Product Guide
Revision A

McAfee Data Loss Prevention Endpoint
9.3.200

for Windows and Mac

For use with ePolicy Orchestrator 4.6 - 5.1 Software
McAfee Data Loss Prevention Endpoint 9.3.200
for Windows and Mac

LICENSE INFORMATION

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

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

**1 Introduction**
- How McAfee DLP Endpoint works ............... 10
- Classify .................................. 10
- Track ................................... 11
- Protect ................................... 12
- Monitor ................................... 13
- Product components and how they interact .... 14
- McAfee DLP Endpoint client software ......... 15

**Deployment**

**2 Deployment options and scenarios**
- Choosing an endpoint product option .......... 19
- Recommended installation ..................... 21
- Understanding backward compatibility ......... 22

**3 Planning your deployment**
- Verify the system requirements ............... 24
- Configure the server .................................. 26
- Working in a cluster environment ............... 26
  - Prepare the cluster .................................. 27
  - Test the cluster .................................. 27
- Create and configure repository folders ....... 27
  - Configure folders on Windows Server 2008 .... 28
  - Configure folders on Windows Server 2003 .... 29
- Deployment checklist .................................. 30

**Installation**

**4 Installing the McAfee DLP Endpoint software**
- Install the McAfee DLP Endpoint extension ........ 33
- Initialize the McAfee DLP Endpoint policy console ........ 34
- Upgrade the license .................................. 36
- Check in the McAfee DLP Endpoint package to ePolicy Orchestrator ........ 37

**5 Installing a version upgrade**
- Upgrade McAfee DLP Endpoint software .......... 41
- Phased upgrade .................................. 42
Restore the policy after upgrade ........................................ 43

6 Deploying McAfee DLP Endpoint ........................................ 45
   Deploy the client software ........................................ 45
      Define a default rule ........................................ 45
   Deploy McAfee DLP Endpoint client with ePolicy Orchestrator .......... 46
   Verify the installation ........................................ 47
   Deploy policies with ePolicy Orchestrator ................................ 48
      Apply the system policy ........................................ 49
      Assign a policy or agent configuration ................................ 49
      Import policies and editing policy descriptions ....................... 49
      Refresh the policy ........................................ 50

Configuration and use

7 McAfee Device Control ......................................................... 53
   Categorizing devices with device classes ................................ 54
      Define a device class ........................................ 55
   Controlling devices with device definitions ................................ 57
      Avoiding conflicts in removable storage device definitions ........ 58
      Importing device parameters .................................... 58
      Create device definitions ...................................... 59
   Device rules ........................................ 62
      Create and define device rules .................................. 66
   Device parameters ........................................ 70

8 Configuring system components ............................................. 73
   Agent configuration ........................................ 73
      OS X support for Agent Configuration parameters .................... 74
   Apply the global agent configuration .................................. 74
   Import the global agent configuration .................................. 74
   Reset the Agent Configuration values .................................. 75
   Configure Safe Mode operation ..................................... 75

9 Classifying sensitive content .................................................. 77
   Classifying by content ........................................ 77
      Using dictionaries to classify content ................................ 77
      Classifying content with document properties or file extensions .... 79
      Text pattern definitions ....................................... 79
      Whitelist ........................................ 84
   Classifying by file location ........................................ 85
      How discovery scanning works .................................. 86
      Defining network file shares ................................... 93
      Defining network parameters ................................... 94
      Defining registered document repositories ............................ 95
   Classifying by file destination ........................................ 97
      How sensitive content is controlled in email ......................... 97
      Defining local and network printers ................................ 100
      Controlling information uploaded to websites ....................... 102
   Classification in use ........................................ 104
      How McAfee DLP Endpoint categorizes applications .................. 104
      Applications and how to use them .................................. 105
      Adding and removing applications .................................. 110
      Defining file types ........................................ 111
   Classification rules ........................................ 112
      How classification rules link categories to content ................. 113
Create and define classification rules ........................................... 113

10 Tracking content with tags and classifications .......................... 117
How tags and content categories are used to classify content ................ 117
Create tags, content categories, catalogs, and groups ....................... 118
How tagging rules link tags to content ......................................... 120
Create and define tagging rules .................................................... 120
Manual tags .................................................................................. 122
Tag files manually ........................................................................ 123
Remove manual tags from content ............................................... 123

11 Applying McAfee DLP protection ................................................. 125
Protecting files with rights management ........................................ 125
How Data Loss Prevention works with rights management .................. 126
Adobe rights management users .................................................... 128
Define an Adobe RM server and synchronize policies ....................... 129
Define a Microsoft Rights Management Service server and synchronize templates ........................................ 129
Define a Seclore server and synchronize policies ................................ 130
Controlling sensitive content with protection rules ......................... 131
How protection rules work .............................................................. 131
Improved clipboard protection rules ............................................. 134
Cloud protection rules ................................................................. 134
Removable storage protection rule enhancement ............................... 135
Definitions and how they define rules .......................................... 135
Delete rules, definitions, device classes, or user groups .................. 149
Using predefined definitions ......................................................... 149
Limiting rules with assignment groups .......................................... 150
User assignment .......................................................................... 151
Computer assignment groups ....................................................... 153

Monitoring and reporting

12 Monitoring and reporting events ................................................ 157
Collecting and managing data ....................................................... 157
DLP Incident Manager/DLP Operational Events ................................. 158
Incident tasks ............................................................................. 162
Edit the task runner ..................................................................... 163
Creating reports .......................................................................... 163
Working with the database ........................................................... 167
Documenting events with evidence .............................................. 167
Redaction and role-based access control ...................................... 169
Protecting confidentiality with redaction ....................................... 170
Role-based access control ............................................................ 172

13 Users and permission sets ............................................................. 175
DLP Permission Sets ..................................................................... 175
Create and define McAfee DLP administrators ................................ 176
Create and define permission sets .................................................. 177

14 Non-routine operations ............................................................... 179
Agent bypass and related features ................................................. 179
Request an override key ............................................................... 180
Advanced topics: Running the PST crawler from the command line ...... 183

15 Diagnostics .............................................................................. 185
System tools ................................................................................ 185
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

McAfee provides the information you need during each phase of product implementation, from installation to daily use and troubleshooting. After a product is released, information about the product is entered into the McAfee online KnowledgeBase.

Task
2. Under Self Service, access the type of information you need:

<table>
<thead>
<tr>
<th>To access...</th>
<th>Do this...</th>
</tr>
</thead>
<tbody>
<tr>
<td>User documentation</td>
<td>1. Click Product Documentation.</td>
</tr>
<tr>
<td></td>
<td>2. Select a product, then select a version.</td>
</tr>
<tr>
<td>KnowledgeBase</td>
<td>• Click Search the KnowledgeBase for answers to your product questions.</td>
</tr>
<tr>
<td></td>
<td>• Click Browse the KnowledgeBase for articles listed by product and version.</td>
</tr>
</tbody>
</table>
Introduction

McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) protects enterprises from the risk associated with unauthorized transfer of data from within or outside of the organization.

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

This guide provides the necessary information for installing, deploying, and using McAfee DLP Endpoint software: configuring agents, creating device rules, tagging and protecting content, and monitoring policies to prevent data loss.

McAfee DLP Endpoint version 9.3.x runs in McAfee® ePolicy Orchestrator® (McAfee ePO™) software, the centralized policy manager for security products and systems.

**McAfee DLP Endpoint on the Microsoft Windows platform**

McAfee DLP Endpoint uses advanced discovery technology, text pattern recognition, and predefined dictionaries to identify this sensitive content, and incorporates device management and encryption for additional layers of control. It works with third-party protection software such as Adobe LiveCycle Rights Management, Microsoft Rights Management Service, Seclore FileSecure, and Titus Message Classification to extend security of your data. Policies and rules can be configured to be applied within the enterprise network, outside it, or both.

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

The current release version introduces McAfee DLP Endpoint for OS X computers. In this release, only a limited version of McAfee® Device Control is supported.

**Contents**

- *How McAfee DLP Endpoint works*
- *Product components and how they interact*
How McAfee DLP Endpoint works

McAfee DLP Endpoint safeguards sensitive enterprise information by deploying policies which are made up of classification rules, protection rules, device rules, and user and group assignments.

McAfee DLP Endpoint monitors policies, and blocks or monitors defined actions containing sensitive content, as required. Alternately, it can encrypt sensitive content before allowing the action to proceed. McAfee DLP Endpoint creates reports for review and control of the process, and can store sensitive content as evidence.

Classify

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

- With text dictionaries
- With text patterns
- By content type
- By location
Location

Locations can be defined according to where the content comes from (for example, the Finance department folder) or where it is being copied to (for example, an unencrypted USB drive.) A special category is the Registered Document Repository.

- **Location from** that is, location-based tagging rules, are not supported in McAfee Device Control.

Content type

Content types include encrypted content, content with specified document properties or file types, or content with tags or content categories.

Specific terms

Dictionaries define lists of sensitive words. For example, to protect private medical information, the HIPAA dictionary lists medical terms that may be required to be kept confidential.

Text patterns

Defined strings, such as Company Confidential, or regular expressions, which can be used to identify credit card numbers or other regular patterns, can be used to classify information.

Email can be classified using the Titus Message Classification application. The Titus classifications are recognized as text patterns which are used to create email protection rules.

- **Titus Message Classification** is not supported in McAfee Device Control.

Classification rules

Classification rules apply content categories based on parsing the content and matching it against predefined patterns or keywords. There are two types of classification rules:

- **Content Classification Rules** — Match content against predefined strings and text patterns or dictionaries.

- **Registered Documents Classification Rules** — Classify all specified content in a defined group of folders.

See also

Create a registered document repository definition on page 96

Track

You keep track of sensitive content by applying a tag or content category to the file containing the sensitive content. 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.

- **Tags and tagging rules** are not supported in McAfee Device Control. Content categories are supported.

Support for persistent tag information

For file systems that do not support EA or ADS, McAfee DLP Endpoint software stores tag information as a meta-file on the disk. The meta-files are stored in a hidden folder named ODB$, which is created automatically by the McAfee DLP Endpoint client software.
Tagging rules

Tagging rules, based on enterprise requirements, identify confidential information and its sources. Data can be classified by:

- **Application** — Application-based tagging rules apply tags generically based on the application or applications that create a file, as specified in application definitions, or based on the file type or file extension.

- **Location** — When files are copied or accessed by local processes, location-based tagging rules apply tags based on the location of the source file. For example, a file being copied locally from a share on a network server.

You can add text patterns and dictionaries to a location- or application-based tagging rule, combining the two types of rules.

In addition to using tagging rules, tags can be applied manually or during the discovery process.

Discovery rules

McAfee DLP Endpoint Discovery is a crawler that runs on managed computers. File system and email storage discovery rules can define the content being searched for, whether it is to be monitored, quarantined, or tagged, and whether evidence is to be stored. File system discovery rules can also be used to encrypt or apply RM policies to files. Settings in the Global Agent Configuration determine where and when the search is performed.

Discovery rules are not supported in McAfee Device Control.

Protect

Protection is defined with device and protection rules that can be filtered by user (application) groups. The rules are applied with policies. Exceptions are defined with whitelists.

Protection rules

Protection rules prevent unauthorized distribution of tagged data. When a user attempts to copy or attach tagged data, protection rules determine whether this should be allowed, monitored, or blocked. In addition to tags and content categories, protection rules are defined with applications or application groups, user assignments, and definitions such as email destinations, document properties, or text patterns.

In McAfee Device Control, only removable storage protection rules are available. In McAfee DLP Endpoint for Mac, no protection rules are available in this release.

Device rules

Device 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 classes and device definitions are used to define device rules.

Assignment groups

Assignment groups apply specific protection rules to different groups, users, and computers in the enterprise.
Policies and policy deployment

A policy is the combination of tagging rules, protection rules, definitions, and assignment groups. Policies are deployed by ePolicy Orchestrator software to the enterprise’s managed computers (computers with McAfee Agent installed).

Whitelists

Whitelists are collections of items that you want the system to ignore. McAfee DLP Endpoint software uses four types of whitelists:

• **Application** — Device rules can block applications run from removable devices. To allow necessary applications such as encryption software, whitelisted application definitions can be created to exempt such applications from the blocking rule. The definitions apply to removable storage devices only.

• **Content** — The whitelist folder contains text files defining content (typically boilerplate) that is not tagged and restricted. The main purpose of this is to improve the efficiency of the tagging process by skipping standard content that does not need to be protected.

• **Plug and Play devices** — Some Plug and Play devices do not handle device management well. Attempting to manage them might cause the system to stop responding or cause other serious problems. Whitelisted Plug and Play devices are automatically excluded when a policy is applied.

• **Printers** — To prevent printing of confidential data, McAfee DLP Endpoint software replaces the original printer driver with a proxy driver that intercepts printing operations and passes them through to the original driver. In some cases printer drivers cannot work in this architecture, causing the printer to stop responding. Whitelisted printers are excluded from the proxy driver installation process.

McAfee Device Control does not support printer definitions or printer whitelists.

Monitor

When the application of a rule blocks, monitors, or causes some other action, an event is generated, sent to the ePolicy Orchestrator Event Parser, and stored in a database. The event can contain evidence of the rule violation. In addition, administrative events are generated by system events such as policy deployment or discovery scans. The policy monitor function includes:

• **Incident monitoring** — The DLP Incident Manager page in ePolicy Orchestrator allows administrators to view agent events and evidence as they are received.

• **Administrative event monitoring** — The DLP Operational Events page in ePolicy Orchestrator 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 ePolicy Orchestrator dashboards.
Product components and how they interact

McAfee DLP Endpoint software consists of several components. Each component plays a part in defending your network from data loss.

Figure 1–2   McAfee DLP Endpoint software

Policy console

The McAfee DLP Endpoint policy console is the interface where the administrator defines and enforces the enterprise information security policy. It is used to create the information security policy and administer the McAfee DLP Endpoint software components.

The McAfee DLP Endpoint policy console is accessed in ePolicy Orchestrator by selecting Menu | Data Protection | DLP Policy.

Event monitoring

DLP monitoring is now a native ePolicy Orchestrator feature. Events generated by DLP policies are now referred to as "incidents" to differentiate them from administrative events generated by ePolicy Orchestrator.

Incidents are displayed on the DLP Incident Manager | Incident List page. DLP events are displayed on the DLP Operational Events List page. These pages are accessed from Menu | Data Protection in ePolicy Orchestrator. All events can be filtered and sorted based on criteria such as protection rules, severity, date, time, user, computer name, or policy version. Events can be labeled by the administrator for tracking purposes.

By defining ePolicy Orchestrator permission sets, you can set incident or event list viewing permissions to assign reviewers to different sets of events. You can have a different reviewer responsible for viewing redacted information.

See also

Create and define permission sets on page 177
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 Endpoint 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 ePolicy Orchestrator Event Parser.

Online/offline operation

Device and protection rules can monitor or protect sensitive data when the managed computer is online, offline, or both. A computer is considered online when it is connected to the ePolicy Orchestrator server.

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. You can view the user sessions on the ePolicy Orchestrator System Tree | DLP User Sessions page.

Event parser

Events generated by the McAfee DLP Endpoint client software are sent to the ePolicy Orchestrator Event Parser, and recorded in tables in the ePolicy Orchestrator 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 Agent Configuration | User Interface Service tab.

On Microsoft Windows computers, the console is activated from the icon in the system tray by selecting Manage Features | DLP Endpoint Console. Fully configured, has four tabbed pages:

- **Events History** — displays events, including details of aggregated events
- **Discovery** — displays details of discovery scans
- **Tasks** — generate ID codes and enter release codes for agent bypass and quarantine
- **About** — information on 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® Endpoint Protection 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.

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

This section describes the options for planning your McAfee DLP product deployment.

It covers differences in McAfee Data Loss Prevention products, recommended installation, and issues of backward compatibility for those upgrading a previous version.

Because McAfee DLP products work with McAfee ePolicy Orchestrator, this section also covers McAfee ePO and Microsoft SQL setup issues, and server configuration for the McAfee DLP product software's requirements.

When you have completed this section, you should be ready to install the McAfee DLP software extension in ePolicy Orchestrator, check the agent package into the McAfee ePO repository, and deploy the client software to your endpoint computers.
Deployment options and scenarios

Classifying corporate information into different data loss prevention categories is a key step in deploying and administering McAfee Data Loss Prevention Endpoint software. 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 ePolicy Orchestrator 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 McAfee Device Control or full McAfee DLP Endpoint versions.

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

For enterprises upgrading older McAfee DLP Endpoint versions, two previous versions of client software are supported in backward-compatible mode.

Contents

- Choosing an endpoint product option
- Recommended installation
- Understanding backward compatibility

Choosing an endpoint product option

McAfee offers two endpoint Data Loss Prevention options: McAfee Device Control and McAfee DLP Endpoint. The two products use the same installed software, and are differentiated by licensing.

Understanding McAfee endpoint DLP options

McAfee DLP software is available in two configurations: a device control-only configuration, and full McAfee DLP. On installation, the McAfee Device Control configuration is activated by default. Changing to the full-featured configuration is accomplished by upgrading the license key in the Help menu.

The current release supports OS X only with the McAfee Device Control option.
What is McAfee Device Control?

McAfee Device Control software prevents unauthorized use of removable media devices, the most widespread and costly source of data loss in many companies today. It is the default configuration on installation.

McAfee Device Control software provides:

- **Persistent content-aware data protection for devices** — Controls what data can be copied to removable devices. 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.

The default installation of McAfee DLP software is for a 90-day trial license for McAfee Device Control software. Upgrade to the full McAfee DLP software configuration by upgrading the license. License options for either version of the software are 90-day trial or unlimited. When upgrading, you do not need to reinstall the software.

> McAfee Device Control for OS X in the current release is limited to removable storage device rules. Content-aware data protection is not currently supported.

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 Prevention 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.

What is the difference between configurations?

The following definitions are turned off (unavailable) in McAfee Device Control software:

- Discovery
- Email Destinations
- File Servers
- Network

- Printers
- Rights Management
- Web Destinations

The following features are unavailable:

- Protection rules (except for removable storage rules)
- Tags and tagging rules
**Recommended installation**

The recommended installation for a simple McAfee Data Loss Prevention Endpoint implementation is on a single server together with McAfee ePolicy Orchestrator software.

For recommendations on whether to use a separate server for the ePolicy Orchestrator database see the ePolicy Orchestrator 4.6 Hardware Sizing and Bandwidth Usage Guide.

![Diagram of McAfee DLP Endpoint components and relationships]

**Figure 2-1  McAfee DLP Endpoint components and relationships**

The recommended architecture includes:

- **ePolicy Orchestrator server** — Hosts the embedded McAfee DLP Endpoint policy console interface and communicates with McAfee Agent software on the endpoint computers

  - In version 9.3 the embedded interface for McAfee DLP Monitor has been replaced with two ePolicy Orchestrator components: DLP Incident Manager and DLP Operational Events. This improves security by eliminating the WCF communications link.

- **McAfee ePO Reports** — A list of McAfee DLP Endpoint Events within the McAfee ePolicy Orchestrator reporting service replaces DLP Reports

- **ePolicy Orchestrator Event Parser** — Communicates with the McAfee Agent and stores event information in a database

- **DLP Event Parser** — Collects McAfee DLP Endpoint events from the ePolicy Orchestrator Event Parser and stores them in DLP tables in the SQL database

- **ePO database** — Communicates with the ePolicy Orchestrator Policy Distributor to distribute policies, and with the DLP Event Parser to collect events and evidence

- **Administrator workstation** — Accesses ePolicy Orchestrator 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 ePolicy Orchestrator server and the McAfee DLP Endpoint client software

---

**Understanding backward compatibility**

To allow an orderly upgrade in large enterprises that have deployed previous versions of McAfee DLP Endpoint in their production environment, an option exists to deploy backward-compatible policies to computers still running the older agents.

Host DLP Agent 9.1 is the earliest version supported by this feature. Enterprises running earlier versions must upgrade to Host DLP Agent 9.1 or later before upgrading to McAfee DLP Endpoint 9.3.

The backward compatibility option that allows communication with both old and new agents has three levels:
  • No compatibility (all endpoints are version 9.3 and later)
  • McAfee DLP Endpoint Agent 9.2 and later
  • McAfee DLP Endpoint Agent 9.1 and later

The agent compatibility option is selected during the McAfee DLP Endpoint policy console initialization. It can be edited at any time from **Tools | Options**.
Planning your deployment

Prepare your environment to install McAfee DLP Endpoint software in ePolicy Orchestrator. Before installing McAfee DLP Endpoint software, configure the ePolicy Orchestrator server and create and configure the repository folders.

When installing ePolicy Orchestrator, consider the following:

- In the ePolicy Orchestrator installation options, we recommend selecting the Install Server and Console option.

- McAfee DLP Endpoint software requires Microsoft SQL Server 2005 or later. When installing on Windows Server 2003, we recommend using the SQL Server 2005 Express installer included in the McAfee ePO installer.

  After verification that you want to install the software, the SQL installation continues without user input. If prompted to install SQL Server 2005 Backward Compatibility, you must install it.

  The preferred option when installing on Windows Server 2008 is to create an ePolicy Orchestrator instance on an existing SQL Server 2005 or 2008 server and select it. We recommend using an SQL Server account. If preferred, an NT account can also be used.

- During the installation, you might see a warning about trusted sites. Write down the recommended additions to the Internet Explorer trusted sites list before clicking OK. You will need to add them later.

  Some of the installation scripts require the NETWORK SERVICE account to have write permission for the C:\Windows\Temp folder. In secure systems, this folder might be locked down. In that case, you must temporarily change the permissions for this folder. Otherwise, the installation fails. We recommend completing all software installations before resetting the permissions.

Roles and permissions

Consider the administrator roles you need to manage the system, and create the necessary user profiles. Roles such as McAfee DLP administrators, policy makers, monitor viewers, manual taggers, and others may be necessary, depending on the size of the system and how centralized you want control to be. The system can be modified at any time, so the list does not have to be comprehensive.

See Chapter 12 Users and permission sets in this guide for more information.

Contents

- Verify the system requirements
- Configure the server
- Working in a cluster environment
- Create and configure repository folders
- Deployment checklist
Verify the system requirements

The following hardware is recommended for running McAfee DLP Endpoint software version 9.3.x for Windows and Mac.

Table 3-1 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 3-2 Operating systems supported

<table>
<thead>
<tr>
<th>Computer type</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>Microsoft Windows operating systems</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2003 Standard (SE) SP1 or later 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2003 Enterprise (EE) SP1 or later 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 Enterprise SP1 or later 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 64-bit</td>
</tr>
<tr>
<td>Endpoint computers</td>
<td>Microsoft Windows operating systems</td>
</tr>
<tr>
<td></td>
<td>• Windows XP Professional SP3 or later 32-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Vista SP2 or later 32-bit only</td>
</tr>
<tr>
<td></td>
<td>• Windows 7 SP1 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows 8 or 8.1 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>File System Discovery Rules and Network Communication Protection Rules are not supported on servers.</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2003 SP2 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2003 R2 SP2 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 SP2 32-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2008 R2 SP1 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 64-bit</td>
</tr>
<tr>
<td></td>
<td>Apple OS X operating systems (McAfee Device Control only)</td>
</tr>
<tr>
<td></td>
<td>• OS X Lion 10.7.5 or later</td>
</tr>
<tr>
<td></td>
<td>• OS X Mountain Lion 10.8.0 or later</td>
</tr>
<tr>
<td></td>
<td>• OS X Mavericks 10.9.0</td>
</tr>
</tbody>
</table>
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 3-3  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, and 7.0</td>
</tr>
<tr>
<td></td>
<td>• VMware View 4.6, 5.0, 5.1, and 5.2</td>
</tr>
<tr>
<td>Remote desktops</td>
<td>• Citrix XenApp 6.0 and 6.5 Feature Pack 2</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 3-4  Server software requirements**

<table>
<thead>
<tr>
<th>Software</th>
<th>Supported versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePolicy Orchestrator</td>
<td>• 4.6 (latest Patch)</td>
</tr>
<tr>
<td></td>
<td>• 5.0.0 or later</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>• 4.6 Patch 3 or later</td>
</tr>
<tr>
<td></td>
<td>• 4.8 or later</td>
</tr>
<tr>
<td>McAfee Agent for Mac</td>
<td>• McAfee Agent for Mac</td>
</tr>
<tr>
<td></td>
<td>• 4.6 Patch 3 or later</td>
</tr>
<tr>
<td></td>
<td>• 4.8 or later</td>
</tr>
<tr>
<td>Microsoft .NET</td>
<td>3.5 SP1, 4.0, or 4.5</td>
</tr>
<tr>
<td></td>
<td><img src="image" alt="Agent handlers on remote servers no longer require the .NET Framework." /></td>
</tr>
<tr>
<td>Microsoft SQL Server</td>
<td>• 2005 or 2008, Advanced Express or Enterprise, 32- or 64-bit</td>
</tr>
<tr>
<td></td>
<td>• 2012 Express or Enterprise, 32-, or 64-bit</td>
</tr>
<tr>
<td>Microsoft SQL Server Management Studio</td>
<td>Install the version that matches the version of Microsoft SQL Server you are using.</td>
</tr>
</tbody>
</table>

The McAfee DLP Endpoint version 9.3.200.x package (DLPE_Package_9_3_200_xx_x.zip) includes the following extensions installed through ePolicy Orchestrator:

- McAfee DLP Endpoint extension version 9.3.200.x
- McAfee Help Desk extension version 2.0
- McAfee DLP Endpoint Help extension module version 9.3.200
- McAfee Help Desk Help extension module version 2.0

The McAfee DLP Endpoint client (McAfee Agent plug-in) includes the files for distributing the client software to endpoint computers from the ePolicy Orchestrator repository: HDLP_Agent_9_3_200_x.zip for Microsoft Windows.
Configure the server

Basic configuration of the McAfee ePO server includes setting the security configuration and verifying the .NET installation.

**Before you begin**
Verify that the server meets the minimum system requirements.

**Task**


2. Install Windows Installer 3.0 (Windows Server 2003) or 4.5 (Windows Server 2008) and restart the system. Install all Microsoft Windows service packs.

3. Run Windows Update and install all patches and updates.

   - In Windows Server 2003, open the Windows Control Panel, then select *Add/Remove Windows Components*.
   - In Windows Server 2008, open the Server Manager, then select *Configure IE ESC in the Security Information* section.

   This Microsoft product can hinder proper installation of McAfee DLP Endpoint components. Disable it before installation, then reconfigure it after installation if it is required.

5. Verify that Microsoft .NET Framework 3.5 SP1, 4.0, or 4.5 is installed.

6. Set the server to a static IP address.

   We recommend using a subnet separate from your company’s production network for initial testing. If you are setting up a production environment, set the server’s static IP address within that range.

**See also**

*Verify the system requirements on page 24*

---

Working in a cluster environment

McAfee DLP Endpoint software provides High Availability for environments running ePolicy Orchestrator in a cluster.

We recommend cluster installation on a Microsoft Windows Server 2008 with Failover Clustering role. Installation on other operating systems has not been tested and is not currently supported.

Before running ePolicy Orchestrator software in a cluster environment, ensure the following:

- Microsoft Failover Clustering is set up and running on a cluster of two or more servers.
- Two separate drives are configured for clustering: a Quorum drive and a Data drive.
- There is a supported database server (SQL Server 2005 or SQL Server 2008) in the network.
- ePolicy Orchestrator is set up according to the McAfee ePolicy Orchestrator cluster installation guidelines. See the McAfee ePolicy Orchestrator product and installation guides for your ePolicy Orchestrator version. Also, consult the KnowledgeBase for updates and specific version information.
Tasks

- **Prepare the cluster on page 27**
  Before running McAfee DLP Endpoint software in a cluster environment, ensure the following.
- **Test the cluster on page 27**
  Cluster installations should be tested before use.

**Prepare the cluster**

Before running McAfee DLP Endpoint software in a cluster environment, ensure the following.

- Microsoft Failover Clustering is set up and running on a cluster of two or more servers.
- Two separate drives are configured for clustering: a Quorum drive and a Data drive.
- There is a supported database server (SQL Server 2005 or SQL Server 2008) in the network.
- ePolicy Orchestrator is set up correctly.

For ePolicy Orchestrator 4.6, see the cluster installation section in the *McAfee ePolicy Orchestrator 4.6 Installation Guide*. The guide can be found at: https://kc.mcafee.com/resources/sites/mcafee/content/live/product_documentation/22000/pd22974/en_us/epo_460_install_guide_en-us.pdf.

**Test the cluster**

Cluster installations should be tested before use.

When the McAfee DLP Endpoint cluster is set up and online, use this task to ensure that it functions in a failover situation.

**Task**

1. Restart the system functioning as the active node.
   The passive node automatically becomes the active node.

2. Log on to McAfee ePolicy Orchestrator, select **Data Protection | DLP Policy**, and click **Apply** to apply the policy.
   If the apply policy screen finishes successfully you can conclude that the McAfee DLP Endpoint cluster has continued to function during the failover.

**Create and configure repository folders**

Repository folders contain information used by the McAfee DLP Endpoint software for creating policies and for reporting.

Two 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 Endpoint Database server, but it is usually convenient to put them there.

We suggest the following folder paths, folder names, and share names, but you can create others as appropriate for your environment.
c:\dlp_resources\
c:\dlp_resources\evidence
c:\dlp_resources\whitelist

• **Evidence folder** — Certain protection rules allow for storing evidence, so you must designate, in advance, a place to put it. If, for example, an email is blocked, a copy of the email is placed in the Evidence folder.

• **Whitelist folder** — Text fingerprints to be ignored by the endpoint software are placed in a whitelist repository folder. An example is standardized text such as disclaimers or copyright. McAfee DLP Endpoint software saves time by skipping these chunks of text that are known to not include sensitive content.

### Configure folders on Windows Server 2008

Configuration of the repository folders on Windows Server 2008 requires specific security settings.

**Before you begin**
Create the evidence and whitelist folders, as described in Before you install the extension.

Both folders are configured in the same manner. Repeat this task for each folder.

**Task**

1. Right-click the evidence / whitelist folder and select **Properties**.
2. Click the **Sharing** tab, then click **Advanced sharing**. Select the **Share this folder** option.
3. Modify **Share name** to evidence$ / whitelist$. Click **OK**.
   - The $ ensures that the share is hidden.
4. Click **Permissions** and select **Full Control for Everyone**. Click **OK** twice.
5. Click the **Security** tab, then click **Advanced**.
6. In the **Permissions** tab, deselect the **Include inheritable permissions from the object's parent** option.
   - A confirmation message explains the effect this change will have on the folder.
7. Click **Remove**.
   - The **Permissions** tab in the Advanced Security Settings window shows all permissions eliminated.
8. Click **Add** to select an object type.
9. In the **Enter the object name to select** field, type **Domain Computers**, then click **OK**.
   - The Permission Entry dialog box is displayed.
10. In the **Allow** column, select:
    - **Create Files/Write Data** and **Create Folders/Append Data** for the evidence folder
    - **List Folder/Read Data** for the whitelist folder
   - Verify that the **Apply onto** option says **This folder, subfolders and files**, then click **OK**.
   - The Advanced Security Settings window now includes Domain Computers.
11. Click **Add** again to select an object type.
12 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 required for the whitelist folder. It is optional for the evidence folder, but can be added as a security precaution. Alternately, you can add permissions only for those administrators who deploy policies.

13 Click OK twice to close the dialog box.

**Configure folders on Windows Server 2003**

Configuration of the repository folders on Windows Server 2003 requires specific security settings.

**Before you begin**

Create the evidence and whitelist folders, as described in Before you install the extension.

Both folders are configured in the same manner. Repeat this task for each folder.

**Task**

1 Right-click the evidence / whitelist folder and select Sharing and Security.

2 In the window that appears, select Share this folder. Modify Share name to evidence$ / whitelist$.

Click OK.

The $ ensures that the share is hidden.

3 Click the Security tab, then click Advanced.

4 In the Permissions tab of the Advanced Security Settings for evidence dialog box, deselect Allow inheritable permissions.

A confirmation message explains the effect this change will have on the folder.

5 Click Remove. The Permissions tab on the Advanced Security Settings dialog box shows all permissions eliminated except administrators.

Setting permissions for administrators is required for the whitelist folder. It is optional for the evidence folder, but can be added as a security precaution. Alternately, you can add permissions only for those administrators who deploy policies.

6 Double-click Administrators entry to open the Permission Entry dialog box. Change the Apply onto option to This folder, subfolders and files. Click OK.

7 Click Add to select an object type.

8 In the Enter the object name to select field, type Domain Computers, then click OK to display the Permission Entry dialog box.

9 In the Allow column, select:
   - Create Files/Write Data and Create Folders/Append Data for the evidence folder
   - List Folder/Read Data for the whitelist folder

Verify that the Apply onto option says This folder, subfolders and files, then click OK.

The Advanced Security Settings dialog box now includes Domain Computers.

10 Click OK twice to close the dialog box.
Deployment checklist

Review your server configuration and ePolicy Orchestrator installation using this checklist.

**Table 3-5 Server configuration**

<table>
<thead>
<tr>
<th>Workflow step</th>
<th>Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Server operating system software installed with McAfee DLP</td>
<td></td>
</tr>
<tr>
<td>Endpoint-supported .NET version</td>
<td></td>
</tr>
<tr>
<td>Microsoft Internet Explorer Enhanced Security, if used, disabled for McAfee DLP</td>
<td></td>
</tr>
<tr>
<td>Endpoint installation, then re-enabled.</td>
<td></td>
</tr>
<tr>
<td>NETWORK SERVICE account permissions altered for McAfee DLP Endpoint installation then restored.</td>
<td></td>
</tr>
<tr>
<td>Repository folders created and shared with correct permissions</td>
<td></td>
</tr>
<tr>
<td>Microsoft SQL Server installed as recommended.</td>
<td></td>
</tr>
<tr>
<td>McAfee ePolicy Orchestrator installed with recommended options.</td>
<td></td>
</tr>
</tbody>
</table>
Installation

This section describes the installation of the McAfee DLP Endpoint extension in ePolicy Orchestrator and deploying the client software to the endpoint computers.

Chapter 4  Installing the McAfee DLP Endpoint software
Chapter 5  Installing a version upgrade
Chapter 6  Deploying McAfee DLP Endpoint
Installing the McAfee DLP Endpoint software

McAfee DLP Endpoint Version 9.3.2 can be installed in ePolicy Orchestrator 4.6, 5.0, or 5.1.

Contents

- Install the McAfee Data Loss Prevention Endpoint extension
- Check in the McAfee DLP Endpoint package to ePolicy Orchestrator

Install the McAfee Data Loss Prevention Endpoint extension

The McAfee DLP Endpoint software extension is installed in ePolicy Orchestrator.

Before you begin

Download the McAfee DLP Endpoint extension from the McAfee download site for McAfee Data Loss Prevention Endpoint software.

The v Help extension module is now bundled in the software extension, and no longer needs to be installed separately.

McAfee DLP Endpoint software does not currently support the McAfee ePolicy Orchestrator 4.6 and 5.x Software Manager feature.

Verify that the ePolicy Orchestrator server name is listed under Trusted Sites in the Internet Explorer security settings.

For option definitions, click ? in the interface.

The default installation is a 90-day license for McAfee Device Control software. If you purchased a license for full McAfee Data Loss Prevention Endpoint software, you must upgrade the license after you complete the installation.

Task

1. In ePolicy Orchestrator, select Menu | Software | Extensions, then click Install Extension.

2. Click Browse and select the McAfee DLP Endpoint .zip file (.\DLPE_package_9_3_200_xx.zip). Click Open, then 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.
The following applications are installed in ePolicy Orchestrator:

- McAfee DLP Endpoint 9.3.200 policy console (in Menu | Data Protection)
- DLP Incident Manager and DLP Operational Events (in Menu | Data Protection)
- DLP Event Parser
- McAfee Help Desk 2.0.0
- McAfee DLP Endpoint and McAfee Help Desk Help Content

4 Click OK.

**Tasks**

- *Initialize the McAfee DLP Endpoint policy console on page 34*
  The first time you open the McAfee Data Loss Prevention Endpoint policy console, a wizard runs for first-time initialization.

- *Upgrade the license on page 36*
  McAfee DLP Endpoint software comes in two versions, McAfee Device Control and full McAfee Data Loss Prevention Endpoint, with two licensing options for each, 90-day trial and unlimited. The default installation is McAfee Device Control with a 90-day trial license.

**Initialize the McAfee DLP Endpoint policy console**

The first time you open the McAfee Data Loss Prevention Endpoint policy console, a wizard runs for first-time initialization.

The wizard can be run at any time by selecting *Initialization Wizard* from the *Tools* menu in the McAfee DLP policy console.

The McAfee DLP Endpoint Management Tools installer and McAfee DLP Endpoint policy console initialization wizard use ActiveX technology. To prevent the installer from being blocked, verify that the following are enabled in Internet Explorer *Tools | Internet Options | Security | Custom level*:

- Automatic prompting for ActiveX controls
- Download signed ActiveX controls

**Task**

1 **In ePolicy Orchestrator, select Menu | Data Protection | DLP Policy.**

   The McAfee DLP Endpoint Management Tools installer runs and, after a brief delay, the *Welcome* window of the *DLP Management Tools Setup* wizard appears. Complete the steps in the wizard.

2 **After the McAfee DLP Endpoint Management Tools installation has completed, the McAfee DLP Endpoint policy console begins loading. If you have an existing policy, you are prompted to convert it to the new format. Click *Convert* and skip to step 4.**

   *McAfee DLP Endpoint version 9.3 adds a number of new text pattern definitions. These are not added to the policy during conversion. To add these new definitions, use the Template Synchronization Wizard.*

3 **If no previous policy exists, the message DLP global policy is unavailable. Loading default policy appears. Click *OK* to continue.**

4 **When the message Agent configuration is unavailable. Loading default agent. appears, click *OK*.**

5 **When the McAfee DLP Endpoint policy console First Time Initialization wizard appears, complete the following steps:**
### Option Description

**1 of 8**  
Click **Next**.

**2 of 8**  
Normally, file system discovery rules give you the option of applying an RM policy, tagging, or quarantining sensitive files. Though we do not recommend it, you can add a **Delete** option by selecting the **Support file system discovery delete** option.

![This option is not available until you update to the full McAfee Data Loss Prevention Endpoint installation.]

For troubleshooting, when you need to review an easily readable version of the policy, select **Generate verbose policy**. For most installations, we recommend leaving these checkboxes deselected.

In very large organizations where the rollout of McAfee DLP Endpoint 9.3 is staged over time, earlier versions of the plug-in need to coexist. Select the appropriate **Backward compatibility mode**:

- No compatibility (all endpoints are version 9.3.200)
- McAfee DLP Endpoint client 9.3 and later
- McAfee DLP Endpoint client 9.2 and later
- McAfee DLP Endpoint client 9.1 and later

Select your directory access protocol: Microsoft Active Directory or OpenLDAP. When using Microsoft AD in very large organizations where search times could be excessive, select **Restrict AD searches to default domain**.

When you have completed all changes, click **Next**.

**3 of 8**  
This step is not available when installing McAfee Device Control.

Type user names for manual tagging authorization, or click one of the buttons to search for user names in Active Directory or Open LDAP (optional). Click **Next**.

![We recommend creating a role-based group such as DLP Manual Tagging Users, and using the group when configuring Access Control.]

**4 of 8**  
Type a password and confirmation (required). McAfee DLP Endpoint software requires strong passwords, that is, at least 8 characters with at least one each uppercase, lowercase, digit, and special character (symbol). If you are upgrading, this is not implemented until you change a password or use a new policy.

If you don't want endpoint key generation events reported to the database, deselect the checkbox. If you want to use short challenge/response (8 digits instead of 16), select the checkbox.

Click **Next**.

**5 of 8**  
Browse to the Whitelist storage share, then click **Next**. The UNC whitelist path is required to apply the policy to ePolicy Orchestrator. Size limits are displayed, but cannot be changed in the Initialization wizard.

**6 of 8**  
Modify the agent pop-up service options (optional). Agent pop-up managed features are displayed, but cannot be changed in the Initialization wizard. Manual/automatic pop-up close and release code lockout policy can be set.

Modify the default notification messages (optional). Select each event type in turn, and type the message in the text field. Click **Next**.
**Option**  **Description**

7 of 8  Browse to the evidence storage share and click Next. The evidence storage path is required to apply the policy to ePolicy Orchestrator. Select a user account and password for copying evidence (optional). Set the required Evidence Replication option. Click Next.

8 of 8  Click Finish.

6  Answer the Apply initial configuration message.
- If you have not skipped any required steps, click Yes and apply the initial policy.
- If you have skipped required steps, click No to complete the initialization.

A password and the evidence storage share are required to complete initialization. The other steps indicated as required are necessary to complete the policy. They can be skipped during initialization and completed at a later time. If you did not apply the policy, select File | Save to save the policy to a file.

7  Click Finish.

**Upgrade the license**

McAfee DLP Endpoint software comes in two versions, McAfee Device Control and full McAfee Data Loss Prevention Endpoint, with two licensing options for each, 90-day trial and unlimited. The default installation is McAfee Device Control with a 90-day trial license.

**Before you begin**

Before starting this task, purchase your upgrade license and get an activation key from your McAfee sales representative.

**Task**

1  In the McAfee DLP Endpoint policy console menu bar, select Help | Update License.

   The View and Update License window displays the current (default) activation key and expiration date.

2  Click Update.

3  Type or paste the activation key Activation Key field and click Apply.

   A warning that you must log on again for the change to take effect appears.

4  Click OK to close the message box, and click Close to close the View and Update License window, then log off ePolicy Orchestrator.

5  Log on to ePolicy Orchestrator to complete the upgrade.

6  From the Agent Configuration menu, select Edit Global Agent Configuration.

   a  In the Evidence tab, set the Storage share.

      A storage share is required for applying the configuration to ePolicy Orchestrator.

   b  In the File Tracking tab, verify the required Operation Mode.

      Device control and full content protection is the default when you upgrade the license.

   c  In the Miscellaneous tab, select the modules you require.

      Do not enable modules you don't use. They increase the McAfee DLP Endpoint agent size and slow its operation unnecessarily.
You can set other options at this time, or accept the defaults and modify the options later.

7 Click **OK**.

8 On the toolbar, click **Apply**.
   
The policy changes are applied to ePolicy Orchestrator.

9 In ePolicy Orchestrator, issue a wake-up call to deploy the policy change to the workstations.

---

**Check in the McAfee DLP Endpoint package to ePolicy Orchestrator**

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 ePolicy Orchestrator infrastructure.

For option definitions, click ?? in the interface.

**Task**

1 In McAfee ePolicy Orchestrator, select **Menu | Software | Master Repository**.

2 In the Master Repository, select **Actions | Check In Package**.

3 Select package type **Product or Update (.ZIP)**, browse to ..\HDLP_Agent_9_3_200_xx.zip, then click **Next**.
   
The **Check in Package** page appears.

4 Review the details on the screen, then click **Save**.
   
The package is added to the Master Repository.
Installing the McAfee DLP Endpoint software
Check in the McAfee DLP Endpoint package to ePolicy Orchestrator
Installing a version upgrade

Upgrading the software has consequences in ePolicy Orchestrator and in the McAfee DLP Endpoint setup.

**Legacy software**

The following programs are no longer used. If these programs appear in *Programs and Features* in Windows Control Panel, remove them.

- McAfee DLP WCF Service
- McAfee DLP Event Collector Service
- McAfee DLP Migration Tool
- McAfee DLP Tools

The McAfee DLP Management Tools program should also be removed before installing an upgrade, as it must be updated every time you update the McAfee DLP Endpoint policy console.

**Event parser**

After upgrading the McAfee DLP Endpoint software suite in ePolicy Orchestrator, you must restart the ePolicy Orchestrator Event Parser using *Administrative Tools | Services*.

![Figure 5-1  Restarting the event parser](image)
Backward compatibility

McAfee DLP Endpoint software version 9.3.x contains several changes that make policies incompatible with earlier versions of the McAfee DLP Endpoint client software. In large enterprises, upgrading McAfee DLP Endpoint on all workstation nodes can take several weeks or even months.

The McAfee DLP Endpoint policy console version 9.3.x initialization has a backward compatibility option that, when selected, allows communication with both old and new clients. Backward compatibility can be set to “no compatibility” (McAfee DLP Endpoint 9.3.200), DLP Agent 9.1 and later, DLP Agent 9.2 and later or DLP Agent 9.3 and later.

Unsupported items

If the policy contains any of the following when backward compatibility mode is selected, the policy fails to be applied to ePolicy Orchestrator. These unsupported items are cumulative, that is, the McAfee Data Loss Prevention Endpoint 9.2 and above section lists Version 9.2 features not supported in Version 9.1. For compatibility with Version 9.1 endpoints, both sections apply.

Table 5-1  Items unsupported in backward-compatible mode

<table>
<thead>
<tr>
<th>Compatibility mode</th>
<th>Unsupported items</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Data Loss Prevention Endpoint 9.1 and later backward compatibility mode</td>
<td>• An application file access, email, file system, removable storage, or web post protection rule contains a document property definition containing a File Name property.</td>
</tr>
<tr>
<td></td>
<td>• An application file access protection rule contains a Store Evidence action.</td>
</tr>
<tr>
<td></td>
<td>• A discovery or protection rule contains a Content Category or Tag Group.</td>
</tr>
<tr>
<td></td>
<td>• An application file access protection rule contains a file type definition.</td>
</tr>
<tr>
<td></td>
<td>• A policy contains an email storage discovery rule.</td>
</tr>
<tr>
<td></td>
<td>• A clipboard rule restricts pasting into all applications.</td>
</tr>
<tr>
<td></td>
<td>• A policy contains a TrueCrypt device rule.</td>
</tr>
<tr>
<td>McAfee Data Loss Prevention Endpoint 9.2 and later backward compatibility mode</td>
<td>• A policy contains a Seclore FileSecure server definition or policy, or a protection rule restricts a rule to Seclore encryption.</td>
</tr>
<tr>
<td></td>
<td>• A policy contains a Fixed Hard Drive or Citrix XenApp device rule.</td>
</tr>
<tr>
<td></td>
<td>• A policy contains a cloud protection rule.</td>
</tr>
<tr>
<td></td>
<td>• A policy contains MTP support (uses the Portable Devices handler)</td>
</tr>
<tr>
<td></td>
<td>• A text pattern definition contains one of the validators introduced in version 9.3.</td>
</tr>
<tr>
<td></td>
<td>• A clipboard protection rule contains an application definition.</td>
</tr>
<tr>
<td></td>
<td>• A removable storage file access rule contains a file extension.</td>
</tr>
<tr>
<td></td>
<td>• A document property definition contains only a file size parameter.</td>
</tr>
</tbody>
</table>

Queries and computer assignments

Queries and Dashboards are saved when you upgrade McAfee DLP Endpoint software, as long as you use the recommended procedure. If you remove the existing Data Loss Prevention extension before installing the new one, all queries and Dashboards are lost.

To customize a sample query, we recommend using the Duplicate option, to rename the query before changing it. To use the new sample queries in My Queries in a Dashboard, use the Make Public option. If a public query exists with the same name, remove or rename the public query first.
ePolicy Orchestrator requires all query names to be unique. The first time you install McAfee DLP Endpoint software in ePolicy Orchestrator, the sample queries are installed as Public Queries. To view this, select Reporting | Queries, and scroll down the queries on the left side of the screen. When you upgrade McAfee DLP Endpoint, ePolicy Orchestrator notices that the names of the sample queries are already used, and installs the samples in My Queries instead. However, to use a query in a Dashboard, it must be a public query.

Contents
- Upgrade McAfee DLP Endpoint software
- Phased upgrade
- Restore the policy after upgrade

Upgrade McAfee DLP Endpoint software
Upgrading an earlier version of McAfee DLP Endpoint software to version 9.3 in ePolicy Orchestrator is similar to a clean installation.

Before you begin
- Back up your policy. In the McAfee DLP Endpoint policy console, use the Save icon (or File | Save) to save the GlobalPolicy.opg file to disk.
- Log off of ePolicy Orchestrator and close the browser window. Uninstall McAfee DLP Endpoint Management Tools from the Windows Control Panel.
- Verify system software requirements for
  - Server and client operating system versions
  - ePolicy Orchestrator and McAfee Agent versions

If you want to view previous events in the DLP Incident Manager, do not remove the existing McAfee DLP Endpoint extension in ePolicy Orchestrator. Removing the extension removes all events from the DLP Database.

Task
1 In ePolicy Orchestrator, select Menu | Software | Extensions.
2 Click Install Extension, then click Browse and select the McAfee DLP Endpoint policy manager option you want to install:
   - HDLP_extension_9_3_200_xxx.zip — installs the McAfee DLP Endpoint Policy, DLP Incident Manager, and DLP Operational Events consoles.
   - DLPE_Package_9_3_200_xxx_1.zip — installs the McAfee DLP Endpoint consoles, McAfee Help Desk, and the related Help modules.
3 Click Open, then click OK twice.
   If you are installing without removing the previous extension, you see a warning that the new extension will replace the existing one. Click OK.
   The extension is installed, and appears in the extension list.
4 Log off of ePolicy Orchestrator, then log on again.
   New features not supported by the previous installed version might not work if you do not do this.

5 In Windows Administrative Tools | Services, verify that McAfee ePolicy Orchestrator Event Parser has the status Started.
   The Event Parser normally starts itself (except when upgrading), but it’s a good idea to check.

Phased upgrade

Successful upgrading to McAfee Data Loss Prevention Endpoint version 9.3.x from an earlier version requires following a phased procedure that takes into account many variables. It also has certain prerequisites that must be met.

Before you begin

Before beginning an upgrade, you must do the following:

• **Verify that all computers are ready for the upgrade.** You can check the client version of computers in the network on the DLP: Status Summary dashboard in McAfee ePolicy Orchestrator. Look on the DLP: Agent version report to make sure that all product versions are McAfee DLP Endpoint 9.1 or later.

  Upgrade all McAfee DLP Endpoint clients to McAfee DLP Endpoint 9.1 or later. Earlier client versions are not supported.
- **Back up the current DLP policy.** Saving the policy to disk allows you to convert the policy to the new format for reuse. You can back up the policy from the McAfee DLP Endpoint policy console. The *Save As* option on the File menu saves the policy in .opg format.

- **Save the agent configuration and computer assignment groups.** You can save the agent configuration and computer assignment groups from the McAfee ePolicy Orchestrator Menu | Policy | Policy Catalog page. Select the product (Data Loss Prevention x.x.0.0) and the category (Computers Assignment Group or Agent Configuration) from the drop-down lists, and edit the selection. From the Edit page, you can select *Save to File* and specify a destination for the backup file.

---

**Policy Catalog**

![Policy Catalog](image)

**Figure 5-2 Saving the agent configuration**

---

**Restore the policy after upgrade**

After upgrading the McAfee DLP Endpoint software, you must restore the DLP policy, computer assignment groups, and agent configurations from your previous installation.

Install and initialize the McAfee DLP Endpoint policy console. See the sections *Upgrade McAfee Data Loss Prevention Endpoint software* and *Initialize the McAfee DLP Endpoint policy console* in this manual. When you have completed the basic installation, continue with this task.

**Task**

1. Restore the policy.
   a. Start the McAfee DLP Endpoint policy console, select *File* | *Open*, and browse to the location where you saved the backup of the previous policy.
   b. When prompted, click *Convert* to convert it.
   c. Select *Tools* | *Options* and verify in the **Backward compatibility mode** section that the required version is selected.
   d. Click *Apply* to save the policy to McAfee ePolicy Orchestrator.
2  Restore the computer assignment groups.
   a  In ePolicy Orchestrator, select Policy | Policy Catalog. From the Product drop-down list, select Data Loss Prevention 9.3.0.0 policies.
   b  From the Category drop-down list, select Computers Assignment Group.
   c  Select Actions | New Policy, type a policy name, and create a new computers assignment group policy.
   d  Click Load from file and browse to the computers assignment group backup file.

![Policy Catalog](image)

Figure 5-3  Restoring the computers assignment group settings

3  Restore the agent configurations.
   a  In ePolicy Orchestrator, select System | Policy Catalog. From the Product drop-down list, select Data Loss Prevention 9.3.0.0 policies.
   b  From the Category drop-down list, select Agent Configuration.
   c  Type a name and create an agent configuration.
   d  Click Load from file and browse to the agent configuration backup file.

See also
Initialize the McAfee DLP Endpoint policy console on page 34
Deploying McAfee DLP Endpoint

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

Contents
- Deploy the client software
- Deploy policies with ePolicy Orchestrator

Deploy the client software

Deploying McAfee DLP Endpoint client software is the final step of software installation, and the first step of policy deployment.

Tasks
- Define a default rule on page 45
  To verify that the McAfee DLP Endpoint software has been deployed properly, we recommend defining a default rule before deploying to the managed computers.
- Deploy McAfee DLP Endpoint client with ePolicy Orchestrator on page 46
  Before policies can be applied, McAfee DLP Endpoint client must be deployed to the endpoint computers by ePolicy Orchestrator.
- Verify the installation on page 47
  After installing McAfee DLP Endpoint software, you should verify the installation in the DLP Operational Events console.

Define a default rule

To verify that the McAfee DLP Endpoint software has been deployed properly, we recommend defining a default rule before deploying to the managed computers.

The rule described is an example of a simple rule that can be used to test the system.

Task
For option definitions, press F1.

1. Create a classification rule:
   a. In the McAfee DLP Endpoint policy console navigation pane under Content Protection, select Classification Rules.
   b. Right-click in the Classification Rules window and select Add New | Content Classification Rule. Rename the rule Email Classification Rule.
   c. Double-click the rule icon to modify the rule.
d In step 1 of the rule creation wizard, select either of the options (ANY or ALL) then scroll down the text patterns list and select Email Address. Click Next three times, skipping to step 4.

e In step 4 of the rule creation wizard, click Add New to create a new category. Name it Email Category, click OK to accept the new category, then click Finish.

f Right-click the rule icon and select Enable.

2 Create a protection rule:
   a In the McAfee DLP Endpoint policy console navigation pane under Content Protection, select Protection Rules.
   
   b Right-click in the Protection Rules window and select Add New | Removable Storage Protection Rule.
   
   c Double-click the rule icon to modify the rule.
   
   d Click through to step 2 of the rule creation wizard and add the Email Category created when creating the classification rule in the Included column.
   
   e Click through to step 7 of the rule creation wizard. Select Monitor, then click Finish.
   
   f Right-click the rule icon and select Enable.

3 From the Tools menu, select Run Policy Analyzer. You should receive warnings, but no errors. If you receive errors, they probably come from improper initialization, such as not specifying an evidence folder or override password. You can rerun the initialization from the Tools menu to correct this.

4 On the toolbar, click Apply. The policy is applied to McAfee ePolicy Orchestrator.

**Deploy McAfee DLP Endpoint client with ePolicy Orchestrator**

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

**Before you begin**

A current version of McAfee Agent must be installed in ePolicy Orchestrator and deployed to the target computers before McAfee DLP Endpoint is deployed. For all Microsoft Windows endpoint computers:

- For ePolicy Orchestrator 4.6, install McAfee Agent 4.6 Patch 3 or later.
- For ePolicy Orchestrator 5.0 and 5.1, install McAfee Agent 4.8 or later.

For all Mac OS endpoint computers, install McAfee Agent for Mac 4.6 Patch 3 or later.

Consult the ePolicy Orchestrator documentation on how to verify the version, and how to install it if necessary.

For option definitions, click ? in the interface.
Task
1. In ePolicy Orchestrator, select Menu | System Tree.

2. In the System Tree, select the level at which to deploy McAfee DLP Endpoint.

   ![Tip]

   Leaving the level at My Organization deploys to all workstations managed by ePolicy Orchestrator.

   If you select a level under My Organization, the right pane displays the available workstations. You can also deploy McAfee DLP Endpoint to individual workstations.

3. Open the Client Task Builder wizard: click the Assigned Client Tasks tab. Select Actions | New Client Task Assignment.

   The Client Task Builder wizard opens.


5. In the Products and Components field, select Data Loss Prevention 9.3.200.xx. The Action field automatically resets to Install.

6. Complete the Task Builder: 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, you should verify the installation in the DLP Operational Events console.

Task
1. Select Menu | Data Protection | DLP Operational Events. Click an event to view the details.

   ![Figure 6-1 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 ePolicy Orchestrator

McAfee DLP Endpoint policies contain definitions, rules, assignment groups and agent configuration. A policy is first applied (saved) to the ePolicy Orchestrator server, then assigned (deployed) to the endpoints.

McAfee DLP Endpoint works with three policies:

- DLPE policy
- Agent configuration
- Computer assignment group

DLPE policy is created in the McAfee DLP Endpoint policy console; agent configuration and computer assignment group are created in ePolicy Orchestrator.

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 an agent bypass or uninstall key. Both the McAfee DLP Endpoint policy console in ePolicy Orchestrator and the DLP Endpoint console on the client computer display the current policy revision numbers.

Before applying a policy, verify that:

- All settings are configured correctly.
- All rules are enabled.
- User assignment groups (where required) are assigned to each rule.
- The agent configuration and the computer assignment groups are assigned to the relevant groups and computers in the ePolicy Orchestrator Policy Catalog.

Tasks

- **Apply the system policy on page 49**
  When a policy is completed, it must be applied to ePolicy Orchestrator. From there, it is deployed to the managed computers that enforce the policy.

- **Assign a policy or agent configuration on page 49**
  Policies applied to ePolicy Orchestrator must be assigned and deployed to managed computers in order to be used.

- **Import policies and editing policy descriptions on page 49**
  Use these tasks to import policies from ePolicy Orchestrator, or to modify policy descriptions.

- **Refresh the policy on page 50**
  Normally, the system policy deployment relies on the ePolicy Orchestrator server, and the policy refresh on the managed computer is performed in accordance with the McAfee Agent settings. Policy refresh can, however, be performed on demand.
Apply the system policy
When a policy is completed, it must be applied to ePolicy Orchestrator. From there, it is deployed to the managed computers that enforce the policy.

Task
1. In ePolicy Orchestrator, select Menu | Data Protection | DLP Policy.
2. Verify the policy before applying it: select Tools | Run Policy Analyzer.

Policies can be applied to ePolicy Orchestrator with warnings, but not if they contain errors. If you see errors, resolve the problem(s) causing the error(s), or customize the policy analyzer options. If you are using the agent backward compatibility option and a policy contains a feature that is unsupported in older agent versions, it will generate an error. See Upgrading issues in this guide for a list of unsupported features.

3. From the McAfee DLP Endpoint policy console File menu, select Apply to ePO. The Applying to ePO window appears.

If you have activated the browser Status Bar, you see the message “Validation succeeded.”

The policy is saved to the ePolicy Orchestrator database, and an administrative event is generated.

Assign a policy or agent configuration
Policies applied to ePolicy Orchestrator must be assigned and deployed to managed computers in order to be used.

For option definitions, click ? in the interface.

Task
1. In ePolicy Orchestrator, click 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.
6. On the Assign Policy page, select the Product, Category, and Policy to be applied.
7. Click Save.

Import policies and editing policy descriptions
Use these tasks to import policies from ePolicy Orchestrator, or to modify policy descriptions.

Tasks
- Import a policy from ePolicy Orchestrator on page 50
  The policy last applied to ePolicy Orchestrator can be imported into the McAfee DLP Endpoint policy console. This is typically done when the policy console is updated, or any time you want to throw away changes and restore an old policy.
- Edit a policy description on page 50
  Policy name and description are editable fields, accessible from the console File menu.
**Import a policy from ePolicy Orchestrator**

The policy last applied to ePolicy Orchestrator can be imported into the McAfee DLP Endpoint policy console. This is typically done when the policy console is updated, or any time you want to throw away changes and restore an old policy.

**Task**

For option definitions, click ? in the interface.

1. From the McAfee DLP Endpoint policy console File menu, select **Import Policy from ePO**.
2. Click Yes in the confirmation window.

**Edit a policy description**

Policy name and description are editable fields, accessible from the console File menu.

**Task**

1. From the McAfee DLP Endpoint policy console menu, select **File | Edit Policy Description**.
2. Edit the policy name and description in the Security Policy window.
3. Click OK.

**Refresh the policy**

Normally, the system policy deployment relies on the ePolicy Orchestrator server, and the policy refresh on the managed computer is performed in accordance with the McAfee Agent settings. Policy refresh can, however, be performed on demand.

Use this task to update a policy in ePolicy Orchestrator without waiting for the scheduled refresh.

**Task**

For option definitions, click ? in the interface.

1. In the ePolicy Orchestrator system tree, 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 ePolicy Orchestrator server. Users of managed computers do not refresh policies manually unless specifically instructed to do so.*
Configuration and use

This section covers system configuration and policy creation.

After installation, the software is configured for optimized use in the enterprise environment. Then, policies are created based on management decisions of what content needs to be protected, and how best to protect it.

For new installations, we recommend an information gathering period, where rules are set to Monitor rather than Block, and data is collected to aid the decision-making process.
Device control is the prevention of unauthorized use of removable media devices to prevent data leaks.

McAfee Device Control is the component of McAfee DLP Endpoint that protects removable media and storage devices. It is sold as a separate product as well as bundled in the McAfee Endpoint Suite. It is currently available for Microsoft Windows and OS X operating systems. The Microsoft Windows version can be upgraded to the full-featured McAfee DLP Endpoint option by upgrading the license. Full McAfee DLP Endpoint protection for OS X is scheduled for a future release.

McAfee Device Control for OS X in the current release is limited to removable storage device rules. Content-aware data protection is not currently supported.

McAfee Device Control can monitor or block devices — such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or Plug and Play devices — attached to enterprise-managed computers, allowing you to monitor and control their use in the distribution of sensitive information. Recent software versions extend this protection to include non-system hard disks. For many organizations, this level of data loss prevention is the primary goal.

### Table 7-1 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.</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 users or user groups.</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 McAfee 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>
</tbody>
</table>
Table 7-1 Terminology (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Applies to operating systems</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unmanaged device</td>
<td>Windows</td>
<td>A device class status indicating that the devices in that class are not managed by McAfee Device Control. New device classes are added to the device class list with this status. A system administrator can change the status to managed.</td>
</tr>
<tr>
<td>Unmanageable device</td>
<td>Windows</td>
<td>A device class status indicating that the devices in that class cannot be managed by McAfee Device Control because attempts to manage them can affect the managed computer, system health, or efficiency. The unmanageable device class list is a closed list that cannot be edited.</td>
</tr>
</tbody>
</table>

Contents

- Categorizing devices with device classes
- Controlling devices with device definitions
- Device rules
- Device parameters

Categorizing devices with device classes

Device classes name and identify the devices used by the system. Each class of devices is identified by a name, an (optional) description, and one or more globally unique identifiers (GUIDs).

Device classes are not supported on OS X.

A *device class* is a collection of devices that have similar characteristics and that can be managed in a similar manner. 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. When you install McAfee DLP Endpoint, you find built-in device classes listed under *Device Management | Device Classes*. The devices are categorized by *status*:

- **Managed** — Specific Plug and Play or removable storage devices, defined by device class, that can be managed by McAfee DLP Endpoint
- **Unmanaged** — Device classes not managed by McAfee DLP Endpoint, but whose status can be changed to *Managed* by the system administrator
- **Unmanageable** — Device classes not managed by McAfee DLP Endpoint because attempts to manage them can affect the managed computer, system health, or efficiency; new classes of devices cannot be added to this list

In day-to-day tasks, the system administrator should not tamper with the device classes list because improper use (for example, blocking the managed computer’s hard disk controller) can cause a system or operating system malfunction.

Instead of editing an existing item to suit the needs of a device protection rule, add a new, user-defined class to the list.
Use case — changing a device class status

When troubleshooting device classes, you might want to change a particular device class status temporarily to **Unmanaged**. To change a device class status between managed and unmanaged, right-click the class icon and select the appropriate status change option.

---

**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.

**Tasks**

- **Obtain a GUID on page 55**
  
  Device class definitions require a name and one or more globally unique identifiers (GUIDs).

- **Create a new device class on page 56**
  
  Device classes name and identify the devices used by the system. Each class of devices is identified by a name, an (optional) description, and one or more globally unique identifiers (GUIDs).

**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 McAfee DLP Endpoint 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, press F1.

1. In ePolicy Orchestrator, open the DLP Incident Manager (Menu | Data Protection | DLP Incident Manager).
2. Click Edit next to the Filter drop-down list to edit the filter criteria.
3. In the Available Properties list, select Event Type.
4 Verify that the **Comparison** drop-down list value is **Equals**.

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

![Figure 7-1 Setting filter criteria](image)

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 new device class**

Device classes name and identify the devices used by the system. Each class of devices is identified by a name, an (optional) description, and one or more globally unique identifiers (GUIDs).

**Before you begin**

Obtain the device GUID before beginning this task.

**Task**

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under **Device Management**, select **Device Classes**.

   The available devices appear in the right pane.

2 Right-click in the **Device Classes** pane and select **Add New | Device Class**.

   A new **Device Class** icon appears (default name **Device Class**) in the unmanaged device class section.

3 Double-click the icon.

   The edit dialog box appears.

4 Type a name, a description (optional), and the device's globally unique identifier (GUID) in the appropriate text boxes.

   **A GUID in the correct format is required. The OK button remains unavailable until you enter a GUID in the correct format.**

5 To move the device to **Managed** status, select the checkbox.

6 Click **OK**.
Controlling devices with device definitions

Device definitions serve as filter criteria for controlling devices, providing the advantage of using portable devices while maintaining the company policy for sensitive information. Built-in definitions for McAfee Endpoint Encryption for Files and Folders and McAfee Endpoint Encryption for Removable Media facilitate the use of those products.

Device definitions control specific devices by fine-tuning the device properties such as the device class, device Product ID/Vendor ID (PID/VID), or USB class code.

Device definition groups can be created as a flexible and accurate way to maintain the required level of security. They combine a different set of properties for each device needing to be blocked or monitored by the system. The device definitions and groups are available for three types. Each type of device definition is matched by a device rule type.

In this release, only removable storage devices are supported on OS X.

- **Plug and Play devices** — Devices that can be added to the managed computer without any configuration or manual installation of DLLs and drivers; Plug and Play devices include most Microsoft Windows devices

- **Fixed Hard Drive devices** — Fixed disk drives attached to the computer and not marked by the operating system as removable storage

- **Removable Storage devices** — External devices containing a file system that appear on the managed computer as drives

Some device properties are the same for Plug and Play and removable storage device definitions, while others are exclusive to the specific device type. Removable storage device definitions are more flexible, and include additional properties related to the removable storage devices. We recommend using the removable storage device definitions and rules to control devices that can be classified as either, such as USB mass storage devices.

Predefined device definitions

In addition to user-defined removable storage devices, three predefined device definitions are included: **All Removable Storage Devices**, **Content encrypted by McAfee Endpoint Encryption**, and **McAfee Encrypted USB Devices**. These can be used in removable storage and removable storage file access rules by selecting the required parameters.

We do not recommend editing the parameter definitions for predefined device definitions.

Whitelisted Plug and Play devices

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 device definitions are added automatically to the excluded list in every Plug and Play device rule. They are never managed, even if their parent device class is managed.

If you inspect the device rules, you do not see the whitelist definition because the definition is not added to the rule until the policy is applied. You do not have to rewrite existing rules to include new whitelisted devices.
Avoiding conflicts in removable storage device definitions

Depending on the parameters specified, a removable storage device definition can be Microsoft Windows-only, OS X-only, or both.

If you add bus properties to a removable storage definition that can be used in either Microsoft Windows or OS X, the definition applies to both.

Adding a Windows-only property (PCMCIA) or a Mac-only property (Thunderbolt) to this definition changes it to a Windows-only or Mac-only definition. If you attempt to add both PCMCIA and Thunderbolt to the same bus properties definition, the software detects a conflict and does not let you create the definition.

Another way of creating a conflict is to create a Mac-only bus type and add a Windows-only property such as PCI Vendor ID/Device ID. As in the previous example, a red conflict notice is displayed and the OK button is not available to save the definition.

Importing device parameters

Device parameters can be entered from lists saved in CSV format.

A device parameter list can be made by selecting multiple events in DLP Incident Manager, then selecting Export Device Incident Parameters from the Actions menu. Lists can also be created manually.

See the online Help for information on formatting the CSV file.
Create device definitions

When you create a device definition with multiple parameters, the parameters defined in each Parameter Name are added to the definition as logical ORs, and multiple Parameter Names are added as logical ANDs.

For example, the following parameter selection creates this device definition:

<table>
<thead>
<tr>
<th>Device definition</th>
<th>Selected parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus Type</td>
<td>Firewire; USB</td>
</tr>
<tr>
<td>Device Class</td>
<td>Memory Devices; Windows Portable Devices</td>
</tr>
</tbody>
</table>

- 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 Plug and Play device definition on page 59**
  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 definitions allow you to manage and control most available devices.

- **Create a whitelisted Plug and Play definition on page 60**
  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 60**
  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.

- **Import device definitions on page 61**
  You can create a device definition by importing parameters from lists saved in CSV format. You can import a new definition from a file, or import a parameter to an existing definition.

- **Import a parameter to an existing device definition on page 62**
  Device parameters can be imported from lists saved in CSV format. You can import a new definition from a file, or import a parameter to an existing definition.

- **Create a device definition group on page 62**
  Device definition groups simplify rules while maintaining granularity by combining several device definitions into one group.

Create a Plug and Play device definition

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 definitions allow you to manage and control most available devices.

Task

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under **Device Management**, select **Device Definitions**.

   The available device definitions and device definition groups appear in the right pane.
In the Device Definitions pane, right-click and select Add New | Plug and Play Device Definition. The new Plug and Play Device Definition icon appears.

3 Name the new device definition and double-click the icon. The edit dialog box appears.

4 Type a description (optional).

5 Select the device parameters from the available list.

6 Click OK.

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, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under Device Management, select Device Definitions. The available device definitions and device definition groups appear in the right pane.

2 In the Device Definitions pane, right-click and select Add New | Whitelisted Plug and Play Device Definition. The new Whitelisted Plug and Play Device Definition icon appears.

3 Name the new device definition and double-click the icon. The edit dialog box appears.

4 Type a description (optional).

5 Select an item from the Parameter Name list. The Edit the definition parameter dialog box opens.

6 Click Add New and type in the parameter information.

7 Click OK twice.

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, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under **Device Management**, select **Device Definitions**.
   
The available device definitions and device definition groups appear in the right pane.

2. In the **Device Definitions** pane, right-click and select **Add New | Removable Storage Device Definition**.
   
The new **Removable Storage Device Definition** icon appears.

3. Name the new device definition and double-click the icon.
   
The edit dialog box appears.

4. Type a description (optional).

5. Select the device parameters from the available list.

6. Click **OK**.

**Import device definitions**

You can create a device definition by importing parameters from lists saved in CSV format. You can import a new definition from a file, or import a parameter to an existing definition.

---

**Before you begin**

Create a device parameter list, one comma-separated row per parameter, and save in CSV format. The list can be made by selecting multiple events from the DLP Incident Manager display and selecting **Actions | Export Device Incident Parameters** on the context menu. You can also use open-source/third-party CSV libraries to create the file.

---

**Task**

1. In the McAfee DLP Endpoint policy console navigation pane under **Device Management**, select **Device Definitions**.
   
The available device definitions and device definition groups appear in the right-hand pane.

2. In the **Device Definitions** pane, right-click and select **Import from file**. Select the type of definition:
   - Plug and Play
   - Removable storage

3. In the **Import From** dialog box, navigate to the CSV file and click **Open**. The parameters are imported to the new device definition.
   
   If the file contains parameters that do not match the type of device definition selected, for example a **File Volume Serial Number** imported into a Plug and Play definition, the definition is ignored and the import continues. If the format is not correct, the import fails.

4. Name the new device definition and click **OK** to create it.
**Import a parameter to an existing device definition**
Device parameters can be imported from lists saved in CSV format. You can import a new definition from a file, or import a parameter to an existing definition.

**Before you begin**
Create a file containing the device definition parameter to import.

**Task**
1. Open an existing device definition by double-clicking on it.
2. Select a parameter to edit. In the parameter definition edit dialog box, click **Import**.
3. In the **Import From** dialog box, navigate to a file and click **Open**. The parameter values are imported to the parameter definition.
4. Click **OK** to accept the changes to the device definition.

**Create a device definition group**
Device definition groups simplify rules while maintaining granularity by combining several device definitions into one group.

**Task**
For option definitions, press F1.
1. In the McAfee DLP Endpoint policy console navigation pane under **Device Management**, select **Device Definitions**.
   The available device definitions and device definition groups appear in the right-hand pane.
2. In the **Device Definitions** pane, right-click and select **Add New** | **Plug and Play Device Definition Group** or **Add New** | **Removable Storage Device Definition Group**.
   The new **Device Definition Group** icon appears.
3. Name the new device definition group and double-click the icon.
   The edit dialog box appears.
4. Type a description (optional).
5. Select the relevant Plug and Play device or removable storage device definition entries from the available list.
6. Click **OK**.

**Device rules**
Device rules define the action taken when particular devices are used.
There are six types of endpoint device rules. Only removable storage device rules are supported on OS X in this release.

- **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 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.
• **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.

**Plug and Play device rules**

Plug and Play device rules are supported on Microsoft Windows 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 — blocking Bluetooth adapters with a Plug and Play device rule

There are three steps to creating a simple Plug and Play device rule to block the use of Bluetooth devices.

1. Verify that the Bluetooth device class is a Managed Device Class.

<table>
<thead>
<tr>
<th>Device Class Name</th>
<th>Type</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed Device Class</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bluetooth Devices</td>
<td>Built-In Device Class</td>
<td>Managed Device Class</td>
</tr>
<tr>
<td>CD/DVD Drives</td>
<td>Built-In Device Class</td>
<td>Managed Device Class</td>
</tr>
<tr>
<td>Floppy Disk Drives</td>
<td>Built-In Device Class</td>
<td>Managed Device Class</td>
</tr>
</tbody>
</table>

2. Create a device definition that matches the properties of the specific Bluetooth devices you want to control.

<table>
<thead>
<tr>
<th>Parameter Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus Type (e.g. USB, PCI)</td>
</tr>
<tr>
<td>Device Class</td>
</tr>
<tr>
<td>Select the bus types</td>
</tr>
<tr>
<td>Bluetooth</td>
</tr>
<tr>
<td>Firewire (IEEE 1394)</td>
</tr>
<tr>
<td>IDE/SATA</td>
</tr>
</tbody>
</table>

3. Create a device rule to include the device definition and set the action to Block.
Removable storage device rules

Removable storage device rules are supported on both Microsoft Windows and OS X computers. Removable storage device rules do not require a managed device class. This is 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 — allow MP3 player as read-only**

Since a managed device class is not necessary, removable storage device rules have two basic steps:

1. Create the device definition.
2. Create the device rule.

Removable storage file access rules

Removable storage file access rules are supported on Microsoft Windows computers only. Removable storage file access rules block removable storage devices from running applications. Because some executables, such as encryption applications on encrypted devices, must be allowed to run, Whitelisted Application definitions can be included in the rule to exempt specifically named files from the blocking rule.

File access rules determine if a file is an executable by its extension. The following extensions are blocked by default: .bat, .cgi, .cmd, .com, .cpl, .dll, .exe, .jar, .msi, .py, .pyc, .scr, .vb, .vbs, .ws, and .wsf. To block files that might be executed from within archives, .cab, .rar, and .zip files are also blocked. In addition, you can add any extension you want to the list.

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 supported on Microsoft Windows computers only. Fixed hard drive rules include a fixed hard drive definition along with an action (Block, Monitor, Notify User, Read Only) and an optional user assignment group.

Citrix XenApp device rules

Citrix XenApp device rules are supported on Microsoft Windows computers only. McAfee DLP Endpoint software can block Citrix devices mapped to shared desktop sessions. Floppy disks, fixed, CD, removable, and network drives can all be blocked, as well as printers and clipboard redirection. The rule can be filtered by adding user assignment groups.

Rules are assigned using computer assignment groups (Menu | Systems | System Tree | Assigned Policies) to Citrix servers. In the System Tree, a new DLP User Sessions tab has been added to the System Information page to view the user sessions and the rules that are applied to each session.
TrueCrypt device rules

TrueCrypt device rules are supported on Microsoft Windows computers only. TrueCrypt device rules are used to block or monitor TrueCrypt virtual encryption devices, or set them to read-only. TrueCrypt rules are a subset of removable storage device rules.

TrueCrypt for OS X is not supported in this release.

TrueCrypt devices can also be protected with removable storage protection rules. See Controlling sensitive content with protection rules in this guide for using protection rules with TrueCrypt devices.

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

Create and define device rules

Create and define device rules to assign actions to device definitions.

Tasks

- Create and define a Plug and Play device rule on page 66

  Plug and Play device definitions are incorporated into Plug and Play device rules to control devices. Plug and Play device rules can be used with Microsoft Windows computers only.

- Create and define a removable storage device rule on page 67

  Removable storage device rules are the recommend way of blocking USB devices. They can be used with either Microsoft Windows or OS X computers or both, depending on the device definitions included in the rule.

- Create and define a removable storage file access rule on page 68

  File access rules block removable storage media from running applications. Whitelisted application definitions specified in step 2 provide lists of specific files that are exempt from the blocking rule. File access rules can be used with Microsoft Windows computers only.

- Create and define a fixed hard drive device rule on page 69

  Fixed hard drive device rules control the copying of sensitive information to local fixed drives, and can set fixed drives to read-only. Dynamic drives are not supported. Fixed hard drive device rules can be used with Microsoft Windows computers only.

- Create and define a Citrix XenApp device rule on page 69

  Citrix XenApp device rules block floppy, CD, fixed, or network drives running in Citrix desktop sessions. Citrix XenApp device rules can be used with Microsoft Windows computers only.

- Create a whitelisted application definition on page 70

  Whitelisted application definitions are used in removable storage file access rules to exempt specifically named files from being blocked. Whitelisted application definitions are used with Microsoft Windows computers only.

Create and define a Plug and Play device rule

Plug and Play device definitions are incorporated into Plug and Play device rules to control devices. Plug and Play device rules can be used with Microsoft Windows computers only.

Task

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane, select Device Management | Device Rules.

   The available device management rules appear in the right-hand pane.
2 In the Device Rules pane, right-click and select Add New | Plug and Play Device Rule.

You can use the Plug and Play device blocking rule to block USB devices, but we recommend using the removable storage device blocking rule instead. Using the Plug and Play device blocking rule can result in blocking the entire USB hub/controller. The removable storage device blocking rule allows the device to initialize and register with the operating system. It also allows you to define the device as read-only.

3 Rename the new device rule and double-click the icon. Follow these steps in the wizard.

Step | Action
--- | ---
1 of 3 | Select one or more Plug and Play device definitions or a group from the available list. You can include or exclude definitions. Click Add item to create a new Plug and Play definition. Click Add group to create a new Plug and Play group. When you have finished, click Next.

2 of 3 | Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text.

3 of 3 (optional) | Select an assignment group or groups, or define a new group by clicking Add. Click Finish.

4 To activate the rule, right-click the rule icon and click Enable.

Create and define a removable storage device rule

Removable storage device rules are the recommend way of blocking USB devices. They can be used with either Microsoft Windows or OS X computers or both, depending on the device definitions included in the rule.

TrueCrypt device rules (Microsoft Windows only) are a essentially a subset of removable storage device rules, with the device definition preset in the rule so that only two steps are required to define a rule.

Task

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane, select Device Management | Device Rules.

The available device management rules appear in the right-hand pane.

2 In the Device Rules pane, right-click and select Add New | Removable Storage Device Rule.

We recommend using the removable storage device blocking rule to block USB devices. While it is possible to use a Plug and Play device blocking rule, this can result in blocking the entire USB hub/controller. The removable storage device blocking rule allows the device to initialize and register with the operating system. It also allows you to define the device as read-only.
3 Rename the new device rule and double-click the icon. Follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 3</td>
<td>Select one or more removable storage device definitions or a group from the available list. You may include or exclude definitions. Click Add item to create a new removable storage device definition. Click Add group to create a new removable storage device group. When you have finished, click Next.</td>
</tr>
<tr>
<td>2 of 3</td>
<td>Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text. Click Next.</td>
</tr>
<tr>
<td>3 of 3 (optional)</td>
<td>Select an assignment group or groups, or define a new group by clicking Add. Click Finish.</td>
</tr>
</tbody>
</table>

4 To activate the rule, right-click the rule icon and select Enable.

Create and define a removable storage file access rule

File access rules block removable storage media from running applications. Whitelisted application definitions specified in step 2 provide lists of specific files that are exempt from the blocking rule. File access rules can be used with Microsoft Windows computers only.

The OS X version of the McAfee DLP client software does not support removable storage file access rules.

For option definitions, press F1.

Task

1 In the McAfee DLP Endpoint policy console navigation pane under Device Management, select Device Rules.

The available device management rules appear in the right-hand pane.

2 In the Device Rules pane, right-click and select Add New | Removable Storage File Access Rule.

3 Rename the new device rule and double-click the icon. Follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 of 4</td>
<td>Select one or more removable storage device definitions or a group from the available list. You may include or exclude definitions. Click Add item to create a new removable storage device definition. Click Add group to create a new removable storage device group. When you have finished, click Next.</td>
</tr>
<tr>
<td>Step 2 of 4</td>
<td>Select the Select from list option, then select file extensions from the available list. Click Next.</td>
</tr>
<tr>
<td>Step 3 of 4</td>
<td>Select a whitelisted application or applications from the available list. Click Add to create a new whitelisted application definition or Edit to modify an existing definition. When you have finished, click Next.</td>
</tr>
<tr>
<td>Step 4 of 4</td>
<td>Select an assignment group or groups, or define a new group by clicking Add. Click Finish.</td>
</tr>
</tbody>
</table>

4 To activate the rule, right-click the rule icon and click Enable.
Create and define a fixed hard drive device rule

Fixed hard drive device rules control the copying of sensitive information to local fixed drives, and can set fixed drives to read-only. Dynamic drives are not supported. Fixed hard drive device rules can be used with Microsoft Windows computers only. System and boot drives are always excluded from fixed hard disk device rules.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane select Device Management | Device Rules. The available device management rules appear in the right-hand pane.

2. In the Device Rules pane, right-click and select Add New | Fixed Hard Drive Rule.

3. Rename the new device rule and double-click the icon. Follow these steps in the wizard.

   **Step** | **Action**
   ---|---
   1 of 3 | Select one or more Fixed Hard Drive device definitions or a group from the available list. You can include or exclude definitions. Click Add item to create a new definition. Click Add group to create a new group. When you have finished, click Next.
   2 of 3 | Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text.
   3 of 3 (optional) | Select an assignment group or groups, or define a new group by clicking Add. Click Finish.

4. To activate the rule, right-click the rule icon and click Enable.

Create and define a Citrix XenApp device rule

Citrix XenApp device rules block floppy, CD, fixed, or network drives running in Citrix desktop sessions. Citrix XenApp device rules can be used with Microsoft Windows computers only. Citrix XenApp device rules cannot be used with organizational units (OUs). If a User Assignment Group (UAG) is chosen that contains an OU, the rule is not enabled.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane select Device Management | Device Rules. The available device management rules appear in the right-hand pane.


3. Rename the new device rule (optional) and double-click the icon. Follow these steps in the wizard.

   **Step** | **Action**
   ---|---
   1 of 2 | Select the storage devices you want to block. When you have finished, click Next.
   2 of 2 (optional) | Select an assignment group or groups, or define a new group by clicking Add. Click Finish.

4. To activate the rule, right-click the rule icon and click Enable.
Create a whitelisted application definition

Whitelisted application definitions are used in removable storage file access rules to exempt specifically named files from being blocked. Whitelisted application definitions are used with Microsoft Windows computers only.

Task
For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under Device Management, select Whitelisted Applications.

   The available whitelisted applications appear in the right-hand pane.

2 Right-click in the Whitelisted Applications pane and select Add New | Whitelisted Application.

   A new whitelisted application icon appears.

3 Double-click the icon.

   The edit dialog box appears.

4 Type a name, a description (optional), and the file name of the executable you want to allow to run in the appropriate text boxes.

5 Click Add to add the file name to the list. Repeat typing and adding file names as required.

6 When you have finished adding file names, click Save.

Device parameters

Device parameters are used to define device definitions

The following table provides definitions for all parameters used in device definitions. It indicates which type of device the parameter is found in and whether it can be imported as a list from a file (see Device definition parameter management.)

Table 7-3  Device definitions for Plug and Play and removable storage devices

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Found in...</th>
<th>Operating system</th>
<th>Import parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bus Type</td>
<td>All</td>
<td>Bluetooth, PCI, PCMI, SCSI – Microsoft Windows only SD, Thunderbolt – OS X only Firewire (IEEE1394), IDE/ SATA, USB – both</td>
<td>Yes</td>
<td>Selects the device BUS type from the available list.</td>
</tr>
<tr>
<td>CD/DVD Drives</td>
<td>RS only</td>
<td>Microsoft Windows OS X</td>
<td>No</td>
<td>Select to indicate any CD or DVD drive.</td>
</tr>
<tr>
<td>Parameter name</td>
<td>Found in...</td>
<td>Operating system</td>
<td>Import parameters</td>
<td>Description</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td>------------------</td>
<td>------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Content encrypted by McAfee Endpoint Encryption for Files and Folders</td>
<td>RS only</td>
<td>Microsoft Windows only</td>
<td>No</td>
<td>Select to indicate a device protected with McAfee Endpoint Encryption for Files and Folders.</td>
</tr>
<tr>
<td>Device Class</td>
<td>PnP only</td>
<td>Microsoft Windows only</td>
<td>No</td>
<td>Selects the device class from the available managed list.</td>
</tr>
<tr>
<td>Device Compatible IDs</td>
<td>All</td>
<td>Microsoft Windows only</td>
<td>Yes</td>
<td>A list of physical device descriptions. Effective especially with device types other than USB and PCI, which are more easily identified using PCI VendorID/DeviceID or USB PID/VID.</td>
</tr>
<tr>
<td>Device Instance ID (Microsoft Windows XP)</td>
<td>All</td>
<td>Microsoft Windows only</td>
<td>Yes</td>
<td>A Windows-generated string that uniquely identifies the device in the system. For example, USB\VID_0930&amp;PID_6533\5&amp;26450FC&amp;0&amp;6.</td>
</tr>
<tr>
<td>Device Name</td>
<td>All</td>
<td>Microsoft Windows OS X</td>
<td>Yes</td>
<td>The name attached to a hardware device, representing its physical address.</td>
</tr>
<tr>
<td>File System Type</td>
<td>RS and Hard disk</td>
<td>HFS/HFS+ – OS X only CDFS, exFAT, FAT16, FAT32, NTFS, UDFS – both</td>
<td>No</td>
<td>The type of file system. For hard disks, select one of exFAT, FAT16, FAT32, or NTFS. For removable storage devices, any of the above plus CDFS or UDFS.</td>
</tr>
<tr>
<td>File System Access</td>
<td>RS only</td>
<td>Microsoft Windows OS X</td>
<td>No</td>
<td>The access to the file system: read only or read-write.</td>
</tr>
</tbody>
</table>
Table 7-3  Device definitions for Plug and Play and removable storage devices (continued)

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Found in...</th>
<th>Operating system</th>
<th>Import parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System Volume Label</td>
<td>RS and Hard disk</td>
<td>Microsoft Windows</td>
<td>Yes</td>
<td>The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.</td>
</tr>
<tr>
<td>File System Volume Serial Number</td>
<td>RS and Hard disk</td>
<td>Microsoft Windows</td>
<td>Yes</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 <code>dir x:</code>, where x: is the drive letter.</td>
</tr>
<tr>
<td>PCI VendorID / DeviceID</td>
<td>All</td>
<td>Microsoft Windows</td>
<td>Yes</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, for example, <code>PCI\VEN_8086&amp;DEV_2580&amp;SUBSYS_00000000&amp;REV_04</code>.</td>
</tr>
<tr>
<td>TrueCrypt devices</td>
<td>RS only</td>
<td>Microsoft Windows</td>
<td>No</td>
<td>Select to specify a TrueCrypt device.</td>
</tr>
<tr>
<td>USB Class Code</td>
<td>PnP only</td>
<td>Microsoft Windows</td>
<td>No</td>
<td>Identifies a physical USB device by its general function. Select the class code from the available list.</td>
</tr>
<tr>
<td>USB Device Serial Number</td>
<td>RS and PnP</td>
<td>Microsoft Windows</td>
<td>Yes</td>
<td>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; for example, USB\VID_3538&amp;PID_0042\0000000002CD8. A valid serial number must have a minimum of 5 alphanumeric characters and must not contain ampersands (&amp;). If the last part of the instance ID does not follow these requirements, it is not a serial number.</td>
</tr>
</tbody>
</table>
| USB Vendor ID / Product ID | RS and PnP | Microsoft Windows | Yes | The USB VendorID and ProductID are embedded in the USB device. These parameters can be obtained from the Hardware ID string of physical devices, for example: USB\VID_3538&PID_0042.`
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.

You can configure and fine-tune these options and components:

- **Agent configuration** — Sends the McAfee DLP Endpoint client software all relevant information about event storage locations, customized user notifications, whitelisted content limitations and locations, file tracing parameters, Microsoft Outlook logon settings, and agent module selections

- **System options** — Allows you to set the policy analyzer settings, system logging options, and system report printing options

### Contents

- Agent configuration
- Configure Safe Mode operation

### Agent 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. Agent configuration is stored in the policy, which is deployed to managed computers.

To define the behavior of McAfee DLP Endpoint software and other system components on managed computers, click **Agent Configuration** on the McAfee DLP Endpoint policy console toolbar. The configuration is stored in the policy, which is deployed to managed computers by ePolicy Orchestrator. If the configuration is updated, the policy needs to be redeployed.

To configure the client software for full protection in Safe Mode, set the functionality in the **Agent Configuration** | **Advanced Configuration** tab. This option is disabled by default.

### Agent 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 **Agent Service WatchDog** (ASWD). This service monitors the McAfee DLP Endpoint software, and restarts it if it stops running for any reason. ASWD is enabled by default. If you want to verify that ASWD is running, look in the Microsoft Windows Task Manager processes for a service named fcagswd.exe.
OS X support for Agent Configuration parameters

Agent 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 8-1  Events and Logging tab**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Operating system support</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative events reported by the agents</td>
<td>The filter settings that apply to both OS X and Microsoft Windows are:</td>
</tr>
<tr>
<td></td>
<td>• Agent Enters Bypass Mode</td>
</tr>
<tr>
<td></td>
<td>• Agent Leaves Bypass Mode</td>
</tr>
<tr>
<td></td>
<td>• Agent Installed</td>
</tr>
<tr>
<td>Logging</td>
<td>Supported on both Microsoft Windows and OS X.</td>
</tr>
<tr>
<td></td>
<td>All other settings apply to Microsoft Windows endpoints only.</td>
</tr>
</tbody>
</table>

**Table 8-2  User Interface Service tab**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Operating system support</th>
</tr>
</thead>
<tbody>
<tr>
<td>DLP Endpoint console</td>
<td>Microsoft Windows only</td>
</tr>
<tr>
<td>Enable end-user notification popup</td>
<td>OS X and Microsoft Windows</td>
</tr>
<tr>
<td>Customize Bypass Screen</td>
<td>OS X and Microsoft Windows</td>
</tr>
<tr>
<td>Release code lockout policy</td>
<td>OS X and Microsoft Windows</td>
</tr>
<tr>
<td>Agent Notification Messages</td>
<td>Device management event — OS X and Microsoft Windows</td>
</tr>
<tr>
<td></td>
<td>all other messages — Microsoft Windows only</td>
</tr>
</tbody>
</table>

Apply the global agent configuration

Global agent configuration is applied from the McAfee DLP Endpoint policy console.

**Task**

- From the McAfee DLP Endpoint policy console menu bar, select Agent Configuration | Apply Global Agent Configuration.

  The Agent Configuration progress bar window appears as the configuration is applied to ePolicy Orchestrator.

Import the global agent configuration

Importing the global agent configuration is performed from the McAfee DLP Endpoint policy console.

**Task**

1. Select Agent Configuration | Import Global Agent Configuration from ePO.

2. Click Yes to confirm.
**Reset the Agent Configuration values**
Agent Configuration values are set from the McAfee DLP Endpoint policy console.

**Task**
1. From the Agent Configuration menu, select Reset Agent Configuration values.
2. Click Yes to restore default settings.

---

**Configure Safe Mode operation**
McAfee DLP Endpoint software is fully functional when the computer is started in Safe Mode. Functionality is disabled by default, but can be activated in the Agent Configuration | Advanced Configuration tab.

An administrative event, User Logged Into Safe Mode, can be displayed in the DLP Operational Events console by selecting an option in the Agent Configuration | Events and Logging tab.

**Task**
For option definitions, press F1.
1. From the McAfee DLP Endpoint policy console, select Agent Configuration | Edit Global Agent Configuration.
2. Click the Advanced Configuration tab.
3. Select Activate DLP full functionality in safe mode and change the setting to Enabled.
   Full McAfee DLP Endpoint functionality is now available in Safe Mode, not just the Watch Dog, as in previous versions. There is a recovery mechanism in case McAfee DLP Endpoint is the cause of the boot failure.
4. Click OK.
Configuring system components
Configure Safe Mode operation
McAfee DLP Endpoint software gives you several ways of classifying sensitive content. The different classifications help you create granular tagging and protection rules to control different content in different ways.

Contents

- Classifying by content
- Classifying by file location
- Classifying by file destination
- Classification in use
- Classification rules

Classifying by content

Documents can be classified by defining the sensitive content you need to protect, or by document properties.

Using dictionaries to classify content

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

The difference between a dictionary entry and a string in a text pattern definition is the assigned weight. A string text pattern tagging rule always tags the document if the phrase is present. A dictionary tagging rule gives you more flexibility because you can set a threshold, which makes the rule relative. The assigned weights can be negative or positive, which allows you to look for words or phrases in the presence of other words or phrases.

In addition to the ability to create your own dictionaries, McAfee DLP Endpoint software comes with several built-in dictionaries with terms commonly used in health, banking, finance, and other industries.

Dictionaries can be created (and edited) manually or by copying and pasting from other documents.

Limitations

This section describes the design of the dictionary feature and some limitations this design entails. Dictionaries are saved in Unicode (UTF-8), and therefore can be written in any language. The following descriptions are specifically for dictionaries written in English. Other languages should behave in a similar manner, but there may be unforeseen problems in certain languages.
Dictionary matching has the following characteristics:

- It is not case-sensitive.
- It can optionally match substrings or whole phrases.
- It matches phrases including spaces.

If substring matching is specified you should use caution when entering short words because of the potential of false positives. For example, a dictionary entry of "cat" would flag both "cataracts" and "duplicate." To prevent false positives of this type, use the whole phrase matching option, or use statistically improbable phrases (SIPs) to give the best results. Another source of false positives is similar entries. 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 gets two hits — one for each entry — skewing the total score.

Create a dictionary
Dictionary definitions are used to define content classification rules.

**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under **Content Based Definitions**, select **Dictionaries**.
   The available dictionaries appear in the right-hand pane.

2. In the **Dictionaries** window, right-click and select **Add New | Dictionary**.
   A new **Dictionary** icon appears.

3. Name the new dictionary and double-click the icon.

4. (Optional) Enter an optional description.

5. To create a new entry:
   - Click **Add** to create a new text box. Type the new word or phrase in the text box.
     The default weight is added as "1".
   - To change the default weight, select the number and edit.

6. If you want to import entries from other documents:
   - Single entry — Click **Import Entries**
   - Multiple entries — Set up a source document with one entry per line separated by a single carriage return
     A text window opens that allows you to copy and paste entries. The text window is limited to 10,000 lines of 50 characters per line.

7. Select the **Count multiple entries** checkbox to have each appearance of a term contribute to the total score.
   Default behavior is for a term to be counted only once, no matter how many times it appears in the document.

8. Deselect the **Match whole phrase only** option if you want to match substrings.
   Default behavior is to match whole phrases only because this tends to reduce false positives.
Classifying content with document properties or file extensions

Document property definitions classify content by predefined metadata values. File extension definitions classify content by filename extension.

Document properties

Document properties can be retrieved from any Microsoft Office document. They are used in protection rules as well as discovery rules. The Date Created property has both exact and relative date options (document is stored more than X days.)

For most properties, partial matching is permitted. This feature appears in the McAfee Device Control version of the software, where it is an optional filter in removable storage protection rules, as well as the full McAfee DLP Endpoint version. It is also included as a tab in the template synchronization wizard. There are three types of document properties:

- **Predefined properties** — Standard properties such as author and title.
- **User-defined properties** — Custom properties added to the document metadata allowed by some applications such as Microsoft Word. A user-defined 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.

The Filename document property is applicable to all file types, not just Microsoft Office documents. It is exact match by default, but can be set to partial match.

File extensions

File extension definitions are used in protection, discovery, and tagging rules to increase granularity. A predefined list of extensions is included, and new definitions can be added. File extension groups can be used to simplify rules by defining, for example, all graphic file formats as a single definition.

Text pattern definitions

Tagging rules and content classification rules use text patterns to classify data according to specific words or patterns. They can identify known strings, such as Company Classified or Internal Use Only, or regular expressions (Regex), which allow complex pattern matching, such as in social security numbers or credit card numbers.

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

Text patterns can include a validator — an algorithm used to test regular expressions. Use of the proper validator can also significantly reduce false positives.

Text patterns can be marked as sensitive. Files containing sensitive patterns are encrypted in hit highlighted evidence.

If multiple text patterns are used for matching similar content, text pattern groups can be used to associate multiple patterns to a single group. This simplifies the creation of content categories if you defined many text patterns.

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.
Classifying content with text patterns

Text patterns can be used as individual definitions or as text pattern groups. McAfee DLP Endpoint software has a feature that tests text patterns for accuracy before they are used.

Use these tasks to classify content with text patterns.

**Tasks**

- *Create a text pattern on page 80*
  Text patterns can be used to define content classification rules. A text pattern definition can consist of a single pattern or a combination of included and excluded patterns.

- *Test a text pattern on page 82*
  Before using a text pattern in a rule you should test it to see that it identifies the text you want and does not give false positives.

- *Create a text pattern group on page 83*
  Text pattern groups can be created from existing text patterns. Using text pattern groups simplifies rules when multiple text patterns are required while maintaining the granularity of separate text patterns.

**Create a text pattern**

Text patterns can be used to define content classification rules. A text pattern definition can consist of a single pattern or a combination of included and excluded patterns.

Many, but not all, text 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, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Content Based Definitions, select Text Patterns.

   The available text patterns appear in the right-hand pane.

2. In the Text Patterns window, right-click and select Add New | Text Pattern.

   A new text patterns icon appears.
3 Name the new text pattern and double-click the icon.

![Credit Card Number (Visa) dialog box](image)

**Figure 9-1** Text pattern dialog box

4 Add a description (optional).

5 Under **Included Patterns**, do the following:
   a Select the pattern recognition method (**All** or **Any** patterns).
   b Click **Add** to define the new pattern, then type the text string.
      If you have text patterns stored in an external document, you can copy-paste them into the definition with **Import Entries**.
   c Select **Is Regex** if the string is a regular expression.
   d If you select **Is Regex**, select an appropriate validator (optional). The default is **No Validation**.
   e Under **Threshold**, type the number of times the pattern must be found in the data for it to be considered a match. For example, finding one credit card in an email may be acceptable, but adding a threshold of 5 requires five or more matches of the credit card pattern.

6 Under **Excluded Patterns**, do the following:
   a Click **Add** to add an exclusion pattern, then type the text strings that, when found, are ignored by the system.
   b Select **Is Regex** if the string is a regular expression.
   c If you select **Is Regex**, select an appropriate validator (optional). The default is **No Validation**.
d Under Threshold, add the number of times the pattern must be found to be considered a match.

e Click OK.

**Test a text pattern**
Before using a text pattern in a rule you should test it to see that it identifies the text you want and does not give false positives.

**Before you begin**
Create a new text pattern definition, or add a new item to an existing definition. You do not have to save the definition before testing.

**Task**
For option definitions, press F1.

1 In the text pattern definition, click the Edit button ( ) of the item to be tested. The test dialog box appears with the search text or regular expression in the **Pattern** text box.

2 If applicable, select the **Regular expression** checkbox and select a validation method from the drop-down list.

3 Type some test patterns in the **Test** text box and click **Check**. The matches and validated matches are displayed.

4 If results are unacceptable, modify the text pattern and retest. When you click **OK** the text pattern in the definition is modified to match the last pattern you tested.
Create a text pattern group
Text pattern groups can be created from existing text patterns. Using text pattern groups simplifies rules when multiple text patterns are required while maintaining the granularity of separate text patterns.

Task
For option definitions, press F1.
1 In the McAfee DLP Endpoint policy console navigation pane under Content Based Definitions, select Text Pattern.
   The available text patterns and groups appear in the right-hand pane.
2 In the Text Patterns window, right-click and select Add New | Text Pattern Group.
   The new Text Pattern Group icon appears.
3 Double-click the icon.
   The edit window appears.
4 Name the new text pattern group.
5 Type a description (optional).
6 Select the text patterns from the available list.
7 Click OK.

Integrate Titus Message Classification software with text patterns
Specific text patterns are required to define an email protection rule that recognizes Titus classifications.

Before you begin
Integration is enabled or disabled in the Agent Configuration | Advanced Configuration tab.

Titus Message Classification for Microsoft Outlook is a widely used email solution that ensures every email is classified and protectively marked before it is sent. McAfee DLP Endpoint software can integrate with Titus and block emails based on Titus classifications.

The McAfee DLP Endpoint client software determines if an email has been classified by Titus (to reduce false positives), and what the classification is. You use both of these strings to define the protection rule.
Task
For option definitions, press F1.

1  In the McAfee DLP Endpoint policy console navigation pane under **Text Patterns**, create the text pattern `TLPropertyRoot=[Organization Name]`.

   The Organization Name must match the name from the Titus Message Classification Administration Tool **License Info** page.

   ![This is the string used to reduce false positives.]

   For example, for the McAfee implementation of Titus Message Classification, we create the text pattern:

   ![Include content which matches the following patterns:](image)

   ![Recognize pattern if ALL of the following patterns are matched](image)

     | Text                      | Is Regex | Validator | Threshold | Edit |
     |---------------------------|----------|-----------|-----------|------|
     | TLPropertyRoot=McafeeSIA |          |           |           |      |

2  Create the text pattern `Classification=[Titus classification]`.

   For example, if you want to block emails based on the Titus classification *Confidential*, create the text pattern `Classification=Confidential`.

   Repeat this step, creating a text pattern for each Titus classification you want to add to the email protection rule.

   ![You can combine the text patterns into a text pattern group.]

3  Define a classification rule using the text patterns or text pattern group with the Titus strings.

   McAfee DLP Endpoint client considers the Titus classification to be part of the body, so you can select **Scan body** in step 3 of the **Content Classification Rule** wizard.

   The rule creates a content category based on the Titus classification, if you have not already created one.

4  Include the content category in the email protection rule (step 2 of the **Email Protection Rule** wizard).

**Whitelist**

The whitelist is a shared folder containing files that McAfee DLP Endpoint software references when tagging or categorizing data. The files define text that is ignored by the McAfee DLP Endpoint tracking mechanism. This allows users to distribute standard content that would otherwise be tagged or categorized and restricted by the system.

A typical use for the whitelist is to define text that is often added to documents, such as a disclaimer, license and trademark attributions, or copyright notes.
To use the whitelist, a file share must be created with read-only access by the group domain computers. See the Installation Guide for instructions. The file share must be defined in the agent configuration options.

Each file in the whitelist folder must contain at least 400 characters for it to be ignored by the system. If a file contains both tagged or categorized data and whitelisted data, it is not ignored by the system. However, all relevant tags and content categories associated with the content remain in effect.

Some files in the whitelist folder might not be added to the policy distribution because of configuration. These files are listed in the Warning tab when you select Tools | Run Policy Analyzer.

Add new whitelist content
To save time parsing documents, place standard text such as disclaimers in the whitelist folder.
For option definitions, click ? in the interface.

**Task**
1. Create a file containing only the text you want to add to the whitelist, and copy it to the Whitelist folder.
2. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Whitelist. The available whitelist files appear in the right-hand pane.
3. Right-click in the Whitelist window and click Refresh. The window is updated with the latest list of files.

Delete whitelist files
Content that is no longer relevant should be removed from the whitelist folder.
For option definitions, click ? in the interface.

**Task**
1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Whitelist. The available whitelist files appear in the right-hand pane.
2. Select the file to remove from the whitelist folder, right-click, and select Delete.
3. Click Yes to confirm the deletion.
4. Click OK.

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 Discover finds your data-at-rest. It can search for content in endpoint computer files or email storage (PST, mapped PST, and OST) files.
How discovery scanning works

McAfee DLP Discover scans are used to locate data-at-rest. There are currently two versions of the Discover software: network and endpoint. This document describes the endpoint version.

McAfee DLP Discover is a crawler that runs on client computers. When it finds predefined content, it can monitor, quarantine, tag, or apply an RM policy to the files containing that content. McAfee DLP Discover can scan computer files or email storage (PST, mapped PST, and OST) files. Email storage files are cached on a per-user basis.

At the end of each discovery scan, the McAfee DLP Endpoint client sends a Discovery Summary event to the DLP Operational Events console in ePolicy Orchestrator 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. To use this feature, you must enable the Discovery Summary Report on the Agent Configuration | Events and Logging tab.

When can you search?

Scheduling is set in the Agent Configuration dialog box. 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?

There are two ways to define sensitive content.
• Using tags or content categories. Categories match specific text patterns, dictionaries, or registered documents repositories to the files. Tags define files in specified locations or produced with specified applications.

If no tag or category is defined, a document property is required. The new document property **filename** allows this option for any file type, not just Microsoft Office files.

• Using file context. You can specify file types, file extensions, document properties, encryption type, and user assignment in the discovery rule.

**What happens to discovered files with sensitive content?**

You can apply RM protection (file system discovery only), encrypt, monitor, quarantine, or tag the files. RM protection, encryption, and quarantine are mutually exclusive. Monitoring and tagging can be added to other actions. When you monitor, you can also choose to store evidence.

A setting in the **Tools | Options | General** tab allows you to delete files instead of quarantining them. This option was requested by a specific customer. For general use, we do not recommend using this option.

**Find content with the McAfee DLP Discover crawler**

Use these tasks to set up and run the discovery crawler.

There are three steps to running the discovery crawler. They can be done in any order.

• Create and define a discovery rule.

• Set up the scan parameters.

• Set the scheduling.

**Tasks**

• **Create and define a file system discovery rule on page 87**
  File system discovery rules define the content the McAfee DLP Discover crawler searches for, and what to do when this content is found.

• **Create and define an email storage discovery rule on page 89**
  McAfee DLP Discover can find sensitive content in email storage (PST, mapped PST, and OST) files. The crawler scans email items (body and attachments), calendar items, and tasks. It does not scan public folders or sticky notes. Actions are limited to Monitor, Quarantine, Store Evidence, and Tag.

• **Set up a McAfee DLP Discover scan on page 90**
  McAfee DLP Discover scans are first defined, then scheduled, using the **Agent Configuration** menu.

• **Schedule a McAfee DLP Discover scan on page 91**
  McAfee DLP Discover scans are first defined, then scheduled, using the **Agent Configuration** menu.

• **Restore quarantined files or email items on page 92**
  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 file system discovery rule**

File system discovery rules define the content the McAfee DLP Discover crawler searches for, and what to do when this content is found.

Changes to a discovery rule take effect as soon as the policy is deployed. Even if a scan is in progress, a new rule takes effect immediately.
You can specify a document property instead of a tag or content category. Either is valid. A new action allows matched files to be tagged. Tagging is additive to other selected actions.

When excluding tags or content categories in discovery rules, the exclude rule works relative to the include rule. You must include at least one tag or content category to exclude any other tags or content categories.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection** | **Discovery Rules**. The available discovery rules appear in the right-hand pane.

2. In the **Discovery Rules** pane, right-click and select **Add New** | **File System Discovery Rule**.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

   **Step**  |  **Action**
   --------  |  --------
   1 of 7 (optional)  |  Select the **Select from list** option, then select file types from the available list. Use the **Other File Types** option to select unlisted (unknown) file types. Click **Next**.
   2 of 7 (optional)  |  Select the **Select from list** option, then select file extensions from the available list. Default exclusions are: .avi, .bmp, .exe, .gif, .jar, .jpeg, .jpg, .mkv, .ico, .mp3, .mpeg, .png, .mov, .tif, and .tiff. Click **Next**.
   3 of 7 (required*)  |  Select tags, content categories, and groups to be included or excluded from the rule. Click **Add item** to create a new tag or content category. Click **Add group** to create a new tag and content category group. Click **Next**.
   4 of 7 (required*)  |  Select an existing document property definition or group by selecting one of the checkboxes to indicate whether the definition is included or excluded. Click **Add item** to create a new document property definition, or **Add group** to create a new group. Click **Next**.
   5 of 7 (optional)  |  Select the **Select from list** option, then select an encryption type.
   6 of 7 (required)  |  Select actions from the available list.
   |  - **Apply RM Policy**: Click **Select RM Policy** to select an RM Policy and the server where it is located.
   |  - **Encrypt**: Click **Select an Encryption key** to select an encryption key or add a new key.
   |  - **Monitor**: Click **Severity** to modify the value.
   |  - **Quarantine**
   |  - **Store Evidence**: Linked to **Monitor**. (If you did not select **Monitor**, it is selected automatically.)
### Step Action

- **1 of 7 (optional)** Select the Select from list option, then select file types from the available list. Use the Other File Types option to select unlisted (unknown) file types. Click Next.

- **2 of 7 (optional)** Select the Select from list option, then select file extensions from the available list. Click Next.

- **3 of 7 (required)** Select tags, content categories, and groups to be included or excluded from the rule. Click Add item to create a new tag or content category. Click Add group to create a new tag and content category group. Click Next.

---

**Apply RM Policy, Quarantine, and Encrypt** are mutually exclusive actions; selecting one deselects the others. Other actions are additive.

- If you select Apply RM Policy and the specified RM policy cannot be applied, the content is monitored. If you select Encrypt and McAfee Endpoint Encryption for Files and Folders is not installed, the content is quarantined.

- If you select the Support file system discovery delete option in Tools | Options, the Delete action appears, and can be used instead of Encrypt or Quarantine. We do not recommend activating the discovery delete option.

---

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Discovery Rules. The available discovery rules appear in the right-hand pane.

2. In the Discovery Rules pane, right-click and select Add New | Email Storage Discovery Rule.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 7 (optional)</td>
<td>Select the Select from list option, then select file types from the available list. Use the Other File Types option to select unlisted (unknown) file types. Click Next.</td>
</tr>
<tr>
<td>2 of 7 (optional)</td>
<td>Select the Select from list option, then select file extensions from the available list. Click Next.</td>
</tr>
<tr>
<td>3 of 7 (required)</td>
<td>Select tags, content categories, and groups to be included or excluded from the rule. Click Add item to create a new tag or content category. Click Add group to create a new tag and content category group. Click Next.</td>
</tr>
</tbody>
</table>

---

Task

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Discovery Rules. The available discovery rules appear in the right-hand pane.

2. In the Discovery Rules pane, right-click and select Add New | Email Storage Discovery Rule.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 7 (optional)</td>
<td>Select the Select from list option, then select file types from the available list. Use the Other File Types option to select unlisted (unknown) file types. Click Next.</td>
</tr>
<tr>
<td>2 of 7 (optional)</td>
<td>Select the Select from list option, then select file extensions from the available list. Click Next.</td>
</tr>
<tr>
<td>3 of 7 (required)</td>
<td>Select tags, content categories, and groups to be included or excluded from the rule. Click Add item to create a new tag or content category. Click Add group to create a new tag and content category group. Click Next.</td>
</tr>
</tbody>
</table>
**Step**  
**4 of 7 (required*)** Select an existing document property definition or group by selecting one of the checkboxes to indicate whether the definition is included or excluded. Click Add item to create a new document property definition, or Add group to create a new group. Click Next.

**5 of 7 (optional)** Select the Select from list option, then select an encryption type.

**6 of 7 (required)** Select actions from the available list.
- **Monitor**: Click Severity to modify the value.
- Quarantine
- Report in DLP Endpoint Console
- **Store Evidence**: Linked to Monitor. (If you did not select Monitor, it is selected automatically.)
- **Tag**: Click Select a tag. The tag you use must be predefined. There is no option for adding a tag.

Click Next.

**7 of 7 (optional)** Select an assignment group or groups, or define a new group by clicking Add. Click Finish.

(required*) means that at least one of the properties must be defined.

To activate the rule, right-click the discovery rule icon and select Enable.

If you leave a rule disabled, Apply the rule to the database, and deploy it to agents, the disabled status will terminate any email discovery rule that is running.

### Set up a McAfee DLP Discover scan

McAfee DLP Discover scans are first defined, then scheduled, using the Agent Configuration menu. Changes in discovery setting parameters take effect on the next scan. They are not applied to scans already in progress.

### Task

For option definitions, press F1.

1. **In the Agent Configuration | Discovery settings tab**, set the performance parameters.

   Use the pause controls to minimize the impact of the scan on system performance. The options are:
   - **Suspend scan when the system’s CPU is above (%)**
   - **Suspend scan when the system’s used RAM is above (%)**
   - **Do not scan files larger than (MB)**

   Most files of interest are small. Skipping large files can significantly shorten the scan time.
2 Set the notification details.

File and email storage notification details are set separately.

When the Quarantine action is selected in a discovery rule, discovery removes files with sensitive content to the quarantine folder. If no notifications are set, users might wonder why their files disappeared. The notification feature replaces files with stand-in files with the same name containing the notification text. If the discovery rule is set to encrypt files, no notification is needed because the files remain in place.

To get files out of quarantine, users must request a quarantine release key from the administrator. This works in a similar manner to the agent override key. To unlock encrypted files, users must have the encryption key specified in the discovery rule.

The default path for the quarantine folder is now %USERPROFILE%\McAfee DLP Quarantined Files. We recommend using only this default folder, as accidental file deletion has occurred in other scenarios.

3 Select the folders to scan and the folders to skip.

   a Click Edit in the Folders section.

   b Use Windows Explorer to browse to a folder.

   c Copy and paste the address into the Enter folder text box.

   d Use the plus icon to add the folder to the scan list; Use the minus icon to remove folders.

   If you don't specify any folders for either scan or skip, all folders on the computer are scanned except C:\Windows, C:\Program Files, and the McAfee DLP Endpoint quarantine folder. The following file types will always be skipped, no matter which folder they are in:

   • The specific files ntldr, boot.ini, and .cekey
   • Executable files (*.com, *.exe, *.sys)

4 Select the email storage types to be scanned. Select the email folders to scan and the folders to skip.

   When Microsoft Outlook is running in non-cached Exchange mode, OST files are not present and cannot be scanned. If you create a shared mailbox when running in non-cached Exchange mode (OST mailbox) McAfee DLP Endpoint recognizes it as a Mapped PST mailbox. You must, therefore, specify Mapped PST as a storage type in the discovery rule to scan the mailbox.

**Schedule a McAfee DLP Discover scan**

McAfee DLP Discover scans are first defined, then scheduled, using the Agent Configuration menu. The discovery scan scheduler is in the Agent Configuration | Discovery Settings dialog box.

**Task**

For option definitions, press F1.

1 In the Agent Configuration | Discovery Settings tab, click the File system scan schedule button ( ). Alternately, to schedule a mail storage scan, click the PST and OST scan schedule icon.

   A pop-up window appears.
2 Set the time of day for the scan to start using the thumbwheel.

3 Set the scanning frequency using the option buttons and checkboxes.

4 If you want to run a discovery scan immediately, select Run now.

5 If you want to prevent runs being missed because of the user being logged off, select Resume discovery missed runs after login.

6 Set the start and end dates for discovery scans.

**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 Agent Configuration | Miscellaneous.

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 Discover software attaches a prefix to the Outlook Subject to indicate to users that their emails have been quarantined. Emails can have either the email body or attachments or both quarantined. If the body is quarantined, the replacement text appears in the body, and the body text appears as an encrypted attachment.

Microsoft Outlook calendar items and tasks can also be quarantined.

![Figure 9-4 Quarantined email example](image)

**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 Manual Decryption.
   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).

   i. 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

Defining network file shares
The file server list is a list of file shares used for location-based tagging rules.
The file server list is created by an LDAP query or network scan. Define the network servers that are used in location-based tagging rules. If a server doesn’t contain a file share used for a location-based tagging rule, you don’t need to include it in this list.

Create a file server list
The file server list is a list of file shares used for location-based tagging rules.

Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select File Servers.
   The available file servers appear in the right-hand pane.

2. In the File Servers window, right-click and select Scan for these scanning options:

   i. You cannot scan network servers in OpenLDAP.

   • All Network Servers - By Organizational Units — Select the organizational unit to search and click OK.
   • All Network Servers - By Net View — Find all available file servers on the local network.
   • Network Servers By LDAP Selection — Select the file servers and click OK.

Add a single server to a list
The file server list is a list of file shares used for location-based tagging rules.
For option definitions, click ? in the interface.

Task
1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select File Servers.
   The available file servers appear in the right-hand pane.
2  In the File Servers window, right-click and select Add New | Server.
   The new Server icon appears.

3  Type the server name.

Defining network parameters
Network definitions serve as filter criteria in network-related protection rules.

- The Network Port Range allows you to use network port ranges to enforce the network-related rules to a specific service.
- The Network Address Range monitors network connections between an external source and a managed computer.
- The Network Address Ranges Group allows you to use multiple network ranges for network-related rules.

Create a network address range
Network address ranges serve as filter criteria in network-related protection rules.

Task
For option definitions, press F1.

1  In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Network.
   The available network address ranges appear in the right-hand pane.

2  In the Network window, right-click and select Add New | Network Address Range.
   The new Network Address Range icon appears.

3  Double-click the icon.
   The edit window appears.

4  Type the name of the network address range.

5  Type a description (optional).

6  Type the IP address range using one of these methods:
   - Define using address range
   - Define using a network mask
   - Define using CIDR notation

7  Click OK.

Create a network address range group
Network address ranges serve as filter criteria in network-related protection rules. Network address range groups simplify rules while maintaining granularity by combining several address range definitions into one group.

Task
For option definitions, press F1.

1  In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Network.
   The available network address range groups appear in the right-hand pane.
2 In the Network window, right-click and select Add New | Network Address Range Group.

   The new Network Address Range Group icon appears.

3 Double-click the icon.

   The edit window appears.

4 Type the name of the network address group.

5 Type a description (optional).

6 Select the network address ranges from the available list.

7 Click OK.

Create a new network port range

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

Task

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Network.

   The available network port ranges appear in the right-hand pane.

2 In the Network window, right-click and select Add New | Network Port Range.

   The new Network Port Range icon appears.

3 Double-click the icon.

   The edit window appears.

4 Type the name of the network port range.

5 Type a description (optional).

6 Type the port range (single port, multiple ports, range.).

7 Select the protocol type (UDP, TCP or both).

8 Click OK.

Defining registered document repositories

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

To use registered document repositories, the administrator selects a list of shared folders to be registered. The definition can be limited to specified file extensions within those folders, and to a maximum file size. The content of these folders is categorized, fingerprinted and distributed to all endpoint workstations. McAfee DLP Endpoint software on the managed computers blocks distribution of documents containing registered content fragments outside of the enterprise.

When setting up registered document repositories, we recommend setting both share and security permissions for the repository folders and giving full permission to SYSTEM.

Advantages of registering documents

Two advantages of registered documents over traditional location-based tagging are:
• Documents that existed before the location-based tag was defined are not detected by location-based tagging rules unless the user opens or copies the original file from its network location. Registered documents classification rules detect all files in the defined folders.

• If the same confidential content exists in several documents, you need to categorize it only once using a registered document repository. When you use location-based tagging you have to identify every network share where the confidential content is located, and tag each one.

Registering documents on managed computers

Two advantages of registering documents over traditional location-based tagging are:

• Documents that existed before the location-based tag was defined are not detected by location-based tagging rules unless the user opens or copies the original file from its network location. Registered documents classification rules detect all files in the defined folders.

• If the same confidential content exists in several documents, you need to categorize it only once using a registered document repository. When you use location-based tagging you have to identify every network share where the confidential content is located, and tag each one.

Indexing registered document repositories

Registered document repositories are indexed periodically using ePolicy Orchestrator Server Tasks. The indexing process creates a package (reg_docs9300_x.zip) that is added to the ePolicy Orchestrator repository and deployed to the managed computers.

Content in registered document folders is protected with registered documents classification rules. The classification rule associates a specified content category with the files in the registered document repository. The separation of definitions, groups, and categories increases modularity, and allows the creation of new classification rules, or modification of existing ones, without the need to re-index and re-deploy.

When you have defined a registered documents classification rule, add the associated categories to a protection rule that accepts content categories.

When an index, a registered documents classification rule, and a protection rule specifying the category are deployed to a managed computer, all content leaving the managed computer is checked against all registered document fingerprints, and the content is blocked or monitored according to the protection rule.

Whitelisted content is removed from the registered document repository database. Registered documents classification rules apply only to content in the repository that is not whitelisted.

Create a registered document repository definition

Registered document repositories are used to define Registered Documents Classification rules.

Task

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under Content Based Definitions, select Registered Documents Repositories.
   
   The available registered documents appear in the right-hand pane.

2 In the Registered Documents Repositories window, right-click and select Add New | Registered Document Repository.
   
   A new Registered Documents Repository icon appears.

3 Name the new registered document repository and double-click the icon.
4 Add a description (optional).
5 Type the UNC path to the folder you are defining, or click Browse to locate the folder.
6 Type a user name to access the folder, and a password if required.
7 Specify document extensions to include or exclude (optional). You can Add a new extension, or Edit an existing one, if required.
8 Specify the maximum file size (optional) and click OK.

Create a registered document repository group
Registered document repository groups are used to define registered documents classification rules.

Task
For option definitions, press F1.
1 In the McAfee DLP Endpoint policy console navigation pane under Content Based Definitions, select Registered Documents Repositories.
   The available registered documents repositories and groups appear in the right-hand pane.
2 In the Registered Documents Repositories window, right-click and select Add New | Registered Document Repository Group.
   The new Registered Document Repository Group icon appears.
3 Double-click the icon. The edit window appears.
4 Name the new registered document group.
5 Type a description (optional).
6 Select the registered document definitions from the available list.
7 Click OK.

Classifying 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.

This chapter describes the destinations you can control, and the creation of definitions to exercise that control.

Contents
- How sensitive content is controlled in email
- Defining local and network printers
- Controlling information uploaded to websites

How sensitive content is controlled in email
Email destination objects are predefined email domains or specific email addresses that can be referenced in email protection rules. The email protection rule can block tagged data from being emailed to specific domains, or can prevent tagged data from being emailed to undefined domains.
Typically, the email destinations section defines any internal domains and external domains where emailing tagged data is allowed.

Email destination groups allow protection rules to reference a single entity that defines multiple destinations. A typical use of this feature is to create an email destination group for all internal domains.

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. The option is set in the Agent Configuration | Email Probe tab. The MAPI option supports McAfee DLP Endpoint 9.1 Patch 2, 9.2 Patches 1 and 2, and 9.3.x clients only.

A new administrative event, Agent Exceeds Memory Limit On Load, can be selected in the Agent Configuration | Events and Logging tab to record when the agent process (fcag.exe) exceeds the configured memory after client software has been restarted.

**Create email destinations**

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

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Email Destinations.
   
   The available email destinations and groups appear in the right-hand pane.

2. In the Email Destinations window, right-click and select Add New | Email destination.
   
   A new Email Destination icon appears.

3. Double-click the icon.
   
   The edit window appears.
4 Add the email destination name: under Email address, type the domain name and click Add.

- To create an email destination of external domains, Add a domain entry for every internal domain, then deselect all domains and select Other email domain.

![Email Destination Edit Dialog Box](image)

**Figure 9-5 Email destination edit dialog box**

- To add a specific email address from this domain, right-click the domain name, select Add | Email User, then type the user name and click OK.

- To exclude a particular email address from the domain, add the user to the domain, right-click the domain name and select Add | Other email user, then deselect the user.

5 Click OK.

### Create an email group

Email groups simplify rules while maintaining granularity by combining several email definitions into one group.

**Task**

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Email Destinations. The available email destinations and groups appear in the right-hand pane.

2 In the Email Destinations window, right-click and select Add New | Email Group.

A new Email Group icon appears.

3 Double-click the icon. The edit window appears.

4 Type the name of the email group.

5 Type a description (optional).

6 Select the email destination definitions from the available list.

7 Click OK.
Defining local and network printers

Printer definitions are used to define printing protection rules. Printing protection rules are used to manage both local and network printers and either block or monitor the printing of confidential material.

There are two types of printer definitions: network printers and unmanaged printers (whitelisted printers). Network printers can be added manually by creating a definition that specifies the UNC path to the printer, or automatically from a printer list. The printer list is created by an LDAP query or network scan. Printers from the scan list are then selected to add them to the printer definitions.

Whitelisted printers are printers that cannot work with the proxy driver architecture required for Data Loss Prevention management. To prevent operational problems, these printers are defined as unmanaged. Unmanaged printer definitions are created manually using printer model information from the operating system printer properties.

For reporting purposes, there is a third category of printer. When a printer is connected to a managed computer and the McAfee DLP Endpoint software fails to install its printer driver, it is reported as an unsupported printer. After investigation of the reason for the failure, these printers are placed on the whitelist if no other solution is found.

Create a printer list and add printers

Printer lists are used to manage sensitive content sent to printers. Use these tasks to create a printer list and add printers to it.

Tasks

- **Create a printer list on page 100**
  Printer lists are used to manage sensitive content sent to printers.

- **Add a printer to the printer list on page 101**
  Before network printers can be defined in printer protection rules, they must be added to the printer list.

- **Add an unmanaged printer to the printer list on page 101**
  Some printers stop responding when the McAfee DLP Endpoint software assigns them a proxy driver. These printers cannot be managed, and must be exempted from printer rules to avoid problems. In other cases, you might choose to exempt a printer, such as one belonging to a top executive, from printer rules. In either case, you define these printers as unmanaged, placing them on the printer whitelist.

- **Add an existing printer to the printer whitelist on page 102**
  When an existing network printer malfunctions, you can add it to the printer whitelist temporarily until the problem is clarified. In this procedure, the printer remains on the network printer list but is also whitelisted, preventing printer protection rules from being applied to it. When the problem is resolved, the definition is removed.

Create a printer list

Printer lists are used to manage sensitive content sent to printers.

Task

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under **Definitions**, select **Printers**.
   
   The available printers appear in the right-hand pane.
2 In the **Printers** window, right-click, select **Scan** and select a scanning option:

- Network Printers By Organizational Units
- Network Printers By LDAP Selection
- Scan Shared Printers

3 Edit the search parameters (optional), add a filter (optional), then click **Search**.

4 Select the printers to add to the printer list and click **OK**.

**Add a printer to the printer list**

Before network printers can be defined in printer protection rules, they must be added to the printer list.

**Task**

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under **Definitions**, select **Printers**.

   The printers that have already been added appear in the right-hand pane.

2 In the **Printers** window, right-click and select **Add New | Network Printer**.

   The new **Network Printer** icon appears.

3 Double-click the **Network Printer** icon.

   The edit window appears.

4 Type the name of the network printer.

5 Type the UNC path of the network printer.

6 Click **OK**.

**Add an unmanaged printer to the printer list**

Some printers stop responding when the McAfee DLP Endpoint software assigns them a proxy driver. These printers cannot be managed, and must be exempted from printer rules to avoid problems. In other cases, you might choose to exempt a printer, such as one belonging to a top executive, from printer rules. In either case, you define these printers as unmanaged, placing them on the printer whitelist.

**Task**

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane under **Definitions**, select **Printers**.

   The printers that have already been added appear in the right pane.

2 In the **Printers** window, right-click and select **Add New | Unmanaged Printer Model**. Type a name into the text box.
3 Double-click the icon. The edit window appears.

4 Type the printer model. You can copy and paste the information using the Model information from the printer properties:
   a From the Microsoft Windows Start menu, select Printers and Faxes.
   b Right-click the printer you are whitelisting and select Properties.
   c In the General tab, copy the Model information (below the Comment text box).

![Figure 9-6  Copying the printer model information](image)

5 Paste the model information into the Model text box in the Unmanaged Printer Model dialog box.

6 Add a definition (optional).

7 Click OK.

Add an existing printer to the printer whitelist
When an existing network printer malfunctions, you can add it to the printer whitelist temporarily until the problem is clarified. In this procedure, the printer remains on the network printer list but is also whitelisted, preventing printer protection rules from being applied to it. When the problem is resolved, the definition is removed.

- Right-click an existing network printer definition and click Add as Unmanaged Printer. The printer appears in the Unmanaged Printer Model section of the Printers pane.

Controlling information uploaded to websites
Web destination objects are predefined web addresses that can be referenced in web post protection rules. You can use web destination 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 destinations section defines any internal websites as well as external websites where posting tagged data is allowed.

If you have defined numerous web destinations, you can create web destination groups so that protection rules can reference a single entity. A typical use of this feature is to create a web destination group for all internal websites.

**Create a web destination**

Web destination objects are predefined web addresses that can be referenced in web post protection rules.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Web Servers. The available web servers appear in the main pane.
2. In the Web Servers window, right-click and select Add New | Web Server. A new Web Server icon appears.
3. Double-click the icon. The edit window appears.
4. In the text box at the bottom of the window, type the web server URL, and click Add to add a web server address.
5. To add a resource path, right-click the web server address, and select Add | Resource Path. Type the path and click OK.
6. Type a description (optional).
7. Click OK.

**Create a web destination group**

Web destination groups simplify rules while maintaining granularity by combining several web destination definitions into one group.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Web Servers. The available web servers groups appear in the right-hand pane.
3. Double-click the icon. The edit window appears.
4. Type the name of the web server group.
5. Type a description (optional).
6 Select the web servers from the available list.
7 Click OK.

Classification in use

*Data-in-use* is the term used to define content by how or where it is used.

McAfee DLP Endpoint definitions and rules classify your data-in-use. These definitions provide granularity to help you protect only those files that need to be protected.

Contents
- How McAfee DLP Endpoint categorizes applications
- Applications and how to use them
- Adding and removing applications
- Defining file types

How McAfee DLP Endpoint categorizes applications

Before you create rules 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.

<table>
<thead>
<tr>
<th>Application Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Application Definition</td>
</tr>
<tr>
<td>Email Client Applications</td>
</tr>
<tr>
<td>Encryption Applications</td>
</tr>
<tr>
<td>Explorer</td>
</tr>
<tr>
<td>IM Applications</td>
</tr>
<tr>
<td>Installers</td>
</tr>
<tr>
<td>Media Burner Applications</td>
</tr>
<tr>
<td>Microsoft Office Applications</td>
</tr>
<tr>
<td>P2P Applications</td>
</tr>
<tr>
<td>Scanners and Indexers</td>
</tr>
<tr>
<td>Web Browsers</td>
</tr>
<tr>
<td>Windows OS Files</td>
</tr>
<tr>
<td>WinRAR Archiver</td>
</tr>
<tr>
<td>Zip Applications</td>
</tr>
</tbody>
</table>

*Figure 9-7* Strategies displayed in the Application Definitions window

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 for Files and Folders 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.

**Applications and how to use them**

Applications can be specified in tagging and protection rules by creating application definitions. Importing an applications list and creating application definitions are efficient ways of handling all application related tagging and protection rules. System administrators can import a list of all relevant applications available within the enterprise, create different application definitions based on their needs, and implement these definitions with relevant rules to maintain policies.

• **Enterprise Applications List** — A comprehensive list of applications used by the enterprise. You can scan for new applications and merge them with the existing list, modify the list, and group by any column.

• **Application Definitions** — The details that define templates you use to customize rules about specific applications. You can add applications to application definitions from the Enterprise Applications List, or create them directly. Tagging rules and protection rules always refer to application definitions rather than individual applications.

When a user opens files with an application that is defined in a rule by an application definition, it produces one event in the DLP Incident Manager *per application session*, not per sensitive file opened. The event includes all files that matched the specified conditions in that application session. If the **Store Evidence** action was selected, only files from that application session matching the conditions are stored.

**The Enterprise Application List**

The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.

Application-based tagging rules and most protection rules reference application definitions. For example, to control the data in Excel files, add Excel to the **Enterprise Applications List**, then create a rule that defines whether Excel files or their contents can be printed or copied.

The information in the first five columns of the Enterprise Applications List is read from each application file’s property list. In cases where the property has no value listed, it is displayed as **unknown**.

Applications must be defined in the Enterprise Applications List before they can be referenced in a rule. If applications you want to control do not appear on the list, you must add them.
Application definitions and how they are categorized

Application definitions control specific applications using properties such as product or vendor name, executable file name, or window title.

Application definitions replace the application groups used in previous versions of McAfee DLP Endpoint software. Because they are defined in a similar manner to device definitions, they are more intuitive, granular, scalable, and configurable. They also reduce policy size by using a different data model.

A subcategory, web application definitions, creates a URL-based template. Files, screenshots, or clipboards saved from a browser can now be tagged and blocked based on URL.

Application definitions can be identified by any of the following parameters:

- **Command line** — Allows command line arguments, for example: java-jar, that can control previously uncontrollable 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 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 2003, 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 filename.

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

With the exception of the SHA2 application name and working directory, all parameters accept substring matches.

As a result of this data model, application strategy is defined in the application definitions not in the Enterprise Applications List, as was done in earlier versions. One result of this is that the same application can be included in several application definitions and can therefore be assigned more than one strategy. McAfee DLP Endpoint software 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 definition and anything else in another, McAfee DLP Endpoint software does not treat the application as an editor.
A new option allows analysis of memory mapped files. This option was added for compatibility with Autodesk 3ds Max graphic files. Although the option is available on all definition windows, it is automatically selected only on the 3ds Max application definition. Due to processing overhead, we do not recommend using this option unless it is specifically required.

![Application definition window](image)

**Figure 9-8 Application definition window**

**Create application definitions**

Use these tasks to create application definitions.
Tasks

- Create an application definition on page 108
  Application definitions control specific applications using properties such as product or vendor name, executable file name, or window title.

- Create an application definition from the Enterprise Applications List on page 109
  Application definitions control specific applications using properties such as product or vendor name, executable file name, or window title.

- Create a web application definition on page 109
  Web application definitions are used to create tagging and protection rules for files saved from browsers, based on the browsed URL.

Create an application definition

Application definitions control specific applications using properties such as product or vendor name, executable file name, or window title.

Use this task to create an application definition directly. You can also create an application definition from the Enterprise Application List. Application definitions have replaced the application groups used in earlier versions of McAfee DLP Endpoint.

Task

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Application Definitions.
   The available definitions appear in the right-hand pane.

2. In the Application Definitions window, right-click and select Add New | Application Definition.
   A new application definition icon appears.

3. Name the new application definition and double-click the icon.
   The edit window appears.

4. Type a description (optional).

5. Select parameters.
   As you select each parameter, its edit window appears.

6. Click Add New, and type a value and optional description. Some parameters allow partial matching. Select the option if you want to use it.
   ![Tip: If you select partial matching, the typed in value is matched as a substring.]

7. Click Add New to add more values. When you have finished, click OK to close the parameter edit window.

8. When you are finished adding parameters, click OK to save the edited definition.

9. By default, all new application definitions are created with the Editor strategy. To change the strategy, right-click the definition name and select Process Strategy.
   ![Warning: Because the strategy affects the system’s observation level, it can strongly affect system performance.]
Create an application definition from the Enterprise Applications List

Application definitions control specific applications using properties such as product or vendor name, executable file name, or window title.

Use this task to create an application definition from the Enterprise Applications List. You can also create application definitions directly.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Applications, select Enterprise Applications List.

   The available applications list appears in the right-hand pane.

2. Right-click an application and select Create Application Definition.

   The edit window appears with several parameters selected, based on the information available. You can modify the definition now or after creating it. You can also add multiple applications to a definition. Select them, using the usual Shift-click and Ctrl-click selection rules, before right-clicking.

   If application definitions that include the selected application already exist, the Go To option is enabled. Clicking a Go To option opens Application Definitions in the main pane and selects the application.

3. Type a description (optional).

4. Click OK. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Application Definitions to view the new definition.

5. By default, all new application definitions are created with the Editor strategy. To change the strategy, right-click the definition name and select Process Strategy.

   Because the strategy affects the system's observation level, it can strongly affect system performance.

Create a web application definition

Web application definitions are used to create tagging and protection rules for files saved from browsers, based on the browsed URL.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Application Definitions.

   The available definitions appear in the right-hand pane.

2. In the Application Definitions window, right-click and select Add New | Web Application Definition.

   A new web application definition icon appears.

3. Name the new web application definition and double-click the icon.

   The edit window appears. The window contains one parameter: Browser URL.

4. Type a description (optional).

5. Select the browser URL parameter to open its edit window.
6 Click Add New, and type a value and optional description. Select partial matching if you want the typed value to be used as a substring.

7 Click Add New to add more URL values. When you are finished, click OK to close the parameter edit window.

8 Click OK to save the edited definition.

**Adding and removing applications**

Use these tasks to add or remove applications from the Enterprise Applications List.

**Tasks**

- *Import an application manually on page 110*
  The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.

- *Import new applications by scanning on page 110*
  The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.

- *Remove applications from the list on page 111*
  The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.

**Import an application manually**

The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.

**Task**

1 In the Enterprise Applications List window, right-click and select Add.

   The Add Executable window appears.

2 Click Browse and select the application .exe file.

3 Select an application and click Open.

   The application details appear.

4 Click Add to import the application to the list.

   You can also add an application by selecting the executable, then dragging and dropping it into the Enterprise Applications List window.

**Import new applications by scanning**

The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.

You can add groups of applications to the Enterprise Applications List from specific drives or folders. You must use the Merge option to do this.

**Task**

1 In the Enterprise Applications List window, right-click and select Scan Applications.

   The Scan for Applications window appears.

2 Click the Start button and select the drives and folders to scan for applications.

   All available applications appear.
3 Select the required action from the list:
   • The Clear button discards the current list.
   • The Merge button adds the applications to the Enterprise Applications List.

4 Close the Scan for Applications window.
   The merged applications appear in the Enterprise Applications List.

Remove applications from the list
The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.

Task
1 In the McAfee DLP Endpoint policy console navigation pane under Applications, select Enterprise Applications List.
   The available applications appear in the right-hand pane.
2 Right-click the application’s main executable (.exe) file, and select Remove.
3 Click Yes to confirm the deletion.
   The entire application is removed, that is, the executable and all associated files.

   You cannot remove an application if it is included in an application definition. Right-click and select Application Definitions | Go To to see if the application is included in any definitions before removing.

Defining file types
File extension definitions restrict tagging rules and protection rules to particular file types.
A list of default file extensions used in tagging rules and protection rules is available in the software. You can manually add file extensions as needed for your environment.

Tasks
• Create file extensions on page 111
   File extension definitions restrict tagging rules and protection rules to particular file types.
• Create file extension groups on page 112
   File extension definitions restrict tagging rules and protection rules to particular file types.
   They simplify rules while maintaining granularity by combining several file extension definitions into one group.

Create file extensions
File extension definitions restrict tagging rules and protection rules to particular file types.

Task
For option definitions, press F1.
1 In the McAfee DLP Endpoint policy console navigation pane under Definitions, select File Extensions.
   The available file extensions appear in the right-hand pane.
2 In the File Extensions window, right-click and select Add New | File Extension.
   The new File Extension icon appears.
3 Double-click the icon.
   The edit window appears.
4 Type the name of the new file extension entry and double-click the icon. The edit window appears.
5 In the Extension text box, type the extension preceded with a period, for example .GIF.
6 Type a description for the file extension (optional).
7 Click OK.

Create file extension groups
File extension definitions restrict tagging rules and protection rules to particular file types. They simplify rules while maintaining granularity by combining several file extension definitions into one group.

Task
For option definitions, press F1.
1 In the McAfee DLP Endpoint policy console navigation pane under Definitions, select File Extensions.
   The available file extension groups appear in the right-hand pane.
2 Click Add New | File Extension Group either on the McAfee DLP Endpoint policy console toolbar, or after right-clicking in the File Extensions window.
   The new File Extension Group icon appears.
3 Double-click the icon.
   The edit window appears.
4 Type the name of the file extension group.
5 Add a description for this group (optional).
6 Select the file extensions from the available list.
7 Click OK.

Classification rules
Classification rules assign content categories to files or registered document repository definitions. Rules can be filtered by text patterns and dictionaries, or applied to specific document parts (header, footer, body).

Contents
- How classification rules link categories to content
- Create and define classification rules
How classification rules link categories to content
Classification rules associate files and data with the appropriate content categories.

Content categories
Content category definitions are created in the Tags and Categories definition pane. Categories can be grouped to simplify rule making. A content category definition consists of a suitable name, an optional description, and a GUID assigned by the system.

Content classification rules
Content classification rules associate specified text pattern and dictionary definitions with content categories. When those categories are added to protection rules, content containing the specified text is monitored or blocked. Rules can contain any combination of text patterns and dictionaries. For Microsoft Word files, you can also specify where in the document (header/body/footer) the specified content is found.

Text extractor
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, a suitable content category is applied to the content.

The text extractor can run multiple processes depending on the number of cores in the processor: with a single core processor only one process runs, 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, so 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.

Memory usage by the text extractor can be configured in the Agent Configuration | Advanced Configuration tab. If the maximum memory is exceeded, the text extractor restarts. The default is 75 MB. This configuration option is available only to 9.2 Patch 1 and later clients.

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 is not a defect, but rather a known issue for all text extraction programs. There is no known method or technique to identify the ANSI code page in such a 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 problem, McAfee DLP Endpoint client software uses a fallback code page when the code page cannot be determined. The fallback is set in the Agent Configuration | File Tracking tab, and is either the default language of the computer or a different language set by the administrator.

Registered documents classification rules
Registered documents classification rules associate all content matching a specified registered documents repository definition to a content category. As with content classification rules, when categories are added to protection rules, content containing the specified text is monitored or blocked.

Create and define classification rules
Classification rules associate content with the appropriate content categories. There are two types: content rules and registered document rules.

Use these tasks to create and define classification rules.
Tasks

- **Create and define a content classification rule on page 114**
  Content classification rules link text patterns or dictionaries to content classifications. In previous versions of McAfee DLP Endpoint, they were known as content-based tagging rules.

- **Create and define a registered documents classification rule on page 114**
  Registered documents classification rules apply repository definitions and content categories to files.

Create and define a content classification rule
Content classification rules link text patterns or dictionaries to content classifications. In previous versions of McAfee DLP Endpoint, they were known as content-based tagging rules.

Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Classification Rules**.
   The available classification rules appear in the right-hand pane.

2. In the **Classification Rules** pane, right-click and select **Add New | Content Classification Rule**.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:
   - **Step 1 of 4**
     Select one of the text pattern options, **ANY** (logical OR) or **ALL** (logical AND), then select one or more text patterns or text pattern groups from the available list. Click **Add item** to create a new text pattern, or click **Add group** to create a new text pattern group. Click **Edit** to modify an existing text pattern or group. Click **Next**.
   - **Step 2 of 4**
     Select one of the dictionary options,
   - **Step 3 of 4 (optional)**
     Select the part of the document where the text pattern or dictionary matching takes place. This option is primarily intended to be used with Microsoft Word files, but applies to any file type that has a header / footer.
   - **Step 4 of 4**
     Select a content category, or create a new one by clicking **Add New**. Click **Finish**.

5. To activate the rule, right-click the classification rule icon and select **Enable**.

Create and define a registered documents classification rule
Registered documents classification rules apply repository definitions and content categories to files.

Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Classification Rules**.
   The available classification rules appear in the right-hand pane.

2. In the **Classification Rules** pane, right-click and select **Add New | Registered Documents Classification Rule**.

3. Rename the rule to something that will help you recognize its specific function.
4 Double-click the rule icon and follow these steps in the wizard:

**Step** | **Action**
--- | ---
1 of 2 | Select one or more registered documents repository definitions or groups from the available list. Click **Add item** to create a new registered documents repository definition, or **Add Group** to create a new registered documents repository group. Click **Next**.

2 of 2 | Select a content category, or create a new one by clicking **Add New**. Click **Finish**.

5 To activate the rule, right-click the classification rule icon and select **Enable**.

**Tasks**
- **Index the registered documents repositories on page 115**
  Indexing of registered document repositories is scheduled in ePolicy Orchestrator server tasks.
- **Deploy a registered document package to the client computers on page 115**
  Indexed registered document repository packages are distributed to the managed computers as a product deployment.

**Index the registered documents repositories**
Indexing of registered document repositories is scheduled in ePolicy Orchestrator server tasks.

**Before you begin**
Create a registered documents repository definition, then create and enable a registered documents classification rule and a protection rule using the content category specified in the classification rule. Apply the policy to ePolicy Orchestrator.

For option definitions, click ? in the interface.

**Task**
1 In ePolicy Orchestrator, select **Menu** | **Automation** | **Server Tasks**.

2 Select **New Task**.

3 In the Server Task Builder, name the new task and click **Next**.

4 On the **Actions** page, select **DLP Register Documents Scanner** from the drop-down list. Click **Next** to schedule the scan. Review your task, then click **Save**.
   The task now appears in the Server Tasks list. Select it and click **Run** to run the scan immediately.

**Deploy a registered document package to the client computers**
Indexed registered document repository packages are distributed to the managed computers as a product deployment.

**Before you begin**
The registered document package must be indexed in ePolicy Orchestrator.

For option definitions, click ? in the interface.
Task
1. In ePolicy Orchestrator select **Menu | System Tree**.

2. In the System Tree, select the level at which to deploy the registered document package.

   ![Tip](Leaving the level at **My Organization** deploys to all workstations managed by ePolicy Orchestrator.)

   If you select a level under **My Organization**, the right-hand pane displays the available workstations. You can also deploy the registered document package to individual workstations.

3. Open the Client Task Builder wizard: click the **Assigned Client Tasks** tab. Under **Actions**, select **New Client Task Assignment**.

4. Select the deployment type: in the **Product** field select McAfee Agent. In the **Task Type** field select **Product Deployment**. Click **Create New Task**.

5. In the **Name** field, type a suitable name, for example, **Install DLP Registered Documents**. Typing a description is optional.

6. In the **Products and Components** field, select **DLP Registered Documents 9.2.0.0** or **DLP Registered Documents 9.3.0.0**. Leave the **Action** field on **Install**.

   Choose the registered documents version based on which McAfee DLP Endpoint clients you are deploying to. Registered document packages are not compatible between versions, so if you are supporting two client versions, you must make two separate packages. Click **Save**.

7. Select a suitable **Schedule type** and set the **Options**, date, and **Schedule** parameters. Click **Next**.

8. Review the task summary. When you are satisfied that it is correct, click **Save**.
Tracking content with tags and classifications

McAfee DLP Endpoint software tracks and controls sensitive information using two similar mechanisms: tags and content categories.

Tagging rules associate files and data with the appropriate tags. Classification rules associate files and data with content categories. In both cases, the sensitive information is labeled, and the label stays with the content even if it is copied into another document or saved to a different format.

Contents
- How tags and content categories are used to classify content
- How tagging rules link tags to content
- Manual tags

How tags and content categories are used to classify content

Tags give you a method for classifying content and reusing that classification.

Tagging rules assign tags to content from specific applications or locations. Once assigned, the tag stays with the content as it is moved or copied, or included in or attached to other files or file types.

Content categories

Content categories, known as content tags in earlier versions of McAfee DLP Endpoint software, are another way of classifying content. Content categories are used with classification rules to classify content and registered document groups. They can also be specified directly in most protection rules.

In McAfee Device Control software only content categories are available, not tags.

To protect data, follow this high-level process:

1. Classify the information that needs to be protected.
2. Create tags or content categories for each classification of data.
3. Create tagging rules and classification rules that associate sensitive data with the appropriate tags and content categories.
4. Define protection rules incorporating the tags and content categories that block, monitor, or encrypt the sensitive data when users send it to portable devices or specified network locations.
Category catalogs

Category catalogs are sets of content categories and associated predefined classification rules that can be used as an out-of-the-box building block for policies. When you select a content category from a catalog, it automatically adds both the content category and the related classification rules to the policy. If you have already created a category with that name, only the rules are added.

Create tags, content categories, catalogs, and groups

Use these tasks to create tags, content categories, and tag and category groups, which are then attached to files with tagging or classification rules. Or create content catalogs, which add a content category and the related classification rule simultaneously.

Consider the distinctions you need to make between different types of content, and make a tag or content category for each type.

Tasks

- Create a tag on page 118
  Tags give you a method for classifying content and reusing that classification.

- Create a content category on page 118
  A content category definition consists of a suitable name, an optional description, and a GUID assigned by the system.

- Import a category catalog on page 119
  Category catalogs are sets of content categories and associated predefined classification rules. Once a category catalog is imported into the policy, the classification rules can be used as is or modified as required. If a content category with the same name already exists, only the classification rules are imported.

- Create a tag and category group on page 119
  Tag and category groups are used to place multiple tags and content categories on files more efficiently.

Create a tag

Tags give you a method for classifying content and reusing that classification.

Task

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Tags and Categories.
   The available tags, content categories, and groups appear in the right-hand pane.

2. In the Tags and Categories window, right-click and select Add New | Tag.
   The new tag icon appears with the name selected.

3. Type a name, then double-click the icon.

4. Add a description (optional).

5. Click OK.
   You can also create a new tag while creating a tagging or protection rule.

Create a content category

A content category definition consists of a suitable name, an optional description, and a GUID assigned by the system.
Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Tags and Categories.
   
The available tags, content categories, and groups appear in the right-hand pane.

2. In the Tags and Categories window, right-click and select Add New | Content Category.
   
The new content category icon appears with the name selected.

3. Type a name, then double-click the icon.

4. Add a description (optional).

5. Click OK.

   You can also create a new content category while creating a classification or protection rule.

Import a category catalog
Category catalogs are sets of content categories and associated predefined classification rules. Once a category catalog is imported into the policy, the classification rules can be used as is or modified as required. If a content category with the same name already exists, only the classification rules are imported.

Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Tags and Categories.
   
The available tags, content categories, and groups appear in the right-hand pane.

2. In the Tags and Categories window, right-click and select Import Categories.
   
   After a few seconds, the Category Catalog window opens.

3. Select the categories you want to import, then click OK.
   
The categories and related classification rules are imported.

Create a tag and category group
Tag and category groups are used to place multiple tags and content categories on files more efficiently.

Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under Definitions, select Tags and Categories.
   
The available tags, content categories, and groups appear in the right-hand pane.

2. In the Tags and Categories window, right-click and select Add New | Tag and Category Group.
   
The new tag and category group icon appears.

3. Name the new group and double-click the icon.
   
The edit window appears.
How tagging rules link tags to content

Tagging rules associate files and data with the appropriate tags.

Tags

Tag definitions are created in the Tags and Categories definition pane. Tags can be grouped to simplify rule making. A tag definition consists of a suitable name, an optional description, and a GUID assigned by the system.

Tagging rules

Simple application-based tagging rules monitor or block all files created by the application or applications designated in an application definition. Simple location-based tagging rules monitor or block all files in the specified location. Adding conditions to a simple rule restricts it by adding a logical AND.

File types and extensions are predefined in the system and cannot be modified by the administrator. Adding a specific file type or extension to an application-based or location-based tagging rule attaches a tag only on files created by a specific application or in a specific location, AND with the selected file type or extension.

Using the text pattern or dictionary restriction in application-based or location-based tagging rules attaches tags only to files in a specific location, or created by a specific application, AND containing the specific pattern or dictionary threshold. This option allows you to combine features of content categories with tagging. Multiple text patterns or dictionaries can be selected, specified as ANY of the following or ALL the following. For the Microsoft Word file type, you can also specify where in the document (header/body/footer) the specified content is found.

Once a tag is attached to a file, the tag stays with the content, even when that content is copied to a file of different type or location.

A specific tag can be used by more than one tagging rule. For example, an application-based tagging rule can attach a tag called “Finance” to specific file types, irrespective of location. A location-based tagging rule can attach the same “Finance” tag to files in a specific location, irrespective of file type.

Create and define tagging rules

Creating tagging rules is a three-step process. A tagging rule must first be created, then defined, then enabled before it can be used.

Use these tasks to create and define tagging rules.

Tasks

- Create and define an application-based tagging rule on page 121
  Tagging rules associate files and data with the appropriate tags.
- Create and define a location-based tagging rule on page 121
  Tagging rules associate files and data with the appropriate tags.
Create and define an application-based tagging rule

Tagging rules associate files and data with the appropriate tags.

For option definitions, press F1.

**Task**

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Tagging Rules**. The available tagging rules appear in the right-hand pane.

2. In the Tagging Rules pane, right-click and select **Add New | Application Based Tagging Rule**.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

   **Step** | **Action**
   --- | ---
   1 of 7 | Select an application definition or definitions from the available list. You can include or exclude definitions. Click **Add item** to create a new application definition. Click **Next**.
   2 of 7 (optional) | Select the **Select from list** option, then select file types from the available list. Use the **Other File Types** option to select unlisted (unknown) file types. Click **Next**.
   3 of 7 (optional) | Select the **Select from list** option, then select file extensions from the available list. Click **Next**.
   4 of 7 (optional) | Select one of the text pattern options, **ANY** (logical OR) or **ALL** (logical AND), then select one or more text patterns or text pattern groups from the available list. Click **Add item** to create a new text pattern, or click **Add group** to create a new text pattern group. Click **Edit** to modify an existing text pattern or group. Click **Next**.
   5 of 7 (optional) | Select one of the dictionary options, **ANY** (logical OR) or **ALL** (logical AND), then select one or more dictionaries. Click **Add** to create a new dictionary or **Edit** to modify an existing dictionary. Click **Next**.
   6 of 7 (optional) | Select the part of the document where the text pattern or dictionary matching takes place. This option is intended to be used with Microsoft Word files.
   7 of 7 | Select an available tag for this rule, or create a new one by clicking **Add New**. Click **Finish**.

5. To activate the rule, right-click the protection rule icon and select **Enable**.

When you create an application definition tagging rule with multiple applications, all included applications are added in one line of the rule with logical OR and all excluded applications are added to a second line with logical OR. The two lines are a logical AND. For example:

...definition is 'Email Client Applications' OR 'Microsoft Office Applications' AND the definition is not 'Media Burner Applications'

**Tip:** If you do not include at least one application definition, the rule applies to all applications not specifically excluded.

Create and define a location-based tagging rule

Tagging rules associate files and data with the appropriate tags.
**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Tagging Rules**. The available tagging rules appear in the right-hand pane.

2. In the Tagging Rules pane, right-click and select **Add New | Location Based Tagging Rule**.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

   **Step** | **Action**
   --- | ---
   1 of 7 | Select one or more locations from the available list. If you select a **Network File Server**, a **Configure Selection** dialog box opens. Type a network location, or click **Browse** and locate the server. Alternately, you can select **Any Network File Servers**. Click **OK**. When you have completed all selections, click **Next**.
   2 of 7 (optional) | Select the **Select from list** option, then select file types from the available list. Use the **Other File Types** option to select unlisted (unknown) file types. Click **Next**.
   3 of 7 (optional) | Select the **Select from list** option, then select file extensions from the available list. Click **Next**.
   4 of 7 (optional) | Select one of the text pattern options, ANY (logical OR) or ALL (logical AND), then select the text patterns from the available list. Click **Add item** to create a new text pattern, or click **Add group** to create a new text pattern group. Click **Edit** to modify an existing text pattern or group. Click **Next**.
   5 of 7 (optional) | Select one of the dictionary options, ANY (logical OR) or ALL (logical AND), then select one or more dictionaries. Click **Add** to create a new dictionary or **Edit** to modify an existing dictionary. Click **Next**.
   6 of 7 (optional) | Select the part of the document where the text pattern or dictionary matching takes place. This option is intended to be used with Microsoft Word files.
   7 of 7 | Select an available tag for this rule, or create a new one by clicking **Add New**. Click **Finish**.

5. To activate the rule, right-click the protection rule icon and select **Enable**.

---

**Manual tags**

The Manual Tagging option allows authorized users to add or remove tags from files without using tagging rules. This option is accessed from the managed computer.

Manual tagging provides the ability to maintain your organization’s classification policy even in special cases of sensitive or unique information that is not being tagged by the system automatically. To apply or remove tags manually, a user must be authorized. This authorization is set on the **Security** tab of the Agent Configuration, using either Microsoft Active Directory or OpenLDAP.

Tags that are applied to files manually affect the transmission options of the content immediately, based on the relevant protection rules.

**Contents**
- Tag files manually
- Remove manual tags from content
Tag files manually

When necessary, tags can be applied to files manually by authorized users.

- A user must be authorized to use manual tagging. Permission for manual tagging is defined in the McAfee DLP Endpoint policy console on the Agent Configuration | Edit Global Agent Configuration | Security tab.

Task

1. On a managed computer, open Windows Explorer.
2. Right-click the file, then select Manual Tagging.
   - The Manual Tags window with the available tags appears.
3. Select the tags that are appropriate for the file.
4. Click OK.

Remove manual tags from content

Tags that were applied manually must be removed manually.

- A user must be authorized to use manual tagging. Permission for manual tagging is defined in the McAfee DLP Endpoint policy console on the Agent Configuration | Edit Global Agent Configuration | Security tab, using either Microsoft Active Directory or OpenLDAP.

Task

1. On a managed computer, open Windows Explorer.
2. Right-click the file with tags you want to remove, and select Manual Tagging.
   - The Manual Tags window with all the assigned tags appears.
3. Select the tags that need to be removed from these files.
4. Click OK.

   When selecting multiple files with several assigned tags, only those tags assigned to all selected files are removed.
Tracking content with tags and classifications

Manual tags
Applying McAfee DLP protection

McAfee DLP Endpoint protects sensitive content with a combination of device and protection rules. Rules are applied with policies that are distributed to the managed computers.

Contents
- Protecting files with rights management
- Controlling sensitive content with protection rules
- Limiting rules with assignment groups

Protecting files with rights management


Two rights management (RM) use cases are currently supported:
- McAfee DLP Endpoint file system discovery can apply RM policies to files detected in discovery scans.
- Email, removable storage, file system, and web post protection rules can recognize RM protected files. These files can be included or excluded from the rule.

Adobe RM

McAfee DLP Endpoint supports Adobe LiveCycle Rights Management ES2 and the Extension for Microsoft Office. You can apply RM protection to:
- PDF documents

Microsoft Windows Rights Management Services

McAfee DLP Endpoint supports Rights Management Services on Windows Server 2003 and Active Directory RMS (AD-RMS) on Windows Server 2008. You can apply Windows Rights Management Services protection to:
• SharePoint 2007 documents
• Exchange Server 2007 documents

**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 DLP integration both online and offline.


**How Data Loss Prevention works with rights management**
Rights Management (RM) in McAfee DLP Endpoint software is managed from the **RM and Encryption** section of the navigation pane. In this section, you define the RM server and manage the RM policies used by file system discovery rules, and email, removable storage, and web post protection rules.

When you select the **Apply RM Policy** action in a file system discovery rule, you must specify the RM server and policy as properties.

**Adobe LiveCycle Rights Management workflow**
When the McAfee DLP Endpoint software applying the file system discovery rule finds a file to protect, it sends the file to the RM server. The protection is applied according to the selected policy and the file is sent back to the managed computer. If the operation fails on the RM server side (because you cannot connect to the server for any reason) the file is monitored and an event (RM Failed) is sent to...
the DLP Incident Manager console. If the operation fails on the McAfee DLP Endpoint side (for example, you try to protect an unsupported file type) the file is monitored, but no error event appears in the DLP Incident Manager display.

You must enable the Apply RM Policy Failed event in Agent Configuration | Events and Logging for the event to be logged.

![Diagram of Adobe LiveCycle Rights Management protection flow](image)

**Figure 11-1  Adobe LiveCycle Rights Management protection flow diagram**

We recommend creating a Policy Set on the Adobe LiveCycle Rights Management server exclusively for policies used with McAfee DLP Endpoint software. At least one policy in the policy set must be enabled for the policy set to appear in the policy synchronization dialog box. If you disable a policy on the RM server, the policy is deleted from the RM policies page when you re-synchronize. If the disabled policy is used in a file system discovery rule, it is not deleted but becomes Not Active (with a different icon) and creates an error in the DLP Policy Analyzer.

If a policy is disabled on the RM server, but you do not re-synchronize, the policy remains active. When the McAfee DLP Endpoint software attempts to apply the policy, an Administrative RM Protect Failed event is sent to the DLP Incident Manager.

**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.
Windows Rights Management Services workflow

When the McAfee DLP Endpoint 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.

Figure 11-2  Windows Rights Management Services protection flow diagram

With Windows Rights Management Services, McAfee DLP Endpoint software can inspect the content of protected files if the current user has view permissions.

Adobe rights management users

McAfee Data Loss Prevention Endpoint requires two types of Adobe LiveCycle Rights Management users.

Adobe LiveCycle Rights Management users are named in the Rights Management Server definition. Before they can be used in McAfee DLP Endpoint, they must be created, and their roles defined, in the Settings | User Management section of the Adobe LiveCycle Rights Management ES2 server. In all cases, McAfee DLP Endpoint users must be on the Document Publisher list for the DLP Policy Set and must have the role of Services User. These are set on the RM server by the Adobe LiveCycle Rights Management administrator.

- McAfee DLP Endpoint Policy User — Logs on to the Adobe server and synchronizes policies.
- McAfee DLP Endpoint User — Applies RM policies to files on the managed computer. There are two ways to set up this user:
  - Using Windows authentication — The user must have Kerberos credentials (Service Principal Name – SPN) defined on the Adobe LiveCycle server. See the Adobe LiveCycle Help for details.
  - Using Adobe LiveCycle authentication — The user must be on the Document Publisher list for the DLP Policy Set and must have the role of Services User.
Define an Adobe RM server and synchronize policies
Set up users in the Adobe LiveCycle Rights Management server with appropriate roles and permissions.

**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select RM and Encryption | Rights Management Servers.
4. Enter the Adobe RM server URL path and Adobe RM user name and password, then test the connection.
   We recommend creating a single Policy Set for all DLP-related policies. The named user should be a Document Publisher for this policy set.
5. Enter the DLP Agent user credentials.
6. Select the Import RM Policies on OK checkbox to synchronize policies immediately, then click OK.
   If you don't select the checkbox, you can synchronize at any time from the context-sensitive menu. You must synchronize policies to use RM policies in DLP file system discovery rules.
   When you synchronize, the Adobe LiveCycle Rights Management Server dialog box appears listing all policy sets available to the logged on user.
7. Select the policy sets to import. All enabled policies in the set are imported and can be viewed in the Rights Management Policies pane.

Define a Microsoft Rights Management Service server and synchronize templates
Set up users in the Microsoft Rights Management Service server with appropriate roles and permissions.

**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select RM and Encryption | Rights Management Servers.
2. In the Rights Management Servers pane, right-click and select Add New | Microsoft RMS Server.
3. Double-click the rule icon.
   The Microsoft RMS Server dialog box appears.
4. Click Edit to set up the RMS template source. Enter the path and password, if required. Click OK.
   You can retrieve templates from either a network share or a web service.
5. Enter the URL of the RMS server, or select Using Auto service discovery to find the server.
6. Enter a User ID to specify a specific user, or select the Use end point logged in user option.
Select the Import RMS Templates on OK checkbox to synchronize policies immediately, then click OK. If you don’t select the checkbox, you can synchronize at any time from the context-sensitive menu. You must synchronize policies to use RMS templates in McAfee DLP Endpoint file system discovery rules.

There is an option in the RMS template settings to allow trusted browsers, such as Rights Management Update for Internet Explorer, to view the content of RMS protected documents. This option is NOT supported by McAfee DLP Endpoint software. If such a template is applied by a McAfee DLP Endpoint file system discovery rule, the protected files cannot be viewed by trusted browsers.

Select Rights Management Policies in the navigation pane to view the imported templates.

Define a Seclore server and synchronize policies

McAfee DLP Endpoint client integrates with Seclore FileSecure desktop client for file system discovery and protection rule creation.

Before you begin

Set up a Seclore FileSecure server and create users and policies. You will need to know the server URLs for all available servers, Hot Folder Cabinet ID, and passphrase to set up the McAfee DLP Endpoint integration.

Seclore server synchronization is supported through ePolicy Orchestrator. You cannot set up Seclore integration from a McAfee DLP Endpoint standalone extension.

Task

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select RM and Encryption | Rights Management Servers.
2. In the Rights Management Servers pane, right-click and select Add New | Seclore FileSecure server.
3. Double-click the rule icon. The Seclore Fileserver dialog box appears.
4. Edit the Name if required, and type a Description (optional).
5. Enter a Seclore policy server URL and click Add to add it to the list. Repeat until all available servers are listed.
   Seclore supports multiple servers. The Seclore API decides which server to connect to.
6. Enter the Seclore Hot Folder Cabinet ID and passphrase and click Test Connection to verify that you can connect to the server.
   The test connection button is not available if you are running a standalone version of the McAfee DLP Endpoint policy console.
   The connection might fail if you are running an evaluation version of FileSecure. If this happens, contact your McAfee service representative for a workaround.
7. Select the license types that apply.
8. Select the Import Hot Folders on OK (optional). Click OK.
   If you do not choose to import when you create the definition, you can import at any time by selecting Synchronize from the right-click menu. You should also synchronize whenever the policies on the server are updated.
Hot folders and descriptions from the server appear in the RM and Encryption | Rights Management Policies pane. Use these policies to define protection and discovery rules.

Controlling sensitive content with protection rules

Protection rules control the flow of data by defining the action taken when an attempt is made to transfer or transmit sensitive data. They do this by linking actions with definitions, tags and content categories, and user assignment groups.

You can define protection rules to include or exclude specific tags, file extensions, or document properties. You can also specify file types, users, and encryption (including password protection). (Not all options are available for all rules.) These options allow creation of rules with considerable granularity.

When excluding tags or content categories in protection rules, the exclude rule works relative to the include rule. You must include at least one tag or content category to exclude any other tags or content categories.

Working with TrueCrypt

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. You must enable the TrueCrypt option in the Agent Configuration | Advanced Configuration tag to use removable storage protection rules to protect TrueCrypt volumes.

TrueCrypt volumes do not support extended file attributes, causing tagged content copied to TrueCrypt volumes to lose its tags. You can, however, specify file types, file extensions, document properties, encryption types, or user assignment groups to define the protection rule.

How protection rules work

Protection rules specify the transfer method, named tag or tags, and how the system should react to attempts to transfer data. Each event is given a severity level and options for responding to the event. In some cases, protection rules merely log the event. In other cases, the protection rules might prevent the transfer of data and notify the user of the violation. Protection rules are optionally applied to assignment groups, allowing a rule to apply only to particular user groups.

Protection rules define the action taken when an attempt is made to transfer or transmit tagged data. The following tables describe the actions available for each rule, the content types associated with the rules, and whether the default alert displayed when the rule is triggered is customizable.

When Notify User is selected, and multiple events are triggered, the pop-up message states: There are new DLP events in your DLP console, rather than displaying multiple messages.
### Table 11-1 Actions/Rules matrix

<table>
<thead>
<tr>
<th>Rules</th>
<th>Actions</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Block</td>
<td>Monitor</td>
<td>Notify</td>
<td>Justification</td>
<td>Request</td>
<td>Store</td>
<td>Evidence</td>
<td>Encrypt</td>
<td>Quarantine</td>
<td>RM Policy</td>
<td>Apply</td>
</tr>
<tr>
<td>Device Rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix XenApp device rule</td>
<td>D</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed hard drive device rule</td>
<td>A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Plug and Play device rules</td>
<td>A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removable storage device rules (includes TrueCrypt device rules)</td>
<td>A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removable storage file access device rules</td>
<td>D p ^1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Protection Rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application file access protection rules</td>
<td>A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clipboard protection rules</td>
<td>D A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cloud protection rules</td>
<td>A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email protection rules</td>
<td>A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File system protection rules</td>
<td>A A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network communication protection rules</td>
<td>A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PDF/Image Writer protection rules</td>
<td>A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Printing protection rules</td>
<td>A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Removable storage protection rules</td>
<td>A A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Screen capture protection rules</td>
<td>A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web post protection rules</td>
<td>A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Discovery Rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>File system discovery rules</td>
<td>A A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Email discovery rules</td>
<td>A A A A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 11-2 Content/Rules matrix

<table>
<thead>
<tr>
<th>Rules</th>
<th>Content types</th>
<th>Change default alert</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Tags</td>
<td>Content categories</td>
<td>Document properties</td>
<td>Encryption types</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device Rules</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citrix XenApp device rule</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 11-2 Content/Rules matrix (continued)

<table>
<thead>
<tr>
<th>Rules</th>
<th>Content types</th>
<th>Change default alert</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>A</td>
</tr>
<tr>
<td>Fixed hard drive device rule</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Plug and Play device rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Removable storage device rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Removable storage file access device rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Tagging Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application based tagging rules</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Location based tagging rules</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Classification Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Content classification rules</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Registered document tagging rules</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Protection Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application file access protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Clipboard protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Cloud protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Email protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>File system protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Network communication protection rules</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>PDF/Image Writer protection rules</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Printing protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Removable storage protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Screen capture protection rules</td>
<td>A</td>
<td></td>
</tr>
<tr>
<td>Web post protection rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Discovery Rules</td>
<td></td>
<td></td>
</tr>
<tr>
<td>File system discovery rules</td>
<td>A</td>
<td>A</td>
</tr>
<tr>
<td>Email discovery rules</td>
<td>A</td>
<td>A</td>
</tr>
</tbody>
</table>

#### Legend (for both tables)

- A available (for actions)
- associated (for content types)

#### Notes
- 1 Windows displays a message. McAfee DLP Endpoint does not display a message.
**Improved clipboard protection rules**

Clipboard protection rules block use of the clipboard to copy sensitive data. Clipboard protection rules control use of the clipboard. Blocked content can be limited to data copied from specified applications or web sites, having specific tags or content categories, or copied by specified users or user groups.

The paste operation can be allowed into the same application the content was copied from, the same document only, or into specified applications, with all other possibilities being blocked. Specified applications can be included or excluded (allowed or blocked) and can include ICQ, IM, and Skype, application types that could not be blocked in previous versions of McAfee DLP Endpoint software.

**Paste into behavior**

The default option is to block pasting outside the current application. This option allows pasting within the document, or between documents opened by the same application. The other option is to specify, by means of Include and Exclude checkboxes, which applications are allowed and which are blocked. When using this option, pasting into the current document is always allowed, but pasting between documents in the current application is blocked, unless the application is specifically excluded from the rule.

**Actions**

Clipboard protection rule actions include Block, Monitor, Store Evidence, and Notify User. If evidence is to be stored, the Monitor action must also be selected. When the User Notification action is selected, the user notification pop-up is activated. (The Clipboard Agent notification message in the Agent Configuration | User Interface Service tab is no longer grayed out, and can be edited.) Clipboard text is not replaced with a notification, as in previous McAfee DLP Endpoint software versions. The Block action is no longer mandatory, as with previous McAfee DLP Endpoint software versions; the Monitor action (alone) is also an option.

**Limitations**

Opening a new document from the File menu is not recognized as a new document, and pasting into it is always allowed.

**Cloud protection rules**

Cloud protection rules manage files uploaded to cloud applications. Cloud applications are increasingly popular ways of backing up and sharing files. Most cloud applications create a special folder on the disk drive that synchronizes with the cloud server. McAfee DLP Endpoint intercepts file creation in the cloud application folder, scans the files, and applies the relevant policies. If McAfee DLP Endpoint allows synchronizing the file to the cloud application folder, and the file is later modified, it is rescanned and the policy reapplied. If the modified file violates a policy, it cannot be synchronized to the cloud.

The McAfee DLP Endpoint Cloud Protection rule currently supports Google Drive, Dropbox, SkyDrive, Syncplicity, and Box.inc.
**Actions**

Available actions are Monitor, Notify User, Business Justification, Store Evidence, and Apply RM Policy. Due to a limitation in Adobe LiveCycle, the Apply RM Policy action is only available for Microsoft RMS and Seclore FileSecure.

**Agent configuration**

To support the Cloud protection rule, a new Cloud Protection Handler appears on the Agent Configuration | Miscellaneous tab. The handler and all supported applications are selected by default. You can deselect individual applications for more granular control.

**Removable storage protection rule enhancement**

Devices using media transfer protocol can be protected using an enhancement of the removable storage protection rule.

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. An enhancement to the removable storage protection rule allows it to intercept MTP transfers and apply security policies. Only USB connections are currently supported.

When the Portable Devices handler on the Agent Configuration | Miscellaneous tab is enabled, all removable storage protection rules can be applied to MTP devices as well as other removable devices.

**Limitation**

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.

**Definitions and how they define rules**

Definitions are the fundamental building blocks used to create rules. You create a definition for each category you want to control. When you modify a definition, the modification is automatically propagated to all rules that use the definition.

Definitions let you customize the system to enforce your enterprise security policy and other requirements, such as compliance issues and privacy laws. Customizing these definitions creates an efficient method of maintaining company policies.

Definitions can be assigned to any new or existing rule. Changes take effect immediately upon redeploying the system policy to the agents.

Definitions are created in a two-step process: first you create the definition (right-click, select Add New), then you define it (double-click the newly created definition.) These two steps should always be done together. Leaving a definition empty (undefined) will, in most cases, generate an error when you try to apply the policy to ePolicy Orchestrator. At the very least, it will generate a warning.

**Table 11-3 Definitions and the tagging and protection rules that use them**

<table>
<thead>
<tr>
<th>Definition</th>
<th>Associated tagging/classification rules</th>
<th>Associated protection rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>Application-based tagging</td>
<td>Application File Access, Clipboard, File System, Network Communication, Printing, Removable Storage, Screen Capture</td>
</tr>
<tr>
<td>Dictionary</td>
<td>Content classification</td>
<td>NA</td>
</tr>
</tbody>
</table>
### Table 11-3 Definitions and the tagging and protection rules that use them (continued)

<table>
<thead>
<tr>
<th>Definition</th>
<th>Associated tagging/classification rules</th>
<th>Associated protection rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Destination</td>
<td>NA</td>
<td>Email</td>
</tr>
<tr>
<td>File Server</td>
<td>NA</td>
<td>File System Protection</td>
</tr>
<tr>
<td>Network</td>
<td>NA</td>
<td>Network Communication Protection</td>
</tr>
<tr>
<td>Printer</td>
<td>NA</td>
<td>Printing Protection</td>
</tr>
<tr>
<td>Registered document repository</td>
<td>Registered document classification</td>
<td>NA</td>
</tr>
<tr>
<td>Tag/Content Category</td>
<td>Application-based tagging, Location-based tagging, Content classification, Registered document classification</td>
<td>all Protection Rules</td>
</tr>
<tr>
<td>Text Pattern</td>
<td>Content classification, Application-based tagging, Location-based tagging</td>
<td>NA</td>
</tr>
<tr>
<td>Web Destination</td>
<td>NA</td>
<td>Web Post Protection</td>
</tr>
<tr>
<td>Whitelist</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

If you are also working with McAfee Endpoint Encryption for Files and Folders, be aware that including McAfee DLP Endpoint processes on a McAfee Endpoint Encryption for Files and Folders Blocked Processes list will prevent protection rules with encryption definitions from triggering, and might cause the McAfee DLP Endpoint software to malfunction.

**Create and define an application file access protection rule**

Protection rules for application file access monitor or block files based on the application or applications that created them. By selecting different combinations of application definitions and file extensions, you have considerable granularity in deciding which files are blocked.

You can specify content categories as well as tags to filter the rule.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection** | **Protection Rules**

   The available protection rules appear in the right pane.

2. In the **Protection Rules** pane, right-click and select **Add New** | **Application File Access Protection Rule**.

3. Rename the rule to something that will help you recognize its specific function.
4 Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 7</td>
<td>Select an application definition or definitions from the available list. You can include or exclude definitions. Click Add item to create a new application definition. Click Next.</td>
</tr>
</tbody>
</table>

You must select at least one application definition, and that definition must not have the Explorer or Trusted strategy. An error message is generated if you violate this rule.

| 2 of 7 | Select available tags or content categories to be included or excluded from the rule. You must include at least one tag or content category to use the exclude tag option. Click Add item to create a new tag. Click Next. |

| 3 of 7 (optional) | Select the Select from list option, then select file types from the available list. Use the Other File Types option to select unlisted (unknown) file types. Click Next. |

| 4 of 7 (optional) | Select the Select from list option, then select file extensions from the available list. Click Next. |

The extensions .dll and .exe are preselected as Exclude. This is because certain applications open a great many such files, and including them can cause a serious deterioration in performance. You can deselect the exclusion for greater protection, but be aware of the potential performance tradeoff.

| 5 of 7 (optional) | Select a document properties definition or definition group from the available list. You can include or exclude definitions. Click Add item to create a new document properties definition or Add group to create a new document properties group. Click Next. |

| 6 of 6 | Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. The only options for application file access rules are Monitor, Notify User, and Store Evidence. If you select Monitor, click Severity to modify the value. |

| 7 of 7 (optional) | Select an assignment group or groups, or define a new group by clicking Add. Click Finish. |

You can include or exclude tags and file extensions as well as application definitions.

5 To activate the rule, right-click the protection rule icon and select Enable.

**Create and define a clipboard protection rule**

Clipboard protection rules block use of the clipboard to copy sensitive data.

Clipboard protection has been enhanced to include the following:

- Blocking copy/paste from any application into ICQ or IM
- Blocking copy/paste of any data to Skype
- Blocking copy/paste from Microsoft Office applications (Word, Excel, PowerPoint) to Microsoft Office Communicator

These enhancements are in addition to the previous capability to:
• Block copy/paste from Microsoft Word, Excel, or PowerPoint to any other application (that is, allow copy/paste only from Word to Word, from Excel to Excel, or from PowerPoint to PowerPoint)

• Block copy/paste from one Word document to another

**Task**

For option definitions, press F1.

1 In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**

   The available protection rules appear in the right-hand pane.

2 In the **Protection Rules** pane, right-click and select **Add New | Clipboard Protection Rule**.

3 Rename the rule to something that will help you recognize its specific function.

4 Double-click the rule icon and follow these steps in the wizard:

   **Step** | **Action**
   --- | ---
   1 of 6 (optional) | Select an application definition or definitions from the available list. You can include or exclude definitions. Click **Add item** to create a new application definition. Click **Next**.
   2 of 6 (optional) | Type the title of a specific application window and click **Add**. Repeat as required. Click **Next**.
   3 of 6 (optional) | Select tags, content categories, and groups to be included or excluded from the rule. You must include at least one tag, content category, or group to use the exclude option. Click **Add item** to create a new tag or content category. Click **Add group** to create a new tag and content category group. Click **Next**.
   4 of 6 | Select the pasting limitation. By default, the rule will block pasting outside the current application. The second option is to restrict pasting into different documents in the current application. This more restrictive rule also blocks pasting into the Find and Replace dialog box, but prevents sensitive information from being copied from tagged documents to untagged documents in the same application. The third option blocks pasting into specified applications, either by including or excluding the selected applications.
   5 of 6 | Select actions from the available list. By default, selecting an action selects both **Online** and **Offline**. Deselect either as required. If you select **Monitor**, click **Severity** to modify the value. If you select **Notify User**, click **Change default alert** to modify the alert message. Click **Next**.
   6 of 6 (optional) | Select an assignment group or groups, or define a new group by clicking **Add**. Click **Finish**.

You can include or exclude tags as well as application definitions.

5 To activate the rule, right-click the protection rule icon and select **Enable**.

**See also**

*Improved clipboard protection rules on page 134*
Create and define a cloud protection rule

Cloud protection rules monitor or block sensitive content being uploaded to the cloud with common cloud applications.

**Before you begin**

Verify that required cloud protection handlers are activated on the Agent Configuration | Miscellaneous tab. Verify that cloud protection event notification messages are specified on the Agent Configuration | User Interface Service tab.

Supported cloud applications are:

- Box.inc
- Dropbox
- Google Drive
- SkyDrive
- Syncplicity

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Protection Rules. The available protection rules appear in the right pane.

2. Right-click in the right pane and select Add New | Cloud Protection Rule.

3. Rename the rule to something that helps you recognize its specific function.
4 Double-click the rule icon and follow these steps in the wizard. Click Next after each step.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 8</td>
<td>Select one or more cloud applications to manage. Click Next.</td>
</tr>
<tr>
<td>2 of 8 (optional)</td>
<td>Select tags, content categories, and groups to include or exclude from the rule. You must include at least one tag, content category, or group to use the exclude option. Click Add item to create a tag or content category. Click Add group to create a tag and content category group.</td>
</tr>
<tr>
<td>3 of 8 (optional)</td>
<td>Select the Select from list option, then select file types from the available list. Use the Other File Types option to select unlisted (unknown) file types.</td>
</tr>
<tr>
<td>4 of 8 (optional)</td>
<td>Select the Select from list option, then select file extensions from the available list.</td>
</tr>
<tr>
<td>5 of 8 (optional)</td>
<td>Select a document properties definition or definition group from the available list. You can include or exclude definitions. Click Add item to create a document properties definition or Add group to create a document properties group.</td>
</tr>
<tr>
<td>6 of 8 (optional)</td>
<td>To apply the rule to specific encryption types, select the Select from list option, and select one or more encryption types.</td>
</tr>
<tr>
<td>7 of 8</td>
<td>Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text.</td>
</tr>
</tbody>
</table>

Due to a limitation in Adobe LiveCycle, the Apply RM Policy action is only available for Microsoft RMS and Seclore FileSecure.

| 8 of 8 (optional) | Select an assignment group or groups, or define a new group by clicking Add. Click Finish. |

You can include or exclude tags and file extensions.

5 To activate the rule, right-click the protection rule icon and select Enable.

See also
Cloud protection rules on page 134

Create and define an email protection rule
Email protection rules monitor or block email sent to specific destinations or users.

Before you begin
To activate Lotus Notes support, select the Lotus Notes Handler on the Agent Configuration | Miscellaneous tab. 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 Titus Message Classification lists as content categories, see the section on setting up integration, and verify that the Agent Configuration settings specified in that section are correct.
**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**. The available protection rules appear in the right-hand pane.

2. In the **Protection Rules** pane, right-click and select **Add New | Email Protection Rule**.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 9 (optional)</td>
<td>Select <strong>Select from list</strong> option, and select one or more email destination definitions. Click <strong>Add item</strong> to create a new email destination definition, or <strong>Add group</strong> to create a new destination group. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>2 of 9 (optional)</td>
<td>Select tags, content categories, and groups to be included or excluded from the rule. You must include at least one tag to use the exclude tag option. Click <strong>Add item</strong> to create a new tag or content category. Click <strong>Add group</strong> to create a new tag and content category group. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>3 of 9 (optional)</td>
<td>Select the <strong>Select from list</strong> option, then select file types from the available list. Use the <strong>Other File Types</strong> option to select unlisted (unknown) file types. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>4 of 9 (optional)</td>
<td>Select the <strong>Select from list</strong> option, then select file extensions from the available list. Click <strong>Next</strong>. You can include or exclude file extensions.</td>
</tr>
<tr>
<td>5 of 9 (optional)</td>
<td>Select a document properties definition or definition group from the available list. You can include or exclude definitions. Click <strong>Add item</strong> to create a new document properties definition or <strong>Add group</strong> to create a new document properties group. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>6 of 9 (optional)</td>
<td>To apply the rule to attachments of specific encryption types, select the <strong>Select from list</strong> option, and select one or more attachment encryption types.</td>
</tr>
<tr>
<td>7 of 9 (optional)</td>
<td><strong>Email bypass feature:</strong> To exclude an email based on subject, select <strong>Do not apply this rule if the email subject contains this pattern</strong> and select a pattern.</td>
</tr>
<tr>
<td>8 of 9</td>
<td>Select actions from the available list. By default, selecting an action selects both <strong>Online</strong> and <strong>Offline</strong>. Deselect either as required. If you select <strong>Monitor</strong>, click <strong>Severity</strong> to modify the value. If you select <strong>Notify User</strong>, click <strong>Change default alert</strong> to modify the alert message, URL, or link text. If you want <strong>Request Justification</strong> to block email when no justification is provided, you must also select <strong>Block</strong>. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>9 of 9 (optional)</td>
<td>Select an assignment group or groups, or define a new group by clicking <strong>Add</strong>. Click <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>

5. To activate the rule, right-click the protection rule icon and select **Enable**.

**See also**
*How sensitive content is controlled in email on page 97*
Create and define a file system protection rule

File system protection rules protect files on specific file servers or mass storage devices. Files can be monitored, but not blocked. You can save evidence, and notify the user when files are monitored. You can specify applications, file types, file extensions, or tags to limit to the rule.

Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Protection Rules

   The available protection rules appear in the right-hand pane.

2. In the Protection Rules pane, right-click and select Add New | File System Protection Rule.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

   Step   Action
   1 of 9  Select a destination or destinations where files are being sent. If you select File Servers, the Configure Selection window opens. Type a network path and click Add, or click Browse to select a new network destination, then Add to add it to the list. Click Next.

   2 of 9 (optional)  Select an application definition or definitions from the available list. You can include or exclude definitions. Click Add item to create a new application definition. Click Next.

   3 of 9 (optional)  Select tags, content categories, and groups to be included or excluded from the rule. You must include at least one tag, content category, or group to use the exclude option. Click Add item to create a new tag or content category. Click Add group to create a new tag and content category group. Click Next.

   4 of 9 (optional)  Select the Select from list option, then select file types from the available list. Use the Other File Types option to select unlisted (unknown) file types. Click Next.

   5 of 9 (optional)  Select the Select from list option, then select file extensions from the available list. Click Next.

   6 of 9 (optional)  Select a document properties definition or definition group from the available list. You can include or exclude definitions. Click Add item to create a new document properties definition or Add group to create a new document properties group. Click Next.

   7 of 9 (optional)  To apply the rule to files with specific encryption types, select the Select from list option, and select one or more encryption types.

   8 of 9  Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you want Request Justification to encrypt files when no justification is provided, you must also select Encrypt. Click Next.

   9 of 9 (optional)  Select an assignment group or groups, or define a new group by clicking Add. Click Finish.

   You can include or exclude tags and file extensions as well as application definitions.

5. To activate the rule, right-click the protection rule icon and select Enable.
Create and define a network communication protection rule

Network communication protection rules monitor or block incoming or outgoing data on your network. You can limit the rule with specific applications or tags.

Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Protection Rules. The available protection rules appear in the right-hand pane.

2. In the Protection Rules pane, right-click and select Add New | Network Communication Protection Rule.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

   - **Step 1 of 7 (optional)** Select the Select from list option, then select one or more available network address ranges. You can protect or exclude range definitions. Click Add item to create a new network address range definition. Click Add group to create a new network address range group. Click Next.

   - **Step 2 of 7 (optional)** Select the Select from list option, then select one or more available network port ranges. You can protect or exclude range definitions. Click Add item to create a new network port range definition. Click Add group to create a new network port range group. Click Next.

   - **Step 3 of 7** Select the network connection direction. You can protect incoming or outgoing connections or both directions. Click Next.

   - **Step 4 of 7 (optional)** Select an application definition or definitions from the available list. You can include or exclude definitions. Click Add item to create a new application definition. Click Next.

   - **Step 5 of 7 (optional)** Select tags to be included or excluded from the rule. You must include at least one tag to use the exclude tag option. Click Add item to create a new tag. Click Next.

   - **Step 6 of 7** Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text. Click Next.

   - **Step 7 of 7 (optional)** Select an assignment group or groups, or define a new group by clicking Add. Click Finish.

   - You can include or exclude tags as well as application definitions.

5. To activate the rule, right-click the protection rule icon and select Enable.

Create and define a PDF/Image Writer protection rule

McAfee DLP Endpoint software can block PDF and Image Writer print drivers that print to files.
**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**. The available protection rules appear in the right-hand pane.

2. In the **Protection Rules** pane, right-click and select **Add New | PDF/Image Writers Protection Rule**.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

   **Step** | **Action**
   --- | ---
   **1 of 2** | Select actions from the available list. By default, selecting an action selects both **Online** and **Offline**. Deselect either as required. If you select **Monitor**, click **Severity** to modify the value. If you select **Notify User**, click **Change default alert** to modify the alert message, URL, or link text. If you want **Request Justification** to block printing when no justification is provided, you must also select **Block**. Click **Next**.

   **2 of 2 (optional)** | Select an assignment group or groups, or define a new group by clicking **Add**. Click **Finish**.

5. To activate the rule, right-click the protection rule icon and select **Enable**.

**Create and define a printing protection rule**
Printing protection rules monitor or block files from being printed. You can limit the rule to specific applications or tags.

Printer add-ins, enabled on the **Agent Configuration | Miscellaneous** tab, can improve printer performance when using certain common applications. The add-ins are only installed when a printing protection rule is enabled on the managed computer.

**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**. The available protection rules appear in the right-hand pane.

2. In the **Protection Rules** pane, right-click and select **Add New | Printing Protection Rule**.

3. Rename the rule to something that will help you recognize its specific function.
Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 6 (optional)</td>
<td>Select the Select from list option, then select an available network printer. Select Other network printer to protect all network printers that have not been defined, including PDF and Image Writer printer drivers. Click Next.</td>
</tr>
<tr>
<td>2 of 6 (optional)</td>
<td>Select the Select from list option, then select Any local printer to protect printing from local printers. Click Next.</td>
</tr>
<tr>
<td>3 of 6 (optional)</td>
<td>Select an application definition or definitions from the available list. You can include or exclude definitions. Click Add item to create a new application definition. Click Next.</td>
</tr>
<tr>
<td>4 of 6 (optional)</td>
<td>Select tags, content categories, and groups to be included or excluded from the rule. You must include at least one tag, content category, or group to use the exclude option. Click Add item to create a new tag or content category. Click Add group to create a new tag and content category group. Click Next.</td>
</tr>
<tr>
<td>5 of 6</td>
<td>Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text. If you want Request Justification to block printing when no justification is provided, you must also select Block. Click Next.</td>
</tr>
<tr>
<td>6 of 6 (optional)</td>
<td>Select an assignment group or groups, or define a new group by clicking Add. Click Finish.</td>
</tr>
</tbody>
</table>

Only one of the first two steps can be optional. You must select a network printer, local printers, or both.

You can include or exclude tags as well as application definitions.

To activate the rule, right-click the protection rule icon and select Enable.

Create and define a removable storage protection rule
Removable storage protection rules monitor or block data from being written to removable storage devices.

**Task**
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Protection Rules. The available protection rules appear in the right-hand pane.
2. In the Protection Rules pane, right-click and select Add New | Removable Storage Protection Rule.
3. Rename the rule to something that will help you recognize its specific function.
4 Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 8 (optional)</td>
<td>Select an application definition or definitions from the available list. You can include or exclude definitions. Click <strong>Add item</strong> to create a new application definition. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>2 of 8 (optional)</td>
<td>Select tags, content categories, and groups to be included or excluded from the rule. You must include at least one tag, content category, or group to use the exclude option. Click <strong>Add item</strong> to create a new tag or content category. Click <strong>Add group</strong> to create a new tag and content category group. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>3 of 8 (optional)</td>
<td>Select the <strong>Select from list</strong> option, then select file types from the available list. Use the <strong>Other File Types</strong> option to select unlisted (unknown) file types. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>4 of 8 (optional)</td>
<td>Select the <strong>Select from list</strong> option, then select file extensions from the available list. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>5 of 8 (optional)</td>
<td>Select a document properties definition or definition group from the available list. You can include or exclude definitions. Click <strong>Add item</strong> to create a new document properties definition or <strong>Add group</strong> to create a new document properties group. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>6 of 8 (optional)</td>
<td>To apply the rule to specific encryption types, select the <strong>Select from list</strong> option, and select one or more encryption types.</td>
</tr>
<tr>
<td>7 of 8</td>
<td>Select actions from the available list. By default, selecting an action selects both <strong>Online</strong> and <strong>Offline</strong>. Deselect either as required. If you select <strong>Encrypt</strong>, click <strong>Select an Encryption key</strong> to select an encryption key or add a new key. If you select <strong>Monitor</strong>, click <strong>Severity</strong> to modify the value. If you select <strong>Notify User</strong>, click <strong>Change default alert</strong> to modify the alert message, URL, or link text. If you want <strong>Request Justification</strong> to block files when no justification is provided, you must also select <strong>Block</strong>. If you want <strong>Request Justification</strong> to encrypt files when no justification is provided, you must also select <strong>Encrypt</strong>. Click <strong>Next</strong>.</td>
</tr>
<tr>
<td>8 of 8 (optional)</td>
<td>Select an assignment group or groups, or define a new group by clicking <strong>Add</strong>. Click <strong>Finish</strong>.</td>
</tr>
</tbody>
</table>

You can include or exclude tags and file extensions as well as application definitions.

5 To activate the rule, right-click the protection rule icon and select **Enable**.

See also

*Removable storage protection rule enhancement on page 135*

**Create and define a screen capture protection rule**

Screen capture protection rules control data copy/pasted from a screen.

---

**Before you begin**

The screen capture module must be enabled in the Agent configuration. In the **Miscellaneous** tab, select **Screen Capture** and at least one of the options: the **Print Screen key handler** option enables keyboard screen capture blocking; the **Applications handler** option allows blocking of third-party screen capture programs. If you select the **Applications handler** option, specify which applications are blocked in the **Advanced Configuration** tab with **Screen capture applications | Settings**.

The screen capture feature supports only Graphics Device Interface (GDI) API blocking. Applications capturing the screen through DirectX or the Windows Media Player API are not blocked.
Task
For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Protection Rules. The available protection rules appear in the right-hand pane.

2. In the Protection Rules pane, right-click and select Add New | screen Capture Protection Rule.

3. Rename the rule to something that will help you recognize its specific function.

4. Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 5 (optional)</td>
<td>Select an application definition or definitions from the available list. You can include or exclude definitions. Click Add item to create a new application definition. Click Next.</td>
</tr>
</tbody>
</table>

- Trusted processes are not part of the screen capture rule logic. Applications with a Trusted strategy are therefore not exempt from screen capture rules, and will be blocked like any other applications.

| 2 of 5 | Type the title of a specific application window and click Add. Repeat as required. Click Next. |

| 3 of 5 (optional) | Select tags to be included or excluded from the rule. You must include at least one tag to use the exclude tag option. Click Add item to create a new tag. Click Next. |

| 4 of 5 | Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text. Click Next. |

| 5 of 5 (optional) | Select an assignment group or groups, or define a new group by clicking Add. Click Finish. |

You can include or exclude tags as well as application definitions.

5. To activate the rule, right-click the protection rule icon and select Enable.

Create and define a web post protection rule
Web post protection rules monitor or block data from being posted to websites, including web-based email sites.

The web post protection rule is supported for Microsoft Internet Explorer 6 and later, and Mozilla Firefox 3.6 and later. For other browsers, use network communication protection rules.

Web post protection rules can block or monitor content uploaded to websites based on AJAX or Flash technologies. This includes the following sites:

- Microsoft Outlook Web Access
- Gmail
- Google Docs
- Yahoo
- Hotmail

When a web post protection rule is enabled, web post file uploads continue in the background after the upload bar indicates that the upload is finished.
Task
For option definitions, click ? in the interface.

1  In the McAfee DLP Endpoint policy console navigation pane, select Content Protection | Protection Rules.
The available protection rules appear in the right-hand pane.

2  In the Protection Rules pane, right-click and select Add New | Web Post Protection Rule.

3  Rename the rule to something that will help you recognize its specific function.

4  Double-click the rule icon and follow these steps in the wizard:

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 of 8 (optional)</td>
<td>Select the Select from list option, then select an available web destination or web destination group for this rule. Click Add item to create a new web destination definition. Click Add group to create a new web destination group. Click Next.</td>
</tr>
<tr>
<td>2 of 8 (optional)</td>
<td>Select tags, content categories, and groups to be included or excluded from the rule. You must include at least one tag, content category, or group to use the exclude option. Click Add item to create a new tag or content category. Click Add group to create a new tag and content category group. Click Next.</td>
</tr>
<tr>
<td>3 of 8 (optional)</td>
<td>Select the Select from list option, then select file types from the available list. Use the Other File Types option to select unlisted (unknown) file types. Click Next.</td>
</tr>
<tr>
<td>4 of 8 (optional)</td>
<td>Select the Select from list option, then select file extensions from the available list. Click Next.</td>
</tr>
<tr>
<td>5 of 8 (optional)</td>
<td>Select a document properties definition or definition group from the available list. You can include or exclude definitions. Click Add item to create a new document properties definition or Add group to create a new document properties group. Click Next.</td>
</tr>
<tr>
<td>6 of 8 (optional)</td>
<td>To apply the rule to specific encryption types, select the Select from list option, and select one or more encryption types.</td>
</tr>
<tr>
<td>7 of 8</td>
<td>Select actions from the available list. By default, selecting an action selects both Online and Offline. Deselect either as required. If you select Monitor, click Severity to modify the value. If you select Notify User, click Change default alert to modify the alert message, URL, or link text. If you want Request Justification to block web posts when no justification is provided, you must also select Block. Click Next.</td>
</tr>
<tr>
<td>8 of 8 (optional)</td>
<td>Select an assignment group or groups, or define a new group by clicking Add. Click Finish.</td>
</tr>
</tbody>
</table>

You can include or exclude tags and file extensions.

5  To activate the rule, right-click the protection rule icon and select Enable.
Delete rules, definitions, device classes, or user groups
Rules, device classes, or definitions can be deleted from policies, but not if they are in use.
You cannot remove a definition or device class that is in use. Before removing, you must deselect it in all rules and groups that contain it. To remove tags, you must either remove the rules that use them, or remove the tags from the rules, before proceeding.

If you don't know if or where the item is in use, attempt to remove it. If the item is in use, a message identifies which rules or groups contain it.

Task
1 In the McAfee DLP Endpoint policy console navigation pane, select the category (for example, Network definition) of the item you want to remove.
   The available items and groups appear in the main panel.
2 Select the item or group to remove, right-click and select Delete.
3 Click Yes to confirm the deletion.

Using predefined definitions
Templates are predefined system definitions such as application definitions or text patterns.
Using the template synchronizer wizard, you can copy templates to an existing policy or create new templates from definitions created for the current system policy. Policy definitions stored in the templates directory can be shared or used later.

When distributing a template to create a Plug and Play device definition, make sure that any device classes used in definitions are included in the system’s defaults. If you use a device class that is not in the system default, the definition is removed with a notification message.

Synchronize templates
Templates are predefined system definitions such as application definitions or text patterns.
Use this task to synchronize templates with the current policy.

Task
For option definitions, press F1.
1 From the McAfee DLP Endpoint policy console File menu, select Synchronize Templates.
   The Template Synchronization wizard appears.
2 Select the template type from the tabs.
Where there is no match between the templates folder and the current system policy the definition will be displayed as missing.

![Figure 11-3 The Template Synchronization Wizard](image)

3 To view the selected definition properties, click View ( ). To remove the selected definition, click Delete ( ).

4 To copy a template to the current policy, or create a new template from a current policy definition, select the definition and click one of the Move icons or .

The definition entry is changed from Missing to the definition name.

5 Click OK.

Limiting rules with assignment groups

Device and protection rules are applied equally for every computer and user receiving a policy, unless otherwise specified in the rule. However, when required, rules can be applied to particular users, groups, organizational units, or computers.

Defining assignment groups can be done with either Microsoft Active Directory or OpenLDAP. The flexibility to define specific users or groups allows administrators to apply rules that are appropriate for a user’s job function. Individuals or computers that should not access sensitive data can have restrictive rule sets, while a manager’s rule set can be much less restrictive. When protection rules are created, they can be applied to a specific user or group by using the assignment group, or to computers by using ePolicy Orchestrator deployment.

Contents
- User assignment
- Computer assignment groups
**User assignment**

Device and protection rules are applied equally for every computer and user receiving a policy, unless otherwise specified in the rule. However, when required, rules can be applied to particular users, groups, organizational units, or computers.

The **Privileged Users** setting can be used to override blocking or monitoring rules for certain users. There are two strategies available for privileged users: **Monitor only** and **Override all**. You create the list in a similar manner to creating the user assignment groups — by scanning the user list and selecting names.

In addition, you can include or exclude users from the rule the group is assigned to, or add local users to a user assignment group.

Excluded users are similar to privileged users, in that they are exempt from particular rules. The difference is that the excluded user is defined in the assignment group, so only that one group need be assigned to a rule. On the other hand, you can’t monitor that user if the group is being blocked. The option to use excluded users or privileged users gives the administrator considerable flexibility in how rules are applied.

Local users are defined as users logged on remotely who have local authentication.

**Create a user assignment group**

User assignment groups define groups of users to be included or excluded from rules.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under **Policy Assignment**, select **User Assignment Groups**.
   
   The available assignment groups appear in the right-hand pane.

2. In the **User Assignment Groups** pane, right-click and select **Add New | User Assignment Group**.

   The new **User Assignment Group** icon appears.

3. Name the new User Assignment Group entry and double-click the icon.

   The edit window appears with the **Policy Assignment** tab displayed.

4. Click **Add** to select the objects for this group (domains, organizational units, groups, and users).

   A search window appears.

5. Select the **Object Types** to search for, then type in a filter and click **Search** to find users and groups.

6. Select the users and groups to be added to the assignment group, and click **OK**.
7. Users and groups are included by default. To exclude any of them from the rules the group is assigned to, make the appropriate selection.

<table>
<thead>
<tr>
<th>Policy assignments</th>
<th>Protection rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the participating user-groups and organizational units:</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Path</td>
</tr>
<tr>
<td>Domain Guests (demo.loc)</td>
<td>demo.loc\Users\Domain Guests</td>
</tr>
<tr>
<td>Guests (Bulk)</td>
<td>demo.loc\Guests</td>
</tr>
<tr>
<td>Mail Users (demo.loc)</td>
<td>demo.loc\Marketing\Mail Users</td>
</tr>
<tr>
<td>Marketing (demo.loc)</td>
<td>demo.loc\Marketing</td>
</tr>
<tr>
<td>Sales Users (demo.loc)</td>
<td>demo.loc\Sales</td>
</tr>
<tr>
<td>Local Users (demo.loc)</td>
<td>demo.loc\Local Users</td>
</tr>
</tbody>
</table>

Identify LDAP Objects using:

- Add Local Users
- Add...
- Remove

**Figure 11-4 Including and excluding users**

8. To add local users to the group, click **Add Local Users**.

9. If you created rules to assign the group to, click the **Protection Rules** tab to select the protection rules for this assignment group. When you have finished making selections, click **OK**.

   - The order doesn’t matter. You can create rules first and assign them to a group in this step, or create groups first and assign them to rules when you create the rules.

**Create a privileged users group**

The Privileged Users setting can be used to override blocking or monitoring rules for certain users.

**Task**

For option definitions, press F1.

1. In the McAfee DLP Endpoint policy console navigation pane under **Policy Assignment**, select **Privileged Users**.

   - The available groups appear in the right-hand pane.

2. In the **Privileged Users** pane, right-click, and select **Scan users and groups**.

   - A search window opens.

3. Select the **Object Types** to search for, then type in a filter and click **Search** to find users and groups.

4. Select the users and groups to be added to the privileged users group, and click **OK**.

   - The new **Privileged Users** icon appears in the window.

5. The default strategy for privileged users is **Override All**. To change this, right-click the group icon and click **Set Strategy | Monitor Only**.
Computer assignment groups

Computer assignment groups specify which computers are assigned which policies. You can use this feature to apply different policies to groups of computers in your network. When a computer group is assigned specific policies, those policies are enforced on the named computers, and user assignment groups in McAfee DLP Endpoint rules are lost.

Computer assignment groups is a feature of ePolicy Orchestrator. It is being described here because of the effect on McAfee DLP Endpoint rules. Computer assignment groups are accessed from the Policy Catalog by specifying the Computer Assignment Group Category.

Assigning policies with computer assignment groups

The computer assignment group feature allows you to choose which McAfee DLP Endpoint rules you want to assign to a particular group of computers.

Figure 11-5  Assigning rules with ePO computer assignment groups

If, for example, you have assigned Marketing computers to a group, and then select an email protection rule and a web post protection rule in the computer assignment group definition, those DLP rules are applied to all users in the Marketing computer group, and not according to any User Assignment Groups defined in the DLP protection rule. Any rules not included in the computer assignment group (for example, a removable storage protection rule) are applied according to the User Assignment Group definition in the rule.
Monitoring and reporting

This section describes the DLP Incident Manager and how to use it to track and review policy violations, and DLP Operational Events, which is used to track administrative events such as agent deployment, policy refresh, and so forth.

Chapter 12  Monitoring and reporting events
Chapter 13  Users and permission sets
Chapter 14  Non-routine operations
Chapter 15  Diagnostics
Monitoring and reporting events

Administrators view security events in the DLP Incident Manager.

McAfee DLP Endpoint version 9.3.x 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 the McAfee DLP Endpoino software on a managed computer determines a policy violation has occurred, it generates an event and sends it to the ePolicy Orchestrator 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 Endpoint 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
- Collecting and managing data
- Redaction and role-based access control

Collecting and managing data

Monitoring the system consists of gathering and reviewing evidence and events, and producing reports. Data from the DLP tables in the ePolicy Orchestrator 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
- DLP Incident Manager/DLP Operational Events
- Incident tasks
- Edit the task runner
- Creating reports
- Working with the database
- Documenting events with evidence
DLP Incident Manager/DLP Operational Events

Administrators use the DLP Incident Manager page in ePolicy Orchestrator to view the security events from policy violations along with the evidence and hit highlighting specified in the agent configuration, as well as hit counts and other details. It also defines Incident Tasks. Administrators use the DLP Operational Events page to view administrative events such as agent deployments.

To improve security, McAfee DLP Endpoint software version 9.3 has eliminated the WCF communications link formerly used to connect the ePolicy Orchestrator database to the McAfee DLP Monitor. The new monitor interface is an integral part of ePolicy Orchestrator and consists of two ePolicy Orchestrator pages:

- DLP Incident Manager — to display security events
- DLP Operational Events — to display administrative events

A new feature, Incident Tasks, is included as a tab in the Incident Manager. In version 9.3, three tasks are available: email notification of policy violations, purging according to predefined criteria, and setting a reviewer.

How it works

The Incident List tab of the DLP Incident Manager has all of the functionality of the old McAfee DLP Monitor. Event details are viewed by clicking on a specific event. You can create and save filters to modify the view. You can also modify the view by selecting and ordering columns. You can label individual events (for filtering by label) and set properties for status, resolution, and assigned reviewer. Color-coded icons and numerical ratings for severity have been added to facilitate quick visual scanning of events. A new feature allows collating evidence files from multiple events to a single email. The DLP Operational Events page works in an identical manner with administrative events.

How it works

The Incident List tab of the DLP Incident Manager has all of the functionality of the old McAfee DLP Monitor. Event details are viewed by clicking on a specific event. You can create and save filters to modify the view. You can also modify the view by selecting and ordering columns. You can label individual events (for filtering by label) and set properties for status, resolution, and assigned reviewer. Color-coded icons and numerical ratings for severity have been added to facilitate quick visual scanning of events. A new feature allows collating evidence files from multiple events to a single email. The DLP Operational Events page works in an identical manner with administrative events.

Figure 12-1  DLP Incident Manager

Use the Incident Tasks tab to set criteria for scheduled tasks. For email tasks you set up the email (recipients, subject, body) as well as define the criteria that will trigger it being sent.

The Incident Tasks tab works with ePolicy Orchestrator Server Tasks to schedule tasks. A new server task, DLP tasks runner, is installed with the McAfee DLP Endpoint software for this purpose. The Incident List tab works with ePolicy Orchestrator Queries & Reports to create reports and display data on ePolicy Orchestrator dashboards.
**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
- Reviewer

The reviewer can be any ePolicy Orchestrator 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.

**View event details**

You can view event details and evidence from the DLP Incident Manager page. You can also assign a reviewer, and edit the severity, status, and resolution of the incident.

**Task**

1. In ePolicy Orchestrator, select **Menu | Data Protection | DLP Incident Manager**.
2. In the **Incident List** pane, sort the list by clicking any column. Sort by severity, time of day, user, and so forth.
3. Click an event in the list to display its full details. The event information appears in the **DLP Incident Information** pane.
4 To view redacted fields, select Actions | Release Redaction. In the dialog box that appears, enter the user name and password of an administrator with permission to reveal sensitive data. Redacted evidence is viewed in a similar manner.

Depending on how the role-based permissions are set up, two administrators might be required: one with permission to view the DLP Incident Manager display (except sensitive text), the other with permission to view sensitive text. See Create and define permission sets in this guide for information on setting up the permission sets.

5 If Store Evidence is part of the protection or discovery rule producing the event, the number of evidence files is displayed on the Evidence tab in the lower section of the DLP Incident Information pane. To view the evidence file, select the tab to display the file list. Click a link to display the evidence file.

Figure 12-2 Incident List detail

Define filters
When viewing events on the DLP Incident Manager or DLP Operational Events pages, you might need to reduce the amount of information shown to see relevant details at a glance. You can apply a filter to define specific criteria to reduce the list of events to only relevant data.

The McAfee DLP Endpoint version 9.3 monitoring features (DLP Incident Manager and DLP Operational Events) do not have predefined filters (except for time filters), only user-defined filters.

For DLP Operational Events, only DLP operational event properties and DLP labels are displayed as filter options.

When you create a new filter, it is displayed as unsaved in the Filter window, and is preserved for that user session. That is, you can switch between unsaved and no custom filter without losing the filter. You must save the filter before closing the user session (that is, logging off of ePolicy Orchestrator) or if you want to work with more than one filter.

Filter parameters can define events (Event ID, Event Type), aspects of the policy (File Types, Reactions), or properties (Resolution, Status). If you have created DLP Labels, you can use them to define filters.
Task
For option definitions, click ? in the interface.

1 Select the event list you want to filter:
   - Select Menu | Data Protection | DLP Incident Manager for the Incidents List page.
   - Select Menu | Data Protection | DLP Operational Events for the Operational Events List page.

2 Select Actions | Filter | Edit Filter – or click Edit next to the Filter window.

3 Add properties from the Available Properties list by clicking the arrow to the right of the property name. Fill in the Comparison and Value fields using the drop-down lists or by typing in the value.
   - You can remove a property by clicking the arrow to the left of the Property field, or add more values to a property by clicking +.

   Use the property Occurred (UTC) to add times and Occurred (Endpoint) to add dates. The property Occurred refers to online/offline status.

4 Click Update Filter to apply the filter.

   The message (unsaved) appears in the Filter drop-down list window. An unsaved filter remains available until you log off ePolicy Orchestrator.

5 To save the filter for future use, select Actions | Filter | Save Filter.
   - You are prompted for a name, and are asked to define the filter as Private or Public. Click OK when you are finished.

   To delete a filter, select it from the Filter drop-down list, then select Actions | Filter | Delete Filter.

Example - Filter by agent version
If you are using McAfee DLP Endpoint in backward-compatible mode and have multiple client versions deployed, you might want to look only at results from a particular client version. To do this, do the following:

1 In the DLP Incidents section of the property list, select Agent version.
   - This property refers to the McAfee DLP Endpoint client version, not the McAfee Agent version. That property is listed as Product Version (Agent).

2 In the Comparison field, select a value that includes or excludes the targeted agent version. The Value field must be entered from a list. The software scans all incidents and only lists existing values.

See also
Use labels to mark events on page 161

Use labels to mark events
Customized labels allow you to mark events with a unique tag. The events can then be easily sorted and filtered by these customized labels.

Task
1 In ePolicy Orchestrator, select Menu | Data Protection | DLP Incident Manager.
   - Labels can be used with DLP Operational Events in a similar manner. They also appear in incident queries.
To add a label select an event or several events.

- Select Add then type a new label name. Click OK.
- Select Replace All then select an existing label or labels. Click OK.

The label or labels are attached to the events. You can now use these labels to filter or sort the list.

To remove labels:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>To remove a label from specific events</td>
<td>Select the event or events, then select Actions</td>
</tr>
<tr>
<td>To remove a label from all events</td>
<td>select Actions</td>
</tr>
</tbody>
</table>

See also

*Define filters on page 160*

**Incident tasks**

The Incident Tasks tab of the DLP Incident Manager uses ePolicy Orchestrator Server Tasks to perform operations when certain criteria are met.

In the current version, three incident tasks are supported:

- **Mail notification** — used to inform users, managers, or others based on specified criteria
- **Set reviewer** — used to restrict viewing access when assigning incidents to a reviewer or group
- **Purge** — used to purge incidents from the database. Criteria can include any incident field, as well as ePolicy Orchestrator tags or system tree path.

The tasks are run by the DLP tasks runner server task.

**Use case — creating a new incident task**

Click Actions | New and select one of the three task types. Fill in required and optional fields in the Task Properties pane. Add and define properties in the incident properties pane. Save the task.

Incident property values can only be added from values that exist in the database. You cannot create a task based on theoretically expected results.

**Use case — changing the view**

The Incident Tasks view is customizable. Select Actions | Choose columns to view the Select the Columns to Display page. You can add or delete columns and rearrange the order. Click Save to enable the customized view, or Use Default to return to the standard view.

**Use case — enabling/disabling, editing, deleting**

In the default view, the Actions column is displayed, allowing you to Edit, Enable/Disable, or Delete the task directly in the Incident Tasks page. If the column is not displayed, select Actions | Set to enable/disable, Actions | Edit to edit, or Actions | Delete to remove a task.
**Edit the task runner**

The ePolicy Orchestrator server task DLP task runner schedules and runs tasks set up in DLP Incident Manager Incident Tasks.

**Before you begin**

Set up one or more tasks in DLP Incident Manager Incident Tasks.

The DLP task runner has a default schedule of once a day, but no tasks are enabled by default. You must edit the default settings to run any tasks, or create a new task runner task.

**Task**

For option definitions, press F1.

1. On the ePolicy Orchestrator Server Tasks page, click **New Task**.
   
   The Server Task Builder appears.

2. On the **Description** page, type a name for the task. Click **Next**.

3. On the **Actions** page, select **DLP incident tasks runner** from the **Actions** drop-down list. Click **Select Tasks** and select the tasks from the list.

   ![Figure 12-3 Editing the task runner](image)

   Tasks are displayed on the **Actions** page.

4. Use the arrows to set the task order, or delete tasks you don't want to run by clicking X.

5. On the **Schedule** page, adjust the schedule as required. Click **Next**.

6. Review the settings, then click **Save**.

**Creating reports**

McAfee DLP Endpoint uses ePolicy Orchestrator 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.

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 twenty-eight queries, including the rollup queries, can be found in the ePolicy Orchestrator console under **Menu | Reporting | Queries & Reports | Shared Groups**.

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

### Report options

McAfee DLP Endpoint software uses ePolicy Orchestrator Reports to review events. In addition, you can view information on product properties on the ePolicy Orchestrator Dashboard.

### ePolicy Orchestrator Reports

McAfee DLP Endpoint software integrates reporting with the ePolicy Orchestrator reporting service. For information on using the ePolicy Orchestrator reporting service, see the **McAfee ePolicy Orchestrator Product Guide**.

ePolicy Orchestrator rollup queries and rolled up reports, which summarize data from multiple McAfee ePO databases, are supported.

ePolicy Orchestrator Notifications are supported. See the **Sending Notifications** topic in the **McAfee ePolicy Orchestrator Product Guide** for details.

### ePO Dashboard/ePO Reports

You can view information on DLP product properties in the ePolicy Orchestrator **Menu | Reporting | Dashboards** page. Select **DLP: Status Summary** to view the McAfee DLP Endpoint dashboards.

In McAfee ePolicy Orchestrator 4.6 and 5.0, select **DLP: Status Summary** from the **Dashboard** drop-down list

Six predefined monitors are displayed. Monitors can be edited and customized, and new monitors can be created. See the McAfee ePolicy Orchestrator documentation for instructions.

The six dashboard reports and other predefined reports are available by selecting **Menu | Reporting | Queries & Reports**. They are listed under **Shared Groups | Data Loss Prevention**. The nine standard reports that are also available as rolled up reports are indicated in the tables.

### Predefined dashboards

The following table describes the predefined McAfee DLP Endpoint dashboards.

**Table 12-1 Predefined DLP dashboards (Public Queries)**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<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>• Device control only mode</td>
</tr>
<tr>
<td></td>
<td>• Device control and full content protection mode</td>
</tr>
<tr>
<td></td>
<td>• Device control and content aware removable storage protection mode</td>
</tr>
<tr>
<td></td>
<td>• Unknown</td>
</tr>
<tr>
<td>Agent status</td>
<td>Displays all agents and their status.</td>
</tr>
<tr>
<td>Agent version</td>
<td>Displays the distribution of endpoints in the enterprise. Used to monitor agent deployment progress.</td>
</tr>
</tbody>
</table>
Table 12-1  Predefined DLP dashboards (Public Queries) (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bypassed agents</td>
<td>Displays how many DLP nodes are in policy bypass mode. This is a real-time view that refreshes when a bypass begins or expires.</td>
</tr>
<tr>
<td>Enforced rules</td>
<td>Displays the number of user sessions enforcing each rule, grouped by rule type. This dashboard replaces the separate device, protection, and discovery enforced rule dashboards of previous versions.</td>
</tr>
<tr>
<td>Policy distribution</td>
<td>Displays the DLP policy distribution throughout the enterprise. Used to monitor progress when deploying a new policy.</td>
</tr>
</tbody>
</table>

Predefined event reports

The following table describes the predefined McAfee DLP Endpoint event reports.

Table 12-2  Predefined DLP event reports (My Queries)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent operation mode</td>
<td>Displays agents by operation mode.</td>
</tr>
</tbody>
</table>
| Agent status (also rolled up report) | Displays all agents and their status. This report has new values for version 9.3 clients:  
• Driver Installation failed  
• Agent installation failed  
• Agent installed - pending reboot  
• Agent up - no policy  
• Agent is running  
• Agent is not running  
• Agent uninstalled  |
| Agent to ePO communications distribution (also rolled up report) | Displays endpoints according to the date of their last communication with ePolicy Orchestrator.                                                   |
| Agent version (also rolled up report) | Displays the distribution of endpoints in the enterprise. Used to monitor agent deployment progress.                                             |
| Block and block write device events | Displays device events that were blocked or write-blocked.                                                                                  |
| Bypassed agents (also rolled up report) | Displays how many DLP nodes are in policy bypass mode. This is a real-time view that refreshes when a bypass begins or expires.                |
| Daily events distribution by severity | Displays a day's events ordered by severity.                                                                                                  |
| Enforced rules (also rolled up report) | Displays the number of user sessions enforcing each rule, grouped by rule type.                                                             |
| Events by event type (also rolled up report) | Displays the number of events for each event type.                                                                                           |
| Events by protection rule | Displays the number of events for each rule.                                                                                                                                                          |
| Events by protection / discovery rule by date | Displays the number of events for each rule, for different dates.                                                                            |
| Events by severity (also rolled up report) | Displays the number of events for each severity level.                                                                                      |
| Events by tag and category (also rolled up report) | Displays the number of events for each tag and content category that they recognize.                                                        |
Table 12-2 Predefined DLP event reports (My Queries) (continued)

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Evidence path distribution</td>
<td>Displays the different evidence shares used by the agents. Useful when there are several different agent configurations.</td>
</tr>
<tr>
<td>Policy distribution</td>
<td>Displays the DLP policy distribution throughout the enterprise. Used to monitor progress when deploying a new policy.</td>
</tr>
<tr>
<td>(also rolled up report)</td>
<td></td>
</tr>
<tr>
<td>Privileged permissions</td>
<td>Displays the current privileged DLP users. It allows you to drill down to view normal DLP users as well as users with monitor only permissions, and users allowed to bypass all DLP events.</td>
</tr>
<tr>
<td>Undefined device classes</td>
<td>Lists and shows a bar graph of the devices whose device class cannot be determined.</td>
</tr>
<tr>
<td>Unmanaged printers</td>
<td>Lists and shows a bar graph of the unmanaged (whitelisted) printers and the number of nodes attached to each. Clicking either a listed printer or a bar on the graph drills down to a list of the computers connected to it. Clicking on a computer drills down to the properties of the computer.</td>
</tr>
<tr>
<td>Unsupported printers</td>
<td>Lists and shows a bar graph of the unsupported printers (that is, printers detected by the DLP Endpoint that were not whitelisted but failed to install a DLP proxy driver) and the number of nodes attached to each. Clicking either a listed printer or a bar on the graph drills down to a list of the computers connected to it. Clicking on a workstation drills down to the properties of the computer.</td>
</tr>
</tbody>
</table>

Dashboard and report support for pre-9.3 clients

McAfee DLP Endpoint client version prior to 9.3 do not support multiple user sessions. Older clients continue to report properties as previously, and these are displayed in the Product Details page in the ePolicy Orchestrator system tree. These clients are tagged as not supporting multi-user sessions.

To make the DLP MA Properties reporting task is backward compatible, certain properties – Agent Status, Agent to ePO Communication Distribution, Bypassed Agents, and Policy Distribution – have been deprecated, that is, there is a version of the property for new clients and a version for older clients. When upgrading, user-defined and user-modified queries add the note "Deprecated - please see Release Notes". Reports that were not modified are replaced with the new functionality.

Set up Data Loss Prevention rolled up reports

Rolled up reports are a function of ePolicy Orchestrator that can be used with McAfee DLP Endpoint data.

**Task**

For option definitions, click ? in the interface.

1. In ePolicy Orchestrator, select **Menu | Automation | Server Tasks**.
2. Select **New Task** (or **Actions | New Task**).
3. Type a name for the task, and (optional) notes, then click **Next**.
4. From the **Actions** drop-down list, select **Roll Up Data**. From the **Data Type** drop-down list, select one of the McAfee DLP Endpoint report types: **DLP Enforced Rules**, **DLP Enforced Rules (deprecated)**, **DLP Events**, **DLP MA Properties**, **DLP MA Properties (deprecated)**, or **DLP Passwords**.
5. Continue with the configuration as required. Click **Next**.
6  Set the schedule type, date and time. Click Next.
7  Review the setup information, then click Save.

**Working with the database**

McAfee DLP Endpoint software contains two tools for working with the database.

**Administer the database**

Unwanted events can be removed from the events database.

**Before you begin**

When removing events from the database, make sure they have been properly reported and analyzed. We recommend creating a database backup prior to removing events. Removing all events from the system can potentially remove violations before they have been seen by security officers or administrators.

**Task**

For option definitions, click ? in the interface.

1  In the McAfee DLP Endpoint policy console navigation pane, under Database Administration, select Database Administration.

   The administrative actions appear in the right-hand pane.

2  Select an action from the available list. The confirmation window appears.

   Pay attention to the description of each option. Specifically, the Date option removes events older than the date specified.

3  Click Execute to proceed with the operation or Close to cancel the operation.

   The operation progress bar window appears.

**View database statistics**

Database statistics can be viewed directly in the policy console.

**Task**

For option definitions, click ? in the interface.

1  In the McAfee DLP Endpoint policy console navigation pane, under Database Administration, select Database Statistics.

   The list of available statistical values appears in the right-hand pane.

2  On the toolbar, select Refresh Database statistics to update the information.

3  Select any value from the available list to view details.

**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 on the Evidence tab of the Agent Configuration can be used to control the maximum size and age of local evidence storage when the computer is offline.

**Prerequisites for evidence storage**

Evidence storage must be enabled before it can be used. This 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** — Specifying the UNC path to the evidence storage folder is a requirement for applying a policy to ePolicy Orchestrator. See the *Creating and configuring repository folders* in this guide for details on setting up the folder and setting access permissions (also known as Evidence Network Share).

- **Evidence service** — The evidence service is enabled in the Agent Configuration | Miscellaneous. It is a subentry under Reporting Service, which must also be enabled for evidence collection.

- **Evidence replication setting** — A setting in the Agent Configuration | Evidence tab allows you to select evidence collection, hit highlighting, or both.

**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 in the Agent Configuration | Evidence tab. The default is 1,000; permissible entries are 1–10,000.

- When a large number of evidence files are linked to a single event only the first 100 filenames 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 filenames.

- The DLP Incident Manager field **Original Evidence Count** displays the total evidence count.

- For all evidence-storing events and release from quarantine events, the McAfee DLP Endpoint client software creates an **all_evidences.csv** file which is stored with the evidence in the database. The file can be sent to end users for self-remediation. This can be done automatically by selecting the **Attach Evidence CSV** option in a mail notification task.

  The CSV file is coded in UTF-16 to allow for localized filenames, and contains the file name, the full-path location of the folder that contains the file, size, hit count, and https:// links to the evidence and hit highlight in the database.

  When working in backward compatibility mode with previous client versions, evidence files beyond the 100 stored in the database cannot be displayed because the older clients do not create the all_evidences.csv file.

**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 one hundred 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 in the Agent Configuration | Evidence tab:

- **Show abbreviated hits** (default) — Displays 1500 characters (5–7 hits) per section.
- **Show all hits** — Displays all hits, with limitations as described above.

### Rules allowing evidence storage

The following rules have the option of storing evidence:

**Table 12-3  Evidence saved by rules**

<table>
<thead>
<tr>
<th>Rule</th>
<th>What is saved</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud protection rules</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Email protection rules</td>
<td>Copy of the email</td>
</tr>
<tr>
<td>File system protection rules</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Printing protection rules</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Removable storage protection rules</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Screen capture protection rules</td>
<td>JPEG of the screen</td>
</tr>
<tr>
<td>Web post protection rules</td>
<td>Copy of the web post</td>
</tr>
<tr>
<td>File System Discovery rules</td>
<td>Copy of the file</td>
</tr>
<tr>
<td>Email Storage Discovery rules</td>
<td>Copy of the .msg file</td>
</tr>
</tbody>
</table>

### Monitoring activity with hit count

A hit count is the number of tags and content categories that triggered an event. A single event can generate multiple hits.

The DLP Incident Manager maintains *hit counts* — the number of tags and content categories that triggered each event. In the event details pane, the total number of hits is concatenated to each evidence file path. Hit counts are recorded in two fields in the monitor display:

- **Number of hits** — The sum of content category hits. Multiple dictionary hits add to the total. Tags are not counted.
- **Number of tags and categories** — The sum of all content categories and tags found.
- **Content size** — The total file size, in KB.

A single event can generate multiple hits. For example, if an email with two attachments is blocked, the first attachment because it triggered a dictionary, and the second because it triggered a text pattern and contained tagged content, that would be listed as two hits and three tags and categories.

### Redaction and role-based access control

McAfee DLP Endpoint software limits the viewing of incidents in two ways.

To meet legal demands in some markets, and to protect confidential information in all circumstances, McAfee DLP Endpoint software 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.

In addition to specific fields being designated as confidential, reviewers can be restricted to viewing only incidents assigned to them, or to specific user groups.
Protecting confidentiality with redaction

Data redaction is the encrypting of confidential information to prevent unauthorized viewing. Some countries require redaction practices be followed, and it is considered **Best Practice** (even when not required by law) to separate incident and operational events reviewing permissions, and to block sensitive data from those not required to view it.

Redacted information is encrypted in:
- the DLP Incident Manager display
- the DLP Operational Events display

Currently, the fields *computer name* and *user name* are predefined as private.

There are two ways of viewing sensitive data:
- Giving administrators permission to view all fields in the incidents they are allowed to view
- Creating a "redaction reviewer" — a reviewer who cannot view incidents, but can reveal encrypted fields when another reviewer views the incident

(This is the "4-eyes" review model that was the only option in earlier versions of McAfee DLP Endpoint.)

**DLP Permissions in ePolicy Orchestrator**

The following table shows how DLP permissions affect access to features and ePolicy Orchestrator reports:

*Table 12-4 Summary of DLP Incidents and Operational Events permissions and their effects*

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
<th>Effect in DLP Policy Manager</th>
<th>Effect in DLP Incident Manager</th>
<th>Effect in DLP Operational Events</th>
<th>Effect in ePO Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policy</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User cannot view policies.</td>
<td>User is unauthorized to view or create DLP policies.</td>
<td>DLP Policy Mgr tab is not available.</td>
<td>Not relevant. Depends on incident access permissions.</td>
<td>Not relevant. Depends on operational events access permissions.</td>
<td>Not relevant.</td>
</tr>
<tr>
<td>User can only view policies.</td>
<td>User is authorized to view policies, but cannot create or edit them.</td>
<td>DLP Policy Mgr tab is available.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User can view and save policies.</td>
<td>User is authorized to create and edit policies.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Incidents Access Control</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User cannot view DLP incidents.</td>
<td>User is unauthorized to view the DLP Incident Manager.</td>
<td>Not relevant. Depends on policy access permissions.</td>
<td>DLP Incident Manager tab is not available.</td>
<td>Not relevant. Depends on operational events access permissions.</td>
<td>All DLP incidents are filtered out.</td>
</tr>
</tbody>
</table>
### Table 12-4 Summary of DLP Incidents and Operational Events permissions and their effects (continued)

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
<th>Effect in DLP Policy Manager</th>
<th>Effect in DLP Incident Manager</th>
<th>Effect in DLP Operational Events</th>
<th>Effect in ePO Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>User can view incidents assigned to him.</td>
<td>User can view all personally assigned DLP incident data.</td>
<td>DLP Incident Manager tab is available.</td>
<td>Incidents are filtered by user access rights.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User can view incidents assigned to members of the following permissions sets.</td>
<td>User can view DLP incidents assigned to groups he is a member of, and incidents assigned to any member of those groups.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User can view all incidents.</td>
<td>User can view all DLP incident data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Incidents Data Redaction

| Sensitive data is redacted. | User is not authorized to view confidential fields. | Not relevant. Depends on policy access permissions. | The display is available, but sensitive fields are redacted. Evidence is not accessible. | |
| Sensitive data is in clear text. | User can view all fields. | | All fields are displayed, evidence is accessible. | |
| User can reveal redacted sensitive data. | User is not authorized to view DLP incidents, but can decrypt confidential fields in the presence of a user who can view DLP incidents. | Not relevant. | Not relevant. | No DLP Reports are authorized. |

#### Incident Task Creation

| User can create a Mail Notification task. | User can create the selected tasks. | Not relevant. Depends on policy access permissions. | Only available to users with at least partial access. | Not relevant. Depends on incident access permissions. | Not relevant. |
| User can create a Purge task. | | | | |
| User can create a Set Reviewer task. | | | | |

#### Operational Events

| | | | | | |
Table 12-4  Summary of DLP Incidents and Operational Events permissions and their effects (continued)

<table>
<thead>
<tr>
<th>Permission</th>
<th>Description</th>
<th>Effect in DLP Policy Manager</th>
<th>Effect in DLP Incident Manager</th>
<th>Effect in DLP Operational Events</th>
<th>ePO Reports</th>
</tr>
</thead>
<tbody>
<tr>
<td>User cannot view operational events.</td>
<td>User is unauthorized to view the DLP Operational Events display.</td>
<td>Not relevant. Depends on policy access permissions.</td>
<td>Not relevant. Depends on incident access permissions.</td>
<td>DLP Operational Events tab is not available.</td>
<td>Operational events are filtered by user access rights.</td>
</tr>
<tr>
<td>User can view all operational events.</td>
<td>User can view all DLP operational event data.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

See also
Create and define permission sets on page 177

Role-based access control

Incidents in the DLP Incident Manager or DLP Operational Events consoles can be assigned to specific users or user groups.

Role-based access control gives granular control over the viewing of DLP Incident Manager and DLP Operational Events data. By assigning incidents to specific administrators or groups and setting permissions in ePolicy Orchestrator permission sets, you can control which reviewers see which incidents.

Workflow

To use the role-based access control feature, use the following workflow:

- **Create a reviewer** — You can use an existing user or user group, or create a new user in ePolicy Orchestrator Menu | User Management | Users.

- **Create a permission set** — In ePolicy Orchestrator Menu | User Management | Permission Sets, create a new permission set then assign the Data Loss Prevention permission to your user.

- Create a Set Reviewer task in DLP Incident Manager | Incident Tasks to assign reviewers according to preset conditions.

Use case — email protection rules

As an example, lets say you want to assign an administrator to review all violations of email protection rules. The exact order is not important, but you would need to do the following:
1 Create a DLP email policy reviewer. In ePolicy Orchestrator, under User Management | Users, create a user with a suitable name, for example "DLP email reviewer".

2 Create a new permission set, let's call it "Review DLP email," assign your new reviewer to it, and set the Data Loss Prevention permissions. To activate the role-based permissions, you have to allow your user to either "view" or "partially view" incidents and events. If you select "partially view," the reviewer will not be able to view private (redacted) fields.

3 You can assign reviewers manually (from the incident details pane) or automatically. To automatically assign your reviewer all email incidents, go to DLP Incident Manager | Incident Tasks and create a new Set Reviewer task. Select the Process Product property and set it equal to Microsoft Outlook. If you might see incidents from Lotus Notes, add that property as well.

The new reviewer is assigned the next time the ePolicy Orchestrator server task DLP incident tasks runner is run.
Monitoring and reporting events
Redaction and role-based access control
Users and permission sets

We recommend creating specific administrator roles and permissions in ePolicy Orchestrator for McAfee DLP Endpoint policy console and DLP Incident Manager. These roles can include creating and saving policies, viewing (but not changing) policies, generating override, uninstall, and quarantine release keys, viewing the DLP Incident Manager, and revealing sensitive fields.

System tree filtering permissions support

McAfee DLP Endpoint supports ePolicy Orchestrator System Tree filtering permissions in the DLP Incident Manager and DLP Operational Events. As a result, McAfee ePO operators can only see incidents from computers in their permitted System Tree portion. Group Administrators do not have any permissions in the ePolicy Orchestrator System Tree by default, so regardless of permissions assigned in the Data Loss Prevention permission set, they cannot see any incidents in DLP Incident Manager or DLP Operational Events.

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 ePolicy Orchestrator 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 containing confidential information are encrypted to prevent unauthorized viewing, and links to sensitive evidence are hidden. The feature is designed with a "double key" release. This means that to use the feature, you must create two permission sets: one to view the incidents and events and another to view the encrypted fields. Both roles are required to use the feature.

Contents

- DLP Permission Sets
- Create and define McAfee DLP administrators
- Create and define permission sets

DLP Permission Sets

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).

Data Loss Prevention permission sets are divided into five sections:
• Policy
• Incident Access Control
• Incident Data Redaction

This allows you to differentiate between DLP policy administrators, incident and operational event administrators, and incident reviewers. The option User cannot view DLP incidents in the Incidents Access Control section renders the other incident sections unavailable (except for the reveal redacted data option). Otherwise, options are independent, and administrative and review roles can be assigned as you want.

Permissions for setting release keys for Agent Override and Uninstall, and for releasing quarantined emails and files, have been moved to the Help Desk Actions permission set.

**Use case – DLP administrator**
Use the following selections for a DLP administrator who only creates policies and has no event review responsibilities.
- In the Policy section, select User can view and save policies.
- In the Incident Access Control section, select User cannot view DLP incidents.

Optionally, the DLP administrator might be allowed to view operational events.

**Use case — redacted fields reviewer**
This example requires setting permissions for two reviewers: one to review events and incidents, one to view the redacted fields. Assuming that reviewer roles are separated from policy administrator roles, make the following selections:
- For both reviewers — in the Policy section, select User cannot view and save policies.
- For the incident reviewer — in the Incident Access Control section, select either of the partial view options: User can see incidents assigned to him or User can see incidents assigned to members of the following permission sets. In the Incident Data Redaction section, select Sensitive data is redacted.
- For the redaction reviewer — in the Incident Access Control section, select User cannot view DLP incidents. In the Incident Data Redaction section, select User can reveal redacted sensitive data (4 eyes).

**Create and define McAfee DLP administrators**
Administrative users can be created either before or after the permission sets assigned to them.

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

1. In ePolicy Orchestrator, select Menu | User Management | Users.
2. Click New User.
3 Type a user name and specify logon status, authentication type, and permission sets. We recommend creating user groups related to the role, for example DLP Quarantine Administrator.

The order of creating users and permission sets is not critical. If you create users first, user names appear in the permission set form and you can attach them to the set. If you create permission sets first, the permission set names appear in the user form and you can attach the user to them.

4 Click Save.

Create and define permission sets

Permission sets are useful for defining different administrative roles in McAfee DLP Endpoint software.

Task
For option definitions, click ? in the interface.

1 In ePolicy Orchestrator, select Menu | User Management | Permission Sets.

2 Select a predefined permission set or click Actions | New Permission Set to create a new set.
   a Type a name for the set and select users.

   The order of creating users and permission sets is not critical. If you create users first, user names appear in the permission set form and you can attach them to the set. If you create permission sets first, the permission set names appear in the user form and you can attach the user to them.

   b Click Save.

3 In the Data Loss Prevention field for the permission set, click Edit.

4 To define Role Based Access Control (RBAC) for this user or group, select the permissions you want then click Save.

Permissions can be set separately for five categories:

- policies
- incident access control
- incident data redaction
- incident task creation
- operational events

Figure 13-1 Editing a permission set for McAfee DLP Endpoint
Non-routine operations

In some situations, the McAfee DLP Endpoint client must be uninstalled when ePolicy Orchestrator is not available.

Similar, but more common operations include agent bypass and quarantine release.

Contents

- Agent bypass and related features
- Advanced topics: Running the PST crawler from the command line

Agent bypass and related features

Agent bypass is a temporary suspension of blocking rules. It is applied when a user needs temporary permission to send information normally considered sensitive.

Agent bypass temporarily suspends blocking by the endpoint software for a specified amount of time. When in bypass mode, the endpoint software still collects and sends event information to the ePolicy Orchestrator Event Parser. Events are marked with the bypass flag. The user does not receive visual notification of events while in bypass mode.

The bypass mechanism is known as "challenge/response." The user opens a McAfee DLP Endpoint client pop-up that displays an Identification Code and Revision ID. This code and ID are sent to the DLP Administrator to request a release code. The administrator accepts the request by creating a release code and sending it to the user, who enters it in the pop-up Release Code text box. For security, a new ID code is generated each time you open the pop-up window, and the release code is generated from it. Thus, the user must leave the pop-up window open until the matching release code is entered.

Agent bypass is no longer terminated by logging out or restarting the computer. It remains active for the full time period set in the policy. (Bypass duration can range from 5 minutes to 30 days.)

Creating the agent bypass release code requires the McAfee Help Desk utility, which is included in the McAfee DLP installer. See the McAfee Help Desk documentation for more information on release codes.

Related functions

Agent uninstall

McAfee DLP Endpoint client software is protected from unauthorized removal. There are two methods of authorized removal:

- Network uninstall from ePolicy Orchestrator, performed by the McAfee ePO administrator.
- Local uninstall using Windows Add or Remove Programs. This method uses the challenge/response mechanism.

OS X client does not support challenge/response uninstall.
Quarantine release

When the McAfee DLP Discover crawler quarantines sensitive emails or files, the challenge/response mechanism is used to release the information from quarantine. Release from quarantine uses only the Release Code, not the Revision ID.

Use case — master release codes

Normally, release codes are generated from identification codes, and are unique to the user requesting the code. In some cases, however, the administrator might want to issue a release code for multiple computers. The typical case is when a problem occurs with a specific build of McAfee DLP Endpoint client software, and it must be uninstalled from several endpoints. In this case, the administrator creates a master release code that can be used with any McAfee DLP Endpoint client. The master code is time-based, and expires after a specified time.

For more information on master release codes, see the McAfee Help Desk Product Guide.

Request an override key

Occasionally, a user has a valid need to copy something that is blocked by a rule. In such cases, the user requests an override key, which bypasses normal McAfee DLP Endpoint action for a preset amount of time.

Before you begin

The option Show task ‘Request DLP bypass’ in DLP Endpoint Console must be selected on the Agent Configuration | User interface service tab.

When in bypass mode, the endpoint software still collects and sends event information to the ePolicy Orchestrator Event Parser, marking them with the override flag. The user does not receive visual notification of events while in bypass mode.

Task

1 Activate the console. On Microsoft Windows computers, do the following:

   a In the system tray of the managed computer, click the McAfee Agent icon, then select Manage Features | DLP Endpoint Console.

       The DLP Endpoint Console appears.
b  Click the *Tasks* tab.

![DLP Endpoint console Tasks](image)

**Figure 14-1  DLP Endpoint console Tasks**

2  On Mac computers, do the following:

a  From the McAfee menulet on the status bar, select *McAfee Endpoint Protection for Mac Preferences*

   The McAfee Data Loss Prevention bypass request window appears.
In the menu bar, select DLP.

![Data Loss Prevention Interface]

3 Send the Identification Code and Revision ID to the administrator, along with user name and email address. Optional information you can also include are computer name and business justification for the override. When approved, the administrator generates the Release Code and sends it to the user. The system administrator sets the length of time for the override before generating the code.

Each time you select the Tasks tab (DLP preference on Mac) a new Identification Code is generated. You must leave the bypass request window open until you receive your matching Release Code and enter it.

4 Type or paste the Release Code into the text box and click OK.

The release code is an 8- or 16-digit alphanumeric. If the code contains dashes (making it easier to read), you must remove them before pasting the number into the text box. If you enter the code incorrectly three times, and the release code lockout policy has been activated in the Agent Configuration | Notification Service tab, the pop-up window times out for 30 minutes (default setting).

The agent pop-up window displays a verification, and the agent enters bypass mode.
Advanced topics: Running the PST crawler from the command line

Email storage discovery can be run from the command line.

Separation of the PST crawler function to a separate executable, fcpst.exe, creates the possibility of running email storage scans from the command line. By default, the crawler only performs listing of existing items and printing to a log file. The following command line parameters can be used:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>-t1</td>
<td>Scans PST files on the local hard drives</td>
</tr>
<tr>
<td>-t2</td>
<td>Scans OST file</td>
</tr>
<tr>
<td>-t4</td>
<td>Scans mapped PST files</td>
</tr>
</tbody>
</table>

Combining values combines the operations. For example:

<table>
<thead>
<tr>
<th>Command</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcpst.exe &quot;-t3&quot;</td>
<td>Scans PST files on the local drives AND scans OST file</td>
</tr>
<tr>
<td>fcpst.exe &quot;-t7&quot;</td>
<td>Scans everything: all PST files on local drives, mapped PST files, and OST file</td>
</tr>
</tbody>
</table>
Non-routine operations
Advanced topics: Running the PST crawler from the command line
McAfee DLP Endpoint includes a System Tools function for monitoring system health. More advanced features are available in the Diagnostic Tool utility.

Contents

- System tools
- Diagnostic Tool

System tools

Use the system tools in McAfee DLP Endpoint software to keep track of system health alerts and to configure advanced features.

System tools are designed to be the first step in troubleshooting problems. They are accessed from the Tools menu. Tools are included for:

- Analyzing the policy
- Viewing the system log
- Rerunning the initialization wizard
- Setting the tool options

Use case — analyzing a policy

Policies containing errors cannot be applied to the ePolicy Orchestrator database. Before attempting to apply a new policy, verify the policy with the policy analyzer and fix any errors. The policy analyzer also displays warnings, indicating that a rule or definition is incomplete or disabled. Incomplete policies can be applied to the database, thus allowing you to test partial policies in the course of building new policies.

To view the Policy Analyzer, select Tools | Run Policy Analyzer in the McAfee DLP Endpoint policy console (or press F8). The bottom of the window displays the policy analyzer entries.

Use case — viewing the system log

Use the system log to observe and receive alerts about the system health and related events. The system log is crucial for troubleshooting.

To view the system log, select Tools | View Log in the McAfee DLP Endpoint policy console (or press F7). The bottom of the window displays the system log entries.
Diagnostic Tool

The Diagnostic Tool is designed to aid troubleshooting McAfee DLP Endpoint problems on Microsoft Windows endpoint computers. It is not supported on OS X computers.

The Diagnostic Tool gathers information on the performance of McAfee DLP Endpoint client software. The IT team uses this information to troubleshoot problems and tune policies. When severe problems exist, it can be used to collect data for analysis by the McAfee DLP Endpoint development team.

The tool is distributed as a utility to install on problem computers. It consists of seven tabbed pages, each devoted to a different aspect of McAfee DLP Endpoint software operation.

On all pages displaying information in tables (all pages except General information and Tools), you can sort the tables on any column by clicking the column header.

| General information | Collects data such as whether the agent processes and drivers are running and general policy, agent, and logging information. Where an error is detected, information about the error is presented. |
| DLPE Modules | Displays the agent configuration (as shown in the McAfee DLP Endpoint policy console as the Agent Configuration | Miscellaneous page). It shows the status of each module, add-in, and handler, and gives details on any problems. |
| Data Flow | Displays the number of events and the memory used by the McAfee DLP Endpoint client, and displays event details when a specific event is selected. |
| Tools | Allows you to perform several tests and displays the results. When necessary, a data dump is performed for further analysis. |
| Process list | Displays all processes currently running on the computer. Selecting a process displays details and related window titles and application definitions. |
| Devices | Displays all Plug and Play and removable devices currently connected to the computer. Selecting a device displays details of the device and related device definitions. |
| Active policy | Displays all rules contained in the active policy, and the relevant policy definitions. Selecting a rule or definition displays the details. |

Checking the agent status

Use the General information tab to get an overview of the agent status.

The information on the General information tab is designed to confirm expectations and answer basic questions. Are the agent processes and drivers running? What product versions are installed? What is the current operation mode and policy?

Agent processes and drivers

One of the most important questions in troubleshooting is, "Is everything running as expected?" The Agent processes and Drivers sections show this at a glance. The checkboxes show if the process is enabled; the colored dot shows if it is running. If the process or driver is down, the text box gives information on what is wrong.

The default maximum memory is 150 MB. A high value for this parameter can indicate problems.

Table 15-1  Agent processes

<table>
<thead>
<tr>
<th>Term</th>
<th>Process</th>
<th>Expected status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fcag</td>
<td>McAfee DLP Endpoint agent (client)</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Fcags</td>
<td>McAfee DLP Endpoint agent service</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Fcagte</td>
<td>McAfee DLP Endpoint text extractor</td>
<td>enabled; running</td>
</tr>
</tbody>
</table>
Table 15-1  Agent processes (continued)

<table>
<thead>
<tr>
<th>Term</th>
<th>Process</th>
<th>Expected status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fcagwd</td>
<td>McAfee DLP Endpoint watch dog</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Fcagd</td>
<td>McAfee DLP Endpoint agent with automatic dump</td>
<td>enabled only for troubleshooting.</td>
</tr>
</tbody>
</table>

Table 15-2  Drivers

<table>
<thead>
<tr>
<th>Term</th>
<th>Process</th>
<th>Expected status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hdlpflt</td>
<td>McAfee DLP Endpoint minifilter driver (enforces removable storage device rules)</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Hdlpevnt</td>
<td>McAfee DLP Endpoint event</td>
<td>enabled; running</td>
</tr>
<tr>
<td>Hdlpdbk</td>
<td>McAfee DLP Endpoint device filter driver (enforces device Plug and Play rules)</td>
<td>can be disabled in configuration</td>
</tr>
<tr>
<td>Hdlpctrl</td>
<td>McAfee DLP Endpoint control</td>
<td>enabled; running</td>
</tr>
</tbody>
</table>

Agent info section

Operation mode and Agent status are expected to match. The Agent Online indication, together with EPO address, can be useful in troubleshooting.

Run the Diagnostic Tool

The Diagnostic Tool utility provides IT teams with detailed information on the agent status.

Before you begin
Diagnotic Tool requires authentication with McAfee Help Desk.

Each tab (except Tools and Data Flow) has a Refresh button in the lower right corner. Changes that occur when a tab is open do not update the tab information automatically. Click the Refresh button frequently to verify that you are viewing current data.

Task
1. Double-click the AgentDiag.exe file.
   An authentication window opens.
2. Copy the Identification Code to the McAfee Help Desk Identification Code text box on the Generate DLP Client Bypass Key page. Fill in the rest of the information and generate a Release Code.
3. Copy the Release Code to the authentication window Validation Code text box and click OK.
   The diagnostic tool utility opens.

Tuning policies

Diagnostic Tool can be used to troubleshoot or tune policies.

Use case — high CPU usage
Users are sometimes plagued by slow performance when a new policy is enforced. One cause might be high CPU usage. To determine this, go to the Process List tab. If you see an unusually large number of events for a process, this could be the problem. For example, a recent check found that taskmgr.exe was classified as an Editor, and had the second highest number of total events. It is quite unlikely that this application is leaking data, and McAfee DLP Endpoint does not need to monitor it that closely.
Select the application, and note the Original name that is listed in the Process Details. Use this name to create a new application definition in the policy that changes the strategy to Trusted. Apply the policy, and test to see if performance has improved.

**Use case — creating effective tags**

Tagging sensitive data lies at the heart of a data protection policy. Diagnostic Tool displays information that helps you design effective tags. Tags can be too tight, missing data that should be tagged, or too loose, creating false positives.

The Active Policy page lists the tagging rules and the tags that they apply. The Data Flow page lists all tags applied by the policy, and the count for each. When counts are higher than expected, false positives are suspected. In one case, an extremely high count led to the discovery that the tagging rule was triggered by Disclaimer text. Adding the Disclaimer to the whitelist removed the false positives. By the same token, lower than expected counts suggest a tagging rule that is too strict.

If a new file is tagged while the Diagnostic Tool is running, the file path is displayed in the details pane. Use this information to locate files for testing.
Index

A

about this guide 7
actions/rules matrix (graph) 131
administrators, defining 176
Adobe LiveCycle Rights Management, See rights management
agent bypass 179
agent configuration
  assigning with ePolicy Orchestrator 49
  global 74
  Mac OS support 74
agent uninstall 179
aggregated event behavior 105
aggregation, of pop-up messages 131
all_evidences.csv file 167
application definitions
  about 106
  creating 108
  creating from the Enterprise Applications List 109
  removing 149
strategy 104
templates 149
using 105
web applications 109
application strategy 105
applications, in rules 105
archiver, application strategy 105
assignment groups
  computer 153
  creating 151
  definition 12
  privileged users 152
  users, including and excluding 151

B

backward compatibility 22, 34, 39
backward compatibility, errors with 49
Box.inc 134
business justification 140, 147

C

category catalog 119
challenge/response 92
Citrix support 14
Citrix XenApp device rules 62
classification rules 10, 113
clipboard protection
  rules, creating 137
clipboard protection rules 134
cloud protection rules 139
clusters
  preparing the environment 27
  testing the installation 27
  using DLP software in a cluster environment 26
components, Data Loss Prevention (diagram) 21
components, described 14
computer assignment groups 153
computer assignments, when upgrading 39
configuration, server 26
content categories 113, 117, 118
connventions and icons used in this guide 7

dashboards, report options 164
data
classifying 77
data-in-motion 97, 102
data-in-use 111
Data Loss Prevention software, description 19
data-at-rest 86
database
  removing events 167
  statistics, viewing 167
default rule, defining 45
definitions
  application 105
device, See device definitions
dictionaries 77
document properties 79, 95
e-mail destination 97
file extension 79, 95, 111
file server list 93
network 94
printer 100
registered document repository 95
registered documents 97
removing 149
table of 135
definitions (continued)
taggs 117
  text pattern 79
  web destination 102
  whitelist 84
device class
  creating new 56
  removing 149
types of 54
device control, on Mac 58
device definitions
  groups 62
  importing 61
  importing to existing 62
  parameter management 58
  Plug and Play 59
  removable storage 60
device GUID 55
device rules
  about 62
  Citrix XenApp 69
definition 12
  fixed disk 69
  Plug and Play 66
  removable storage 67
devices
  lists, adding Plug and Play definitions 60
  management 54
  parameters, list of 70
  Plug and Play 57
  removable storage 57, 58
  whitelisted 57
diagnostic tool 186
  Diagnostic Tool 187
dictionaries
  about 77
  creating 78
  importing entries 78
discovery
  about 86
  creating a file system discovery rule 87
  creating an email storage discovery rule 89
  scheduling 91
  setup 90
discovery rules 11
  DLP administrators, defining 176
  DLP Agent, See DLP Endpoint
  DLP Agent service watch dog 73
  DLP data, classifying 79
  DLP Discover 86
  DLP Endpoint
    checking in to ePolicy Orchestrator 37
    defined 14
    deploying 46
    deployment verification 47
DLP Endpoint (continued)
  wake-up call 50
DLP events
  viewing database statistics 167
DLP Incident Manager 158
  responding to events 157
  system events and alerts 159
DLP Policy
  console, illustrated 10
  DLP Policy console, installing 33
  DLP repositories, registered document 95
DLP rules
  classification 10
  device 12, 66, 67
  protection 12
  removable storage file access 68
  tagging 11
DLP tasks runner server task 162
document groups
  registered, creating 97
document properties definitions 79
documentation
  audience for this guide 7
  product-specific, finding 8
  typographical conventions and icons 7
Dropbox 134
E
  editor, application strategy 105
  email
    sending DLP events by 162
  email bypass 140
  email destinations
    about 97
    creating 98
    definitions (table) 135
    groups 99
    removing 149
  email protection rules 140
  email storage discovery 183
  endpoint configuration
    about 73
    Safe Mode 75
  endpoint console 15
  enterprise applications list
    about 105
    importing by scanning 110
    importing to 110
    removing applications 111
ePO Event Parser 14
ePO notifications 164
ePO reports 164
ePolicy Orchestrator
  computer assignment groups 153
  policy template synchronization wizard 48
ePolicy Orchestrator (continued)

system policy, assigning 49

event filter 160

event parser, when upgrading 39

events

  marking with labels 161
  monitoring 157
  removing 167
  viewing 159

evidence

  DLP Incident Manager 159
  endpoint events 157
  storage for encrypted content 167

evidence folder 27

evidence folder, configuring on Windows Server 2003 29

evidence folder, configuring on Windows Server 2008 28

eXplorer, application strategy 105

F

file access

  rules, about 62
  rules, removable storage 68

file extensions

  about 111
  creating 111
  creating groups 112
  definitions 79
  definitions (table) 135
  removing 149

date

file server list

  about 93
  adding a server 93
  creating 93
  definitions (table) 135

date

file system protection rule 142

FileSecure 130

filters

  network definitions 94

G

global agent configuration 74

Google Drive 134

groups

  device definitions 62
  email 99
  network address range 94
  text patterns 80, 83

GUID, See device GUID

H

handlers

  cloud protection 134
  hardware requirements 24
  hit count 169

hit highlighting, events 167

I

Image Writer, in printing protection rules 144

incident filter 160

incident manager 158

incident tasks 158, 162, 163

J

justification, See business justification

K

key generator 179

L

labels, marking events with 161

license, Device Control and DLP 36

local users 151

location, classifying by 85

Lotus Notes, email protection rule 140

M

Mac, device control 58

mail notification task 162

manual tags 122

McAfee Endpoint Encryption for Files and Folders 57

McAfee Endpoint Encryption for Removable Media 57

McAfee ServicePortal, accessing 8

media transfer protocol 135

memory mapped files, analyzing 106

monitoring 14, 158

N

network definitions

  (table) 135
  about 94
  address range 94
  address range group 94
  port range 95
  protection rule 143
  removing 149

notifications, ePolicy Orchestrator 164

O

online/offline operation 14

OpenLDAP 151

override

  key, requesting 180

override mode, See policies, bypass

P

parameters, device 70

PDF writer, in printing protection rules 143
permission sets, defining 177
permission sets, system tree filtering 175
phased upgrade 42
Plug and Play devices
device definitions 59
whitelisted 57
whitelisted definition, creating 60
policies
applying to 49
assigning with 49
assignment with 48
bypass 179
definition 12
editing a description 50
importing 50
refreshing 50
user assignment 151
policies, tuning 187
policy bypass 180
Policy console
console, illustrated 10
policy revision numbers 48
policy, initializing 34
policy, restoring after upgrade 43
printer list
adding printers 101
creating 100
definitions (table) 135
printer protection rule 144
printers
about 100
unmanaged 100, 101
unsupported 100
whitelisted 100–102
privileged users assignment group 152
protection rules
application file access 136
clipboard 134, 137
cloud 134, 139
definition 12
e-mail 140
file system 142
how they work 131, 135
network communication 143
printer 144
removable storage 145
screen capture 146
web post 147
protection rules, Data Loss Prevention
how they work 131
purge task 162
Q
quarantine 179
release from 167
quarantine 179 (continued)
restoring files or email items from 92
queries, when upgrading 39
R
RDP support 14
redaction 169, 175
about 170
viewing redacted text 159
registered document repositories 95, 96, 115
registered document repositories, using 96
removable storage
protection rules 145
reporting 163
repositories, registered document 96
revision numbers 48
rights management 128, 130
setting up the server 129
synchronizing policies 129
synchronizing templates 129
users 128
working with Data Loss Prevention 126
role based access control 177
role-based access control 169, 172
roles and permissions 27
rolled up reports 164
rollup queries 163
rules
Citrix XenApp 62
classification 113
removing 149
tagging 11, 120
S
Safe Mode 75
screen capture protection rules 146
Seclore FileSecure 130
server configuration 26
server software requirements 24
ServicePortal, finding product documentation 8
set reviewer task 162
SkyDrive 134
storage devices, removable 57, 58
strategy, See application definitions
strategy, for applications 105
supported operating systems 24
Syncplicity 134
system configuration 73
system log, viewing 185
system requirements 24
system tools 185
tagging rules
   application-based  121
   content-based  114
   creating  120
   definition  11
   dictionary  114
   links to content  120
   location-based  121

tags
   about  117
   content, See content categories
   creating  118
   definitions (table)  135
   linking tags to content  120
   manual  122, 123
   removing  149
   tag groups  119

Technical Support, finding product information  8
templates  149
templates, Data Loss Prevention  149
text patterns
   about  79
   creating  80
   definitions (table)  135
   for Titus Message Classification integration  83
   groups  83
   removing  149
   testing  82

Titus Message Classification, integration  83
TrueCrypt  131
TrueCrypt device rules  62, 67
tested, application strategy  105

users (continued)
   excluding from a user assignment group  151
   local  151

V
validators  79, 82
VDI support  14
verifying the installation  47
VMware support  14

W
wake-up call  50
WatchDog protective service, about  73
web destinations
   about  102
   creating  103
   definitions (table)  135
   groups  103
   removing  149
web post protection rules  147
whitelist
   adding content  85
   definition (table)  135
   deleting content  85
   printer  100
whitelist folder  27
whitelist folder, configuring on Windows Server 2003  29
whitelist folder, configuring on Windows Server 2008  28
whitelisted Plug and Play devices  57
whitelists  12
   about  84
   application definitions  70
   Plug and Play definitions, creating  60
   printers  102
   unmanaged printers  101
window titles, in screen capture protection rules  146
wizards
   Client Task Builder  115
   Template Synchronization  149
whitelists, Data Loss Prevention Template Synchronization  149

U
unmanaged printers, See printers, whitelisted
upgrade (task description)  41
upgrade, phased  42
upgrade, unsupported items  39
user assignment groups
   creating  151
user permissions  169
user sessions  62
users
   assignment groups  151