open the file, except when the file is quarantined. Path opens the folder where the file is located.</td>
</tr>
<tr>
<td>User notification</td>
<td>• Data Protection • Discovery</td>
<td>Sends a message to the endpoint computer to notify the user of the policy violation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>When User Notification is selected, and multiple events are triggered, the pop-up message states: There are new DLP events in your DLP console, rather than displaying multiple messages.</td>
</tr>
<tr>
<td>Report Incident</td>
<td>All</td>
<td>Generates an incident entry of the violation in DLP Incident Manager.</td>
</tr>
<tr>
<td>Store Original File</td>
<td>• Data Protection • Discovery</td>
<td>Saves the file for viewing through the incident manager.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires a specified evidence folder and activation of the evidence copy service.</td>
</tr>
<tr>
<td>Store original email as evidence</td>
<td>• Data Protection Not supported on McAfee DLP Endpoint for Mac</td>
<td>Stores the original message on the evidence share. Applies to McAfee DLP Endpoint email protection rules only.</td>
</tr>
</tbody>
</table>

Table 9-4 Data protection rule actions

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Reactions</th>
<th>No action</th>
<th>Add a header</th>
<th>Block</th>
<th>Encrypt</th>
<th>Request justification</th>
<th>Apply RM policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application file access protection</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clipboard protection</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud protection</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email protection</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network communication protection</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network share protection</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Printer protection</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 9-4  Data protection rule actions (continued)

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Reactions</th>
<th>No action</th>
<th>Add a header</th>
<th>Block</th>
<th>Encrypt</th>
<th>Request justification</th>
<th>Apply RM policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removable storage protection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen capture protection</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web post protection</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Encryption is not supported on McAfee DLP Endpoint for Mac

* Encryption for Cloud protection rules is supported on Box, Dropbox, GoogleDrive, and OneDrive personal. Attempting to upload encrypted files to other cloud applications fails to save the file.

### Table 9-5  Device control rule reactions

<table>
<thead>
<tr>
<th>Rules</th>
<th>Reactions</th>
<th>No action</th>
<th>Block</th>
<th>Read-only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix XenApp device</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed hard drive</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Plug-and-play device</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removable storage device</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Removable storage file access</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TrueCrypt device</td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

### Table 9-6  McAfee DLP Endpoint discovery rule reactions

<table>
<thead>
<tr>
<th>Rules</th>
<th>Reactions</th>
<th>No action</th>
<th>Encrypt</th>
<th>Apply RM policy</th>
<th>Quarantine</th>
<th>Tag</th>
<th>Show file in McAfee DLP Endpoint console</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint file system</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Endpoint mail storage protection</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Create and configure rules and rule sets

Create and configure rules for your McAfee DLP Endpoint, Device Control, and McAfee DLP Discover policies.

**Tasks**

- *Create a rule set on page 114*
  Rule sets combine multiple device protection, data protection, and discovery scan rules.
- *Create a rule on page 114*
  The process for creating a rule is similar for all rule types.
- *Assign rule sets to policies on page 115*
  Before being assigned to endpoint computers, rule sets are assigned to policies and the policies are applied to the McAfee ePO database.
- *Enable, disable, or delete rules on page 116*
  You can delete or change the state of multiple rules at once.
- *Import and export rules and classifications on page 116*
  You can export rules and classifications from a McAfee ePO server and import them onto another McAfee ePO server.
- *Configure rule or rule set columns on page 116*
  Move, add, or remove columns displayed for rules or rule sets.
- *Create a justification definition on page 117*
  For McAfee DLP Endpoint, business justification definitions define parameters for the justification prevent action in rules.
- *Create a notification definition on page 118*
  With McAfee DLP Endpoint, user notifications appear in popups or the end-user console when user actions violate policies.

**Create a rule set**

Rule sets combine multiple device protection, data protection, and discovery scan rules.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.
2. Click the **Rule Sets** tab.
3. Select **Actions | New Rule Set**.
4. Enter the name and optional note, then click **OK**.

**Create a rule**

The process for creating a rule is similar for all rule types.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.
2. Click the **Rule Sets** tab.
3. Click the name of a rule set and if needed, select the appropriate tab for the **Data Protection**, **Device Control**, or **Discovery** rule.
4 Select Actions | New Rule, then select the type of rule.

5 On the Condition tab, enter the information.
   • For some conditions, such as classifications or device definitions, click ... to select an existing, or create a new, item.
   • To add additional criteria, click +.
   • To remove criteria, click –.

6 (Optional) To add exceptions to the rule, click the Exceptions tab.
   a Select Actions | Add Rule Exception.
      Device rules do not display an Actions button. To add exceptions to device rules, select an entry from the displayed list.
   b Fill in the fields as required.

7 On the Reaction tab, configure the Prevent Action, User Notification, and Report Incident options.
   Rules can have different actions, depending on whether the endpoint computer is in the corporate network or not. Some rules can also have a different action when connected to the corporate network by VPN.

8 Click Save to save the rule or Close to exit without saving.

See also
Rule sets on page 101

Assign rule sets to policies
Before being assigned to endpoint computers, rule sets are assigned to policies and the policies are applied to the McAfee ePO database.

Before you begin
On the DLP Policy Manager | Rule Sets page, create one or more rules sets and add the required rules to them.

Task
For details about product features, usage, and best practices, click ? or Help.

1 On the DLP Policy Manager | Policy Assignment page, do one of the following:
   • Select Actions | Assign a Rule Set to policies. In the assignment window, select a rule set from the drop-down list and select the policies to assign it to. Click OK.
   • Select Actions | Assign Rule Sets to a policy. In the assignment window, select a policy from the drop-down list and select the rule sets to assign it to. Click OK.

   If you deselect a rule set or policy previously selected, the rule set is deleted from the policy.

2 Select Actions | Apply selected policies. In the assignment window, select the policies to apply to the McAfee ePO database. Click OK.
   Only policies not yet applied to the database appear in the selection window. If you change a rule set assignment, or a rule in an assigned rule set, the policy appears and the revised policy is applied in place of the previous policy.
**Enable, disable, or delete rules**
You can delete or change the state of multiple rules at once.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Policy Manager.
2. Click the Rule Sets tab.
3. Click the name of a rule set and if needed, click the appropriate tab for the Data Protection, Device Control, or Discovery rule.
4. Select one or more rules.
5. Update or delete the selected rules.
   - To enable the rules, select Actions | Change State | Enable.
   - To disable the rules, select Actions | Change State | Disable.
   - To delete the rules, select Actions | Delete.

**Import and export rules and classifications**
You can export rules and classifications from a McAfee ePO server and import them onto another McAfee ePO server.

**Task**
1. In McAfee ePO, select Data Protection | DLP Settings.
2. Click Backup to file and save the file in a place such as a USB drive or a shared folder.
3. On another McAfee ePO server, and select Data Protection | DLP Settings.
4. Click Restore from file and select the file you saved earlier.

**Configure rule or rule set columns**
Move, add, or remove columns displayed for rules or rule sets.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Policy Manager.
2. Click the Rule Sets tab.
3. Access the Select the Columns to Display page.
   - **Rule sets** — Select Actions | Choose Columns.
   - **Rules** — Select a rule set, then select Actions | Choose Columns.
4 Modify the columns.
   - In the Available Columns pane, click items to add columns.
   - In the Selected Columns pane, click the arrows or x to move or delete columns.
   - Click Use Defaults to restore the columns to the default configuration.

5 Click Save.

Create a justification definition

For McAfee DLP Endpoint, business justification definitions define parameters for the justification prevent action in rules.

Task

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager.

2 Click the Definitions tab, then select Notification | Justification.

3 Select Actions | New.

4 Enter a unique name and optional description.

5 To create justification definitions in more than one language, select Locale Actions | New Locale. For each required locale, select a locale from the drop-down list.

The selected locales are added to the list.

6 For each locale, do the following:
   a In the left pane, select the locale to edit. Enter text in the text boxes and select checkboxes as required.

   Show Match Strings provides a link on the popup to display the hit-highlighted content. More Info provides a link to a document or intranet page for information.

   When entering a locale definition, checkboxes and actions are not available. You can only enter button labels, overview, and title. In the Justification Options section, you can replace the default definitions with the locale version by using the Edit feature in the Actions column.

   b Enter a Justification Overview and optional Dialog Title.

   The overview is a general instruction for the user, for example: This action requires a business justification. Maximum entry is 500 characters.

   c Enter text for button labels and select button actions. Select the Hide button checkbox to create a two-button definition.

   Button actions must match the prevent actions available for the type of rule that uses the definition. For example, network share protection rules can have only No Action, Encrypt, or Request Justification for prevent actions. If you select Block for one of the button actions, and attempt to use the definition in a network share protection rule definition, an error message appears.

   d Enter text in the text box and click Add to add to the list of Justification Options. Select the Show justifications options checkbox if you want the end user to view the list.

   You can use placeholders to customize the text, indicating what caused the popup to trigger.

7 When all locales are complete, click Save.

See also

Customizing end-user messages on page 110
Create a notification definition

With McAfee DLP Endpoint, user notifications appear in popups or the end-user console when user actions violate policies.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.
2. Click the **Definitions** tab, then select **Notification | User Notification**.
3. Select **Actions | New**.
4. Enter a unique name and optional description.
5. To create user notification definitions in more than one language, select **Locale Actions | New Locale**. For each required locale, select a locale from the drop-down list.
   The selected locales are added to the list.
6. For each locale, do the following:
   a. In the left pane, select the locale to edit.
      
      ![i] You can set any locale to be the default by selecting the **Default locale** checkbox.
   b. Enter text in the text box.
      You can use placeholders to customize the text, indicating what caused the popup to trigger.
   c. (Optional) Select the **Show link to more information** checkbox and enter a URL to provide more detailed information.
      
      ![i] Available only in the default locale.
7. When all locales are complete, click **Save**.

**See also**

*Customizing end-user messages on page 110*

---

**Rule use cases**

The following use cases provide examples of using device and data protection rules.
Tasks

- **Use case: Removable storage device rule with a whitelisted process on page 119**
  You can whitelist file names as an exception to a removable storage blocking rule.

- **Use case: Set a removable device as read-only on page 120**
  Removable storage device protection rules, unlike plug-and-play device rules, have a read-only option.

- **Use case: Block and charge an iPhone with a plug-and-play device rule on page 120**
  Apple iPhones can be blocked from use as storage devices while being charged from the computer.

- **Use case: Prevent burning sensitive information to disk on page 121**
  Application file access protection rules can be used to block the use of CD and DVD burners for copying classified information.

- **Use case: Block outbound messages with confidential content unless they are sent to a specified domain on page 122**
  Outbound messages are blocked if they contain the word *Confidential*, unless the recipient is exempt from the rule.

- **Use case: Allow a specified user group to send credit information on page 123**
  Allow people in the human resources user group to send messages that contain personal credit information by obtaining information from your Active Directory.

- **Use case: Classify attachments as NEED-TO-SHARE based on their destination on page 125**
  Create classifications that allow NEED-TO-SHARE attachments to be sent to employees in the United States, Germany, and Israel.

**Use case: Removable storage device rule with a whitelisted process**

You can whitelist file names as an exception to a removable storage blocking rule.

Removable storage device rules are used to block applications from acting on the removable device. Whitelisted file names are defined as processes that are not blocked. In this example, we block Sandisk removable storage devices, but allow anti-virus software to scan the device to remove infected files.

![Feature supported only for Windows-based computers.](image)

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Policy Manager.
2. On the Definitions tab, locate the built-in device definition for All Sandisk removable storage devices (Windows), and click Duplicate.
   The definition uses the Sandisk vendor ID 0781.
   **Best practice:** Duplicate the built-in definitions to customize a definition. For example, you can add other vendor IDs to the duplicated Sandisk definition to add other brands of removable devices.
3. On the Rule Sets tab, select or create a rule set.
5. Enter a name for the rule and select State | Enabled.
6 On the **Conditions** tab, select an End-User or leave the default (is any user). In the **Removable Storage** field, select the device definition you created in step 2.

7 On the **Exceptions** tab, select **Whitelisted File Names**.

8 In the **File Name** field, add the built-in **McAfee AV** definition.

As with the removable storage device definition, you can duplicate this definition and customize it.

9 On the **Reaction** tab, select **Prevent Action | Block**. You can optionally add a user notification and select the **Report Incident** option.

10 Click **Save**, then click **Close**.

**Use case: Set a removable device as read-only**

Removable storage device protection rules, unlike plug-and-play device rules, have a read-only option. By setting removable devices to read-only, you can allow users to use their personal devices as MP3 players while preventing their use as storage devices.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.

2 On the **Definitions** tab, on **Device Definitions** page, create a removable storage device definition.

   Removable storage device definitions must be categorized as Windows or Mac definitions. Start by duplicating one of the built-in definitions for Windows or Mac and customize it. The **Bus Type** can include USB, Bluetooth, and any other bus type you expect to be used. Identify devices with vendor IDs or device names.

3 On the **Rule Sets** tab, select or create a rule set.

4 On the **Device Control** tab, select **Actions | New Rule | Removable Storage Device Rule**.

5 Enter a name for the rule and select **State | Enabled**. In the **Conditions** section, in the **Removable Storage** field, select the device definition you created in step 2.

6 On the **Reaction** tab, select **Prevent Action | Read-only**. You can optionally add a user notification and select the **Report Incident** option.

7 Click **Save**, then click **Close**.

**Use case: Block and charge an iPhone with a plug-and-play device rule**

Apple iPhones can be blocked from use as storage devices while being charged from the computer. This use case creates a rule that blocks a user from using the iPhone as a mass storage device. A plug-and-play device protection rule is used because it allows iPhones to charge no matter how the rule is specified. This feature is not supported for other smartphones, or other Apple mobile devices. It does not prevent an iPhone from charging from the computer.

To define a plug-and-play device rule for specific devices, you create a device definition with the vendor and product ID codes (VID/PID). You can find this information from the Windows **Device Manager** when the device is plugged in. Because this example only requires a VID, you can use the built-in device definition **All Apple devices** rather than looking up the information.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.

2. On the **Rule Sets** tab, select a rule set (or create one). Click the **Device Control** tab, and create a plug-and-play device rule. Use the built-in device definition **All Apple devices** as the included (is one of OR) definition.

3. On the **Reaction** tab, set the prevent action to **Block**.

4. Click **Save**, then click **Close**.

**Use case: Prevent burning sensitive information to disk**
Application file access protection rules can be used to block the use of CD and DVD burners for copying classified information.

**Before you begin**
Create a classification to identify the classified content. Use parameters that are relevant to your environment — keyword, text pattern, file information, and so forth.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.

2. On the **Rule Sets** tab, select a current rule set or select **Actions | New Rule Set** and define a rule set.

3. On the **Data Protection** tab, select **Actions | New Rule | Application File Access Protection**.

4. (Optional) Enter a name in the **Rule Name** field (required). Select options for the **State** and **Severity** fields.

5. On the **Condition** tab, in the **Classification** field, select the classification you created for your sensitive content.

6. In the **End-User** field, select user groups (optional).
   Adding users or groups to the rule limits the rule to specific users.

7. In the **Applications** field, select **Media Burner Application [built-in]** from the available application definitions list.
   You can create your own media burner definition by editing the built-in definition. Editing a built-in definition automatically creates a copy of the original definition.

8. (Optional) On the **Exceptions** tab, create exceptions to the rule.
   Exception definitions can include any field that is in a condition definition. You can define multiple exceptions to use in different situations. One example is to define “privileged users” who are exempt from the rule.

9. On the **Reaction** tab, set the **Prevent Action to Block**. Select a **User Notification** (optional). Click **Save**, then **Close**.
   Other options are to change the default incident reporting and prevent action when the computer is disconnected from the network.
On the Policy Assignment tab, assign the rule set to a policy or policies:

a Select Actions | Assign a Rule Set to policies.

b Select the appropriate rule set from the drop-down list.

c Select the policy or policies to assign it to.

Select Actions | Apply Selected Policies. Select policies to apply to the McAfee ePO database, and click OK.

**Use case: Block outbound messages with confidential content unless they are sent to a specified domain**

Outbound messages are blocked if they contain the word Confidential, unless the recipient is exempt from the rule.

Follow these high-level steps:

- Create an email address definition.
- Create a rule set and a rule that applies to messages that contain Confidential.
- Specify recipients who are exempt from the rule.
- Specify the reaction to messages that contain Confidential.

**Table 9-7 Expected behavior**

<table>
<thead>
<tr>
<th>Email contents</th>
<th>Recipient</th>
<th>Expected result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Body: Confidential</td>
<td><a href="mailto:external_user@external.com">external_user@external.com</a></td>
<td>The message is blocked because it contains the word Confidential.</td>
</tr>
<tr>
<td>Body: Confidential</td>
<td><a href="mailto:internal_user@example.com">internal_user@example.com</a></td>
<td>The message is not blocked because the exception settings mean that confidential</td>
</tr>
<tr>
<td></td>
<td></td>
<td>material can be sent to people at example.com</td>
</tr>
<tr>
<td>Body: Attachment: Confidential</td>
<td><a href="mailto:external_user@external.com">external_user@external.com</a></td>
<td>The message is blocked. The block action for external.com takes the higher priority.</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:internal_user@example.com">internal_user@example.com</a></td>
<td></td>
</tr>
</tbody>
</table>

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Create an email address definition for a domain that is exempt from the rule.

   a In the Data Protection section in McAfee ePO, select DLP Policy Manager and click Definitions.

   b Select the Email Address definition and create a duplicate copy of the built-in My organization email domain.

   c Select the email address definition you created, and click Edit.

   d In Operator, select Domain name is and set the value to example.com.

   e Click Save.

2 Create a rule set with an Email Protection rule.

   a Click Rule Sets, then select Actions | New Rule Set.

   b Name the rule set Block Confidential in email.
c Click **Actions** | **New Rule** | **Email Protection Rule**.

d Name the new rule **Block Confidential** and enable it.

e Enforce the rule on **DLP Endpoint for Windows**.

f Create a duplicate copy of the in-built **Confidential** classification.

An editable copy of the classification appears.

g Select the classification you created and add it to the rule.

h Set the **Recipient** to **any recipient (ALL)**.

   Leave the other settings on the **Condition** tab with the default settings.

3 Add exceptions to the rule.

   a Click **Exceptions**, then select **Actions** | **Add Rule Exception**.

   b Type a name for the exception and enable it.

   c Set the classification to **Confidential**.

   d Set **Recipient** to **at least one recipient belongs to all groups (AND)**, then select the email address definition you created.

4 Configure the reaction to messages that contain the word **Confidential**.

   a Click **Reaction**.

   b In **DLP Endpoint**, set the **Action** to **Block** for computers connected to and disconnected from the corporate network.

5 Save and apply the policy.

**Use case: Allow a specified user group to send credit information**

Allow people in the human resources user group to send messages that contain personal credit information by obtaining information from your Active Directory.

**Before you begin**

Register an Active Directory server with McAfee ePO. See the *McAfee ePolicy Orchestrator Product Guide* for information.

Follow these high-level steps to:

1 Create a personal credit information classification.
2 Create a rule set and a rule that acts on the new classification.
3 Make the human resources user group exempt from the rule.
4 Block messages that contain personal credit information.
5 Apply the policy.

**Best practice**: To ensure that your rules identify potential data loss incidents with minimal false positive results, create your rules using the **No action** setting. Monitor the **DLP Incident Manager** until you are satisfied that the rule identifies incidents correctly, then change the **Action** to **Block**.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. From the McAfee ePO menu, select Classification, and create a duplicate PCI classification.

2. Create the rule set and exceptions to it.
   a. Open the DLP Policy Manager.
   b. In Rule Sets, create a rule set called Block PCI.
   c. Open the rule set you created, select **Action** | **New Rule** | **Email Protection**, and type a name for the rule.
   d. In **Enforce On** select DLP Endpoint for Windows.
   e. In **Classification of**, select the classification you created.
   f. Leave the **End-User**, Email Envelope, and Recipient with the default settings.

3. Specify the user group that you want to exclude from the rule.
   a. Select **Exceptions**, click **Actions** | **Add Rule Exception**, and name it Human resource group exception.
   b. Set the State to Enabled.
   c. In **Classification of**, select contains any data (ALL).
   d. In **Sender** select Belongs to one of groups (OR).
   e. Select **New Item**, and create an end-user group called HR.
   f. Click **Add Groups**, select the group, and click OK.

4. Set the action you want to take if the rule triggers.
   a. Select the group you created and click OK.
   b. Select the **Reaction** tab.
   c. In the **DLP Endpoint** section, set the **Action** to **Block**.
   d. Select **Report Incident**.
   e. Save the rule and click **Close**.

5. Apply the rule.
   a. In the DLP Policy Manager, select **Policy Assignment**.
   b. Select **Actions** | **Assign Rule Sets to a policy**.
   c. Select the rule set you created.
   d. Select **Actions** | **Apply Selected Policies**.
   e. Click **Apply policy**.

   **Pending Changes** shows No.
Use case: Classify attachments as NEED-TO-SHARE based on their destination

Create classifications that allow NEED-TO-SHARE attachments to be sent to employees in the United States, Germany, and Israel.

Follow these high-level steps:

- Create email address definitions.
- Create a rule set and a rule that classifies attachments as NEED-TO-SHARE.
- Specify exceptions to the rule.

The example classifications in the table show how the classifications behave with different classification triggers and recipients.

### Table 9-8 Expected behavior

<table>
<thead>
<tr>
<th>Classification</th>
<th>Recipient</th>
<th>Expected result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us)</td>
<td><a href="mailto:exampleuser1@example1.com">exampleuser1@example1.com</a></td>
<td>Allow — example1.com is allowed to receive all NEED-TO-SHARE attachments</td>
</tr>
<tr>
<td>Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us)</td>
<td><a href="mailto:exampleuser2@example2.com">exampleuser2@example2.com</a></td>
<td>Allow — example2.com is allowed to receive all NEED-TO-SHARE attachments</td>
</tr>
<tr>
<td>Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td><a href="mailto:exampleuser1@example1.com">exampleuser1@example1.com</a></td>
<td>Allow — example1.com and example2.com are allowed to receive both attachments</td>
</tr>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us)</td>
<td><a href="mailto:exampleuser2@example2.com">exampleuser2@example2.com</a></td>
<td>Allow — example2.com is allowed to receive both attachments</td>
</tr>
<tr>
<td>Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td><a href="mailto:exampleuser1@example1.com">exampleuser1@example1.com</a></td>
<td></td>
</tr>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us)</td>
<td><a href="mailto:exampleuser3@gov.il">exampleuser3@gov.il</a></td>
<td>Allow — gov.il is allowed for both attachments</td>
</tr>
<tr>
<td>Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us)</td>
<td><a href="mailto:exampleuser4@gov.us">exampleuser4@gov.us</a></td>
<td>Block — exampleuser4 is not allowed to receive Attachment2</td>
</tr>
<tr>
<td>Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us)</td>
<td><a href="mailto:exampleuser@gov.il">exampleuser@gov.il</a></td>
<td>Block — exampleuser4 is not allowed to receive Attachment2</td>
</tr>
<tr>
<td>Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td><a href="mailto:exampleuser4@gov.us">exampleuser4@gov.us</a></td>
<td></td>
</tr>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us)</td>
<td><a href="mailto:exampleuser1@example1.com">exampleuser1@example1.com</a></td>
<td>Block — exampleuser4 is not allowed to receive Attachment2</td>
</tr>
<tr>
<td>Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td><a href="mailto:exampleuser4@gov.us">exampleuser4@gov.us</a></td>
<td></td>
</tr>
</tbody>
</table>
Table 9-8 Expected behavior (continued)

<table>
<thead>
<tr>
<th>Classification</th>
<th>Recipient</th>
<th>Expected result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us) Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td><a href="mailto:exampleuser2@example2.com">exampleuser2@example2.com</a> <a href="mailto:exampleuser1@example1.com">exampleuser1@example1.com</a> <a href="mailto:exampleuser4@gov.us">exampleuser4@gov.us</a></td>
<td>Allow — exampleuser1 and exampleuser3 are allowed to receive both attachments</td>
</tr>
<tr>
<td>Attachment1: NEED-TO-SHARE, Israel (.il) and United States (.us) Attachment2: NEED-TO-SHARE, Israel (.il) and Germany (.de)</td>
<td><a href="mailto:exampleuser2@example2.com">exampleuser2@example2.com</a> <a href="mailto:exampleuser1@example1.com">exampleuser1@example1.com</a> <a href="mailto:exampleuser4@gov.us">exampleuser4@gov.us</a></td>
<td>Block — exampleuser4 cannot receive Attachment2</td>
</tr>
</tbody>
</table>

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Create an email address definition for the domains that are exempt from the rule.
   a. In the Data Protection section in McAfee ePO, select DLP Policy Manager and click Definitions.
   b. Select the Email Address definition and create a duplicate copy of the built-in My organization email domain.
   c. Select the email address definition you created, and click Edit.
   d. In Operator, select Domain name is and set the value to example1.com.
   e. Create entries for example2.com, .il, and .us.
   f. Click Save.
   g. Repeat these steps to create a definition for gov.il.
   h. Repeat the steps again to create a definition for gov.us.

2. Create a rule set that includes an Email Protection rule.
   a. Click Rule Sets, then select Actions | New Rule Set.
   b. Name the rule set Allow NEED-TO-SHARE email to Israel and United States.

3. Create a rule and add the NEED-TO-SHARE classification criteria.
   a. Click Actions | New Rule | Email Protection Rule.
   b. Name the rule NEED-TO-SHARE, enable it, and enforce it on DLP Endpoint for Windows.
   c. Add a classification criteria called NEED-TO-SHARE.
   d. Set Classification of to one of the attachments (*).
   e. Select contains one of (OR), and select the NEED-TO-SHARE classification criteria.
   f. Set the Recipient to any recipient (ALL).
   g. Leave the other settings on the Condition tab with the default settings.
4 Add exceptions to the rule, and enable each exception.
   • Exception 1
     1 Set Classification of to matched attachment.
     2 Select contains one of (OR), and select the NEED-TO-SHARE classification criteria.
     3 Set the Recipient to matched recipient belongs to one of groups (OR), and select the example1.com and example2.com definitions.
   • Exception 2
     1 Set Classification of to matched attachment.
     2 Select contains all of (AND), and select the NEED-TO-SHARE and .il classification criteria.
     3 Set the Recipient to matched recipient belongs to one of groups (OR), and select gov.il.
   • Exception 3
     1 Set Classification of to matched attachment.
     2 Select contains all of (AND), and select the NEED-TO-SHARE and .us classification criteria.
     3 Set the Recipient to matched recipient belongs to one of groups (OR), and select gov.us.

5 In DLP Endpoint, set the Action to Block.

6 Click Save.

7 Apply the policy.
Protecting sensitive content
Rule use cases
Scanning data with McAfee DLP Endpoint discovery

Discovery is a crawler that runs on endpoint computers. It searches local file system and email storage files, and applies rules to protect sensitive content.

Contents

- Protecting files with discovery rules
- How discovery scanning works
- Find content with the Endpoint Discovery crawler

Protecting files with discovery rules

Discovery rules define the content that McAfee DLP searches for when scanning repositories and determine the action taken when matching content is found.

Depending on the type of rule, files matching a scan can be copied, moved, encrypted, quarantined, tagged, or have a rights management policy applied. All discovery rule conditions include a classification.

When using email storage discovery rules with the Quarantine prevent action, verify that the Outlook Add-in is enabled (Policy Catalog | Data Loss Prevention 9.4 | Client Configuration | Operational Modes and Modules). You cannot release emails from quarantine when the Outlook Add-in is disabled.

Table 10-1 Available discovery rules

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Product</th>
<th>Controls files discovered from...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local File System</td>
<td>McAfee DLP Endpoint</td>
<td>Local file system scans.</td>
</tr>
<tr>
<td>Local Email (OST, PST)</td>
<td>McAfee DLP Endpoint</td>
<td>Email storage system scans.</td>
</tr>
</tbody>
</table>

End-user initiated scans

When activated in the DLP Policy local file system scan configuration, end-users can run enabled scans and can view self-remediation actions. Every scan must have an assigned schedule, and the scan runs according to the schedule whether or not the user chooses to run a scan, but when the user interaction option is enabled, the end-users can also run scans at their convenience. If the self-remediation option is also selected, end-users and also perform remediation actions.
How discovery scanning works

Use endpoint discovery scans to locate local file system or email storage files with sensitive content and tag or quarantine them.

McAfee DLP Endpoint discovery is a crawler that runs on client computers. When it finds predefined content, it can monitor, quarantine, tag, encrypt, or apply an RM policy to the files containing that content. Endpoint discovery can scan computer files or email storage (PST, mapped PST, and OST) files. Email storage files are cached on a per-user basis.

To use endpoint discovery, you must activate the Discovery modules on the Policy Catalog | Client configuration | Operational Mode and Modules page.

At the end of each discovery scan, the McAfee DLP Endpoint client sends a discovery summary event to the DLP Incident Manager console in McAfee ePO to log the details of the scan. The event includes an evidence file that lists the files that could not be scanned and the reason for not scanning each of these files. There is also an evidence file with files matching the classification and the action taken.

In McAfee DLP Endpoint 9.4.0, the summary event was an operational event. To update old summary events to the DLP Incident Manager, use the McAfee ePO server task DLP Incident Event Migration from 9.4 to 9.4.1.

When can you search?

Schedule discovery scans on the Policy Catalog | DLP Policy | Endpoint Discovery page. You can run a scan at a specific time daily, or on specified days of the week or month. You can specify start and stop dates, or run a scan when the McAfee DLP Endpoint configuration is enforced. You can suspend a scan when the computer’s CPU or RAM exceed a specified limit.

If you change the discovery policy while an endpoint scan is running, rules and schedule parameters will change immediately. Changes to which parameters are enabled or disabled will take effect with the next scan. If the computer is restarted while a scan is running, the scan continues where it left off.

What content can be discovered?

You define discovery rules with a classification. Any file property or data condition that can be added to classification criteria can be used to discover content.

What happens to discovered files with sensitive content?

You can quarantine or tag email files. You can encrypt, quarantine, tag, or apply an RM policy to local file system files. You can store evidence for both file types.

Find content with the Endpoint Discovery crawler

There are four steps to running the discovery crawler.

1. Create and define classifications to identify the sensitive content.
2. Create and define a discovery rule. The discovery rule includes the classification as part of the definition.
3. Create a schedule definition.
4. Set up the scan parameters. The scan definition includes the schedule as one of the parameters.
Tasks

- **Create and define a discovery rule on page 131**
  Discovery rules define the content the crawler searches for, and what to do when this content is found.

- **Create a scheduler definition on page 131**
  The scheduler determines when and how frequently a discovery scan is run.

- **Set up a scan on page 132**
  Discovery scans crawl the local file system or mailboxes for sensitive content.

- **Use case: Restore quarantined files or email items on page 133**
  When McAfee DLP Endpoint discovery finds sensitive content, it moves the affected files or email items into a quarantine folder, replacing them with placeholders that notify users that their files or emails have been quarantined. The quarantined files and email items are also encrypted to prevent unauthorized use.

**Create and define a discovery rule**
Discovery rules define the content the crawler searches for, and what to do when this content is found. Changes to a discovery rule take effect when the policy is deployed. Even if a scan is in progress, a new rule takes effect immediately.

For email storage (PST, mapped PST, and OST) scans, the crawler scans email items (body and attachments), calendar items, and tasks. It does not scan public folders or sticky notes.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Policy Manager**.
2. On the **Rule Sets** page, select **Actions | New Rule Set**. Enter a name and click **OK**.
   You can also add discovery rules to an existing rule set.
3. On the **Discovery** tab, select **Actions | New Endpoint Discovery Rule**, then select either **Local Email** or **Local File System**.
   The appropriate page appears.
4. Enter a rule name and select a classification.
5. Click **Reaction**. Select a prevent action from the drop-down list.
6. (Optional) Select **Report Incident** options, set the **State** to **Enabled**, and select a **Severity** designation from the drop-down list.
7. Click **Save**.

**Create a scheduler definition**
The scheduler determines when and how frequently a discovery scan is run. Five schedule types are provided:
Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager.
2 Click the Definitions tab.
3 In the left pane, click Scheduler
   If both McAfee DLP Discover and McAfee DLP Endpoint are installed, the list of existing schedules displayed includes schedules for both.
4 Select Actions | New.
   The New Scheduler page appears.
5 Enter a unique Name, and select the Schedule type from the drop-down list.
   The display changes when you select the schedule type to provide the necessary fields for that type.
6 Fill in the required options and click Save.

Set up a scan
Discovery scans crawl the local file system or mailboxes for sensitive content.

Before you begin
Verify that the rule sets you want to apply to the scans have been applied to the DLP Policy. This information is displayed on the DLP Policy | Rule Sets tab.

Changes in discovery setting parameters take effect on the next scan. They are not applied to scans already in progress.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Policy | Policy Catalog.
2 Select Product | Data Loss Prevention 10, then select the active DLP Policy.
3 On the Endpoint Discovery tab, select Actions | New Endpoint Scan, then select either Local Email or Local File System.
4 Enter a name for the scan, then select a schedule from the drop-down list.
5 Optional: Change the Incident Handling and Error Handling defaults. Set the State to Enabled. Error handling refers to when text cannot be extracted.
6 (Optional) For local file system scans, select the checkbox in the User Interaction field to allow the user to run enabled scans before they are scheduled. You can also enable the user to perform remediation actions from the McAfee DLP Endpoint client console.
On the Folders tab, do one of the following:

- For file system scans, select **Actions | Select Folders**. Select a defined folder definition or click **New Item** to create one. Define the folder as **Include** or **Exclude**.

- For email scans, select the file types (OST, PST) and the mailboxes to be scanned.

(Optional) On the **Filters** tab (file system scans only) select **Actions | Select Filters**. Select a file information definition or click **New Item** to create one. Define the filter as **Include** or **Exclude**. Click **OK**. The default is **All Files**. Defining a filter makes the scan more efficient.

On the **Rules** tab, verify the rules that apply. All discovery rules from rule sets applied to the policy are run.

**Use case: Restore quarantined files or email items**

When McAfee DLP Endpoint discovery finds sensitive content, it moves the affected files or email items into a quarantine folder, replacing them with placeholders that notify users that their files or emails have been quarantined. The quarantined files and email items are also encrypted to prevent unauthorized use.

**Before you begin**

To display the McAfee DLP icon in Microsoft Outlook, the **Show Release from Quarantine Controls in Outlook** option must be enabled in **Policy Catalog | Client Policy | Operational Mode and Modules**. When disabled, both the icon and the right-click option for viewing quarantined emails are blocked, and you cannot release emails from quarantine.

When you set a file system discovery rule to **Quarantine** and the crawler finds sensitive content, it moves the affected files into a quarantine folder, replacing them with placeholders that notify users that their files have been quarantined. The quarantined files are encrypted to prevent unauthorized use.

For quarantined email items, McAfee DLP Endpoint discovery attaches a prefix to the Outlook **Subject** to indicate to users that their emails have been quarantined. Both the email body and any attachments are quarantined.

> The mechanism has been changed from previous McAfee DLP Endpoint versions, which could encrypt either the body or attachments, to prevent signature corruption when working with the email signing system.

Microsoft Outlook calendar items and tasks can also be quarantined.

![Quarantined email example](image)

**Figure 10-1 Quarantined email example**

**Task**

1. To restore quarantined files:
   a. In the system tray of the managed computer, click the **McAfee Agent** icon, and select **Manage Features | DLP Endpoint Console**.

The DLP Endpoint Console opens.
b On the Tasks tab, select **Open Quarantine Folder**.

The quarantine folder opens.

c Select the files to be restored. Right-click and select **Release from Quarantine**.

_The Release from Quarantine context-sensitive menu item only appears when selecting files of type *.dlpenc (DLP encrypted)._ 

The **Release Code** pop-up window appears.

2 To restore quarantined email items: Click the **McAfee DLP** icon, or right-click and select **Release from Quarantine**.

a In Microsoft Outlook, select the emails (or other items) to be restored.

b Click the **McAfee DLP** icon.

The **Release Code** pop-up window appears.

3 Copy the challenge ID code from the pop-up window and send it to the DLP administrator.

4 The administrator generates a response code and sends it to the user. (This also creates an operational event recording all the details.)

5 The user enters the release code in the **Release Code** pop-up window and clicks **OK**.

The decrypted files are restored to their original location. If the release code lockout policy has been activated (in the **Agent Configuration | Notification Service** tab) and you enter the code incorrectly three times, the pop-up window times out for 30 minutes (default setting).

_For files, if the path has been changed or deleted, the original path is restored. If a file with the same name exists in the location, the file is restored as xxx-copy.abc_
Monitoring and reporting

You can use McAfee DLP Endpoint software components to track and review policy violations (DLP Incident Manager), and to track administrative events (DLP Operations).

Chapter 11  Incidents and operational events
Chapter 12  Collecting and managing data
Incidents and operational events

McAfee DLP offers different tools for viewing incidents and operational events.

- **Incidents** — The DLP Incident Manager page displays incidents generated from rules.
- **Operational events** — The DLP Operations page displays errors and administrative information.
- **Cases** — The DLP Case Management page contains cases that have been created to group and manage related incidents.

When both McAfee DLP Discover and McAfee DLP Endpoint are installed, the consoles display incidents and events from both applications.

The display for both DLP Incident Manager and DLP Operations can include information on the computer and logged-on user generating the incident/event, client version, operating system, and other information.

## Monitoring and reporting events

McAfee DLP divides events into two classes: incidents (that is, policy violations) and administrative events. These events are viewed in the two consoles, DLP Incident Manager and DLP Operations.

When McAfee DLP determines a policy violation has occurred, it generates an event and sends it to the McAfee ePO Event Parser. These events are viewed, filtered, and sorted in the DLP Incident Manager console, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.

As McAfee DLP takes a major role in an enterprise’s effort to comply with all regulation and privacy laws, the DLP Incident Manager presents information about the transmission of sensitive data in an accurate and flexible way. Auditors, signing officers, privacy officials and other key workers can use the DLP Incident Manager to observe suspicious or unauthorized activities and act in accordance with enterprise privacy policy, relevant regulations or other laws.

The system administrator or the security officer can follow administrative events regarding agents and policy distribution status.
The DLP Operations console displays

- **McAfee DLP Discover**: Scan or server errors
- **McAfee DLP Endpoint**: Details on client deployment, policy changes, policy deployment, Safe Mode logons, agent overrides, and other administrative events

### DLP Incident Manager

Use the DLP Incident Manager page in McAfee ePO to view the security events from policy violations. The incident manager has three tabbed sections:

- **Incident List** — The current list of policy violation events.
- **Incident Tasks** — A list of actions you can take on the list or selected parts of it. They include assigning reviewers to incidents, setting automatic email notifications, and purging all or part of the list.
- **Incident History** — A list containing all historic incidents. Purging the incident list does not affect the history.

Use the DLP Operations module to view administrative events such as agent deployments. The module is organized identically, with three tabbed pages: Operational Event List, Operational Event Tasks, and Operational Event History.

**How the Incident Manager works**

The Incident List tab of the DLP Incident Manager has all the functionality required for reviewing policy violation incidents. Event details are viewed by clicking a specific event. You can create and save filters to change the view or use the predefined filters in the left pane. You can also change the view by selecting and ordering columns. Color-coded icons and numeric ratings for severity facilitate quick visual scanning of events.

The Incident List tab works with McAfee ePO Queries & Reports to create McAfee DLP Endpoint reports and display data on McAfee ePO dashboards.

Operations you can perform on events include:

- **Case management** — Create cases and add selected incidents to a case
- **Comments** — Add comments to selected incidents
- **Email events** — Send selected events
- **Export device parameters** — Export device parameters to a CSV file (Data in-use/motion list only)
- **Labels** — Set a label for filtering by label
• **Release redaction** — Remove redaction to view protected fields (requires correct permission)
• **Set properties** — Edit the severity, status, or resolution; assign a user or group for incident review

![DLP Incident Manager](image)

**Figure 11-1  DLP Incident Manager**

The DLP Operations page works in an identical manner with administrative events. The events contain information such as why the event was generated and which McAfee DLP product reported the event. It can also include user information connected with the event, such as user logon name, user principle name (username@xyz), or user manager, department, or business unit. Operational events can be filtered by any of these, or by other parameters such as severity, status, client version, policy name, and more.

![DLP Operations](image)

**Figure 11-2 DLP Operations**

### Incident tasks/Operational Event tasks

Use the Incident Tasks or Operational Event Tasks tab to set criteria for scheduled tasks. Tasks set up on the pages work with the McAfee ePO Server Tasks feature to schedule tasks.

Both tasks tabs are organized by the task type (left pane). The Incident Tasks tab is also organized by incident type, so that it is actually a 4 x 3 matrix, the information displayed depending on which two parameters you select.

<table>
<thead>
<tr>
<th></th>
<th>Data in-use/motion</th>
<th>Data at-rest (Endpoint)</th>
<th>Data at-rest (Network)</th>
<th>Data in-use/motion (History)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Reviewer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Automatic mail notification</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Purge events</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Use case: Setting properties
Properties are data added to an incident that requires follow-up. You can add the properties from the details pane of the incident or by selecting Actions | Set Properties. The properties are:

- Severity
- Status
- Resolution
- Reviewing Group
- Reviewing User

The reviewer can be any McAfee ePO user. The reason severity can be changed is that if the administrator determines that the status is false positive, then the original severity is no longer meaningful.

Use case: Changing the view
In addition to using filters to change the view, you can also customize the fields and the order of display. Customized views can be saved and reused.

Creating a filter involves the following tasks:
1. To open the view edit window, click Actions | View | Choose Columns.
2. To move columns to the left or right, use the x icon to delete columns, and the arrow icons.
3. To apply the customized view, click Update View.
4. To save for future use, click Actions | View | Save View.

When you save the view, you can also save the time and custom filters. Saved views can be chosen from the drop-down list at the top of the page.

Working with incidents
When McAfee DLP receives data that matches parameters defined in a rule, a violation is triggered and McAfee DLP generates an incident.

Using the incident manager in McAfee ePO, you can view, sort, group, and filter incidents to find important violations. You can view details of incidents or delete incidents that are not useful.

View incidents
The incident manager displays all incidents reported by McAfee DLP applications. You can alter the way incidents appear to help you locate important violations more efficiently.

The Present field in the DLP Incident Manager sorts the incidents viewed according to the application that produced them:

- Data in-use/motion — Displays incidents from McAfee DLP Endpoint or Device Control.
- Data at rest (Endpoint) — Displays incidents from McAfee DLP Endpoint discovery.
- Data at rest (Network) — Displays incidents from McAfee DLP Discover.

When McAfee DLP processes an object — such as an email message — that triggers multiple rules, the incident manager collates and displays the violations as one incident, rather than separate incidents.
Tasks

- **Sort and filter incidents on page 141**
  Arrange the way incidents appear based on attributes such as time, location, user, or severity.

- **Configure column views on page 141**
  Use views to arrange the type and order of columns displayed in the incident manager.

- **Configure incident filters on page 142**
  Use filters to display incidents that match specified criteria.

- **View incident details on page 143**
  View the information related to an incident.

**Sort and filter incidents**

Arrange the way incidents appear based on attributes such as time, location, user, or severity.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **DLP Incident Manager**.
2. Do one of the following:
   - For Device Control or McAfee DLP Endpoint incidents: From the **Present** drop-down list, select **Data in-use/motion**.
   - For McAfee DLP Endpoint discovery incidents: From the **Present** drop-down list, select **Data at rest (Endpoint)**.
   - For McAfee DLP Discover incidents: From the **Present** drop-down list, select **Data at rest (Network)** and if needed, click the **Scan** link to set the scan.
3. Perform any of these tasks.
   - To sort by column, click a column header.
   - To change columns to a custom view, from the **View** drop-down list, select a custom view.
   - To filter by time, from the **Time** drop-down list, select a time frame.
   - To apply a custom filter, from the **Filter** drop-down list, select a custom filter.
   - To group by attribute:
     1. From the **Group By** drop-down list, select an attribute.
        A list of available options appears. The list contains up to 250 of the most frequently occurring options.
     2. Select an option from the list. Incidents that match the selection are displayed.

**Example**

When working with McAfee DLP Endpoint incidents, select **UserID** to display the names of users that have triggered violations. Select a user name to display all incidents for that user.

**Configure column views**

Use views to arrange the type and order of columns displayed in the incident manager.
Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select DLP Incident Manager.

2 Do one of the following:
   • For Device Control or McAfee DLP Endpoint incidents: From the Present drop-down list, select Data in-use/motion.
   • For McAfee DLP Endpoint discovery incidents: From the Present drop-down list, select Data at rest (Endpoint).
   • For McAfee DLP Discover incidents: From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.

3 From the View drop-down list, select Default and click Edit.

4 Configure the columns.
   a From the Available Columns list, click an option to move it to the Selected Columns area.
   b In the Selected Columns area, arrange and delete columns as needed.
      • To remove a column, click x.
      • To move a column, click the arrow buttons, or drag and drop the column.
   c Click Update View.

5 Configure the view settings.
   a Next to the View drop-down list, click Save.
   b Select one of these options.
      • Save as new view — Specify a name for the view.
      • Override existing view — Select the view to save.
   c Select who can use the view.
      • Public — Any user can use the view.
      • Private — Only the user that created the view can use the view.
   d Specify if you want the current filters or groupings applied to the view.
   e Click OK.

You can also manage views in the Incident Manager by selecting Actions | View.

Configure incident filters
Use filters to display incidents that match specified criteria.
McAfee DLP Endpoint Example: You suspect a particular user has been sending connections containing sensitive data to a range of IP addresses outside the company. You can create a filter to display incidents that match the user name and the range of IP addresses.
Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select DLP Incident Manager.

2 Do one of the following:
   - For Device Control or McAfee DLP Endpoint incidents: From the Present drop-down list, select Data in-use/motion.
   - For McAfee DLP Endpoint discovery incidents: From the Present drop-down list, select Data at rest (Endpoint).
   - For McAfee DLP Discover incidents: From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.

3 From the Filter drop-down list, select (no custom filter) and click Edit.

4 Configure the filter parameters.
   a From the Available Properties list, select a property.
   b Enter the value for the property.
      To add additional values for the same property, click +.
   c Select additional properties as needed.
      To remove a property entry, click <.
   d Click Update Filter.

5 Configure the filter settings.
   a Next to the Filter drop-down list, click Save.
   b Select one of these options.
      • Save as new filter — Specify a name for the filter.
      • Override existing filter — Select the filter to save.
   c Select who can use the filter.
      • Public — Any user can use the filter.
      • Private — Only the user that created the filter can use the filter.
   d Click OK.

You can also manage filters in the incident manager by selecting Actions | Filter.

View incident details
View the information related to an incident.
Task
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select DLP Incident Manager.

2. Do one of the following:
   - For Device Control or McAfee DLP Endpoint incidents: From the Present drop-down list, select Data in-use/motion.
   - For McAfee DLP Endpoint discovery incidents: From the Present drop-down list, select Data at rest (Endpoint).
   - For McAfee DLP Discover incidents: From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.

3. Click an Incident ID.
   In McAfee DLP Endpoint, the page displays general details and source information. Depending on the incident type, destination or device details appear. In McAfee DLP Discover, the page displays general details about the incident.

4. To view additional information, perform any of these tasks.
   - To view user information in McAfee DLP Endpoint, click the user name in the Source area.
   - To view evidence files:
     1. Click the Evidence tab.
     2. Click a file name to open the file with an appropriate program.
     The Evidence tab also displays the Short Match String, which contains up to three hit highlights as a single string.
   - To view rules that triggered the incident, click the Rules tab.
   - To view classifications, click the Classifications tab.
     In McAfee DLP Endpoint, the Classifications tab does not appear for some incident types.
   - To view incident history, click the Audit Logs tab.
   - To view comments added to the incident, click the Comments tab.
   - To email the incident details, including decrypted evidence and hit highlight files, select Actions | Email Selected Events.
   - To return to the incident manager, click OK.

Manage incidents
Use the incident manager to update and manage incidents.
To delete incidents, configure a task to purge events.
Tasks

- **Update a single incident on page 145**
  Update incident information such as the severity, status, and reviewer.

- **Update multiple incidents on page 145**
  Update multiple incidents with the same information simultaneously.

- **Manage labels on page 147**
  A label is a custom attribute used to identify incidents that share similar traits.

**Update a single incident**
Update incident information such as the severity, status, and reviewer.

The Audit Logs tab reports all updates and modifications performed on an incident.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select DLP Incident Manager.

2. Do one of the following:
   - For Device Control or McAfee DLP Endpoint incidents: From the Present drop-down list, select Data in-use/motion.
   - For McAfee DLP Endpoint discovery incidents: From the Present drop-down list, select Data at rest (Endpoint).
   - For McAfee DLP Discover incidents: From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.

3. Click an incident.

4. Perform any of these tasks.
   - To update the severity, status, or resolution:
     1. From the Severity, Status, or Resolution drop-down lists, select an option.
     2. Click Save.
   - To update the reviewer:
     1. Next to the Reviewer field, click ...
     2. Select the group or user and click OK.
     3. Click Save.
   - To add a comment:
     1. Select Actions | Add Comment.
     2. Enter a comment, then click OK.

**Update multiple incidents**
Update multiple incidents with the same information simultaneously.

*Example:* You have applied a filter to display all incidents from a particular user or scan, and you want to change the severity of these incidents to Major.
Task
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **DLP Incident Manager**.

2. Do one of the following:
   - For Device Control or McAfee DLP Endpoint incidents: From the **Present** drop-down list, select **Data in-use/motion**.
   - For McAfee DLP Endpoint discovery incidents: From the **Present** drop-down list, select **Data at rest (Endpoint)**.
   - For McAfee DLP Discover incidents: From the **Present** drop-down list, select **Data at rest (Network)** and if needed, click the **Scan** link to set the scan.

3. Select the checkboxes of the incidents to update.

   ![To update all incidents displayed by the current filter, click **Select all in this page**.]

4. Perform any of these tasks.
   - To add a comment, select **Actions** | **Add Comment**, enter a comment, then click **OK**.
   - To send the incidents in an email, select **Actions** | **Email Selected Events**, enter the information, then click **OK**.

     ![You can select a template, or create a template by entering the information and clicking **Save**.]

   - To change the properties, select **Actions** | **Set Properties**, change the options, then click **OK**.

Tasks
- **Email selected events on page 146**
  The following tables give some details concerning the email and export selected events options.

See also
**Email selected events on page 146**

Email selected events
The following tables give some details concerning the email and export selected events options.

**Table 11-1  Email selected events**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of events to mail</td>
<td>100</td>
</tr>
<tr>
<td>Maximum size of each event</td>
<td>unlimited</td>
</tr>
<tr>
<td>Maximum size of the compressed (ZIP) file</td>
<td>20MB</td>
</tr>
<tr>
<td>From</td>
<td>limited to 100 characters</td>
</tr>
<tr>
<td>To, CC</td>
<td>limited to 500 characters</td>
</tr>
<tr>
<td>Subject</td>
<td>limited to 150 characters</td>
</tr>
<tr>
<td>Body</td>
<td>limited to 1000 characters</td>
</tr>
</tbody>
</table>
### Table 11-2 Export selected events

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of events to export</td>
<td>1000</td>
</tr>
<tr>
<td>Maximum size of each event</td>
<td>unlimited</td>
</tr>
<tr>
<td>Maximum size of the export compressed (ZIP) file</td>
<td>unlimited</td>
</tr>
</tbody>
</table>

### Manage labels

A label is a custom attribute used to identify incidents that share similar traits.

You can assign multiple labels to an incident and you can reuse a label on multiple incidents.

**Example:** You have incidents that relate to several projects your company is developing. You can create labels with the name of each project and assign the labels to the respective incidents.

### Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **DLP Incident Manager**.

2. Do one of the following:
   - For Device Control or McAfee DLP Endpoint incidents: From the **Present** drop-down list, select **Data in-use/motion**.
   - For McAfee DLP Endpoint discovery incidents: From the **Present** drop-down list, select **Data at rest (Endpoint)**.
   - For McAfee DLP Discover incidents: From the **Present** drop-down list, select **Data at rest (Network)** and if needed, click the **Scan** link to set the scan.

3. Select the checkboxes of one or more incidents.

   ![To update all incidents displayed by the current filter, click Select all in this page.](image)

4. Perform any of these tasks.
   - To add labels:
     1. Select **Actions | Labels | Attach**.
     2. To add a new label, enter a name and click **Add**.
     3. Select one or more labels.
     4. Click **OK**.
   - To remove labels from an incident:
     1. Select **Actions | Labels | Detach**.
     2. Select the labels to remove from the incident.
     3. Click **OK**.
   - To delete labels:
     1. Select **Actions | Labels | Delete Labels**.
     2. Select the labels to delete.
     3. Click **OK**.
Working with cases

Cases allow administrators to collaborate on the resolution of related incidents.  
In many situations, a single incident is not an isolated event. You might see multiple incidents in the DLP Incident Manager that share common properties or are related to each other. You can assign these related incidents to a case. Multiple administrators can monitor and manage a case depending on their roles in the organization.

Scenario: You notice that a particular user often generates several incidents after business hours. This could indicate that the user is engaging in suspicious activity or that the user’s system has been compromised. Assign these incidents to a case to keep track of when and how many of these violations occur.

Depending on the nature of the violations, you might need to alert the HR or legal teams about these incidents. You can allow members of these teams to work on the case, such as adding comments, changing the priority, or notifying key stakeholders.

Manage cases

Create and maintain cases for incident resolution.

Create cases

Create a case to group and review related incidents.

Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Select Actions | New.
3. Enter a title name and configure the options.
4. Click OK.

View case information

View audit logs, user comments, and incidents assigned to a case.

Task

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Click on a case ID.
3. Perform any of these tasks.
   • To view incidents assigned to the case, click the Incidents tab.
   • To view user comments, click the Comments tab.
   • To view the audit logs, click the Audit Log tab.
4. Click OK.
Assign incidents to a case
Add related incidents to a new or existing case.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Incident Manager.
2 From the Present drop-down list, select an incident type. For Data at rest (Network) click the Scan link to set the scan if needed.
3 Select the checkboxes of one or more incidents.

   Use options such as Filter or Group By to show related incidents. To update all incidents displayed by the current filter, click Select all in this page.

4 Assign the incidents to a case.
   • To add to a new case, select Actions | Case Management | Add to new case, enter a title name, and configure the options.
   • To add to an existing case, select Actions | Case Management | Add to existing case, filter by the case ID or title, and select the case.

5 Click OK.

Move or remove incidents from a case
If an incident is no longer relevant to a case, you can remove it from the case or move it to another case.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2 Click a case ID.
3 Perform any of these tasks.
   • To move incidents from one case to another:
     1 Click the Incidents tab and select the incidents.
     2 Select Actions | Move, then select whether to move to an existing or new case.
     3 Select the existing case or configure options for a new case, then click OK.
   • To remove incidents from the case:
     1 Click the Incidents tab and select the incidents.
     2 Select Actions | Remove, then click Yes.

4 Click OK.

   You can also move or remove one incident from the Incidents tab by clicking Move or Remove in the Actions column.
**Update cases**

Update case information such as changing the owner, sending notifications, or adding comments. Notifications are sent to the case creator, case owner, and selected users when:

- An email is added or changed.
- Incidents are added to or deleted from the case.
- The case title is changed.
- The owner details are changed.
- The priority is changed.
- The resolution is changed.
- Comments are added.

You can disable automatic email notifications to the case creator and owner from **Menu | Configuration | Server Settings | Data Loss Prevention**.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Data Protection | DLP Case Management**.
2. Click a case ID.
3. Perform any of these tasks.
   - To update the case name, in the **Title** field, enter a new name, then click **Save**.
   - To update the owner:
     1. Next to the **Owner** field, click ...
     2. Select the group or user.
     3. Click OK.
     4. Click **Save**.
   - To update the **Priority**, **Status**, or **Resolution** options, use the drop-down lists to select the items, then click **Save**.
   - To send email notifications:
     1. Next to the **Send notifications to** field, click ...
     2. Select the users to send notifications to.

   If no contacts are listed, specify an email server for McAfee ePO and add email addresses for users. Configure the email server from **Menu | Configuration | Server Settings | Email Server**. Configure users from **Menu | User Management | Users**.

3. Click **Save**.
To add a comment to the case:
1. Click the Comments tab.
2. Enter the comment in the text field.
3. Click Add Comment.
4. Click OK.

Add or remove labels to a case
Use labels to distinguish cases by a custom attribute.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Select the checkboxes of one or more cases.

To update all incidents displayed by the current filter, click Select all in this page.

3. Perform any of these tasks.
   - To add labels to the selected cases:
     1. Select Actions | Manage Labels | Attach.
     2. To add a new label, enter a name and click Add.
     3. Select one or more labels.
     4. Click OK.
   - To remove labels from the selected cases:
     1. Select Actions | Manage Labels | Detach.
     2. Select the labels to remove.
     3. Click OK.

Delete cases
Delete cases that are no longer needed.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Select the checkboxes of one or more cases.

To delete all cases displayed by the current filter, click Select all in this page.

3. Select Actions | Delete, then click Yes.
Incidents and operational events
Manage cases
Collecting and managing data

Monitoring the system consists of gathering and reviewing evidence and events, and producing reports. Incident and event data from the DLP tables in the McAfee ePO database is viewed in the DLP Incident Manager and DLP Operations pages or is collated into reports and dashboards.

By reviewing recorded events and evidence, administrators determine when rules are too restrictive, causing unnecessary work delays, and when they are too lax, allowing data leaks.

Contents

- Edit server tasks
- Monitor task results
- Creating reports

Edit server tasks

McAfee DLP uses the McAfee ePO Server Tasks to run DLP Incident Manager and DLP Operations tasks. Each incident and operational events task is predefined in the server tasks list. The only options available are to enable or disable them or to change the scheduling. The available McAfee DLP server tasks are:

- DLP Incident Events conversion from 9.4 to 9.4.1 and later
- DLP incident migration from 9.3.x to 9.4.1 and later
- DLP incident tasks runner*
- DLP MA properties reporting task
- DLP Operational Events Migration
- DLP Policy Conversion
- DLP Policy Push task
- DLP Purge History of Operational Events and Incidents
- DLP Purge Operational Events and Incidents
- DLP Send Email for Operational Events and Incidents
- DLP Set Reviewer for Operational Events and Incidents
- Mark DLP incidents with HIGH or CRITICAL severity for import by DLP manager

* DLP incident tasks runner is a McAfee DLP 9.3 task. It appears only if you have both versions of McAfee DLP installed.
Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Automation | Server Tasks.

2 Select the task to edit.

   ![Best practice: Enter DLP in the Quick find field to filter the list.]

3 Select Actions | Edit, then click Schedule.

4 Edit the schedule as required, then click Save.

Tasks

- Create a Purge events task on page 154
  You create incident and event purge tasks to clear the database of data that is no longer needed.

- Create an Automatic mail Notification task on page 155
  You can set automatic email notifications of incidents and operational events to administrators, managers, or users.

- Create a Set Reviewer task on page 155
  You can assign reviewers for different incidents and operational events to divide the workload in large organizations.

See also
Create a Set Reviewer task on page 155
Create an Automatic mail Notification task on page 155
Create a Purge events task on page 154

Create a Purge events task
You create incident and event purge tasks to clear the database of data that is no longer needed.

Purge tasks can be created for the Incident List, data in-use incidents on the History list, or the Operational Event List.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Incident Manager or Menu | Data Protection | DLP Operations.

2 Click the Incident Tasks or Operational Event Tasks tab.

3 Select an incident type from the drop-down list (Incident Tasks only), select Purge events in the Task Type pane, then click Actions | New Rule.

   Data in-use/motion (Archive) purges events from the History.

4 Enter a name and optional description, then click Next.

   Rules are enabled by default. You can change this setting to delay running the rule.

5 Click > to add criteria, < to remove them. Set the Comparison and Value parameters. When you have finished defining criteria, click Save.

The task runs daily for live data and every Friday at 10:00 PM for historical data.

See also
Edit server tasks on page 153
Create an Automatic mail Notification task
You can set automatic email notifications of incidents and operational events to administrators, managers, or users.

Task
For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select Menu | Data Protection | DLP Incident Manager or Menu | Data Protection | DLP Operations.
2. Click the Incident Tasks or Operational Events Tasks tab.
3. Select an incident type from the drop-down list (Incident Tasks only), select Automatic mail Notification in the Task Type pane, then click Actions | New Rule.
4. Enter a name and optional description.
   Rules are enabled by default. You can change this setting to delay running the rule.
5. Select the events to process.
   - Process all incidents/events (of the selected incident type).
   - Process incidents/events since the last mail notification run.
6. Select Recipients.
   [This field is required. At least one recipient must be selected.]
7. Enter a subject for the email.
   [This field is required.]
   You can insert variables from the drop-down list as required.
8. Enter the body text of the email.
   You can insert variables from the drop-down list as required.
9. (Optional) Select the checkbox to attach evidence information to the email. Click Next.
10. Click > to add criteria, < to remove them. Set the Comparison and Value parameters. When you have finished defining criteria, click Save.

The task runs hourly.

See also
Edit server tasks on page 153

Create a Set Reviewer task
You can assign reviewers for different incidents and operational events to divide the workload in large organizations.

Before you begin
In McAfee ePO User Management | Permission Sets, create a reviewer, or designate a group reviewer, with Set Reviewer permissions for DLP Incident Manager and DLP Operations.

The Set Reviewer task assigns a reviewer to incidents/events according to the rule criteria. The task only runs on incidents where a reviewer has not been assigned. You cannot use it to reassign incidents to a different reviewer.
Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Data Protection | DLP Incident Manager or Menu | Data Protection | DLP Operations.

2 Click the Incident Tasks or Operational Event Tasks tab.

3 Select an incident type from the drop-down list (Incident Tasks only), select Set Reviewer in the Task Type pane, then click Actions | New Rule.

4 Enter a name and optional description. Select a reviewer or group, then click Next.
   Rules are enabled by default. You can change this setting to delay running the rule.

5 Click > to add criteria, < to remove them. Set the Comparison and Value parameters. When you have finished defining criteria, click Save.

   Best practice: If there are multiple Set Reviewer rules, reorder the rules in the list.

The task runs hourly.

After a reviewer is set, it is not possible to override the reviewer through the Set Reviewer task.

See also
Edit server tasks on page 153

Monitor task results
Monitor the results of incident and operational event tasks.

Task
For details about product features, usage, and best practices, click ? or Help.

1 In McAfee ePO, select Menu | Automation | Server Task Log.

2 Locate the completed McAfee DLP tasks.

   Best practice: Enter DLP in the Quick find field or set a custom filter.

3 Click the name of the task.
   The details of the task appear, including any errors if the task failed.

Creating reports
McAfee DLP uses McAfee ePO reporting features. Several pre-programmed reports are available, as well as the option of designing custom reports.

See the Querying the Database topic in the McAfee ePolicy Orchestrator Product Guide for details.

Report types
Use the McAfee ePO reporting features to monitor McAfee DLP Endpoint performance.

Four types of reports are supported in McAfee ePO dashboards:
• DLP Incident summary
• DLP Endpoint discovery summary
• DLP Policy summary
• DLP Operations summary

The dashboards provide a total of 22 reports, based on the 28 queries found in the McAfee ePO console under Menu | Reporting | Queries & Reports | McAfee Groups | Data Loss Prevention.

Report options
McAfee DLP software uses McAfee ePO Reports to review events. In addition, you can view information on product properties on the McAfee ePO Dashboard.

McAfee ePO Reports
McAfee DLP Endpoint software integrates reporting with the McAfee ePO reporting service. For information on using the McAfee ePO reporting service, see the McAfee ePolicy Orchestrator Product Guide.

McAfee ePO rollup queries and rolled up reports, which summarize data from multiple McAfee ePO databases, are supported.

McAfee ePO Notifications are supported. See the Sending Notifications topic in the McAfee ePolicy Orchestrator Product Guide for details.

ePO Dashboards
You can view information on McAfee DLP product properties in the McAfee ePO Menu | Dashboards page. There are four predefined dashboards:
• DLP Incident summary
• DLP Endpoint discovery summary
• DLP Policy summary
• DLP Operations summary

Dashboards can be edited and customized, and new monitors can be created. See the McAfee ePO documentation for instructions.

The predefined queries summarized in the Dashboards are available by selecting Menu | Queries & Reports. They are listed under McAfee Groups.

Predefined dashboards
The following table describes the predefined McAfee DLP dashboards.

<table>
<thead>
<tr>
<th>Table 12-1 Predefined DLP dashboards</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>DLP: Incident Summary</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>DLP: Operations Summary</td>
</tr>
</tbody>
</table>
**Table 12-1 Predefined DLP dashboards (continued)**

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Version</strong></td>
<td>Displays the distribution of endpoints in the enterprise. Used to monitor agent deployment progress.</td>
<td></td>
</tr>
<tr>
<td><strong>Distribution of DLP products on endpoint computers</strong></td>
<td>Displays a pie chart showing the number of Windows and Mac endpoints, as well as the number of endpoints where no client is installed.</td>
<td></td>
</tr>
<tr>
<td><strong>DLP Discovery (Endpoint): Local File System Scan Status</strong></td>
<td>Displays a pie chart showing the number of local file system discovery scan properties and their states (completed, running, undefined).</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Status</strong></td>
<td>Displays all agents and their status.</td>
<td></td>
</tr>
<tr>
<td><strong>Agent Operation Mode</strong></td>
<td>Displays a pie chart of agents by DLP operation modes. Operation modes are:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device control only mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device control and full content protection mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Device control and content aware removable storage protection mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
<td></td>
</tr>
<tr>
<td><strong>DLP Discovery (Endpoint): Local Email Storage Scan Status</strong></td>
<td>Displays a pie chart showing the number of local email storage scan discovery properties and their states (completed, running, undefined).</td>
<td></td>
</tr>
<tr>
<td><strong>DLP: Policy Summary</strong></td>
<td>Displays the DLP policy distribution by version throughout the enterprise. Used to monitor progress when deploying a new policy.</td>
<td></td>
</tr>
<tr>
<td><strong>Policy distribution</strong></td>
<td>Displays a bar chart showing the rule set name and the number of policies enforced.</td>
<td></td>
</tr>
<tr>
<td><strong>Enforced Rule Sets per endpoint computers</strong></td>
<td>Displays the system name/user name and the number of user session properties.</td>
<td></td>
</tr>
<tr>
<td><strong>Bypassed Users</strong></td>
<td>Displays the undefined device classes for Windows devices.</td>
<td></td>
</tr>
<tr>
<td><strong>Undefined Device Classes (for Windows devices)</strong></td>
<td>Displays the undefined device classes for Windows devices.</td>
<td></td>
</tr>
<tr>
<td><strong>Privileged Users</strong></td>
<td>Displays the system name/user name and the number of user session properties.</td>
<td></td>
</tr>
<tr>
<td><strong>Policy revision distribution</strong></td>
<td>Similar to Policy distribution, but displays revisions – that is, updates to an existing version.</td>
<td></td>
</tr>
<tr>
<td><strong>DLP: Endpoint Discovery Summary</strong></td>
<td>Displays a pie chart showing the run status of all local file system scans.</td>
<td></td>
</tr>
<tr>
<td><strong>DLP Discovery (Endpoint): Local File System Scan Latest Status</strong></td>
<td>Displays a bar chart showing the range of sensitive files found on systems files.</td>
<td></td>
</tr>
<tr>
<td><strong>DLP Discovery (Endpoint): Local File System Scan Latest Sensitive Files</strong></td>
<td>Displays a bar chart showing the range of errors found in systems files.</td>
<td></td>
</tr>
<tr>
<td><strong>DLP Discovery (Endpoint): Local File System Scan Latest Errors</strong></td>
<td>Displays a bar chart showing the classifications applied to systems files.</td>
<td></td>
</tr>
<tr>
<td><strong>DLP Discovery (Endpoint): Local File System Scan Latest Classifications</strong></td>
<td>Displays a pie chart showing the run status of all local email folders.</td>
<td></td>
</tr>
<tr>
<td><strong>DLP Discovery (Endpoint): Local Email Scan Latest Status</strong></td>
<td>Displays a bar chart showing the range of sensitive emails found in local email folders.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 12-1 Predefined DLP dashboards (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Discovery (Endpoint): Local Email Scan Latest Errors</td>
<td>Displays a bar chart showing the range of errors found in local email folders.</td>
<td></td>
</tr>
<tr>
<td>DLP Discovery (Endpoint): Local Email Scan Latest Classifications</td>
<td>Displays a bar chart showing the classifications applied to local emails.</td>
<td></td>
</tr>
</tbody>
</table>

### Create a data rollup server task

McAfee ePO rollup tasks draw data from multiple servers to produce a single report. You can create rollup reports for McAfee DLP operational events and incidents.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In McAfee ePO, select **Menu | Automation | Server Tasks**.
2. Click **New Task**.
3. In the **Server Task Builder**, enter a name and optional note, then click **Next**.
4. From the **Actions** drop-down list, select **Roll Up Data**. The rollup data form appears.
5. (Optional) Select servers in the **Roll up data from** field.
6. From the **Data Type** drop-down list, select **DLP Incidents**, **DLP Operational Event**, or **McAfee DLP Endpoint Discovery**, as required.
7. (Optional) Configure the **Purge**, **Filter**, or **Rollup method** options. Click **Next**.
8. Enter the schedule type, start date, end date, and schedule time. Click **Next**.
9. Review the **Summary** information, then click **Save**.
Maintenance and troubleshooting

Chapter 13  McAfee DLP Endpoint Diagnostics
Use the McAfee DLP Endpoint Diagnostic Tool utility for troubleshooting and monitoring system health.

**Diagnostic Tool**

The Diagnostic Tool is designed to aid troubleshooting McAfee DLP Endpoint problems on Microsoft Windows endpoint computers. It is not supported on OS X computers.

The Diagnostic Tool gathers information on the performance of client software. The IT team uses this information to troubleshoot problems and tune policies. When severe problems exist, it can be used to collect data for analysis by the McAfee DLP development team.

The tool is distributed as a utility to install on problem computers. It consists of seven tabbed pages, each devoted to a different aspect of McAfee DLP Endpoint software operation.

| General information | Collects data such as whether the agent processes and drivers are running and general policy, agent, and logging information. Where an error is detected, information about the error is presented. |
| DLPE Modules        | Displays the agent configuration (as shown in the McAfee DLP Endpoint policy console as the Agent Configuration | Miscellaneous page). It shows the configuration setting and status of each module, add-in, and handler. Selecting a module displays details that can help you determine problems. |
| Data Flow           | Displays the number of events and the memory used by the McAfee DLP Endpoint client, and displays event details when a specific event is selected. |
| Tools               | Allows you to perform several tests and displays the results. When necessary, a data dump is performed for further analysis. |
| Process list        | Displays all processes currently running on the computer. Selecting a process displays details and related window titles and application definitions. |
| Devices             | Displays all Plug and Play and removable devices currently connected to the computer. Selecting a device displays details of the device and related device definitions. Displays all active device control rules and relevant definitions from the device definitions. |
| Active policy       | Displays all rules contained in the active policy, and the relevant policy definitions. Selecting a rule or definition displays the details. |
Checking the agent status

Use the General information tab to get an overview of the agent status. The information on the General information tab is designed to confirm expectations and answer basic questions. Are the agent processes and drivers running? What product versions are installed? What is the current operation mode and policy?

Agent processes and drivers

One of the most important questions in troubleshooting is, "Is everything running as expected?" The Agent processes and Drivers sections show this at a glance. The checkboxes show if the process is enabled; the colored dot shows if it is running. If the process or driver is down, the text box gives information on what is wrong.

The default maximum memory is 150 MB. A high value for this parameter can indicate problems.

Table 13-1  Agent processes

<table>
<thead>
<tr>
<th>Term</th>
<th>Process</th>
<th>Expected status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fcag</td>
<td>McAfee DLP Endpoint agent (client)</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Fcags</td>
<td>McAfee DLP Endpoint agent service</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Fcagte</td>
<td>McAfee DLP Endpoint text extractor</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Fcagwd</td>
<td>McAfee DLP Endpoint watch dog</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Fcagd</td>
<td>McAfee DLP Endpoint agent with automatic dump</td>
<td>enabled only for troubleshooting.</td>
</tr>
</tbody>
</table>

Table 13-2  Drivers

<table>
<thead>
<tr>
<th>Term</th>
<th>Process</th>
<th>Expected status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hdlpflt</td>
<td>McAfee DLP Endpoint minifilter driver (enforces removable storage device rules)</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Hdlpevnt</td>
<td>McAfee DLP Endpoint event</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Hdlpdbk</td>
<td>McAfee DLP Endpoint device filter driver (enforces device Plug and Play rules)</td>
<td>can be disabled in configuration</td>
</tr>
<tr>
<td>Hdlpctrl</td>
<td>McAfee DLP Endpoint control</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Hdlhook</td>
<td>McAfee DLP Endpoint Hook driver</td>
<td>enabled; running</td>
</tr>
</tbody>
</table>

Agent info section

Operation mode and Agent status are expected to match. The Agent Connectivity indication, together with EPO address, can be useful in troubleshooting.

Agent Connectivity has three options: online, offline, or connected by VPN.

Run the Diagnostic Tool

The Diagnostic Tool utility provides IT teams with detailed information on the agent status.

Before you begin
Diagnostic Tool requires authentication with McAfee Help Desk.

Task
1  Double-click the hdlpDiag.exe file.

An authentication window opens.
2 Copy the Identification Code to the Help Desk Identification Code text box on the Generate DLP Client Bypass Key page. Fill in the rest of the information and generate a Release Code.

3 Copy the Release Code to the authentication window Validation Code text box and click OK.

The diagnostic tool utility opens.

The General Information, DLPE Modules, and Process List tabs have a Refresh button in the lower right corner. Changes that occur when a tab is open do not update information automatically on these tabs. Click the Refresh button frequently to verify that you are viewing current data.

**Tuning policies**

Diagnostic Tool can be used to troubleshoot or tune policies.

**Use case: High CPU usage**

Users are sometimes plagued by slow performance when a new policy is enforced. One cause might be high CPU usage. To determine this, go to the Process List tab. If you see an unusually large number of events for a process, this could be the problem. For example, a recent check found that taskmgr.exe was classified as an Editor, and had the second highest number of total events. It is quite unlikely that this application is leaking data, and the McAfee DLP Endpoint client does not need to monitor it that closely.

To test the theory, create an application template. In the Policy Catalog, go to DLP Policy | Settings and set an override to Trusted. Apply the policy, and test to see if performance has improved.

**Use case: Creating effective content classification and content fingerprinting criteria**

Tagging sensitive data lies at the heart of a data protection policy. Diagnostic Tool displays information that helps you design effective content classification and content fingerprinting criteria. Tags can be too tight, missing data that should be tagged, or too loose, creating false positives.

The Active Policy page lists classifications and their content classification and content fingerprinting criteria. The Data Flow page lists all tags applied by the policy, and the count for each. When counts are higher than expected, false positives are suspected. In one case, an extremely high count led to the discovery that the classification was triggered by Disclaimer text. Adding the Disclaimer to the whitelist removed the false positives. By the same token, lower than expected counts suggest a classification that is too strict.

If a new file is tagged while the Diagnostic Tool is running, the file path is displayed in the details pane. Use this information to locate files for testing.
# Index

## A
- about this guide 9
- advanced patterns
  - creating 88
- agent configuration
  - Mac OS support 42
- AJAX web requests, blocking 108
- all_evidences.csv file 45
- application definitions
  - strategy 73
- application templates
  - about 77
- assignment groups
  - definition 14

## B
- backward compatibility 29
- best practices 13, 23, 27, 30, 33, 47, 57, 58, 104, 119
- Boldon James 92
- Box 103
- business justification, customizing 110

## C
- cases
  - about 148
  - adding comments 150
  - assigning incidents 149
  - audit logs 148
  - creating 148
  - deleting 151
  - labels 151
  - sending notifications 150
  - updating 150
- challenge/response 133
- Chrome, supported versions 108
- Citrix XenApp device rules 63
- classification 69
  - criteria 81
  - email 92
  - manual 78
- classification rules 13
- classification, manual 84
- classifications 81
  - about 69
- client configuration 40
  - assigning with ePolicy Orchestrator 35
  - system tree 39
- Client Service WatchDog 40
- cloud protection rules 103
- components, Data Loss Prevention (diagram) 24
- content classification
  - criteria 70
- content fingerprinting
  - criteria 70
- content fingerprinting criteria 13
- conventions and icons used in this guide 9
- conversion 30

## D
- dashboards, report options 157
- data
  - classifying 75
  - data-in-motion 72
- data rollup 159
- data-at-rest 11, 130
- data-in use 11
- data-in-motion 11
- definitions 97
  - dictionaries 75
  - document properties 76
  - file extension 76
  - network 71
  - registered documents 80
  - text pattern 76
  - web destination 72
- device classes 54
- device definitions 57
  - removable storage 59
- device GUID 55
- device rules 114
  - about 63
  - definition 14
- devices
  - lists, adding plug-and-play definitions 58
- devices properties 60
- diagnostic tool 163
Diagnostic Tool 165
dictionaries
  about 75
  creating 87
  importing entries 87
discovery
  about 130
  creating a file system discovery rule 131
  setup 132
DLP data, classifying 76
DLP Discover 130
DLP Endpoint
  checking in to McAfee ePO 31
  deploying 33
  deployment verification 34
  wake-up call 35
DLP Incident Manager 138
  responding to events 137
DLP policy 97
DLP Policy console, installing 27
DLP rules
  classification 13
  device 14
  protection 14
DLP Settings 27
document properties definitions 76
documentation
  audience for this guide 9
  product-specific, finding 10
  typographical conventions and icons 9
Dropbox 103

E
  email 71
  email addresses
    creating 89
  email classification 92
  email protection rules 104
  embedded tags 78, 79
  endpoint console 18, 19
  endpoint discovery 129
  endpoint discovery rules 114
  ePO notifications 157
  ePO reports 157
  event parser 18
  events
    monitoring 137
  evidence
    endpoint events 137
    storage for encrypted content 45
  evidence folder 47
  exceptions to rules 114

F
  file access
    rules, about 63
  file extensions
    definitions 76
  filters
    network definitions 71
    fingerprinting criteria 83

G
  GET requests 108
  Google Chrome, supported versions 108
  GoogleDrive 103
  GUID, See device GUID

H
  handlers
    cloud protection 103
  hit highlighting, events 45

I
  incident manager 138
  incident tasks 138, 153
  incidents
    details 143
    filtering 141, 142
    labels 147
    sorting 141
    updating 145
    views 141

J
  JAWS support 18

L
  location, classifying by 72

M
  manual classification 52, 84
  McAfee ServicePortal, accessing 10
  migration 30
  monitoring 138

N
  network definitions
    about 71
    address range 89
    port range 89
  notifications, ePolicy Orchestrator 157

O
  OneDrive 103
online/offline operation 18
operational event tasks 153
operational events 138
OS X support 19, 53, 57, 63–65, 69, 72, 77, 103, 106
OST files 71
permission sets 48
permission sets, defining 49
permission sets, System Tree filtering 47
placeholders 110
plug-and-play devices
  whitelisted definition, creating 58
policies 15, 39
  assigning with 35
  definition 14
  refreshing 35
policies, tuning 165
policy assignment 97
policy catalog 39
protection rules 114
  definition 14
PST files 71
quarantine
  release from 45
  restoring files or email items from 133
reactions 111
redaction 47
registered documents 13, 80
rights management 42, 44
role-based access control 49
role-based access control
  definition 47
rolled up reports 157
rule sets
  about 101
  creating 114
rule sets, adding to policies 97
rules 102 (continued)
  email protection 104
  exceptions 114
  reactions 111
server tasks 30, 153
server tasks, rollup 159
ServicePortal, finding product documentation 10
ServicePortal
  finding product documentation 10
strategy, See application definitions
Syncplicity 103
tagging 69
  about 70
technical support, finding product information 10
text extractor 72
text patterns
  about 76
timeout strategy, web post 108
Titus, integration 91
TrueCrypt device rules 63
URL lists
  creating 90
user notification, customizing 110
user self-remediation 129
user sessions 63
user-initiated scans 129
validators 76
verifying the installation 34
wake-up call 35
WatchDog service 40
web destinations
  about 72
web post protection rules 108
whitelisted text 82
whitelists 14
  plug-and-play definitions, creating 58