Product Guide
Revision A

McAfee Data Loss Prevention Endpoint
9.4.100

For use with McAfee ePolicy Orchestrator
COPYRIGHT

Copyright © 2015 McAfee, Inc., 2821 Mission College Boulevard, Santa Clara, CA 95054, 1.888.847.8766, www.intelsecurity.com

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.
Preface ............................... 7
  About this guide ............................. 7
  Audience .................................. 7
  Conventions ............................... 7
  Find product documentation ................. 8

1 Introduction to McAfee DLP Endpoint 9
  McAfee DLP Endpoint overview .............. 10
  Classify .................................. 10
  Track .................................... 11
  Protect .................................. 12
  Monitor .................................. 13
  Product modules and how they interact ....... 13
  McAfee DLP Endpoint client software ......... 15

Deployment and installation

2 Deployment options and scenarios 21
  Choosing an endpoint product option ........... 21
  Recommended installation ..................... 23
  Verify the system requirements ................. 24

3 Installing the McAfee DLP Endpoint software 27
  Install and license the McAfee DLP extension ... 27
  Check in the McAfee DLP Endpoint package to McAfee ePO 28
  Convert policies and migrate data ............... 29

4 Deploying the software 31
  Deploying McAfee DLP Endpoint clients .......... 31
    Deploy McAfee DLP Endpoint client with McAfee ePO 31
    Verify the installation ...................... 32
    Deploy policies with McAfee ePO ............... 32

Configuration and use

5 Configuring system components 37
  Policy Catalog ................................ 37
  Edit McAfee DLP server settings ............... 37
  Define a Rights Management server .......... 38
  Documenting events with evidence ............. 39
    Creating evidence folders ................... 40
    Configure evidence folders ................. 41
  Users and permission sets .................. 42
    McAfee DLP permission sets ................. 42
6 Protecting removable media

Protecting devices ........................................... 50
Device classes .................................................. 50
Define a device class ........................................ 51
Obtain a GUID .................................................. 51
Create a device class ........................................ 52
Device definitions ............................................. 53
Working with device definitions .............................. 53
Device properties .............................................. 56
Device control rules ........................................... 58
Removable storage device rules ............................. 59
Plug and Play device rules .................................. 60
Removable storage file access rules ........................ 61
Fixed hard drive rules ......................................... 61
Citrix XenApp device rules .................................. 61
TrueCrypt device rules ........................................ 61
Create device rules ............................................ 62
Create a removable storage device rule .................... 62
Create a plug and Play device rule ......................... 62
Create a removable storage file access device rule ....... 63
Create a fixed hard drive device rule ....................... 64
Create a Citrix device rule .................................. 64
Create a TrueCrypt device rule .............................. 65

7 Classifying sensitive content

The Classification module .................................... 67
Manual classification .......................................... 67
Use case: Manual classification .............................. 68
Using classifications ........................................... 69
Text extraction .................................................. 70
How McAfee DLP Endpoint categorizes applications .... 70
Classification definitions and criteria ....................... 71
Dictionary definitions .......................................... 72
Advanced pattern definitions .................................. 73
Classifying content with document properties or file information ............................................ 74
Application templates ........................................... 74
Create and configure classifications ......................... 75
Create a classification ......................................... 75
Create classification criteria ................................ 75
Create tagging criteria ....................................... 76
Assign manual classification permissions .................. 77
Registered documents .......................................... 78
Whitelisted text ................................................. 78
Upload registered documents .................................. 79
Upload files to whitelist text ................................... 79
Create classification definitions ............................. 80
Create or import a dictionary definition ..................... 80
Create an advanced pattern ................................... 81
Integrate Titus Client with third-party tags ................ 82
8 Using rules to protect sensitive content

Rule sets ..................................... 89
Create and configure rules and rule sets ........................................ 90
Reactions available for rule types ................................................. 94
Application File Access Protection rules ........................................ 97
Use case: prevent burning sensitive information to disk ....................... 97
Email protection rules .............................................................. 98
Network communication protection rules ........................................ 99
Network share protection rules .................................................... 99
Printer protection rules ............................................................. 100
Removable storage protection rules ............................................... 100
Screen capture protection rules .................................................... 101
Web post protection rules ........................................................... 102
Endpoint discovery ................................................................. 102
Protecting files with discovery rules ............................................. 103
How discovery scanning works .................................................... 103
Find content with the Endpoint Discovery crawler ............................ 104
Protecting files with rights management ......................................... 107
How McAfee DLP works with rights management ............................ 108
Supported RM servers .............................................................. 108

9 Working with policies

Using multiple policies ............................................................. 112
How definitions work ............................................................... 112
Edit a DLP policy ................................................................. 113

Monitoring and reporting

10 Monitoring and reporting events

DLP Incident Manager .............................................................. 117
How the Incident Manager works ............................................... 118
Incident types and details ........................................................ 119
View incidents ................................................................. 120
Sort and filter incidents .......................................................... 120
Configure column views .......................................................... 120
Configure incident filters ......................................................... 121
View incident details ............................................................. 122
Manage incidents ................................................................. 122
Update a single incident ......................................................... 123
Update multiple incidents ....................................................... 123
Manage labels ................................................................. 124
Delete incidents ................................................................. 124
Working with cases ............................................................. 125
Manage cases ................................................................. 125

11 Collecting and managing data

Edit server tasks ................................................................. 129
Create a Purge events task ....................................................... 130
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.

*Book title, term, emphasis*  
Title of a book, chapter, or topic; a new term; emphasis.

**Bold**  
Text that is strongly emphasized.

*User input, code, message*  
Commands and other text that the user types; a code sample; a displayed message.

*Interface text*  
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:* Additional information, like an alternate method of accessing an option.

*Tip:* Suggestions and recommendations.

*Important/Caution:* Valuable 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

After a product is released, information about the product is entered into the McAfee online Knowledge Center.

**Task**

1. Go to the Knowledge Center tab of the McAfee ServicePortal at [http://support.mcafee.com](http://support.mcafee.com).

2. In the Knowledge Base pane, click a content source:
   - **Product Documentation** to find user documentation
   - **Technical Articles** to find KnowledgeBase articles

3. Select Do not clear my filters.

4. Enter a product, select a 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>
<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) 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 overview
- Product modules and how they interact
- McAfee DLP Endpoint client software
McAfee DLP Endpoint overview

McAfee DLP Endpoint is a content-based agent solution that inspects enterprise users’ actions concerning sensitive content in their own work environment, their computers.

McAfee DLP safeguards sensitive enterprise information by deploying policies consisting of definitions, classifications, rule sets, and endpoint client configurations. It then monitors the policies and blocks defined actions containing sensitive content, as required. Alternately, it can encrypt sensitive content before allowing the action to proceed. Finally, the McAfee DLP software creates reports for review and control of the process, and can store sensitive content as evidence.

Figure 1-1  The McAfee DLP protection process

The McAfee DLP Endpoint client is responsible for the classify, track, and protect aspects of the process. The McAfee DLP extension in McAfee ePO is responsible for configuring the classification conditions, tracking criteria, and protection rules that apply to data copied, sent, printed, or transmitted from the managed endpoint system. The McAfee DLP extension together with the McAfee ePO user interface are responsible for the monitor aspects of the process.

Classify

To protect sensitive content, the McAfee DLP administrator starts by defining and classifying what is to be protected.

Content is classified by defining classifications and classification criteria. Classification criteria define the conditions to classify data by its true file type, advanced patterns (regular expressions combined with validation algorithms), dictionaries, keywords, proximity between text patterns and keywords and file properties such as author or title.
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.

Third-party classification software is not supported in McAfee Device Control.

Every rule specifies at least one classification to apply. This is done by parsing content and matching it against the definitions in the classification or tagging criteria.

**Track**

McAfee DLP can classify 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. To minimize the number of signatures and the performance implications of this technique, we recommend only using it to track the most sensitive documents.

- **Tagging**

  Tagging is a content tracking technique unique to the McAfee DLP Endpoint product. The administrator creates a set of tagging criteria that define the file location and the classification tag to place on files from that location. McAfee DLP Endpoint client tracks any file that is opened from the locations defined in the tagging criteria and creates 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.

  Tagging criteria can be defined by location (UNC path or URL) or the application used to access the file.
Support for persistent tag information

Tags are stored in a file's extended file attributes (EA) or alternate data streams (ADS). Whenever 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 tagged 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 tag as the original document.

For file systems that do not support EA or ADS, McAfee DLP Endpoint software stores tag 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.

Tags and tagging criteria are not supported in McAfee Device Control.

Protect

Protection is defined in Rule Sets in the DLP Policy Manager. Each rule set can contain multiple Data Protection, Device Control, and Discovery rules. Multiple parameters and Boolean AND, OR, NOT logic allow for rule exceptions and filtering.

A rule set does not need to contain all three types of rules. One rule of one type is enough to define a rule set.

Data Protection rules

Data protection rules prevent unauthorized distribution of classified data. When a user attempts to copy or attach classified data, McAfee DLP Endpoint intercepts the attempt and uses the data protection rules to determine what action to take. Actions include allow (No Action), Block, or Request Justification. In this case, McAfee DLP Endpoint halts the attempt and displays a dialog to the end user. The user inputs the justification for the attempt, and processing continues.

In McAfee Device Control, only removable storage data protection rules are available. For OS X endpoint computers, no data protection rules are available in this release.

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.

Endpoint Discovery rules

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. They can also define whether the classified file or email is reported as an event to the DLP Incident Manager, and whether to store the file or email as evidence for the event.

Discovery rules are not supported in McAfee Device Control.

File system scans are not supported on server operating systems.
Policies and policy deployment

Protection is applied by assigning rule sets to a DLP Policy in the McAfee ePO Policy Catalog. In addition to rule sets, policies contain policy assignment information and definitions. Policies are deployed by McAfee ePO software to the enterprise’s managed computers (computers with McAfee® Agent installed).

Monitor

When the application of a rule blocks, monitors, or causes some other action, an event is generated, sent to the McAfee ePO Event Parser, and stored in a database. The event can also contain evidence of the rule violation. In addition, administrative events are generated by system events such as policy deployment or discovery scans. The events generated by McAfee DLP Endpoint are monitored in DLP Incident Manager, and can be used to create reports and charts which can be displayed in McAfee ePO dashboards. The policy monitor function includes:

- **Incident monitoring** — The DLP Incident Manager page in McAfee ePO allows administrators to view agent events and evidence as they are received.
- **Administrative event monitoring** — The DLP Operational Events page in McAfee ePO allows administrators to view administrative events.
- **Evidence collection** — If protection rules are defined to collect evidence, a copy of the tagged data is saved and linked to the specific event. 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 event. Highlighted evidence is stored as a separate encrypted HTML file.

In addition, event trends can be displayed 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 Endpoint version 9.4 has a reorganized workflow with increased granularity.

Classifications

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

Classifications are required for configuring data protection and endpoint discovery rules.

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.
**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**

**Incident Manager and Operational Events**

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

**Case Management**

The Case Management module allows administrators to collaborate toward 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.

**Policy Catalog**

The McAfee ePO Policy Catalog stores the policies that are deployed to the endpoint computers. To view or edit the McAfee DLP policies, select **Policy Catalog | Product | Data Loss Prevention 9.4**.

McAfee DLP Endpoint policies have three components:

- DLP Policy — Contains Rule Sets, Endpoint Discovery scans, and Settings for privileged users, application strategy, and device class overrides
- Client Configuration — Contains information for the end-user computer

**Table 1-2 Client configuration**

<table>
<thead>
<tr>
<th>Setting</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced configuration</td>
<td>Endpoint and access protection settings</td>
</tr>
<tr>
<td>Application File Access Protection</td>
<td>Used to add whitelisted processes</td>
</tr>
<tr>
<td>Clipboard Protection</td>
<td>Enables the Microsoft Office clipboard; used to add whitelisted processes</td>
</tr>
<tr>
<td>Content Tracking</td>
<td>Text extractor settings</td>
</tr>
<tr>
<td>Corporate connectivity</td>
<td>Used to configure VPN servers for data protection options</td>
</tr>
<tr>
<td>Debugging and Logging</td>
<td>Set up logging and memory dumps for troubleshooting</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>Sets operation mode for Device Control or McAfee DLP Endpoint; activates add-ins and handlers</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>

**McAfee DLP Endpoint client software**

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.
McAfee DLP Endpoint on the OS X platform

McAfee Device Control client for OS X prevents unauthorized use of removable media devices, the most widespread, and costly source of data loss in many companies today, on Macintosh computers.

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.

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.

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.
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.

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.

On OS X 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 History page displays recent McAfee software events. Click an entry to view the details.

![OS X endpoint display](image)

**Figure 1-3 OS X endpoint display**

To activate the agent bypass screen, select Preferences from the menulet.
Introduction to McAfee DLP Endpoint
McAfee DLP Endpoint client software
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  Installing the McAfee DLP Endpoint software
Chapter 4  Deploying the software
Classifying corporate information into different data loss prevention categories is a key step in deploying and administering McAfee Data Loss Prevention Endpoint software. While guidelines and best practices exist, the ideal schema is dependent 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 will be met.

Because it might be difficult to determine in advance exactly what your unique needs are, we recommend initial deployment to a sample group of 15 to 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 should be tested on a larger test group (or, for very large companies, on a series of successively larger groups) before being deployed to the entire enterprise.

McAfee DLP Endpoint policy design and monitoring software is installed in McAfee ePO. In a simple installation, a single 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.

Currently, a version of Device Control is available for OS X computers.

Contents

- Choosing an endpoint product option
- Recommended installation
- Verify the system requirements

Choosing an endpoint product option

McAfee offers several McAfee ePO-based Data Loss Prevention options. The products use the same installed software, and are differentiated by licensing.

Understanding McAfee DLP options

McAfee DLP software is available in two Device Control configurations, full McAfee DLP Endpoint, and McAfee Data Loss Prevention Discover (McAfee DLP Discover).

- McAfee Device Control for Small to Medium Businesses — Provides Device Control only
- McAfee Device Control for Enterprise — Provides removable storage protection rules (content-sensitive rules) in addition to Device Control
• Data Protection and Device — Full McAfee DLP Endpoint, including endpoint discovery
• McAfee DLP Discover — Provides network discovery crawling, and can be installed alone or together with either Device Control or McAfee DLP Endpoint

The current release supports OS X only with the Device Control options.

What is McAfee Device Control?
Device Control software prevents unauthorized use of removable media devices, the most widespread, and costly source of data loss in many companies today.

Device Control software provides:
• **Persistent data protection for devices** — Controls what data can be copied to removable devices, filtering by user, file extension, or file name; controls the devices themselves, blocking them completely or making them read-only. Blocks applications run from removable drives
• **Protection on the go** — For USB drives, iPods, Bluetooth devices, CDs, DVDs, and other removable media, and for non-system hard disks

Device Control for OS X in the current release is limited to removable storage device rules.

What is McAfee Device Control with content-sensitive rules?
Device Control with content-sensitive rules provides:

**Persistent content-aware data protection for devices** — Adds control by content of data copied to devices, using advanced patterns, dictionaries, document properties, or file information

What is full McAfee DLP Endpoint?
McAfee DLP Endpoint software provides:
• **Universal protection** — Protects against data loss through the broadest set of data-loss channels: removable devices, non-system hard disks, email or email attachments, web posts, clipboard and screen capture, printing, file system, and more
• **Persistent content-aware data protection** — Protects against data loss regardless of the format in which data is stored or manipulated. Enforces data loss policies without disrupting legitimate user activities
• **Protection on the go** — Prevents transmission of sensitive data from desktops and laptops, whether they are connected to the enterprise network or used outside the network
**Recommended installation**

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 Operational Events 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
Verify the system requirements

The following hardware is recommended for running McAfee DLP Endpoint software for Windows and Mac.

### Table 2-1 Hardware requirements

<table>
<thead>
<tr>
<th>Hardware type</th>
<th>Specifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>• RAM — 1 GB minimum (2 GB recommended)</td>
</tr>
<tr>
<td></td>
<td>• Hard disk — 80 GB minimum</td>
</tr>
<tr>
<td>Endpoint computers</td>
<td>• RAM — 1 GB minimum (2 GB recommended)</td>
</tr>
<tr>
<td></td>
<td>• Hard disk — 300 MB minimum free disk space (500 MB recommended)</td>
</tr>
<tr>
<td>Network</td>
<td>100 megabit LAN serving all workstations and the McAfee ePO server</td>
</tr>
</tbody>
</table>

The following operating systems are supported.

### Table 2-2 Operating systems supported

<table>
<thead>
<tr>
<th>Computer type</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Endpoint computers</strong></td>
<td>Microsoft Windows operating systems</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 SP1 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 8 or 8.1 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 10 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 SP2 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 SP2 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 SP2 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 SP2 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 SP2 32-bit or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 64-bit</td>
</tr>
</tbody>
</table>

File System Discovery Rules and Network Communication Protection Rules are not supported on servers.

Apple OS X operating systems (Device Control only)

• OS X Mountain Lion 10.8.0 or later
• OS X Mavericks 10.9.0 or later
• OS X Yosemite 10.10.0 or later

OS X Yosemite 10.10 requires McAfee Agent 4.8 Patch 2 or later, or McAfee Agent 5.0 or later.

OS X El Capitan 10.11 requires McAfee Agent 4.8.0.1938 (Patch3) only. See the McAfee Data Loss Prevention Endpoint 9.4.100 Release Notes for important installation information.

The user installing McAfee DLP Endpoint software on the servers must be a member of the local administrators group.

The following virtual operating systems are supported.
Table 2-3  Virtual operating systems supported

<table>
<thead>
<tr>
<th>System type</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>VDI systems</td>
<td>• Citrix XenDesktop 5.5, 5.6, 7.0, and 7.5</td>
</tr>
<tr>
<td></td>
<td>• VMware View 5.3, 6.0, and 6.2</td>
</tr>
<tr>
<td>Remote desktops</td>
<td>• Citrix XenApp 6.0, 6.5 Feature Pack 2, and 7.6</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Remote Desktop</td>
</tr>
</tbody>
</table>

The following software is required on the server running the McAfee DLP Endpoint policy console.

Table 2-4  Server software requirements

<table>
<thead>
<tr>
<th>Software</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO</td>
<td>• 4.6.9 or later</td>
</tr>
<tr>
<td></td>
<td>• 5.1.1 or later</td>
</tr>
<tr>
<td></td>
<td>• 5.3</td>
</tr>
<tr>
<td></td>
<td>![Info icon] When running McAfee ePO in Microsoft Internet Explorer, use version 10.0 or later.</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>• 4.8.2 or later</td>
</tr>
<tr>
<td></td>
<td>• 5.0 or later</td>
</tr>
<tr>
<td>McAfee Agent for Mac</td>
<td>4.6 Patch 3 or later</td>
</tr>
<tr>
<td></td>
<td>• 4.8 Patch 2 or later</td>
</tr>
<tr>
<td></td>
<td>• 5.0 or later</td>
</tr>
<tr>
<td></td>
<td>![Info icon] OS X Yosemite 10.10 requires McAfee Agent 4.8 Patch 2 or later, or McAfee Agent 5.0 or later; OS X El Capitan 10.11 requires McAfee Agent 4.8.0.1938 (Patch3) only.</td>
</tr>
</tbody>
</table>

The McAfee DLP Endpoint package DLP_Mgmt_9_4_Package.zip includes the extensions installed through McAfee ePO.

The McAfee DLP Endpoint client (McAfee Agent plug-in) includes the files for distributing the client software to endpoint computers from the McAfee ePO repository: HDLP_Agent_9_4_0_x.zip for Microsoft Windows, DLPAgentInstaller.zip for Mac OS X.
Installing the McAfee DLP Endpoint 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
- Check in the McAfee DLP Endpoint package to McAfee ePO
- Convert policies and migrate data

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.

Task
For option definitions, click ? in the interface.

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. License options are:
   - McAfee Device Control
   - McAfee DLP Endpoint (Includes McAfee Device Control)
• McAfee DLP Discover
• McAfee Device Control plus McAfee DLP Discover
• McAfee DLP Endpoint plus McAfee DLP Discover

a Select Menu | Data Protection.

b Select either DLP Policy Manager or McAfee DLP Discover and click Yes when prompted to enter the license.

The Server Settings | Data Loss Prevention page opens.

c In the Key field, enter the license, then click Add.

d If necessary, add another license.

5 In the Default Evidence Storage field, enter the path.
  The evidence storage path must be a network path, that is \\[server]\[localpath]. This step is required to save the settings and activate the software.

6 Click Save.

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

See also
Creating evidence folders on page 40
Edit McAfee DLP server settings on page 37
Configure evidence folders on page 41

Check in the McAfee DLP Endpoint package to McAfee ePO

Any enterprise computer with data protected by McAfee software must have the McAfee Agent installed, making it a managed computer. To add data loss protection, you must also deploy the McAfee DLP Endpoint plug-in for McAfee Agent. The installation can be performed using the McAfee ePO infrastructure.

Task
For option definitions, click ? in the interface.

1 In McAfee ePO, select Menu | Software | Master Repository.

2 In the Master Repository, select Check In Package.

3 Select package type Product or Update (.ZIP). Click Browse.
   • For Microsoft Windows client, browse to ...\HDLP_Agent_9_4_0_xxx.zip
   • For Mac OS X client, browse to ...\DLPAgentInstaller

4 Click Next.

5 Review the details on the Check in Package page, then click Save.

   The package is added to the Master Repository.
Convert policies and migrate data

McAfee DLP Endpoint version 9.4 uses new schemas that are incompatible with McAfee DLP Endpoint version 9.3 policies and event formats. Use McAfee ePO server tasks to migrate policies and data to the new schema.

**Before you begin**

Update to McAfee DLP Endpoint 9.3 Patch 5 (9.3.500) or later before converting policies or migrating data to McAfee DLP Endpoint 9.4.100.

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

Run the DLP policy conversion task after installing the McAfee DLP 9.4.100 extension in McAfee ePO. We recommend scheduling the migration tasks for weekends or other non-work hours due to the load they place on the processor.

**Task**

For option definitions, click ? in the interface.

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 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 can be 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. We recommend selecting **Schedule type** | **Hourly**. Set the start date and end date to define a time period over off or non-peak hours, and schedule the task for every hour.

   Incidents are migrated in chunks of 200,000. Schedule repeating the task according to the size of incident database you need to migrate.

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

**See also**

*Edit server tasks on page 129*
Installing the McAfee DLP Endpoint software
Convert policies and migrate data
4 Deploying the software

In order to apply policies and run scans, you must first deploy the software to the endpoint computers and servers.

We recommend using McAfee ePO for deployment, though manual deployment is possible when McAfee ePO deployment is not possible for some reason.

Deploying McAfee DLP Endpoint clients

McAfee DLP Endpoint 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.

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:

- For Microsoft Windows endpoint computers, install McAfee Agent 4.8 Patch 3 or 5.0.2.
- For Mac OS X endpoint computers, install McAfee Agent for Mac 4.6 Patch 3 or later. For OS X 10.10, McAfee Agent 4.8 Patch 2 or later is required or 5.0. For OS X 10.11, install McAfee Agent 4.8.0 Patch 3.

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

Task

For option definitions, click ? in the interface.

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.
Deploying McAfee DLP Endpoint clients

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 Operational Events console.

Task

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

   Figure 4-1 DLP Operational Events details pane

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.

**Tasks**

- **Assign a policy or client configuration on page 33**
  Policies applied to McAfee ePO must be assigned and deployed to managed computers in order to be used.

- **Refresh the policy on page 33**
  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.

**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 option definitions, click ? in the interface.

1. In McAfee ePO, select Menu | System Tree.
2. Locate the directory containing the computers that will be assigned a policy, and select them.
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.
7. The Category column displays two policies: DLP Policy and Client Configuration.
   a. Click Edit Assignment in the Actions column for one of the categories.
   b. Click the Break inheritance... option, then select the policy to assign from the drop-down list. 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 option definitions, click ? in the interface.

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  Using rules to protect sensitive content
Chapter 9  Working with policies
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.

In addition to settings in the McAfee DLP modules, configuration settings that affect the administration of McAfee DLP are found in McAfee ePO Server Settings, Registered Servers, and Server Tasks.

Contents
- Policy Catalog
- Edit McAfee DLP server settings
- Define a Rights Management server
- Documenting events with evidence
- Users and permission sets
- Configuring McAfee DLP in the Policy Catalog

Policy Catalog

The McAfee ePO Policy Catalog displays the following McAfee DLP policy configurations:

- **Client Configuration** — Contains the configuration settings for the McAfee DLP Endpoint clients. The settings determine how clients apply McAfee DLP policies on the endpoint computers.
- **DLP Policy** — Contains the Rule Sets assigned to the policy, scheduled Endpoint Discovery scans, and Settings for application strategy, device class overrides, and privileged users.

McAfee DLP Endpoint 9.4 supports multiple policies and multiple client configurations. You create policies and client configurations in the Policy Catalog by duplicating existing items and editing them. Assign rule sets to policies and apply them to the McAfee ePO database on the Policy Assignment tab of the DLP Policy Manager. Assign policies and client configurations for deployment to the endpoint computers in the McAfee ePO System Tree.

Edit McAfee DLP server settings

McAfee DLP Endpoint inserts default configuration settings in McAfee ePO server settings. These settings can be edited as required.
Task
For option definitions, click ? in the interface.

1. In McAfee ePO, select Menu | Configuration | Server Settings | Data Loss Prevention.
2. Click Edit.
3. You can edit the following parameters.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>License Key</td>
<td>Determines the installed version: McAfee Device Control or full McAfee DLP Endpoint. You can also add a license for McAfee DLP Discover to either.</td>
</tr>
<tr>
<td>Default Evidence Storage</td>
<td>UNC path to the storage share. The path must be a network share, that is, it must include the server name.</td>
</tr>
<tr>
<td>Shared Password</td>
<td>Override password for uninstalling the software, removing files from quarantine, encrypting evidence, and temporary client bypass.</td>
</tr>
<tr>
<td>Challenge-Response key length</td>
<td>Used by Help Desk for releasing quarantined files or setting client bypass mode.</td>
</tr>
<tr>
<td>Enforce system tree permissions</td>
<td>System Tree permissions can be used to filter incidents in the DLP Incident Manager and DLP Operational Events consoles. Use this setting to Use or Ignore System Tree permissions.</td>
</tr>
<tr>
<td>Case Management</td>
<td>Select the email notification options: send to case owner, send to case submitter, or both.</td>
</tr>
<tr>
<td>Last Backup</td>
<td>Displays the last backup, and allows you to save the current settings to a file.</td>
</tr>
<tr>
<td>Last Restore</td>
<td>Displays the last restored version, and allows you to restore saved settings from a file.</td>
</tr>
</tbody>
</table>

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 option definitions, click ? in the interface.

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.

Some 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 Endpoint passes information to the server, the folder is purged and the evidence is stored in the server evidence folder. Settings in Policy Catalog | Client Configuration | Evidence Copy Service | Evidence Copy Service are used to control 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 Endpoint. 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. See Create and configure repository folders in this guide for details about setting up the folder and setting access permissions (also known as Evidence Network Share). Specify the path in the Policy Catalog on the Evidence Copy Service page of the client configuration policy.

- **Evidence copy service** — The evidence copy service is enabled on the Operational Mode and Modules page of the client configuration policy. It is a subentry under Reporting Service, which must also be enabled for evidence collection.

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 Operational Events pages. To handle different evidence requirements, McAfee DLP Endpoint 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 a large number of evidence files are linked to a single 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 file containing extracted text. For tags and content categories, the text consists of a highlighted word or phrase and 100 characters before and after (for context) organized by the tag or content category that triggered the event, and including a count of the number of events per tag/content category. For secured text patterns and dictionaries, the exact text is extracted. Regex and exact match keywords display up to 100 hits per expression; dictionaries can display a maximum of 250 hits per dictionary entry. 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) — Displays 1500 characters (5–7 hits) per section.

• Create all matches — Displays all hits, with limitations as described previously.

• Disabled — Disables the hit highlighting feature.

**Rules allowing evidence storage**

These rules have the option of storing evidence.

**Table 5-1 Evidence saved by rules**

<table>
<thead>
<tr>
<th>Rule</th>
<th>What is saved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application File Access Protection Rule</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Clipboard Protection Rule</td>
<td>Copy of the clipboard</td>
</tr>
<tr>
<td>Cloud Protection Rule</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Email Protection Rule</td>
<td>Copy of the email</td>
</tr>
<tr>
<td>Network Share Protection Rule</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Printer Protection Rule</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Removable Storage Protection Rule</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Screen Capture Protection Rule</td>
<td>JPEG of the screen</td>
</tr>
<tr>
<td>Web Post Protection Rule</td>
<td>Copy of the web post</td>
</tr>
<tr>
<td>File System Discovery Rule</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Email Storage Discovery Rule</td>
<td>Copy of the .msg file</td>
</tr>
</tbody>
</table>

**Creating evidence folders**

Evidence folders contain information used by the McAfee DLP software 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.

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.

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

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

Configuring system components
Documenting events with evidence

Configure evidence folders
Configuration of evidence folders requires specific security settings.

Before you begin
Create the evidence folder.

Task
1. In Windows Explorer, right-click the evidence folder and select Properties.
2. Click the Sharing tab, then click Advanced sharing. Select the Share this folder option.
   a. Modify Share name to evidence$. Click OK.
   i. The $ ensures that the share is hidden.
   b. Click Permissions and select Full Control for Everyone. Click OK twice.
3. Click the Security tab, then click Advanced.
   a. In the Permissions tab, click Change Permissions then deselect the Include inheritable permissions from the object’s parent option.
      A confirmation message explains the effect this change will have on the folder.
   b. Click Remove.
      The Permissions tab in the Advanced Security Settings window shows all permissions eliminated.
   c. Click Add to select an object type.
   d. In the Enter the object name to select field, type Domain Computers, then click OK.
      The Permission Entry dialog box is displayed.
   e. In the Allow column, select Create Files/Write Data and Create Folders/Append Data.
      Verify that the Apply onto option says This folder, subfolders and files, then click OK.
      The Advanced Security Settings window now includes Domain Computers.
Click Add again to select an object type.

In the Enter the object name to select field, type Administrators, then click OK to display the Permission Entry dialog box. Set the required permissions.

Adding administrators is optional, but can be added as a security precaution. Alternately, you can add permissions only for those administrators who deploy policies.

4 Click OK twice to close the dialog box.

Users and permission sets

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

We recommend creating specific McAfee DLP users or groups, and administrator and reviewer permissions in McAfee ePO. You can create different roles by assigning users different permissions for McAfee DLP Endpoint and the DLP Incident Manager.

System Tree filtering permissions support

McAfee DLP Endpoint supports McAfee ePO System Tree filtering permissions in the DLP Incident Manager and DLP Operational Events. When System Tree filtering is enabled, McAfee ePO operators can only see incidents from computers in their permitted System Tree portion. 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 Operational Events. System Tree filtering is disabled by default, but can be enabled in Menu | Server Settings | Data Loss Prevention.

Customers who have been using Group Administrators in Data Loss Prevention permission sets are advised to give Group Administrators View “System Tree” tab permission (under Systems) and 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 Operational Events consoles containing confidential information can be redacted to prevent unauthorized viewing, and 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.

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 9.4. If a previous version of McAfee DLP is installed on the same McAfee ePO server, the Data Loss Prevention permission set also appears.
Permissions in the Data Loss Prevention 9.4 permission set cover all sections of the management console, not just the Incident Manager. 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. The permissions groups are:

- **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.

Create a McAfee DLP permission set

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

For option definitions, click ? in the interface.

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

2. Select a predefined permission set or click **New** to create a permission set.
   - Type a name for the set and select users.
   - Click **Save**.

3. Select a permission set, then click **Edit** in the **Data Loss Prevention 9.4** section.
   - 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.
   - 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 submodules in the Policy Catalog group.
   - Click **Save**.

**Use case: DLP administrator permissions**

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

**Task**

For option definitions, click ? in the interface.

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

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

3. In the **Data Loss Prevention 9.4** 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 Operational Events 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 option definitions, click ? in the interface.

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 9.4 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 9.4 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, however, is optional according to your specific requirements.

e Click Save.

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:

- Client configuration
- DLP Policy

The Client Configuration policy contains settings that determine how the endpoint computers work with policies.

The DLP Policy consists of Rule Sets, the Endpoint Discovery configuration, and Settings.

Import or export the McAfee DLP Endpoint configuration

Policy configurations can be saved in HTML format for backup or to transfer policies to other McAfee ePO servers. Importing and exporting policies is performed from the McAfee ePO Policy Catalog.

Task

For option definitions, click ? in the interface.

1 In McAfee ePO, select Policy Catalog | Product | Data Loss Prevention 9.4.

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 endpoint configuration and endpoint 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.

OS X support for client configuration parameters

Client configuration settings can apply to both Microsoft Windows and OS X endpoint computers. The McAfee DLP Endpoint client software on OS X ignores parameters that are not specifically supported on that operating system.

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 OS X and Microsoft Windows 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>• Policy Change</td>
</tr>
<tr>
<td></td>
<td>• Release Code Locked</td>
</tr>
<tr>
<td>Logging</td>
<td>All other settings apply to Microsoft Windows endpoints only.</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>Microsoft Windows only</td>
</tr>
<tr>
<td></td>
<td>Enable end-user notification popup</td>
<td>OS X and Microsoft Windows</td>
</tr>
<tr>
<td></td>
<td>Show request justification dialog</td>
<td>Microsoft Windows only</td>
</tr>
<tr>
<td>Challenge and Response</td>
<td>All options</td>
<td>OS X and Microsoft Windows</td>
</tr>
<tr>
<td>Release code lockout policy</td>
<td>All options</td>
<td>OS X and Microsoft Windows</td>
</tr>
<tr>
<td>Client Banner Image</td>
<td>All options</td>
<td>Microsoft Windows only</td>
</tr>
</tbody>
</table>

Client configuration settings

Client configuration settings determine how the endpoint software operates.

We recommend reviewing the client configuration settings when configuring the software to verify that they meet your requirements. Most of the settings have reasonable defaults that can be used for initial setup and testing without alteration. The following table lists some of the more important settings to verify.

Table 5-4 Endpoint configuration

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Configuration</td>
<td>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. There is a recovery mechanism 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>
</tbody>
</table>
### Table 5-4  Endpoint configuration (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Corporate connectivity</td>
<td>Server address</td>
<td>You can apply different prevent actions to endpoint computers in the corporate network, outside the network, or connected by VPN. To use the VPN option, set the server IP address.</td>
</tr>
<tr>
<td>Evidence Copy Service</td>
<td>Evidence Storage</td>
<td>Replace the example text with the evidence storage share.</td>
</tr>
<tr>
<td></td>
<td>UNC share</td>
<td></td>
</tr>
<tr>
<td>Operational Mode and</td>
<td></td>
<td>To improve performance, we recommend that you deselect modules you are not using.</td>
</tr>
<tr>
<td>Modules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Post Protection</td>
<td>Supported Chrome</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>
</tr>
<tr>
<td></td>
<td>version</td>
<td></td>
</tr>
</tbody>
</table>
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.

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, Mac</td>
<td>A list of device properties used to identify or group devices.</td>
</tr>
<tr>
<td>Device property</td>
<td>Windows, Mac</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, Mac</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, Mac</td>
<td>Used to block or monitor a device, or set it as read-only. See Device rule.</td>
</tr>
<tr>
<td>Removable storage protection rule</td>
<td>Windows</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>

Contents

- Protecting devices
USB drives are the smallest, easiest, cheapest, and least-traceable 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 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.

**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.

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 52

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 option definitions, click ? in the interface.

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 pre-defined list or is not created automatically when new hardware is installed.

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

Task
For option definitions, click ? in the interface.

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
Device classes on page 50
Device definitions on page 53
**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.
- **Removable storage devices** are external devices containing a file system that appear on the managed computer as drives. Removable storage device definitions support either Windows or 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.

Removable storage device definitions are more flexible and include additional properties related to the removable storage devices. McAfee recommends using 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 52

**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

Tasks

- Create a device definition on page 54
  Device definitions specify the properties of a device to trigger the rule.
- Create a whitelisted plug and play definition on page 54
  The purpose of whitelisted plug and play devices is to deal with those devices that do not handle device management well, and might cause the system to stop responding or cause other serious problems. We recommend adding such devices to the whitelisted device list to avoid compatibility problems.
- Create a removable storage device definition on page 55
  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.

Create a device definition

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

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 option definitions, click ? in the interface.

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 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 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, and might cause the system to stop responding or cause other serious
problems. We recommend adding such devices to the whitelisted device list to avoid compatibility
problems.
Whitelisted plug and play devices are added automatically to the excluded list in all plug and play
device rules when the policy is applied. They are never managed, even if their parent device class is
managed.

**Task**
For option definitions, click ? in the interface.

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 option definitions, click ? in the interface.

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**.
## 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, PCMCIA, SCSI, USB • Mac OS X — Firewire (IEEE1394), IDE/SATA, SD, Thunderbolt, USB</td>
<td>Selects the device BUS type from the available list.</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>
</tbody>
</table>
| Device Instance ID (Microsoft Windows XP) | All          | Windows                       | A Windows-generated string that uniquely identifies the device in the system.  

Example:  

USB\VID_0930&PID_6533\5&26450FC&0&6.  

| Device Instance Path (Windows Vista and later Microsoft Windows operating systems, including servers) | All               | Windows                       |  
| Device Name                            | All               | • Windows • Mac OS X          | The name attached to a hardware device, representing its physical address. |
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>
<tbody>
<tr>
<td>File System Type</td>
<td></td>
<td></td>
<td>The type of file system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- For hard disks, select one of exFAT, FAT16, FAT32, or NTFS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- For removable storage devices, any of the above plus CDFS or UDFS.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows — CDFS, exFAT, FAT16,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FAT32, NTFS, UDFS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mac OS X — CDFS, exFAT, FAT16,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FAT32, HFS/HFS+, NTFS, UDFS</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mac OS X supports FAT only on</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>disks other than the boot disk.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mac OS X supports NTFS as read-only.</td>
<td></td>
</tr>
<tr>
<td>File System Access</td>
<td>Removable storage</td>
<td>• Windows</td>
<td>The access to the file system: read only or read-write.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mac OS X</td>
<td></td>
</tr>
<tr>
<td>File System Volume Label</td>
<td>Fixed hard disk</td>
<td>• Windows</td>
<td>The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Mac OS X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Removable storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File System Volume Serial Number</td>
<td>Fixed hard disk</td>
<td>Windows</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Removable storage</td>
<td></td>
</tr>
<tr>
<td>PCI VendorID / DeviceID</td>
<td>All</td>
<td>Windows</td>
<td>The PCI VendorID and DeviceID are embedded in the PCI device. These parameters can be obtained from the Hardware ID string of physical devices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PCI\VEN_8086&amp;DEV_2580&amp;SUBSYS_00000000 &amp;REV_04</td>
</tr>
<tr>
<td></td>
<td>Removable storage</td>
<td>Windows</td>
<td>Select to specify a TrueCrypt device.</td>
</tr>
<tr>
<td>USB Class Code</td>
<td>Plug and play</td>
<td>Windows</td>
<td>Identifies a physical USB device by its general function. Select the class code from the available list.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### 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\000000000002CD8  
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. |
| 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 |

### Device control rules

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

Of the six types of device control rules, only removable storage device rules are supported on OS X in this release.

- **Removable Storage Device Rule** (Microsoft Windows, OS X) — Used to block or monitor removable storage devices, or set as read-only. The user can be notified of the action taken.

- **Plug and Play Device Rule** (Microsoft Windows only) — Used to block or monitor Plug and Play devices. The user can be notified of the action taken.

- **Removable Storage File Access Rule** (Microsoft Windows only) — Used to block executables on plug-in devices from running.

- **Fixed Hard Drive Rule** (Microsoft Windows only) — 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.

- **Citrix XenApp Device Rule** (Microsoft Windows only) — Used to block Citrix devices mapped to shared desktop sessions.

- **TrueCrypt Device Rule** (Microsoft Windows only) — 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.
Removable storage device rules
Removable storage device rules are used to block or monitor removable storage devices, or set as read-only. You can notify the user of the action taken.

Removable storage device rules are supported on both Microsoft Windows and OS X computers. They 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.

Use case: Removable storage device rule with a whitelisted process
You can whitelist a process as an exception to a removable storage blocking rule.

Removable storage device rules are used to block applications from acting on the device. However, the rule allows one whitelisted process. In this example, we block Sandisk removable storage devices, but allow anti-virus software to scan the device to remove infected files.

This feature is supported only for Windows-based computers.

Task
For option definitions, click ? in the interface.

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

2. On the Definitions tab, locate the built-in device definition for Sandisk removable devices (Windows) and click Duplicate.

   We recommend duplicating the built-in definitions to allow customization. They can, however, be used as-is in simple examples. The definition uses the Sandisk vendor ID 0781. You can add other vendor IDs to add other brands of removable devices to the definition.

3. On the Rule Sets tab, select or create a rule set.


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. In the Process Name field, add the built-in McAfee AV definition.

   As with the removable storage device definition, you can duplicate this definition and customize it.

7. On the Reaction tab, select Prevent Action | Block. You can optionally add a user notification and select the Report Incident option.

8. 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 option definitions, click ? in the interface.

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. You can start by duplicating one of the built-in definitions for Windows or Mac and customizing it. The **Bus Type** can include USB, Bluetooth, and any other bus type you expect to be used. You can 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**.

**Plug and Play device rules**
Plug and Play device rules are used to block or monitor Plug and Play devices. The user can be notified of the action taken.

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. Plug and Play device rules are supported on Windows-based computers only. For Plug and Play device rules to control hardware devices, the device classes specified in device definitions used by the rule must be set to **Managed** status.

**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 option definitions, click ? in the interface.

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**.

### Removable storage file access rules

Removable storage file access rules are used to block executables on plug-in devices from running. Removable storage file access rules are supported on Windows-based 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.

### Fixed hard drive rules

Fixed hard drive rules are 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.

Fixed hard drive rules are supported on Windows-based computers 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.

### Citrix XenApp device rules

Citrix XenApp device rules are used 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.

### TrueCrypt device rules

TrueCrypt device rules are used to block, monitor, or set TrueCrypt devices to read-only. You can notify the user of the action taken.

TrueCrypt device rules are supported on Windows-based computers only. TrueCrypt rules are a subset of removable storage device rules.

> TrueCrypt for OS X is not currently supported.
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.

See also
Reactions available for rule types on page 94

Create device rules
Create device rules to control device usage in your enterprise.

All device rules are supported on Windows. Only removable storage device rules are currently supported on OS X.

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.

Task
For option definitions, click ? in the interface.

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. Optional: change the Status and select a Severity.
6. On the Condition pane, select one or more removable storage device definitions. Optional: assign end-user groups and a Process Name to the rule.
   Device definitions can define devices that are included (is one of) or excluded (is none of). Including at least one definition is required.
   If you don’t select Report Incident there is no record of the incident in the DLP Incident Manager.
8. Optional: Select a different Prevent Action when the end-user is working outside the corporate network.
9. Click Save.

Create a plug and play device rule
Plug and play devices can be added to the managed computer without any configuration or manual installation of dlls and drivers. Use Plug and Play device rules to prevent the endpoint computer from loading these devices.
**Task**

For option definitions, click ? in the interface.

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 | Plug and Play Device Rule**.
5. Enter a unique **Rule Name**. Optional: change the **Status** and select a **Severity**.
6. On the **Condition** pane, select one or more plug and play device definitions. Optional: assign end-user groups to the rule.
   
   Device definitions can define devices that are included (is one of) or excluded (is none of). Including at least one definition is required.

7. Optional: Change the default **True File Type** or **File Extension** definitions according to your requirements.

8. Optional: Enter a **File Name** to be excluded from the rule.
   
   By default, executable files are included in the rule with the **File Extension** option. You can edit this option as required. The **File Name** exclusion is for applications that must be allowed to run. An example is encryption applications on encrypted drives.

9. Click **Save**.

---

**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 option definitions, click ? in the interface.

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 | Removable Storage File Access Rule**.
5. Enter a unique **Rule Name**. Optional: change the **Status** and select a **Severity**.
6. On the **Condition** pane, select one or more removable storage device definitions. Optional: assign end-user groups to the rule.
   
   Device definitions can define devices that are included (is one of) or excluded (is none of). Including at least one definition is required.

7. Optional: Change the default **True File Type** or **File Extension** definitions according to your requirements.

8. Optional: Enter a **File Name** to be excluded from the rule.
   
   By default, executable files are included in the rule with the **File Extension** option. You can edit this option as required. The **File Name** exclusion is for applications that must be allowed to run. An example is encryption applications on encrypted drives.

   
   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 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.

Task
For option definitions, click ? in the interface.

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. Optional: change the Status and select a Severity.
6 On the Condition pane, select one or more fixed hard drive device definitions. Optional: assign end-user groups to the rule.
   Device definitions can define devices that are included (is one of) or excluded (is none of). Including at least one definition is required.
   If you don’t select Report Incident there is no record of the incident in the DLP Incident Manager.
8 Optional: Select a different Prevent Action when the end-user is working outside the corporate network.
9 Click Save.

Create a Citrix device rule
Use Citrix device rules to block Citrix devices mapped to shared desktop sessions.

Task
For option definitions, click ? in the interface.

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. Optional: change the Status and select a Severity.
6 On the Condition pane, select one or more resources. Optional: assign end-user groups to the rule.
7 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.

**Task**

For option definitions, click ? in the interface.

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**. Optional: change the **Status** and select a **Severity**.
6. Optional: On the **Condition** pane, assign end-user groups to the rule.
7. On the **Reaction** pane, 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.
8. Optional: Select a different **Prevent Action** when the end-user is working outside the corporate network.
9. Click **Save**.
Protecting removable media
Create device rules
Classifying sensitive content

Classifications identify and track sensitive content and files.

Contents
- The Classification module
- Manual classification
- Using classifications
- Classification definitions and criteria
- Create and configure classifications
- Registered documents
- Whitelisted text
- Upload registered documents
- Upload files to whitelist text
- Create classification definitions
- Classifying by file location
- Classify by file destination

The Classification module

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

The module provides these features:
- Manual Classification — Configures the end-user groups allowed to manually classify or tag content
- Definitions — Defines the content, properties, and location of files for classification
- Classification — Creates classifications and defines classification and tagging criteria
- Register Documents — Uploads files containing known sensitive content
- Whitelisted Text — Uploads files containing text for whitelisting

Manual classification

End users can manually apply or remove classification or tagging criteria to files.

The simplest method of classifying files or content is manual classification. By default, end users do not have permission to view, add, or remove classifications. You can, however, assign defined classifications to specific user groups. Those users can then apply the classification to files as they work. 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 tag automatically.
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 option definitions, click ? in the interface.

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. Select Actions | Select End-User Groups.
   e. In the Choose from existing values window, select the group or groups you created previously, then click OK.
   f. 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 Manual Tagging, and selecting the appropriate tag.
Using classifications

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

McAfee DLP Endpoint identifies and tracks sensitive content with user-defined classifications. Two basic types are supported: tags and classification criteria. Tags 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.

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).

Tagging criteria

Tagging 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 tagging criteria, allowing tags to combine the functionality of both criteria types.

Tagging criteria 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 tagged content to another file, the tagging criteria are applied to that file. If the tagged content is removed from the file, the tagging criteria are also removed.

McAfee DLP Endpoint applies tagging 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 75
Create tagging criteria on page 76
Assign manual classification permissions on page 77
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.

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.

McAfee DLP Endpoint software 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 tag 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 Endpoint client software uses a fallback code page. The fallback is either the default language of the computer or a different language set by the administrator.

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.

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 7-1 Available conditions

<table>
<thead>
<tr>
<th>Property</th>
<th>Applies to:</th>
<th>Definition</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>
</tr>
<tr>
<td>Dictionary</td>
<td>Definitions, criteria</td>
<td>Collections of related keywords and phrases such as profanity or medical terminology.</td>
</tr>
<tr>
<td>Keyword</td>
<td>Criteria</td>
<td>A string value. You can add multiple keywords to a tag definition. The default Boolean for multiple keywords is OR, but can be changed to AND.</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>
</tr>
<tr>
<td>Document Properties</td>
<td>Definitions, criteria</td>
<td>Contains these options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Any Property</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Author</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Category</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Comments</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Company</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Keywords (Tags)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Any Property is a user-defined property.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Last saved by</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manager Name</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Subject</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Template</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Title</td>
</tr>
<tr>
<td>File Encryption</td>
<td>Criteria</td>
<td>Contains these options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not encrypted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• McAfee Encrypted Self-Extractor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• McAfee Endpoint Encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Microsoft Rights Management encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Seclore Rights Management encryption</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unsupported encryption types or password protected file</td>
</tr>
</tbody>
</table>
**Table 7-1 Available conditions (continued)**

<table>
<thead>
<tr>
<th>Property</th>
<th>Applies to:</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Information</strong></td>
<td>Definitions, criteria</td>
<td>Contains these options:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Date Accessed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Date Created</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Date Modified</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• File Extension</td>
</tr>
<tr>
<td><strong>Location in file</strong></td>
<td>Criteria</td>
<td>The section of the file the data is located in.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Microsoft Word documents — the classification engine can identify Header, Body, and Footer.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• PowerPoint documents — WordArt is considered Header; everything else is identified as Body.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Other documents — Header and Footer are not applicable. The classification criteria does not match the document if they are selected.</td>
</tr>
<tr>
<td><strong>Third Party tags</strong></td>
<td>Criteria</td>
<td>Used to specify Titus field names and values.</td>
</tr>
<tr>
<td><strong>True File Type</strong></td>
<td>Definitions, criteria</td>
<td>Groups of file types.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For example, the built-in Microsoft Excel group includes Excel XLS, XLSX, and XML files, as well as Lotus WK1 and FM3 files, CSV and DIF files, Apple iWork files, and more.</td>
</tr>
<tr>
<td><strong>Application Template</strong></td>
<td>Definitions</td>
<td>The application or executable accessing the file.</td>
</tr>
<tr>
<td><strong>End-User Group</strong></td>
<td>Definitions</td>
<td>Used to define manual classification permissions.</td>
</tr>
<tr>
<td><strong>Network Share</strong></td>
<td>Definitions</td>
<td>The network share the file is stored in.</td>
</tr>
<tr>
<td><strong>URL List</strong></td>
<td>Definitions</td>
<td>The URL the file is accessed from.</td>
</tr>
</tbody>
</table>

**See also**

Create classification definitions on page 80

**Dictionary definitions**

A *dictionary* is a collection of keywords or key phrases where each entry is assigned a score.

Classification and tagging 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 80

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 patterns can also define complex word patterns, as in the cellular operator call log or financial report examples in the built-in patterns.

For word patterns, regex patterns begin and end with \b by default, the standard regex notation for word separation. Thus, text pattern matching for phrases, is, by default, whole-word matching to reduce false positives.

Advanced pattern definitions include a score (required), as with dictionary definitions. They can also include an optional false positive expression, either keyword or regex, and a validator — an algorithm used to test regular expressions. Use of the proper validator can also significantly reduce false positives. You can import multiple keywords at once for false positives.

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

If both an included pattern and an excluded pattern are specified, the excluded 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 81
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.

Application templates 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.

Create and configure classifications
Create classifications and criteria, and upload files for registration or whitelisting.

Tasks
- **Create a classification on page 75**
  Data protection and discovery rules require classification definitions in their configuration.
- **Create classification criteria on page 75**
  Apply classification criteria to files based on file content and properties.
- **Create tagging criteria on page 76**
  Apply tagging criteria to files based on the application or file location.
- **Assign manual classification permissions on page 77**
  Configure users allowed to manually classify files.

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

Task
For option definitions, click ? in the interface.

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 classification criteria or tagging criteria with the **Actions** control.

Create classification criteria
Apply classification criteria to files based on file content and properties.
You build 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 option definitions, click ? in the interface.

1 In McAfee ePO, select **Menu | Data Protection | Classification**.
2 Select the classification to add the criteria to, then select **Actions | New 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 69

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

Task
For option definitions, click ? in the interface.

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

2 Select the classification to add the criteria to.

3 Select Actions | New Tagging Criteria, then select the type of tagging criteria.

4 Enter the name and specify additional information based on the type of tagging 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.

5 (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 –.

6 Click Save.

Tasks
• Use case: application-based tagging on page 76
   You can classify content as sensitive according to the application that produced it.

See also
Using classifications on page 69

Use case: application-based tagging
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 tagging criteria definition, all JPEG files produced by the application are tagged as sensitive. JPEG files produced by other applications are not tagged.
**Task**
For option definitions, click ? in the interface.

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 Tagging Criteria** | **Application**
   The tagging 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 option definitions, click ? in the interface.

1. In McAfee ePO, select **Menu** | **Data Protection** | **Classification**.
2. Click the **Manual Classification** tab.
3. Use the **Group by** drop-down list to select either **Classifications** or **User Groups**.
   You can assign classifications to user groups or user groups to classifications, which ever is more convenient. The **Group by** list controls the display.
4. If you are grouping by classifications:
   a. Select a classification from the displayed list.
   b. Select **Actions** | **Select End-User Groups**.
   c. 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 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.

Registered documents

The registered documents feature is an extension of location-based tagging. 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. The McAfee DLP Endpoint 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.

The Create Package command works on the registered documents list and the whitelisted documents list simultaneously to create a single package. The maximum number of signatures per package is 1 million each for registered documents and whitelisted documents.

See also

Upload registered documents on page 79

Whitelisted text

McAfee DLP Endpoint 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 or tagged, even if parts of it match classification or tagging 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 tagged or classified and whitelisted data, it is not ignored by the system. All relevant tagging or classification criteria associated with the content remain in effect.
Upload registered documents

Select and classify documents to distribute to the endpoint computers.

**Task**
For option definitions, click ? in the interface.

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.

   ![File Upload process a single file. To upload multiple documents, create a .zip file.]

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 78*

Upload files to whitelist text

Upload files containing commonly used text for whitelisting.

**Task**
For option definitions, click ? in the interface.

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

**See also**
- *Whitelisted text on page 78*
Create classification definitions

Predefined classification definitions cannot be modified or deleted. Create new definitions as needed.

Tasks

- Create or import a dictionary definition on page 80
  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 81
  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.

- Integrate Titus Client with third-party tags on page 82
  Classification or tagging criteria can include multiple Titus tag name/tag value pairs.

- Integrate Boldon James Email Classifier with classification criteria on page 82
  Create classification criteria to integrate Boldon James Email Classifier.

See also
Classification definitions and criteria on page 71

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 option definitions, click ? in the interface.

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.

   All entries are assigned a default score of 1.

   If needed, updated the default score of 1 by clicking Edit for the entry.

d  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 option definitions, click ? in the interface.

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.


   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.
In the **Type** field, select **RegEx** from the drop-down list if the string is a regular expression, or **Keyword** if it is text.

Click **Add**.

7 Click **Save**

**Integrate Titus Client with third-party tags**

Classification or tagging 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 option definitions, click ? in the interface.

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 Classification Criteria** or **New Tagging 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**.

**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 option definitions, click ? in the interface.

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 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.
      [Boldon James classification] is the string you selected in the Email Classifier 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 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.

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.

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 option definitions, click ? in the interface.

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 a network port range

Network port ranges serve as filter criteria in network communication protection rules.
Task
For option definitions, click ? in the interface.

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.

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.

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.

Client configuration
Set controls for email functionality behavior in McAfee ePO Policy Catalog | Data Loss Prevention 9.4 | Client Configuration | Email Protection. Settings on this page include:

- Email Caching — Stores tag signatures from emails to disk to eliminate re-parsing emails.
- Email Handling API — 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.
• **Outlook 3rd party add-in integration** — Two third-party classification applications are supported: Titus and Boldon James.

• **Email Timeout Strategy** — Sets the maximum time to analyze an email and the action if the time is exceeded.

### Create email destinations

Email destination 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 option definitions, click ? in the interface.

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.

### 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.

### 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 option definitions, click ? in the interface.

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**.

**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.

**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 option definitions, click ? in the interface.

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**.
Classifying sensitive content
Classify by file destination
Using rules to protect sensitive content

McAfee DLP Endpoint protects sensitive content with a combination of data protection rules, device control rules, and discovery rules. The rules are combined into rule sets and applied to McAfee DLP policies.

McAfee ePO deploys the McAfee DLP policies to the endpoint computers. McAfee DLP Endpoint client software then applies the policies to protect the sensitive content.

Contents

- Rule sets
- Reactions available for rule types
- Application File Access Protection rules
- Email protection rules
- Network communication protection rules
- Network share protection rules
- Printer protection rules
- Removable storage protection rules
- Screen capture protection rules
- Web post protection rules
- Endpoint discovery
- Protecting files with rights management

Rule sets

Rule sets define McAfee DLP Endpoint 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.

![Rule Sets page showing ToolTip information](image)

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 103
Create a rule on page 90

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 90
  Rule sets combine multiple device protection, data protection, and discovery scan rules.
• Create a rule on page 90
  The processes for creating a rule is similar for all rule types.
• Assign rule sets to policies on page 91
  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 91
  You can delete or change the state of multiple rules at once.
• Configure rule or rule set columns on page 92
  Move, add, or remove columns displayed for rules or rule sets.
• Create a justification definition on page 93
  Business justification definitions define parameters for the justification prevent action in rules.
• Create a notification definition on page 94
  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 option definitions, click ? in the interface.

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 processes for creating a rule is similar for all rule types.

Task
For option definitions, click ? in the interface.

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 On the **Reaction** tab, configure the reaction.

7 Click **Save**.

**See also**

*Rule sets* on page 89

### 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 option definitions, click ? in the interface.

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 option definitions, click ? in the interface.

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.

**Configure rule or rule set columns**
Move, add, or remove columns displayed for rules or rule sets.

**Task**
For option definitions, click ? in the interface.

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.

**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.

**User notification**
User notifications are pop up messages that notify the user of a policy violation.

> When multiple events are triggered by a rule, 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)

**Create a justification definition**

Business justification definitions define parameters for the justification prevent action in rules.

**Task**

For option definitions, click ? in the interface.

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.
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.

When all locales are complete, click Save.

See also
Customizing end-user messages on page 92

Create a notification definition
User notifications appear in popups or the end-user console when user actions violate policies.

Task
For option definitions, click ? in the interface.

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.

When all locales are complete, click Save.

See also
Customizing end-user messages on page 92

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.
- Discovery rules are available for McAfee DLP Endpoint discovery.
### Table 8-1 Available reactions

<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>
<tr>
<td>Request justification</td>
<td>Data Protection</td>
<td>Produces a popup 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</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 containing the file.</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>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. Requires a specified evidence folder and activation of the evidence copy service.</td>
</tr>
</tbody>
</table>

### Table 8-2 Data protection rule reactions

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Reaction</th>
<th>No action</th>
<th>Block</th>
<th>Encrypt</th>
<th>Request justification</th>
<th>Apply RM policy</th>
<th>User notification</th>
<th>Report incident</th>
<th>Store original file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application file access protection</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Clipboard protection</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud protection</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
### Table 8-2 Data protection rule reactions (continued)

<table>
<thead>
<tr>
<th>Rule type</th>
<th>Reactions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No action</td>
</tr>
<tr>
<td>Email protection</td>
<td>X</td>
</tr>
<tr>
<td>Network communication protection</td>
<td></td>
</tr>
<tr>
<td>Network share protection</td>
<td>X</td>
</tr>
<tr>
<td>Printer protection</td>
<td>X</td>
</tr>
<tr>
<td>Removable storage protection</td>
<td>X</td>
</tr>
<tr>
<td>Screen capture protection</td>
<td>X</td>
</tr>
<tr>
<td>Web post protection</td>
<td>X</td>
</tr>
</tbody>
</table>

### Table 8-3 Device control rule reactions

<table>
<thead>
<tr>
<th>Rules</th>
<th>Reactions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No action</td>
</tr>
<tr>
<td>Citrix XenApp device</td>
<td></td>
</tr>
<tr>
<td>Fixed hard drive</td>
<td>X</td>
</tr>
<tr>
<td>Plug and play device</td>
<td>X</td>
</tr>
<tr>
<td>Removable storage device</td>
<td>X</td>
</tr>
<tr>
<td>Removable storage file access</td>
<td>X</td>
</tr>
<tr>
<td>TrueCrypt device</td>
<td>X</td>
</tr>
</tbody>
</table>

### Table 8-4 Discovery rule reactions

<table>
<thead>
<tr>
<th>Rules</th>
<th>Reactions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No action</td>
</tr>
<tr>
<td>Endpoint file system</td>
<td>X</td>
</tr>
<tr>
<td>Endpoint mail storage protection</td>
<td>X</td>
</tr>
</tbody>
</table>
Application File Access Protection rules

Protection rules for file access monitor files based on the application or applications that created them.

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

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 option definitions, click ? in the interface.

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.


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.

10 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.

11 Select Actions | Apply Selected Policies. Select policies to apply to the McAfee ePO database, and click OK.

---

**Email protection rules**

Email protection rules monitor or block email sent to specific destinations or users.

Email protection rules can block emails to specified recipients. The Email Envelope field can specify that the email is protected by RMS permissions. This option is usually used to define exceptions.

Use classification definitions to limit the rule to specific tags or classification criteria. The classifications can define the entire 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 actions are Block, Request Justification, 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.

**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. For improved performance, we recommend disabling unused handlers.

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

To use Microsoft Outlook 3rd 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.
Network communication protection rules

Network communication protection rules monitor or block incoming or outgoing data on your network. 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 tags. You can also limit the rule to local users or to specified user groups.

Screen capture protection rules do not check classification criteria. Use tagging 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. 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 tags or classification criteria. You can also limit the rule to local users or to specified user groups.

Actions

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

Use classification definitions to limit the rule to specific tags or classification criteria. You can also limit the rule by specifying users, printers, or applications. 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 applications are listed on the Printer Protection page. Printer protection rules ignore files printed from whitelisted applications.

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.

Removable storage protection rules can control CD and DVD devices, removable storage devices, or both. Limit the rule with tags or classification criteria in classifications (required). You can also define the rule with specified users, applications, or web URLs.

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.

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.

- 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.

> Tags are lost when tagged 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.

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

> Screen capture protection rules do not check classification criteria. Use tagging 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.

Web post protection rules are defined by adding web addresses to the rule.

Use classification definitions to limit the rule to specific tags or 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.

**Web Post Protection page**

The Web Post Protection page contains a list of whitelisted URLs that are excluded from web post protection rules. It also has a setting to enable processing HTTP GET requests. GET requests are disabled by default because they are resource-intensive. Use this option with caution.

The Web Timeout Strategy 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.

The page also contains a list of supported Google Chrome versions. The list is required due to the frequency of Chrome updates. The list is populated by downloading a current list from McAfee Support and using Browse to install the XML file.

**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 8-5 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>

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 104
  Discovery rules define the content the crawler searches for, and what to do when this content is found.
- Create a scheduler definition on page 105
  The scheduler determines when and how frequently a discovery scan is run.
- Set up a scan on page 105
  Discovery scans crawl the local file system or mailboxes for sensitive content.
- Use case: Restore quarantined files or email items on page 106
  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 option definitions, click ? in the interface.

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.
Optional: Select Report Incident options, set the State to Enabled, and select a Severity designation from the drop-down list.

Click Save.

Create a scheduler definition

The scheduler determines when and how frequently a discovery scan is run.

Five schedule types are provided:
- Run immediately
- Once
- Daily
- Weekly
- Monthly

Task

For option definitions, click ? in the interface.

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 option definitions, click ? in the interface.

1. In McAfee ePO, select Menu | Policy | Policy Catalog.
2. Select Product Data Loss Prevention 9.4, 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 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.

7 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.

8 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.

**Figure 8-2 Quarantined email example**

![Quarantined email example](image-url)
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 sends an event to DLP Operational Events 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

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

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

RM policies cannot be used with device control rules.

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

See also
Define a Rights Management server on page 38
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. You can also create a tagging rule to add a tag to RM protected files.

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 tag 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 tagged file is RM protected, only static tags (location and application) are maintained. If a user modifies the file, all tags 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).

**Microsoft RMS**

McAfee DLP Endpoint 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:

- Microsoft PowerPoint 2007, PowerPoint 2010, and PowerPoint 2013 documents
- SharePoint 2007 documents
- Exchange Server 2007 documents

With Microsoft RMS, McAfee DLP Endpoint software 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.
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 module.
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 in the Policy Catalog.

In the Policy Catalog, you can also create new policies by duplicating a default or other existing policy.

**Contents**

- Using multiple policies
- How definitions work
- Edit a DLP policy
Using multiple policies

Use multiple policies to override common settings and definitions.

McAfee DLP policies can be assigned to endpoint computers by McAfee ePO from the System Tree as a global policy or by policy assignment rules. In McAfee DLP version 9.3, there was a single policy, which included common settings and definitions. These settings and definitions were sent to all endpoint computers, no matter which method was used. The settings included the following types of information:

- Tagging rules
- Classification rules
- Tag and classification criteria names
- Whitelisted text
- Application definitions
- Device classes

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 version 9.4 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 9-1 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></td>
</tr>
<tr>
<td>Device Definitions</td>
<td></td>
</tr>
<tr>
<td>Notification</td>
<td></td>
</tr>
<tr>
<td>Justification</td>
<td></td>
</tr>
<tr>
<td>User Notification</td>
<td></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>
</tbody>
</table>
Table 9-1 Definitions available by McAfee DLP feature (continued)

<table>
<thead>
<tr>
<th>Classifications</th>
<th>Rule Sets</th>
</tr>
</thead>
<tbody>
<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 option definitions, click ? in the interface.

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 9.4. 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.
Monitoring and reporting

You can use McAfee DLP Endpoint software components to track and review policy violations, and to track administrative (operational) events.

Chapter 10  Monitoring and reporting events
Chapter 11  Collecting and managing data
Chapter 12  Creating reports
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 Operational Events.

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 Operational Events console displays details on client deployment, policy changes, policy deployment, Safe Mode logons, agent overrides, and other administrative events.

Contents
- DLP Incident Manager
- How the Incident Manager works
- Incident types and details
- Manage incidents
- Working with cases

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.
How the Incident Manager works

The Incident List tab of the DLP Incident Manager has all of the functionality needed to review policy violation incidents. Event details are viewed by clicking on a specific event. You can create and save filters to modify the view or use the predefined filters in the Group By pane. You can also modify the view by selecting and ordering columns. Color-coded icons and numerical ratings for severity facilitate quick visual scanning of events.

The Incident List tab works with McAfee ePO Queries & Reports to create 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

The DLP Operational Events page works in an identical manner with administrative events.

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 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>Data in-use/motion</th>
<th>Data at-rest (Endpoint)</th>
<th>Data in-use/motion (History)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Reviewer</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Automatic mail notification</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Purge events</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 Actions | Set Properties or from the details pane of the incident. 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 modify 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. Click Actions | View | Choose Columns to open the view edit window.
2. Use the x icon to delete columns, and the arrow icons to move columns to the left or right.
3. Click Update View to apply the customized view, and Actions | View | Save View to save for future use. When you save the view, you can also save the time and custom filters. Saved views can be chosen from the drop-down menu at the top of the page.

Incident types and details
Incidents are categorized based on the type of violation that occurred.
The incident manager displays incidents generated by all McAfee DLP software products. The DLP Incident Manager details page displays all details relating to a particular incident.
The information and options displayed vary depending on the type of incident. For example, the details of Network Share Protection incidents contain destination information, while Device Control incidents contain device information.

All incidents contain the Rules, Audit Logs, and Comments tabs, but some incident types, such as Network Share Protection, also contain the Evidence and Classifications tabs.
**View incidents**
The incident manager displays all incidents reported by McAfee DLP devices. You can alter the way incidents appear to help you locate important violations more efficiently.

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.

**Sort and filter incidents**
Arrange the way incidents appear based on attributes such as time, location, user, or severity.

**Task**
For option definitions, click ? in the interface.

1. In McAfee ePO, select DLP Incident Manager.

2. 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.
     2. A list of available options appears. The list contains up to 250 of the most frequently occurring options.
     3. Select an option from the list. Incidents that match the selection are displayed.

**Example**
Select User ID 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 option definitions, click ? in the interface.

1. In McAfee ePO, select DLP Incident Manager.

2. From the View drop-down list, select Default and click Edit.

3. 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.
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.

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 option definitions, click ? in the interface.

1  In McAfee ePO, select DLP Incident Manager.
2  From the Filter drop-down list, select (no custom filter) and click Edit.
3  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.
4  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 option definitions, click ? in the interface.

1 In McAfee ePO, select DLP Incident Manager.

2 Click an Incident ID.
   The page displays general details and source information. Depending on the incident type, destination or device details appear.

3 To view additional information, perform any of these tasks.
   • To view user information, 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.
   • To view rules that triggered the incident, click the Rules tab.
   • To view classifications, click the Classifications tab.
     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 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 123**
  Update incident information such as the severity, status, and reviewer.

- **Update multiple incidents on page 123**
  Update multiple incidents with the same information simultaneously.

- **Manage labels on page 124**
  A label is a custom attribute used to identify incidents that share similar traits.

- **Delete incidents on page 124**
  Delete incidents that are not useful.

**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 option definitions, click ? in the interface.

1. In McAfee ePO, select **DLP Incident Manager**.
2. Click an incident.
3. 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, and you want to change the severity of these incidents to Major.

**Task**

For option definitions, click ? in the interface.

1. In McAfee ePO, select **DLP Incident Manager**.
2. Select the checkboxes of the incidents to update.

> To update all incidents displayed by the current filter, click **Select all in this page**.
3 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**.
   • To modify the properties, select **Actions** | **Set Properties**, modify the options, then click **OK**.

**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 option definitions, click ? in the interface.

1 In McAfee ePO, select **DLP Incident Manager**.

2 Select the checkboxes of one or more incidents.

   ![To update all incidents displayed by the current filter, click Select all in this page.]

3 Perform any of these tasks.
   • To add labels:
      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 an incident:
      1 Select **Actions** | **Manage Labels** | **Detach**.
      2 Select the labels to remove from the incident.
      3 Click **OK**.
   • To delete labels:
      1 Select **Actions** | **Manage Labels** | **Delete Labels**.
      2 Select the labels to delete.
      3 Click **OK**.

**Delete incidents**
Delete incidents that are not useful.
Task
For option definitions, click ? in the interface.

1. In McAfee ePO, select Menu | Data Protection | DLP Incident Manager | Incident Tasks.

2. In the Task Type (left) pane, select Purge events. If multiple incident types are available, select the type (Data in-use/motion, Data at-rest, and so forth) from the drop down list.

   You can purge from the Incident List or the Incident History, according to your selection on this list.

3. Select Actions | New Task
   The Purge Rule page appears.

4. Enter a unique name and optional description. Click Next.
   The State is Enabled by default. You can change the state to Disabled if you do not plan to run the rule right away.

5. Click > to select criteria, select the Comparison, and enter or select the Value. Click < to remove criteria. Click Save.
   By default, purge tasks are set to run daily.

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 option definitions, click ? in the interface.

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.

**Assign incidents to a case**

Add related incidents to a new or existing case.

**Task**

For option definitions, click ? in the interface.

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.

**View case information**

View audit logs, user comments, and incidents assigned to a case.

**Task**

For option definitions, click ? in the interface.

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.

**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 modified.
- Incidents are added to or deleted from the case.
- The case title is modified.
• The owner details are modified.
• The priority is modified.
• The resolution is modified.
• 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 option definitions, click ? in the interface.

1 In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2 Click on 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, you must 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.
   • To remove an incident from the case:
     1 Click the Incidents tab and locate the incident.
     2 In the Actions column, click Delete.
     4 Click OK.

Add or remove labels to a case
Use labels to distinguish cases by a custom attribute.
Task
For option definitions, click ? in the interface.

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 option definitions, click ? in the interface.

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.
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 Operational Events 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

Edit server tasks

McAfee DLP uses the McAfee ePO Server Tasks to run DLP Incident Manager and DLP Operational Events 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 9.4 incident and operational events server tasks are:

- DLP Incident Event Migration from 9.4 to 9.4.1
- DLP Incident Migration
- DLP Operational Events Migration
- 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

DLP incidents task runner is a McAfee DLP 9.3 task. It appears only if you have both versions of McAfee DLP installed.

Task

For option definitions, click ? in the interface.

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

2 Select the task to edit.

Use 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 130
  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 130
  You can set automatic email notifications of incidents and operational events to administrators, managers, or users.

• Create a Set Reviewer task on page 131
  You can assign reviewers for different incidents and operational events to divide the workload in large organizations.

See also

Convert policies and migrate data on page 29
Create a Set Reviewer task on page 131
Create an Automatic mail Notification task on page 130
Create a Purge events task on page 130

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 option definitions, click ? in the interface.

1  In McAfee ePO, select Menu | Data Protection | DLP Incident Manager or Menu | Data Protection | DLP Operational Events.

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 129

Create an Automatic mail Notification task

You can set automatic email notifications of incidents and operational events to administrators, managers, or users.
**Task**

For option definitions, click ? in the interface.

1. In McAfee ePO, select **Menu | Data Protection | DLP Incident Manager** or **Menu | Data Protection | DLP Operational Events**.

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 129*

**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 Operational Events.

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 option definitions, click ? in the interface.

1. In McAfee ePO, select **Menu | Data Protection | DLP Incident Manager** or **Menu | Data Protection | DLP Operational Events**.

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**.

   If there are multiple Set Reviewer rules you can 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 129

Monitor task results
Monitor the results of incident and operational event tasks.

Task
For option definitions, click ? in the interface.

1. In McAfee ePO, select **Menu | Automation | Server Task Log**.

2. Locate the completed McAfee DLP tasks.

   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 Endpoint 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.

Contents
- Report types
- Report options
- Create a data rollup server task

Report types

Use the McAfee ePO reporting features to monitor McAfee DLP Endpoint performance.

Two types of reports are supported:
- DLP properties reports
- DLP events reports

Six DLP properties reports are displayed in the DLP: Status Summary dashboards. Twelve predefined events queries are provided. All 28 queries, including the rollup queries, can be found in the McAfee ePO console under Menu | Reporting | Queries & Reports | Shared Groups.

McAfee ePO includes a rollup function, which runs queries that report on summary data from multiple McAfee ePO databases. All the McAfee DLP Endpoint reports are set up to support rollup queries.

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 three predefined dashboards:

- DLP: Incident Summary
- DLP: Operations Summary
- DLP: Policy Summary

Dashboards can be edited and customized, and new monitors can be created. See the McAfee ePO documentation for instructions.

The predefined reports summarized in the Dashboards are available by selecting Menu | Queries & Reports. They are listed under Shared Groups (McAfee ePO 4.6) or McAfee Groups (McAfee ePO 5.1). In addition, there is a DLP rollup report, Events by type.

Predefined dashboards

The following table describes the predefined McAfee DLP dashboards.

Table 12-1 Predefined DLP dashboards

<table>
<thead>
<tr>
<th>Category</th>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident summary</td>
<td>Number of Incidents per day</td>
<td>These charts show total incidents, and give different breakdowns to help analyze specific problems.</td>
</tr>
<tr>
<td></td>
<td>Number of Incidents per severity</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of Incidents per type</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of Incidents per rule set</td>
<td></td>
</tr>
<tr>
<td>Operations summary</td>
<td>Number of Operational events per day</td>
<td>Displays all administrative events.</td>
</tr>
<tr>
<td></td>
<td>Agent Status</td>
<td>Displays all agents and their status.</td>
</tr>
<tr>
<td></td>
<td>Agent Version</td>
<td>Displays the distribution of endpoints in the enterprise. Used to monitor agent deployment progress.</td>
</tr>
<tr>
<td></td>
<td>Agent Operation Mode</td>
<td>Displays a pie chart of agents by DLP operation modes. Operation modes are:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device control only mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device control and full content protection mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Device control and content aware removable storage protection mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td></td>
<td>Discovery (endpoint) Local File System Scan Status</td>
<td>Displays a pie chart showing the number of local file system discovery scan properties and their states (completed, running, undefined).</td>
</tr>
<tr>
<td></td>
<td>Discovery (Endpoint) Local Email Storage Scan Status</td>
<td>Displays a pie chart showing the number of local email storage scan discovery properties and their states (completed, running, undefined).</td>
</tr>
<tr>
<td>Policy summary</td>
<td>Policy distribution</td>
<td>Displays the DLP policy distribution by version throughout the enterprise. Used to monitor progress when deploying a new policy.</td>
</tr>
<tr>
<td></td>
<td>Enforced Rule Sets per endpoint computers</td>
<td>Displays a bar chart showing the rule set name and the number of policies enforced.</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>Bypassed Users</td>
<td>Displays the system name/user name and the number of user session properties.</td>
<td></td>
</tr>
<tr>
<td>Undefined Device Classes</td>
<td>Displays the undefined device classes for Windows devices.</td>
<td></td>
</tr>
<tr>
<td>Privileged Users</td>
<td>Displays the system name/user name and the number of user session properties.</td>
<td></td>
</tr>
<tr>
<td>Policy revision distribution</td>
<td>Similar to Policy distribution, but displays revisions – that is, updates to an existing version.</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 option definitions, click ? in the interface.

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 or DLP Operational Event, 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.
Creating reports
Create a data rollup server task
# Index

## A

- about this guide 7
- advanced patterns 81
- agent configuration
  - Mac OS support 47
- all_evidences.csv file 39
- application definitions
  - strategy 70
- application templates
  - about 74
- assignment groups
  - definition 12

## B

- Boldon James 82
- business justification, customizing 92

## C

- cases
  - about 125
  - adding comments 126
  - assigning incidents 126
  - audit logs 126
  - creating 125
  - deleting 128
  - labels 127
  - sending notifications 126
  - updating 126
- challenge-response key length 37
- challenge/response 106
- Chrome, supported versions 47, 102
- Citrix XenApp device rules 58
- classification 67
  - criteria 69, 75
  - email 82
  - manual 67
- classification rules 10
- classification, manual 77
- classifications 75
  - about 67
- client configuration 46
  - assigning with ePolicy Orchestrator 33
  - (continued)
    - system tree 37
- components, Data Loss Prevention (diagram) 23
- content tracking 47
- conventions and icons used in this guide 7
- conversion 29

## D

- dashboards, report options 134
- data
  - classifying 72
  - data-in-motion 87
- Data Loss Prevention software, description 21
- data rollup 135
- data-at-rest 9, 103
- data-in use 9
- data-in-motion 9
- definitions 112
  - dictionaries 72
  - document properties 74
  - file extension 74
  - network 84
  - registered documents 78
  - text pattern 73
  - web destination 87
- device classes 50
- device definitions 53
  - removable storage 55
- device GUID 51
- device rules
  - about 58
  - definition 12
- devices
  - lists, adding plug and play definitions 54
- devices properties 56
- dictionaries
  - about 72
  - creating 80
  - importing entries 80
- discovery
  - about 103
  - creating a file system discovery rule 104
  - setup 105
- discovery rules 11
DLP data, classifying 73
DLP Discover 103
DLP Endpoint
  checking in to ePolicy Orchestrator 28
deploying 31
deployment verification 32
wake-up call 33
DLP Incident Manager 117
  responding to events 117
DLP policy 113
DLP Policy console, installing 27
DLP rules
  classification 10
device 12
  protection 12
tagging 11
document properties definitions 74
documentation
  audience for this guide 7
  product-specific, finding 8
  typographical conventions and icons 7
E
email 85
email classification 82
email destinations
  creating 86
endpoint console 15
ePO notifications 133
ePO reports 133
events
  monitoring 117
evidence
  endpoint events 117
  storage for encrypted content 39
evidence folder 40
evidence folder, configuring 41
evidence storage 47
F
file access
  rules, about 58
file extensions
  definitions 74
filters
  network definitions 84
G
Google Chrome, supported versions 47, 102
GUID, See device GUID
H
hardware requirements 24
hit highlighting, events 39
I
incident manager 117, 118
incident tasks 117, 129
incidents
  deleting 124
details 119, 122
  filtering 120, 121
  labels 124
  sorting 120
types 119
  updating 123
  views 120
J
JAWS support 15
L
license key 37
location, classifying by 84
M
manual classification 77
McAfee ServicePortal, accessing 8
migration 29
monitoring 117
N
network definitions
  about 84
  address range 84
  port range 84
notifications, ePolicy Orchestrator 133
O
operational event tasks 129
operational events 118
OS X support 15
OST files 85
P
permission sets 42
permission sets, defining 43
permission sets, system tree filtering 42
placeholders 92
plug and play devices
  whitelisted definition, creating 54
policies 13, 37
  assigning with 33
definition 12
  refreshing 33
  policy assignment 113
policy backup 37
policy catalog 46
protection rules
definition 12
PST files 85

Q
quarantine
release from 39
restoring files or email items from 106

R
reactions 94
redaction 42
registered documents 78
restore a policy 37
rights management 38, 107
role-based access control 43
roles and permissions 40
rolled up reports 133
rule sets
about 89
creating 90
rule sets, adding to policies 113
rules
Citrix XenApp 58
reactions 94
tagging 11

S
safe mode operation 47
server settings 37
server software requirements 24
server tasks 29, 129
server tasks, rollup 135
ServicePortal, finding product documentation 8
strategy, See application definitions
supported operating systems 24
system requirements 24

T
tagging 67
about 69
criteria 69
tagging criteria 76
tagging rules
definition 11
technical support, finding product information 8
text extractor 70
text patterns
about 73
timeout strategy, web post 102
Titus, integration 82
TrueCrypt device rules 58

U
upgrade Device Control to full DLPE, See license key
URL lists
creating 87
user notification, customizing 92
user sessions 58

V
validators 73
verifying the installation 32
VPN connectivity 47

W
wake-up call 33
web destinations
about 87
web post protection rules 102
whitelisted text 79
whitelists 12
plug and play definitions, creating 54