



Product Guide

McAfee Data Loss Prevention 9.2 Software

For Use with ePolicy Orchestrator® 4.6.0 Software

COPYRIGHT

Copyright © 2011 McAfee, Inc. All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAfee SECURITYALLIANCE EXCHANGE), MCAfee, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

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	7
	About this guide	7
	Audience	7
	Conventions	7
	Finding product documentation	8
1	What is McAfee Data Loss Prevention Endpoint?	9
	How McAfee DLP Endpoint works	10
	Product components and how they interact	13
	Strategies for categorizing applications	14
	Encryption	14
	The McAfee DLP Endpoint policy console	15
2	Controlling removable media with device rules	17
	Categorizing devices with device classes	17
	Create a new device class	18
	Change the status of a device class	18
	Controlling devices with device definitions	19
	Importing device parameters	19
	Creating device definitions	20
	Device parameters	23
	Device rules	25
	Create and define a Plug and Play device rule	25
	Create and define a removable storage device rule	26
	Create and define a removable storage file access rule	27
	Create a whitelisted application definition	27
	Device parameters	28
3	Classifying content	31
	Using dictionaries to classify content	31
	Create a dictionary	32
	Classifying content with document properties or file extensions	32
	Defining registered document repositories	33
	Registering documents on managed computers	33
	Indexing registered document repositories	34
	Create a registered document repository definition	34
	Create a registered document repository group	35
	Index registered documents repositories	35
	Deploy a registered document package to the client computers	35
	Text pattern definitions	36
	Classifying content with text patterns	37
	Whitelist	40
	Add new whitelist content	40
	Delete whitelist files	41

4	Tracking content with tags and classifications	43
	How tags and content categories are used to classify content	43
	Creating tags, content categories, catalogs, and groups	44
	How tagging rules link tags to content	46
	Creating and defining tagging rules	46
	How classification rules link categories to content	48
	Creating and defining classification rules	49
	Manual tags	50
	Tag files manually	50
	Remove manual tags from content	50
5	Protecting files with rights management	53
	Adobe rights management users	54
	How Data Loss Prevention works with rights management	54
	Define an Adobe RM server and synchronizing policies	56
	Define a Microsoft Rights Management Service server and synchronizing templates	57
6	Classifying content by file location	59
	How McAfee Data Loss Prevention Discover scanning works	60
	Finding content with the McAfee DLP Discover crawler	61
	Restore quarantined files or email items	65
	Applications and how to use them	66
	The Enterprise Application List	66
	Application definitions and how they are categorized	68
	Defining file types	71
	Create file extensions	71
	Create file extension groups	71
	Defining network file shares	72
	Create a file server list	72
	Add a single server to a list	73
	Defining network parameters	73
	Create a network address range	73
	Create a network address range group	74
	Create a new network port range	74
7	Classifying content by file destination	75
	How sensitive content is controlled in email	75
	Create email destinations	75
	Create an email group	76
	Defining local and network printers	77
	Creating a printer list and adding printers	77
	Controlling information uploaded to websites	80
	Create a web destination	80
	Create a web destination group	80
8	Limiting rules with assignment groups	83
	User assignment	83
	Create a user assignment group	83
	Create a privileged users group	85
	Computer assignment groups	85
9	Controlling sensitive content with protection rules	87
	How protection rules work	87
	Definitions and how they define rules	90
	Create and define an application file access protection rule	91
	Create and define a clipboard protection rule	92

Create and define an email protection rule	93
Create and define a file system protection rule	94
Create and define a network communication protection rule	95
Create and define a PDF/Image Writer protection rule	96
Create and define a printing protection rule	97
Create and define a removable storage protection rule	98
Create and define a screen capture protection rule	99
Create and define a web post protection rule	100
Delete rules, definitions, device classes, or user groups	101
Using predefined definitions	101
Synchronize templates	102
10 Assigning policies	103
Assigning policies with ePolicy Orchestrator	103
Apply the system policy	104
Assign a policy or agent configuration	104
Refresh the policy	105
Importing policies and editing policy descriptions	105
Import a policy from ePolicy Orchestrator	105
Edit a policy description	106
Agent bypass and related features	106
Request an override key	107
Generate an agent override key	109
Generate a quarantine release key	109
11 Collecting and managing administrative data	111
Endpoint events and how they are tracked	111
Agent override	112
Documenting events with evidence	112
Monitoring activity with hit count	113
Protecting confidentiality with redaction	113
View redacted monitor fields	115
Monitor system events and alerts	115
Filter event information	116
Define filters	117
Define date filters	118
Add predefined filters	118
Filter the events monitor list	118
Use labels to mark events	119
Search monitor events by event ID	120
Export monitor events	120
Print monitor events	120
Send monitor events by email	121
12 Creating reports	123
Report options	123
Set up RSS feeds	126
Set up Data Loss Prevention rolled up reports	126
Administer the database	126
View database statistics	127
13 Configuring system components	129
Agent configuration	129
Managing Agent configuration	129
Configure Safe Mode operation	130
System tools	131

View the system log	131
-------------------------------	-----

Index	133
--------------	------------

Preface

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

This guide provides the necessary information for using McAfee DLP Endpoint software, configuring agents, and creating and monitoring policies to prevent data loss. Data loss is defined as confidential or private information leaving the enterprise as a result of unauthorized communication through channels such as applications, physical devices, or network protocols.

McAfee DLP Endpoint software runs in McAfee® ePolicy Orchestrator® software, the centralized policy manager for security products and systems. Version 9.2 can be installed in any version of ePolicy Orchestrator from 4.0 to 4.6.

McAfee DLP Endpoint software is available in two configurations: McAfee® Device Control and full McAfee DLP Endpoint. Each configuration is available with two licensing options, 90-day trial and unlimited. The default installation is a 90-day license for McAfee Device Control software.

Contents

- [About this guide](#)
- [Finding 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 the following typographical conventions and icons.





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

Bold Text that is strongly emphasized.

User input or Path Commands and other text that the user types; the path of a folder or program.

Code

A code sample.

User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a 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.

Finding 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

- 1 Go to the McAfee Technical Support ServicePortal at <http://mysupport.mcafee.com>.
- 2 Under **Self Service**, access the type of information you need:

To access...	Do this...
User documentation	<ol style="list-style-type: none">1 Click Product Documentation.2 Select a product, then select a version.3 Select a product document.
KnowledgeBase	<ul style="list-style-type: none">• Click Search the KnowledgeBase for answers to your product questions.• Click Browse the KnowledgeBase for articles listed by product and version.

1

What is McAfee Data Loss Prevention Endpoint?

McAfee DLP Endpoint software is a content-based agent solution that inspects enterprise users' actions concerning sensitive content in their own work environment, their computers. It uses advanced discovery technology as well as predefined dictionaries to identify this content, and incorporates device management and encryption for additional layers of control.

Understanding McAfee DLP Endpoint configuration options

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

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** — Controls what data can be copied to removable devices, or 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

The default installation of McAfee DLP Endpoint software is for a 90-day trial license for McAfee Device Control software. Upgrade to the full McAfee DLP Endpoint 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 re-install the software.

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, email or email attachments, web posts, 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 or not they are connected to the enterprise's network

What is the difference between configurations?

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

- Discovery
- Printers
- Email Destinations
- Rights Management
- File Servers
- Web Destinations
- Network

The following features are unavailable:

- Protection rules (with the exception of removable storage rules)
- Tags and tagging rules

Contents

- *How McAfee DLP Endpoint works*
- *The McAfee DLP Endpoint policy console*

How McAfee DLP Endpoint works

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

McAfee DLP Endpoint policies are monitored, and defined actions using content identified as sensitive are monitored or blocked, as required. In certain cases, sensitive content is encrypted before the action is allowed. Content is stored as evidence, and reports are created for review and control of the process.

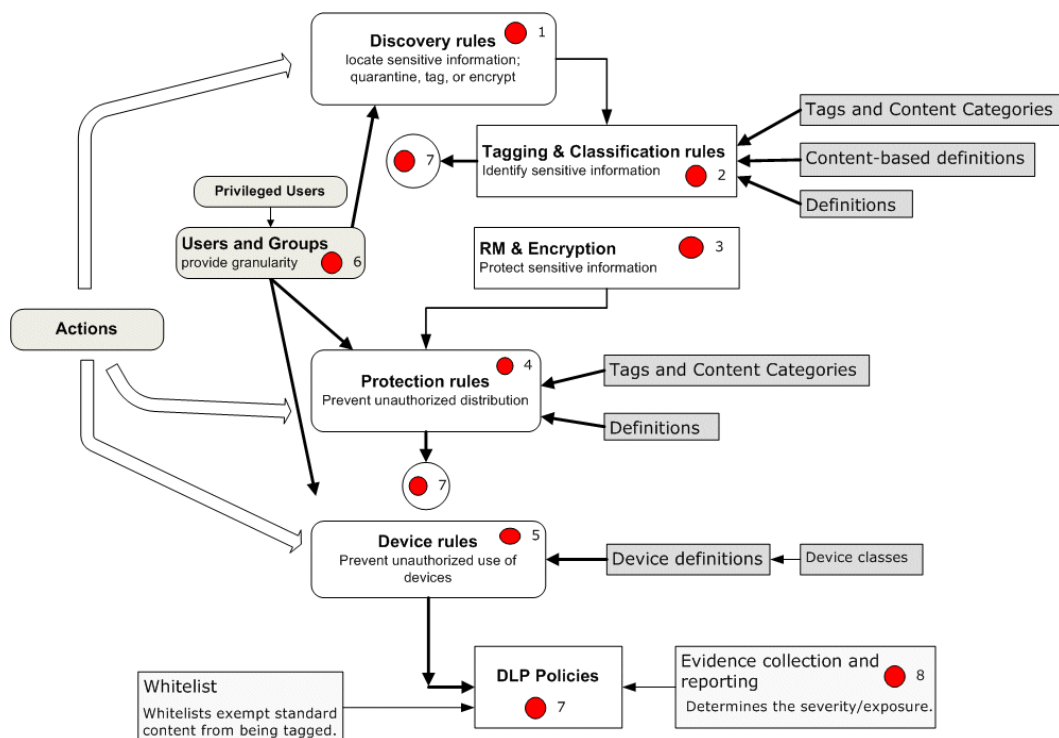


Figure 1-1 McAfee DLP Endpoint workflow

Tagging and classification rules

Tagging and classification 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.
- **Content** — 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.
- **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.

Tags and content categories identify files as containing sensitive information. 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.

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.

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.

Removable storage device rules offer additional functionality to set the device as read-only and prevent writing data to the device.

Discovery rules

McAfee Data Loss Prevention Discover 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.

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).

Monitoring

- **Event monitoring** — McAfee DLP Monitor software allows administrators to view agent events as they are received.
- **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.

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.

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.

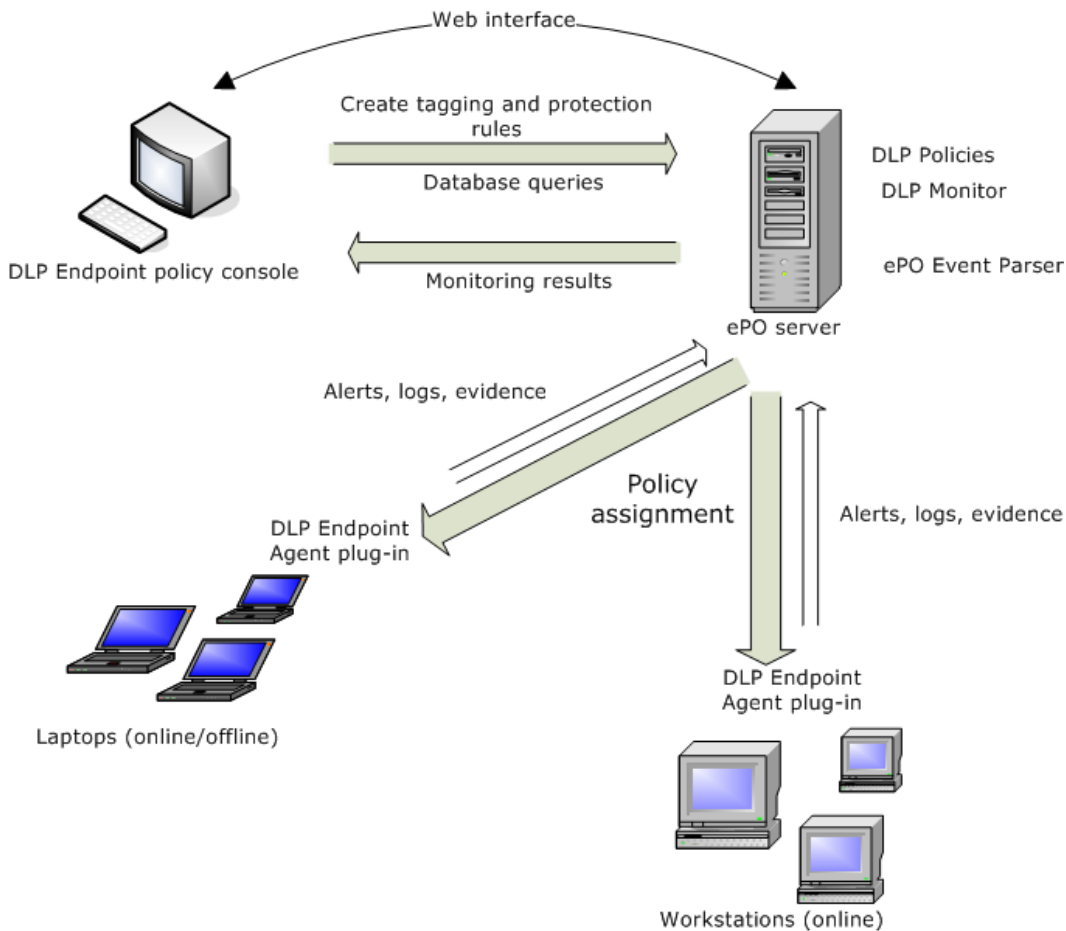


Figure 1-2 McAfee DLP Endpoint software

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 components.

The McAfee DLP Endpoint policy console is accessed from the ePolicy Orchestrator Menu under **Data Protection**.

McAfee Data Loss Prevention Endpoint (McAfee Agent plug-in)

The McAfee DLP Endpoint plug-in resides on enterprise computers, which are referred to as managed computers, and enforces the policies defined in the McAfee DLP Endpoint policy. The McAfee DLP Endpoint software audits user activities to monitor, control, and prevent unauthorized users from copying or transferring sensitive data. It also generates events recorded by the ePolicy Orchestrator Event Parser.

Event Parser

Events that are generated by the McAfee DLP Endpoint plug-in 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.

McAfee Data Loss Prevention Monitor

Events that are sent to the ePolicy Orchestrator Event Parser are displayed in the McAfee DLP Monitor, an interface accessed in ePolicy Orchestrator by navigating to **Menu | Data Protection | DLP Monitor**. 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.

Strategies for categorizing applications

McAfee DLP Endpoint software divides applications into four categories or “strategies”.

A *strategy* is assigned to each application definition. You can change the strategy to achieve a balance between security and the computer’s operating efficiency. The strategies, in order of decreasing security, are:

- **Editor** — Any application that can modify file content. This includes “classic” editors like Microsoft Word and Microsoft Excel, as well as browsers, graphics software, accounting software, and so forth. Most applications are editors.
- **Explorer** — An application that copies or moves files without changing them, such as Microsoft Windows Explorer or certain shell applications.
- **Trusted** — An application that needs unrestricted access to files for scanning purposes. Examples are McAfee® VirusScan® Enterprise, backup software, and desktop search software (Google, Copernic, and so forth.).
- **Archiver** — An application that reprocesses files. Examples are compression software such as WinZip, and encryption applications such as McAfee® Endpoint Encryption for Files and Folders™ software or PGP.

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.

Encryption

Encryption of critical documents is an important part of a strong security policy.

McAfee DLP Endpoint software version 9.x supports encryption in the following ways:

- Built-in device definitions to recognize McAfee Endpoint Encryption for Removable Media devices and content encrypted with McAfee Endpoint Encryption for Files and Folders software
- Support in file system discovery rules for Adobe® LiveCycle® and Microsoft Rights Management protection
- Filtering in rules by document property (encrypted/not encrypted)
- Filtering in file system discovery, email storage discovery, and most protection rules by Adobe LiveCycle or Microsoft Rights Management protection
- Encryption on demand
- Encryption keys definitions

Device definitions

Built-in device definitions for McAfee Endpoint Encryption for Removable Media and McAfee Endpoint Encryption for Files and Folders allow the creation of device rules that permit only encrypted content to be saved to devices. All other content is blocked.

Encryption filters

Email protection, file system, removable storage, and web post protection rules, as well as file system and email storage discovery rules, allow encrypted content to be defined in the rule. Using this feature, you can block unencrypted email or web post attachments, but permit encrypted ones. Two precautions must be observed:

- Email applications treat the body of the email as an attachment. If you create a rule to block unencrypted content and do not use an additional parameter to define the attached file, such as a tag, a file type, or a file extension, all emails will be blocked.
- If you have McAfee Endpoint Encryption for Files and Folders software installed and you drag an encrypted file to an email, the encryption is stripped because you are "opening" the file on your computer, which is allowed. To send an encrypted attachment, attach a self-extractor file rather than one with standard encryption.

You can also use file types in rules to point to encrypted files. The **XML** file type is also associated with McAfee Endpoint Encryption for Files and Folders *.sba files, and the **Executable program files** file type is also associated with self-extractors.

Encrypt on demand

File system protection, removable storage protection, and file system discovery rules have an on-demand encryption option. This means that in addition to the usual actions of Block, Monitor, and so forth, the option **Encrypt** is present on the rule wizard actions page. To use this option, McAfee Endpoint Encryption for Files and Folders software must also be installed, and you must define an encryption key in the McAfee DLP Endpoint policy with a name that matches a defined key in the McAfee Endpoint Encryption for Files and Folders software.

The McAfee DLP Endpoint policy console

The McAfee DLP Endpoint policy console is the interface for McAfee DLP Endpoint software and is accessed from the McAfee ePolicy Orchestrator console.

You use the McAfee DLP Endpoint policy console to create and enforce policies that protect your enterprise's sensitive information. This is where you create, modify and control system rules and objects to prevent information loss.

The McAfee DLP Endpoint policy console is divided into these areas:

- 1 **Navigation pane** — Where the system administrator selects a rule or definition. The main pane displays information about the selected object.
 - **Applications** — Access the *Enterprise Application List* to import applications
 - **Content Based Definitions** — Create *dictionaries*, *text patterns*, and *registered document repositories* to identify sensitive content
 - **Content Protection** — Access *Tagging Rules* or *Classification Rules* to classify content, *Protection Rules* to enforce the defined policies, and *Discovery Rules* to search for sensitive content in your network
 - **Database Administration** — Monitor and maintain the system's database
 - **Definitions** — Create new objects for system rules
 - **Device Management** — Monitor and control the use of physical devices

- **Policy Assignment** — Create and maintain user groups for deploying policies, and groups of privileged users that can bypass policy enforcement
 - **RM and Encryption** — Set up communication with rights management servers, manage policies/templates, and create encryption keys
- 2 **Editing Pane**— Where the system administrator edits and reviews rules or definitions, depending on which object is currently selected in the navigation pane
 - 3 **Details pane** — Displays a detailed description of a single object selected in the main pane

2

Controlling removable media with device rules

A *device rule* consists of a list of the *device definitions* included or excluded from the rule, and the action taken when the rule is triggered by content being sent to or from the named device or devices.

Devices attached to enterprise managed computers — such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or Plug and Play devices — can be monitored or blocked using device rules, allowing you to monitor and control their use in the distribution of sensitive information. For many organizations, this level of data loss prevention is the primary goal. This is the level of protection provided by McAfee Device Control software.

In addition, you can create different sets of rules for the enterprise workforce based on roles and needs. For example, while the majority of workers are not allowed to copy enterprise data to removable storage devices, the IT and sales force can use these devices, and are only monitored by the system. This kind of scenario can be implemented by using the properties of the specific device with a suitable device rule.

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).

When you install McAfee DLP Endpoint software, 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 software.
- **Unmanaged** — Device classes not managed by McAfee DLP Endpoint software, but whose status can be changed to Managed by the system administrator.
- **Unmanageable** — Device classes not managed by McAfee DLP Endpoint software 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.

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).

For option definitions, press **F1**.

Task

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

The available devices appear in the right-hand 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**.

Change the status of a device class

Device classes can be either managed or unmanaged.

Task

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

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

The available devices appear in the right-hand pane.

- 2 Right-click a specific device class and select **Change Device Status to Managed** or **Change Device Status to Unmanaged**, as appropriate.



Details for "Unknown" device classes (classes with no name) can appear in the McAfee DLP Monitor display. These events should be handled by the system administrator, and added to the managed or unmanaged device lists as appropriate.

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 two types:

- **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. Plug and Play device definitions allow you to manage and control most available devices, for example, Bluetooth, Wi-Fi, and PCMCIA, to prevent such devices from being loaded by the system.
- **Removable Storage devices** — External devices containing a file system that appear on the managed computer as drives.



While the Plug and Play device definitions and rules include general device properties, the removable storage device definitions and rules 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.

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.

See also

[Device parameters on page 23](#)

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 inside the McAfee DLP Monitor display and exporting the device parameters (using the context menu) to a CSV file, one comma separated row per event. Lists can also be created manually.

See the online Help for information on formatting the CSV file.

Creating 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 the device definition shown below:

Table 2-1 Device definition example

Device definition	Selected parameters
Bus Type	Firewire; USB
Device Class	Memory Devices; Windows Portable Devices

- 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 20](#)
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 21](#)
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 21](#)
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 22](#)
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 22](#)
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 23](#)
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.

For option definitions, press **F1**.

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 **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.

For option definitions, press **F1**.

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 **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 the **Parameter Name** from the available list.

The **Edit the device 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.

For option definitions, press **F1**.

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 **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 McAfee DLP Monitor display and selecting **Export Device Event 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.

For option definitions, press **F1**.

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 **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 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 2-2 Device definitions for Plug and Play and removable storage devices

Parameter name	Found in...	Import parameters	Description
Bus Type	Both	Yes	Selects the device BUS type from the available list (IDE, PCI, and so forth.)
CD/DVD Drives	RS only	No	A generic category for any CD or DVD drive.

Table 2-2 Device definitions for Plug and Play and removable storage devices *(continued)*

Parameter name	Found in...	Import parameters	Description
Content encrypted by McAfee Endpoint Encryption for Files and Folders	RS only	No	Select to indicate a device protected with McAfee Endpoint Encryption for Files and Folders.
Device Class	PnP only	No	Selects the device class from the available managed list.
Device Compatible IDs	Both	Yes	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.
Device Instance ID (Microsoft Windows XP; Microsoft Windows 2000) Device Instance Path (Microsoft Windows Vista; Microsoft Windows 7)	Both	Yes	A Windows-generated string that uniquely identifies the device in the system. For example, <code>USB\VID_0930&PID_6533\5&26450FC&0&6</code> .
Device Name	Both	Yes	The name attached to a hardware device, representing its physical address.
File System Type	RS only	No	The type of file system, for example NTFS, FAT32, and so forth.
File System Access	RS only	No	The access to the file system: read only or read-write.
File System Volume Label	RS only	Yes	The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.
File System Volume Serial Number	RS only	Yes	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.
PCI VendorID / DeviceID	Both	Yes	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&DEV_2580&SUBSYS_00000000&REV_04</code> .
USB Class Code	PnP only	No	Identifies a physical USB device by its general function. Select the class code from the available list.

Table 2-2 Device definitions for Plug and Play and removable storage devices *(continued)*

Parameter name	Found in...	Import parameters	Description
USB Device Serial Number	Both	Yes	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, <code>USB\VID_3538&PID_0042\000000000002CD8</code> . A valid serial number must have a minimum of 5 alphanumeric characters and must not contain ampersands (&). If the last part of the instance ID does not follow these requirements, it is not a serial number.
USB Vendor ID / Product ID	Both	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: <code>USB\VID_3538&Pid_0042</code> .

Device rules

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

There are three types of device rules: **Plug and Play**, **removable storage** and **removable storage file access**. Plug and play and removable storage rules allow the device to be blocked or monitored, and for the user to be notified of the action taken. Removable storage file access rules block executables on plug-in devices from running.

Removable storage device rules can also define a device as **read only**. A typical use of this feature is to allow users to listen to MP3 players, but block their potential use as storage devices.

Device 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: `.bat`, `.cgi`, `.cmd`, `.com`, `.cpl`, `.dll`, `.exe`, `.jar`, `.msi`, `.py`, `.pyc`, `.scr`, `.vb`, `.vbs`, `.ws`, and `.wsf`. In addition, to block files that might be executed from within archives, `.cab`, `.rar`, and `.zip` files are also blocked.



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.

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. 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 | 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 a Plug and Play device definition or definitions or 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 Edit alert popup 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 Blocking Rule are the recommend way of blocking USB devices.

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 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:

Step	Action
1 of 3	Select a removable storage device definition or definitions or 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 .
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 Edit alert popup to modify the alert message, URL, or link text. Click Next .
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 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.

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:

Step	Action
------	--------

Step 1 of 3	Select a removable storage device definition or definitions or 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 .
--------------------	---

Step 2 of 3	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 .
--------------------	--

Step 3 of 3	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.

For option definitions, press the **F1** key.

Task

- 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 2-3 Device definitions for Plug and Play and removable storage devices

Parameter name	Found in...	Import parameters	Description
Bus Type	Both	Yes	Selects the device BUS type from the available list (IDE, PCI, and so forth.)
CD/DVD Drives	RS only	No	A generic category for any CD or DVD drive.
Content encrypted by McAfee Endpoint Encryption for Files and Folders	RS only	No	Select to indicate a device protected with McAfee Endpoint Encryption for Files and Folders.
Device Class	PnP only	No	Selects the device class from the available managed list.
Device Compatible IDs	Both	Yes	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.
Device Instance ID (Microsoft Windows XP; Microsoft Windows 2000) Device Instance Path (Microsoft Windows Vista; Microsoft Windows 7)	Both	Yes	A Windows-generated string that uniquely identifies the device in the system. For example, <code>USB\VID_0930&PID_6533\5&26450FC&0&6</code> .
Device Name	Both	Yes	The name attached to a hardware device, representing its physical address.
File System Type	RS only	No	The type of file system, for example NTFS, FAT32, and so forth.
File System Access	RS only	No	The access to the file system: read only or read-write.
File System Volume Label	RS only	Yes	The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.
File System Volume Serial Number	RS only	Yes	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.

Table 2-3 Device definitions for Plug and Play and removable storage devices *(continued)*

Parameter name	Found in...	Import parameters	Description
PCI VendorID / DeviceID	Both	Yes	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, PCI\VEN_8086&DEV_2580&SUBSYS_00000000&REV_04.
USB Class Code	PnP only	No	Identifies a physical USB device by its general function. Select the class code from the available list.
USB Device Serial Number	Both	Yes	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&PID_0042\000000000002CD8. A valid serial number must have a minimum of 5 alphanumeric characters and must not contain ampersands (&). If the last part of the instance ID does not follow these requirements, it is not a serial number.
USB Vendor ID / Product ID	Both	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.

3

Classifying content

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

- *Using dictionaries to classify content*
- *Classifying content with document properties or file extensions*
- *Defining registered document repositories*
- *Text pattern definitions*
- *Whitelist*

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 cut and paste 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 "**cat**aracts" and "duplic**ate**." 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.

For option definitions, press the **F1** key.

Task

- 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 Type a description (optional). Click **Add** to create a new text box. Type the new word or phrase in the text box.
- 5 To change the default weight, select the text and edit.
- 6 Repeat steps 4 and 5 as necessary, then click **OK** to save the dictionary.
- 7 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.

- 8 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.
- 9 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.

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

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.

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_docs9200_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.

For option definitions, press **F1**.

Task

- 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 defined registered documents classification rules. For option definitions, press **F1**.

Task

- 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**.

Index 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.

Task

For option definitions, click ? in the interface.

- 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 pull-down menu. 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.

Task

For option definitions, click ? in the interface.

- 1 In ePolicy Orchestrator select **Menu | System Tree**.
- 2 In the System Tree, select the level at which to deploy the registered document package.



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 Click the **Assigned Client Tasks** tab. Under Actions, select **New Client Task Assignment**.

The Client Task Builder wizard opens.

- 4 In the **Product** field select. 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 Endpoint`. Typing a description is optional.
- 6 In the **Products and Components** field, select **DLP Registered Documents 9.2.0.x**. Leave the **Action** field on **Install**.
- 7 Click **Save**.
- 8 Select a suitable **Schedule type** and set the **Options**, date, and **Schedule** parameters. Click **Next**.
- 9 Review the task summary. When you are satisfied that it is correct, click **Save**.

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.

In McAfee DLP Endpoint software version 9.2, 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 37](#)
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 39](#)
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 40](#)
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.

For option definitions, press the **F1** key.

Task

- 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)

Details

Name: Credit Card Number (Visa)

Description: A 16 or 13 digits CCN in the format of 4-4-4-4 | 4 4 4 4 | 4444 or 4 5 4 | 4-5-4 | 454 which b

Include content which matches the following patterns:

Recognize pattern if ANY of the following patterns are matched

Text	Is Regex	Validator	Threshold	Edit
\b4\d{15}\b	<input checked="" type="checkbox"/>	Luhn10	1	...

Add Remove

Ignore matches that also match the following patterns:

Text	Is Regex	Validator	Edit
------	----------	-----------	------

Add Remove Import Entries

OK Cancel

Figure 3-1 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.

For option definitions, press **F1**.

Task

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

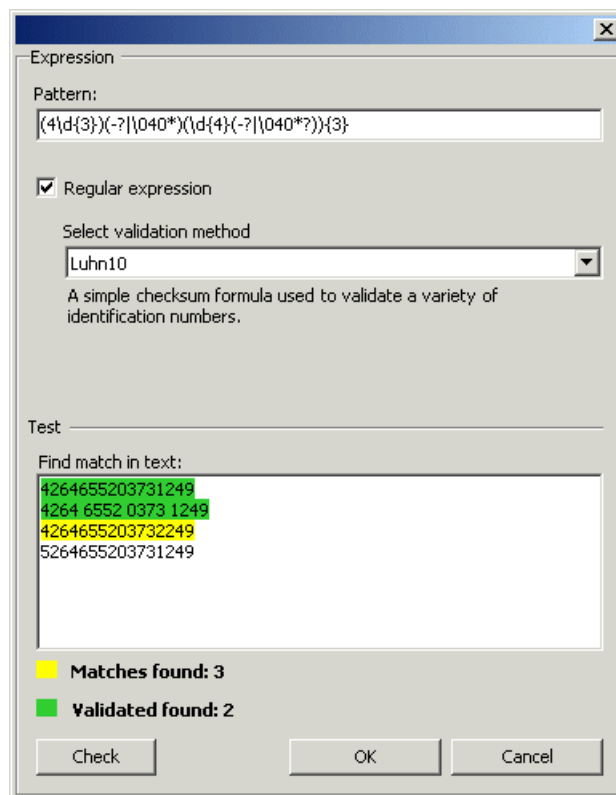


Figure 3-2 Testing a credit card pattern



If you make any changes or additions to the text in the Test box, you must click **Check** again to retest.

- 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.

For option definitions, press **F1**.

Task

- 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**.

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 running the Policy Analyzer.

Add new whitelist content

To save time parsing documents, place standard text such as disclaimers in the whitelist folder.

Task

For option definitions, click ? in the interface.

- 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.

Task

For option definitions, click ? in the interface.

- 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**.

4

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*
- ▶ *How classification rules link categories 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.

Creating 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 44](#)
Tags give you a method for classifying content and reusing that classification.
- [Create a content category on page 44](#)
A content category definition consists of a suitable name, an optional description, and a Globally Unique Identifier (GUID) assigned by the system.
- [Import a category catalog on page 45](#)
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 45](#)
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.

For option definitions, press **F1**.

Task

- 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 Globally Unique Identifier (GUID) assigned by the system.

For option definitions, press **F1**.

Task

- 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.

For option definitions, press **F1**.

Task

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

Task

- 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.
- 4 Add a description (optional).

- 5 Select the tags and content categories for the group.
- 6 Click **OK**.



When using a tag group in protection rules, all tags in the selected group must be available in the specific content for the protection rule to be triggered.

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 Globally Unique Identifier (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.

Creating and defining 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 47](#)
Tagging rules associate files and data with the appropriate tags.
- [Create and define a location-based tagging rule on page 47](#)
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'



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.

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 | 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**.

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 Globally Unique Identifier (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.

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.

Creating and defining 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 49](#)
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 49](#)
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.

For option definitions, press **F1**.

Task

- 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	Action
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 .
2 of 4	Select one of the dictionary options,
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.
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.

For option definitions, press **F1**.

Task

- 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**.

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.

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.

5

Protecting files with rights management

McAfee DLP Endpoint software supports both Adobe LiveCycle Rights Management and Microsoft Windows Rights Management Services.

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 Word 2003, Word 2007, or Word 2010 documents
- Microsoft Excel 2003, Excel 2007, or Excel 2010 documents
- Microsoft PowerPoint 2003, PowerPoint 2007, or PowerPoint 2010 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:

- Microsoft Word 2003, Word 2007, or Word 2010 documents
- Microsoft Excel 2003, Excel 2007, or Excel 2010 documents
- Microsoft PowerPoint 2003, PowerPoint 2007, or PowerPoint 2010 documents
- SharePoint 2007 documents
- Exchange Server 2007 documents

For more information on Adobe LiveCycle Rights Management, go to <http://www.adobe.com/go/rm/>. For more information on Microsoft Rights Management Services, go to <http://www.microsoft.com/windowsserver2003/technologies/rightsmgmt/default.mspx>

Contents

- *Adobe rights management users*
- *How Data Loss Prevention works with rights management*
- *Define an Adobe RM server and synchronizing policies*
- *Define a Microsoft Rights Management Service server and synchronizing templates*

Adobe rights management users

McAfee Data Loss Prevention 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 into 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.

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 McAfee DLP Monitor software. 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 McAfee DLP Monitor display.



You must enable the **Apply RM Policy Failed** event in **Agent Configuration | Events and Logging** for the event to be logged.

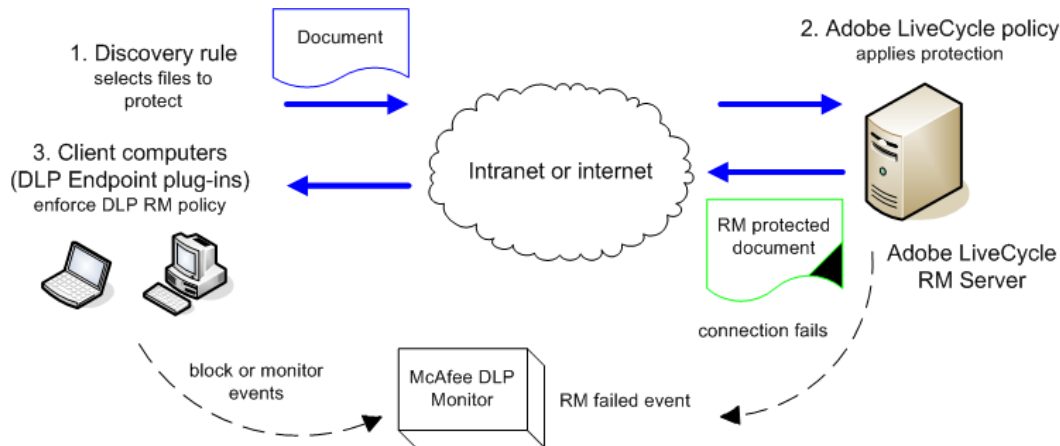


Figure 5-1 Adobe LiveCycle Rights Management protection flow diagram

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 McAfee DLP Monitor software.

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.

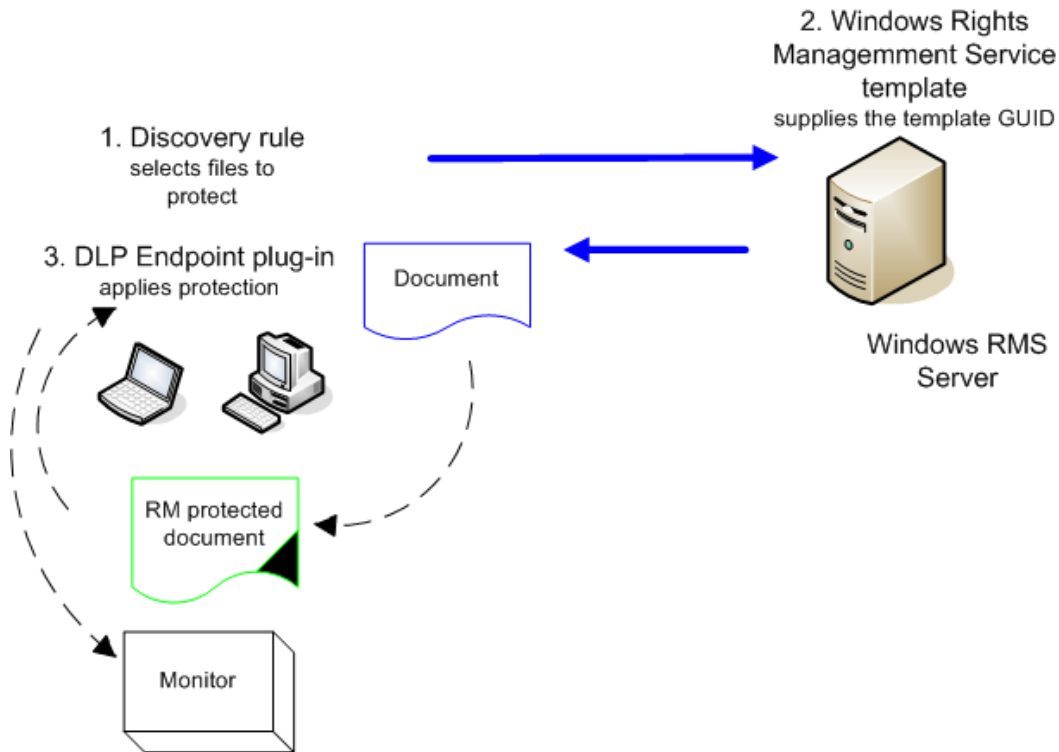


Figure 5-2 Windows Rights Management Services protection flow diagram

With Windows Rights Management Services, McAfee DLP Endpoint software can inspect the content of protected files if the current user has view permissions.

Define an Adobe RM server and synchronizing policies

Set up users in the Adobe LiveCycle Rights Management server with appropriate roles and permissions. For option definitions, press **F1**.

Task

- 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 | Adobe LiveCycle Rights Management Server**.
- 3 Double-click the rule icon. The Adobe LiveCycle Rights Management Server dialog box appears.
- 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 synchronizing templates

Set up users in the Microsoft Rights Management Service server with appropriate roles and permissions. For option definitions, press **F1**.

Task

- 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.
- 7 Select the **Import RMS Templates on OK** checkbox to synchronize policies immediately, then click **OK**.
If you don't select the check box, 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.

- 8 Select **Rights Management Policies** in the navigation pane to view the imported templates.

6

Classifying content by file location

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

This section describes different ways to locate and define the files that contain sensitive data. *Data-at-rest* is the term used to describe actual locations ("where is it in the network?" "which folder is it in?"). McAfee DLP Discover finds your data-at-rest.

McAfee DLP Discover can search for content in endpoint computer files or email storage (PST, mapped PST, and OST) files.

You can also define content by file extension, or by which application created it. This is known as *data-in-use*. These definitions provide granularity to help you protect only those files that need to be protected.

Contents

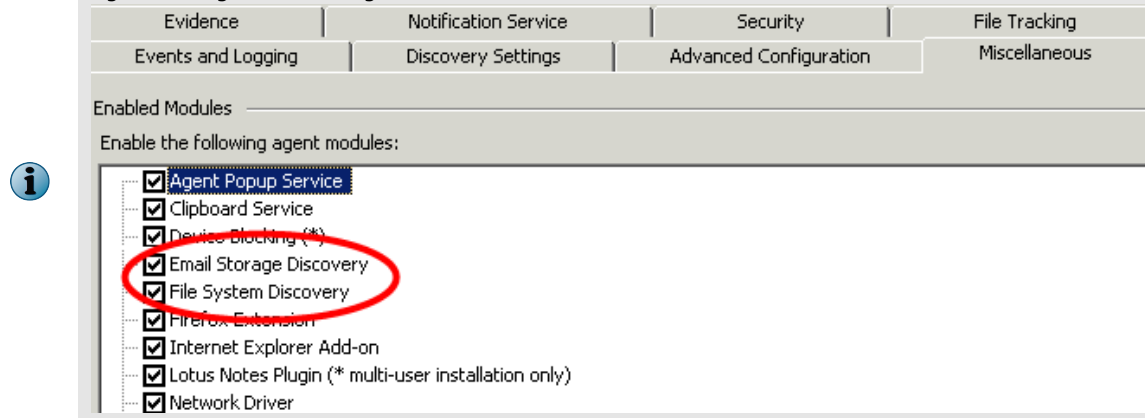
- *How McAfee Data Loss Prevention Discover scanning works*
- *Applications and how to use them*
- *Defining file types*
- *Defining network file shares*
- *Defining network parameters*

How McAfee Data Loss Prevention Discover scanning works

McAfee Data Loss Prevention 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, encrypt, or delete the files containing that content. McAfee DLP Discover can scan computer files or email storage (PST, mapped PST, and OST) files.

To use McAfee DLP Discover, you must activate the discovery modules on the Miscellaneous tab of the Agent Configuration dialog box.



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?

For endpoint discovery scans, you can apply RM protection, 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 on the Policy tab of the **Tools | Options** dialog box in the McAfee DLP Monitor allows you to delete files instead of quarantining them. We do not recommend using this option.

For endpoint scans, you need a release key to release files from quarantine. The user generates a challenge key, sends it to the administrator, and the administrator issues an **Agent Quarantine Release Key**.

Finding 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 61](#)
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 62](#)
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 63](#)
McAfee DLP Discover scans are first defined, then scheduled, using the **Agent Configuration** menu.
- [Schedule a McAfee DLP Discover scan on page 64](#)
McAfee DLP Discover scans are first defined, then scheduled, using the **Agent Configuration** menu.

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.

For option definitions, press **F1**.

Task

- 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	<p>Select actions from the available list.</p> <ul style="list-style-type: none"> • Apply RM Policy: Click Select RM Policy to select a 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. • Tag: Click Select a tag. The tag you use must be predefined. There is no option for adding a tag. <div data-bbox="519 1213 565 1257" data-label="Image"> </div> <p>Apply RM Policy, Quarantine, and Encrypt are mutually exclusive actions; selecting one deselects the others. Other actions are additive.</p> <p>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.</p> <p>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.</p> <p>Click Next.</p>
7 of 7 (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 discovery rule icon and select **Enable**.

Create and define an email storage discovery rule

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.

For option definitions, press **F1**.

Task

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:

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 (optional)	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 (required*)	Select the Select from list option, then select an encryption type.
6 of 7 (required)	Select actions from the available list. If you select Monitor , click Severity to modify the value. Click Next .
7 of 7 (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 discovery rule icon and select **Enable**.

Set up a McAfee DLP Discover scan

McAfee DLP Discover scans are first defined, then scheduled, using the **Agent Configuration** menu.

The McAfee DLP Discover scan is setup on the **Agent Configuration | Discovery settings** dialog box. Changes in discovery setting parameters take effect on the next scan. They are not applied to scans already in progress.

For option definitions, press F1.

Task

1 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.

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.



If you select the **Encrypt** action and McAfee Endpoint Encryption for Files and Folders is not installed, the files are monitored. If you select the **Apply RM policy** action and the RM provider is not available, the files are monitored.

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

- a Click the icon () in the Folders section.
- b Use Windows Explorer to browse to a folder.
- c Cut 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.

PST and OST folders are selected in a separate popup. You must also select the email storage types to be scanned.



If you don't specify any folders for either scan or skip, all folders on the computer are scanned. The only folder that is skipped by default is `C:\Windows`. 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`)

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.

For option definitions, press **F1**.

Task

- 1 On the Discovery Settings tab of the Agent Configuration menu, click the File system scan schedule icon (). Alternately, to schedule a mail storage scan, click the PST and OST scan schedule icon.

A popup 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

Releasing files or email items from quarantine utilizes the challenge-response feature. You can release multiple files or email items recursively using a single key.

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.

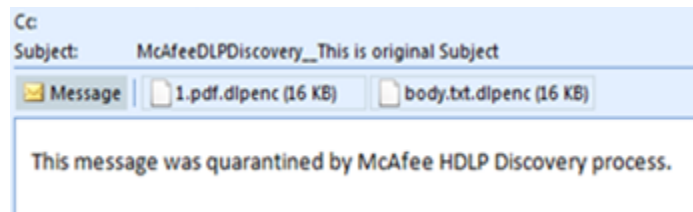


Figure 6-1 Quarantined email example

Calendar items and tasks can also be quarantined.

Task

- 1 **For quarantined files** do the following:
 - a Open the quarantine folder. In the system tray of the managed computer, click the McAfee Agent icon, click **Manage Features**, click **McAfee DLP Agent** and select **Open Quarantine Folder** from the menu.
 - b Select the files to be restored. Right-click and select **Manual Decryption**.

The Challenge/Response popup appears.



The Manual Decryption context-sensitive menu item only appears when selecting files of type *.dlpenc (DLP encrypted).

- 2 **For quarantined email items:** In Microsoft Outlook, select the emails (or other items) to be restored. Click the McAfee DLP icon, or right-click and select **Manual Decryption**.

The Challenge/Response popup appears.

- 3 Copy the challenge ID code from the popup 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 the McAfee DLP Monitor recording all the details.)
- 5 The user enters the response code in the Challenge-Response popup and clicks **OK**.

The decrypted files are restored to their original location. If the release code lockout policy has been activated (on the Notification Service tab of the Agent Configuration) and you enter the code incorrectly three times, the popup times out for 30 minutes (default setting).



For files, if the path has been changed or deleted, the original path is restored. If a file with the same name exists in the location, the file is restored as xxx-copy.abc

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 McAfee DLP Monitor *per application session*, not per sensitive file opened. The event includes all files that matched the specified conditions in that application session. This "aggregated event" behavior is new in McAfee DLP Endpoint software version 9.2. 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.

Adding and removing applications

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

Tasks

- *Import an application manually on page 67*
The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.
- *Import new applications by scanning on page 67*
The Enterprise Applications List is a comprehensive list of the applications whose data you want to control.
- *Remove applications from the list on page 68*
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** icon  discards the current list.
- The **Merge** icon  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.

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.

Creating application definitions

Use these tasks to create application definitions.

Tasks

- [Create an application definition on page 69](#)
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 70](#)
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 70](#)
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 software.

For option definitions, press **F1**.

Task

- 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.



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**.



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.

For option definitions, press **F1**.

Task

- 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.

For option definitions, press **F1**.

Task

- 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.

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.

Create file extensions

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

For option definitions, press **F1**.

Task

- 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.

For option definitions, press **F1**.

Task

- 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**.

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.

For option definitions, press **F1**.

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 **Scan** for these scanning options:



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.

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.

For option definitions, press **F1**.

Task

- 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 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.

For option definitions, press **F1**.

Task

- 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.

For option definitions, press **F1**.

Task

- 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**.

7

Classifying content 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*.

In the following section, the destinations you can control, and the creation of definitions to exercise that control, are described.

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.

See also

Create and define an email protection rule on page 93

Create email destinations

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

For option definitions, press **F1**.

Task

- 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**.

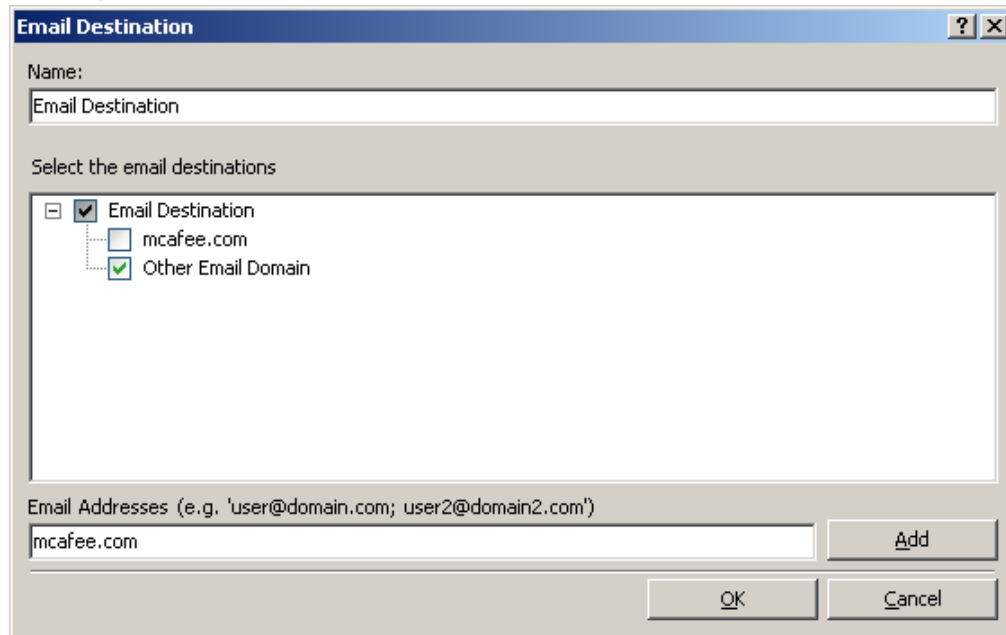


Figure 7-1 Email destination edit dialog box

- 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.

For option definitions, press **F1**.

Task

- 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.

Creating a printer list and adding 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 77](#)
Printer lists are used to manage sensitive content sent to printers.
- [Add a printer to the printer list on page 78](#)
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 78](#)
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 79](#)
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.

For option definitions, press **F1**.

Task

- 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:



You cannot scan for printers in OpenLDAP.

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

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



After editing parameters or adding a filter, you can rerun the search by clicking **Refresh**.

A list of printers appears in the view window.

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

Task

- 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.

For option definitions, press **F1**.

Task

- 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 | 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 cut 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 On the **General** tab, copy the **Model:** information (below the **Comment** text box).

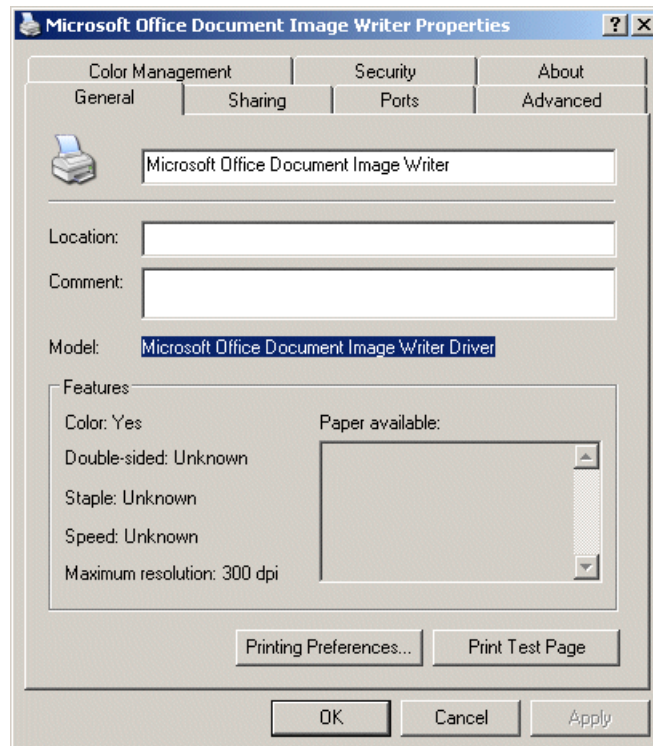


Figure 7-2 Copying the printer model information

- 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.

For option definitions, press **F1**.

- 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 panel.

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.

For option definitions, press **F1**.

Task

- 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.

For option definitions, press **F1**.

Task

- 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.
- 2 In the **Web Servers** window, right-click and select **Add New | Web Server Group**.
A new Web Server Group icon appears.
- 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**.

8

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

User assignment groups define groups of users to be included or excluded from rules. They can be defined using either Microsoft Active Directory or OpenLDAP.

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.

For option definitions, press F1.

Task

- 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.

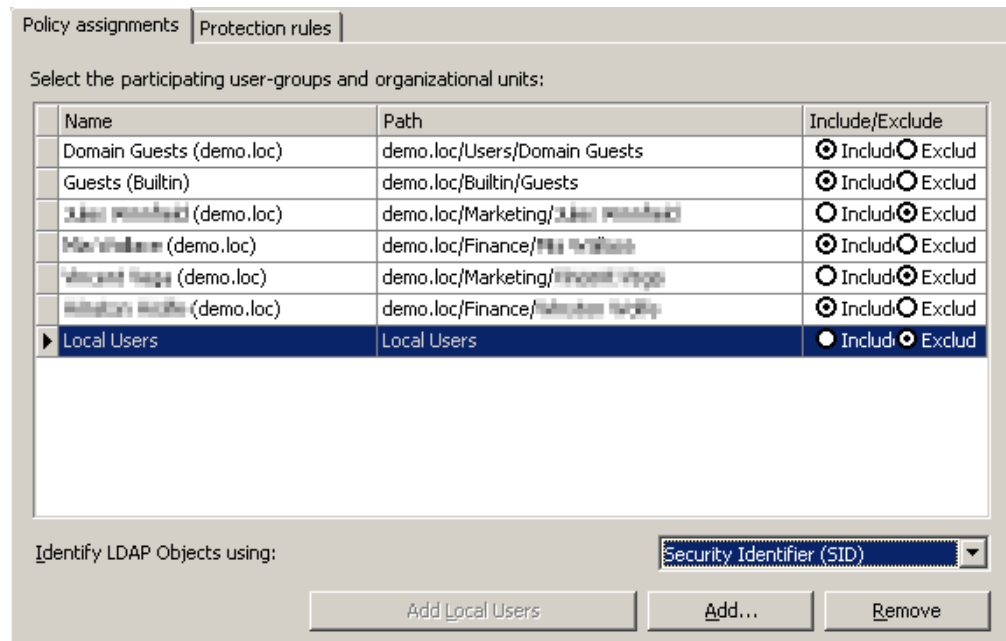


Figure 8-1 Including and excluding users

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

Task

- 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.

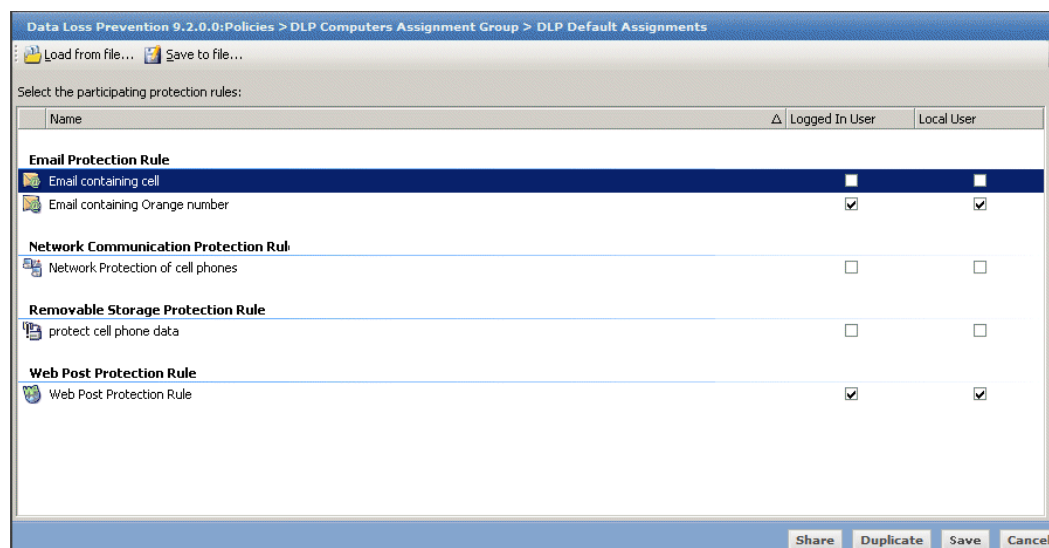


Figure 8-2 Assigning rules with ePO computer assignment groups

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.

9

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.

Contents

- ▶ *How protection rules work*
- ▶ *Definitions and how they define rules*
- ▶ *Delete rules, definitions, device classes, or user groups*
- ▶ *Using predefined definitions*

How protection rules work

Protection rules specify the transfer method, named tag(s), 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 may prevent the transfer of data and notify the user of the violation. Protection rules are optionally applied to assignment groups. This allows 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.

Table 9-1 Actions/Rules matrix

Rules	Actions									
	Block	Monitor	Notify user	Request justification	Store evidence	Encrypt	Quarantine	Apply RM Policy	Apply Tag	Read only
Device Rules										
Plug and Play device rules	A	A	A							
Removable storage device rules	A	A	A							A
Removable storage file access device rules	D		P ¹							
Protection Rules										
Application file access protection rules		A	A							
Clipboard protection rules	A		P ²							
Email protection rules	A	A	A	A	A					
File system protection rules		A	A	A	A	A				
Network communication protection rules	A	A	A							
PDF/Image Writer protection rules	A	A	A	A						
Printing protection rules	A	A	A	A	A					
Removable storage protection rules	A	A	A	A	A	A				
Screen capture protection rules	A	A	A		A					
Web post protection rules	A	A	A	A	A					

Table 9-1 Actions/Rules matrix (continued)

Rules	Actions									
	Block	Monitor	Notify user	Request justification	Store evidence	Encrypt	Quarantine	Apply RM Policy	Apply Tag	Read only
Discovery Rules										
File system discovery rules		A			A	A ³	A	A	A	
Email discovery rules		A			A		A		A	

Table 9-2 Content/Rules matrix

Rules	Content types				Change default alert
	Tags	Content categories	Document properties	Encryption types	
Device Rules					
Plug and Play device rules					A
Removable storage device rules					A
Removable storage file access device rules					
Tagging Rules					
Application based tagging rules	A				
Location based tagging rules	A				
Classification Rules					
Content classification rules		A			
Registered document tagging rules		A			
Protection Rules					
Application file access protection rules	A		A		A
Clipboard protection rules	A	A			P ²
Email protection rules	A	A	A	A	A
File system protection rules	A	A	A	A	A
Network communication protection rules	A				A
PDF/Image Writer protection rules					A
Printing protection rules	A	A			A
Removable storage protection rules	A	A	A	A	A

Table 9-2 Content/Rules matrix *(continued)*

Rules	Content types				Change default alert
	Tags	Content categories	Document properties	Encryption types	
Screen capture protection rules	A				A
Web post protection rules	A	A	A	A	A
Discovery Rules					
File system discovery rules	A	A	A	A	
Email discovery rules	A	A	A	A	
Legend (for both tables)		Notes			
A available (for actions) associated (for content types)		1 Windows displays a message. McAfee DLP Endpoint does not display a message.			
D default		2 Available Only for Block. Clipboard content replaced with specified text. No notification.			
P partial		3 Alternate Delete (not recommended) must be enabled in Tools Options			

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 9-3 Definitions and the tagging and protection rules that use them

Definition	Associated tagging/ classification rules	Associated protection rules
Application	Application-based tagging	Application File Access, Clipboard, File System, Network Communication, Printing, Removable Storage, Screen Capture
Dictionary	Content classification	NA
Email Destination	NA	Email
File Extension	Application-based, Location- based	Application File Access Protection, Email Protection, File System Protection, Network Communication Protection, Removable Storage Protection, Web Post Protection

Table 9-3 Definitions and the tagging and protection rules that use them *(continued)*

Definition	Associated tagging/ classification rules	Associated protection rules
File Server	NA	File System Protection
Network	NA	Network Communication Protection
Printer	NA	Printing Protection
Registered document repository	Registered document classification	NA
Tag/Content Category	Application-based tagging, Location-based tagging, Content classification, Registered document classification	all Protection Rules
Text Pattern	Content classification, Application-based tagging, Location-based tagging	NA
Web Destination	NA	Web Post Protection
Whitelist	NA	NA



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.

For option definitions, press **F1**.

Task

- 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 | 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:

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**.



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.

Step	Action
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 .
	<div>  <p>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.</p> </div>
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.

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

Create and define a clipboard protection rule

Clipboard protection rules monitor or block use of the clipboard. To protect clipboards larger than 1 MB, select the **Protect clipboard of any size** option on the **Advanced Configuration** tab of the **Agent Configuration** dialog box.



Trusted processes are not part of the clipboard rule logic. Applications with a *Trusted* strategy are not exempt from being blocked by clipboard rules.

For option definitions, press **F1**.

Task

- In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**.
The available protection rules appear in the right-hand pane.
- In the Protection Rules pane, right-click and select **Add New | Clipboard Protection Rule**.
- 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 only block pasting into other applications. The other option is to also restrict pasting into different documents in the current application. This more restrictive rule also blocks the Find and Replace dialog, but prevents sensitive information from being copied from tagged documents to untagged documents in the same application.
5 of 6	Select an action from the available list. For clipboard protection rules, Block is the only action, and Online / Offline the only option. Click Next .
5 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**.

Create and define an email protection rule

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

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.

For option definitions, press **F1**.

Task

- 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:

Step	Action
1 of 9 (optional)	Select Select from list option, and select one or more email destination definitions. Click Add item to create a new email destination definition, or Add group to create a new destination group. Click Next .

Step	Action
2 of 9 (optional)	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 Add item to create a new tag or content category. Click Add group to create a new tag and content category group. Click Next .
3 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 .
4 of 9 (optional)	Select the Select from list option, then select file extensions from the available list. Click Next . You can include or exclude file extensions.
5 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 .
6 of 9 (optional)	To apply the rule to attachments of specific encryption types, select the Select from list option, and select one or more attachment encryption types.
7 of 9 (optional)	Email bypass feature: To exclude an email based on subject, select Do not apply this rule if the email subject contains this pattern and select a pattern.
	 Text patterns must be predefined, and only one can be used per rule.
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 select Notify User , click Change default alert to modify the alert message, URL, or link text. If you want Request Justification to block email when no justification is provided, you must also select Block . Click Next .
9 of 9 (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**.

See also

[How sensitive content is controlled in email on page 75](#)

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.

For option definitions, press **F1**.

Task

- 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.

For option definitions, press **F1**.

Task

- 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	Action
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 .
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 .
3 of 7	Select the network connection direction. You can protect incoming or outgoing connections or both directions. Click Next .
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 .
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 .
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 .
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. For option definitions, press **F1**.

Task

- In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**.
The available protection rules appear in the right-hand pane.
- In the Protection Rules pane, right-click and select **Add New | PDF/Image Writers Protection Rule**.
- 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.

For option definitions, press **F1**.

Task

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

Step	Action
1 of 6 (optional)	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 .
2 of 6 (optional)	Select the Select from list option, then select Any local printer to protect printing from local printers. Click Next .



Only one of the first two steps can be optional. You must select a network printer, local printers, or both.

- | | |
|--------------------------|--|
| 3 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 . |
| 4 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 . |

Step	Action
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, URL, or link text. If you want Request Justification to block printing when no justification is provided, you must also select Block . 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.

- 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.

For option definitions, press **F1**.

Task

- In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**.
The available protection rules appear in the right-hand pane.
- In the Protection Rules pane, right-click and select **Add New | Removable Storage Protection Rule**.
- 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:

Step	Action
1 of 8 (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 8 (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 .
3 of 8 (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 8 (optional)	Select the Select from list option, then select file extensions from the available list. Click Next .
5 of 8 (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 8 (optional)	To apply the rule to specific encryption types, select the Select from list option, and select one or more encryption types.

Step	Action
7 of 8	Select actions from the available list. By default, selecting an action selects both Online and Offline . Deselect either as required. If you select Encrypt , click Select an Encryption key to select an encryption key or add a new key. 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 files when no justification is provided, you must also select Block . If you want Request Justification to encrypt files when no justification is provided, you must also select Encrypt . Click Next .
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 as well as application definitions.

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

Create and define a screen capture protection rule

Screen capture protection rules control data copy/pasted from a screen.



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.

For option definitions, press **F1**.

Task

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

- In the Protection Rules pane, right-click and select **Add New | screen Capture Protection Rule**.

- 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:

Step	Action
1 of 5 (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 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 .

Step	Action
------	--------

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.

- 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 Firefox 3.6, 4.0, and 5.0. 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
- Yahoo
- Gmail
- Hotmail
- Google Docs



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.

For option definitions, press **F1**.

Task

- In the McAfee DLP Endpoint policy console navigation pane, select **Content Protection | Protection Rules**

The available protection rules appear in the right-hand pane.

- In the Protection Rules pane, right-click and select **Add New | Web Post Protection Rule**.
- 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:

Step	Action
------	--------

1 of 8(optional)	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 .
-------------------------	---



Not defining any specific web destinations will block all outgoing HTTP content.

2 of 8 (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 .
3 of 8 (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 8 (optional)	Select the Select from list option, then select file extensions from the available list. Click Next .

Step	Action
5 of 8 (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 8 (optional)	To apply the rule to specific encryption types, select the Select from list option, and select one or more encryption types.
7 of 8	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 .
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**.

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.

For option definitions, press **F1**.

Task

- 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**.

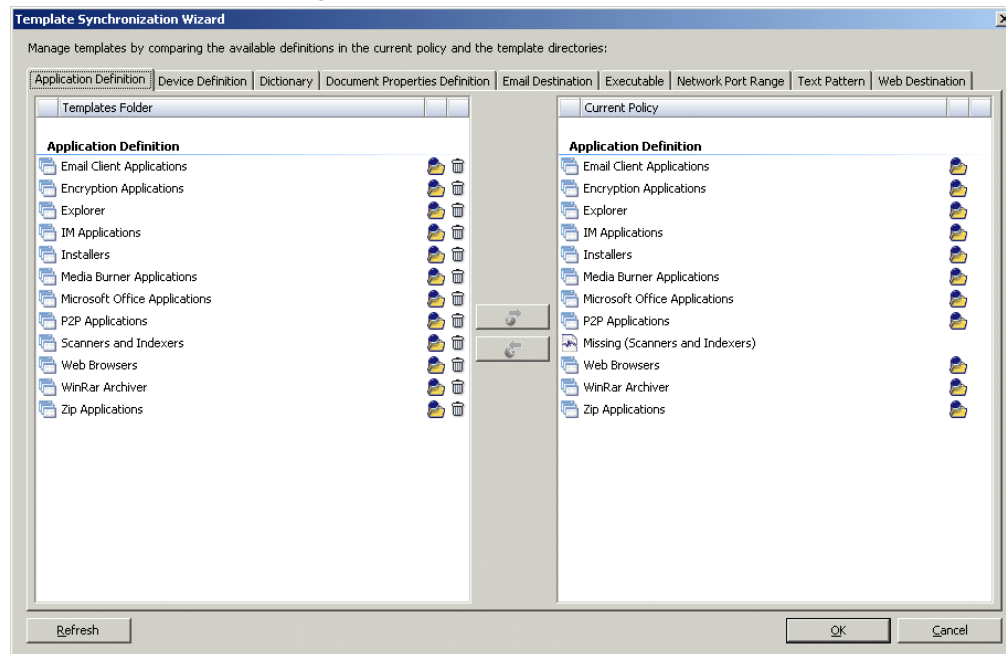






Figure 9-1 The Template Synchronization Wizard

- 3 Click the View icon  to view the selected definition properties or the Delete icon  to remove the selected definition.
 - 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**.

10 Assigning policies

Policies are made up of classification rules, tagging rules, protection rules, device rules, and user and group assignments. They are deployed to managed computers and used to control sensitive information. After creating the rules and definitions required for your enterprise, you enforce them by assigning the policy to your managed computers. Once the policy is in place, use the McAfee DLP Monitor software to audit the state of your enterprise's sensitive information.

Using McAfee DLP Endpoint software involves the following tasks:

- **Assigning policy** — Deploying the McAfee DLP Endpoint policy to managed computers.
- **Monitoring events** — Using McAfee DLP Monitor software to audit, view, filter, and sort events in your enterprise network.
- **Performing administrative maintenance** — Keeping the McAfee DLP Endpoint software up-to-date and generating agent override, agent uninstall, and quarantine release keys as required.



To review a policy quickly, select **File | Export Policy to HTML**. This outputs the policy in an easily readable format for review and analysis. You can control exactly what is output on the **Tools | Options | HTML Export** tab.

Contents

- *Assigning policies with ePolicy Orchestrator*
- *Importing policies and editing policy descriptions*
- *Agent bypass and related features*

Assigning 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.

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 104](#)
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 104](#)
Policies applied to ePolicy Orchestrator must be assigned and deployed to managed computers in order to be used.
- [Refresh the policy on page 105](#)
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, click **Menu | Data Protection | DLP Policy**.
- 2 Verify the policy before applying it: click **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 the *McAfee Data Loss Prevention Endpoint 9.2 Installation 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.

Task

For option definitions, click ? in the interface.

- 1 In ePolicy Orchestrator, click **System Tree**.
- 2 Locate the directory containing the computers that will be assigned a policy, and select them.
- 3 Click **Actions | Agent | Wake Up Agents**.
- 4 Select **Agent Wake-Up Call**, and set **Randomization** to 0 minutes. Click **OK**.

- 5 When the agent wake-up call is completed, you are returned to the System Tree. Reselect the computers that will be assigned a policy, and click **Actions | Agent | Set Policy & Inheritance**.
- 6 On the **Assign Policy** page, select the **Product**, **Category**, and **Policy** to be applied.
- 7 Click **Save**.

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.

Importing 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 105](#)
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 106](#)
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

- 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**.

Agent bypass and related features

Challenge-response refers to the process of bypassing data loss prevention policies when there is a legitimate business need. The two methods provided are agent bypass and business justification.

Occasionally there is a legitimate business need to bypass the McAfee DLP Endpoint system. There are two methods of doing this.

- Business justification action
- Agent bypass

Business justification

Most protection rules offer the option of a **Business Justification** action. When this action is added to a protection rule, the user is prompted when copying or sending sensitive content. Justifications are entered in the Global Agent Configuration window, are customizable, and are part of the global policy. If a user types in a preset justification when prompted, the action is monitored. Otherwise, the action is blocked.

Agent bypass

A user can be given permission to access or transfer sensitive information for a limited time. When this is done, all sensitive information is monitored, rather than blocked, according to existing rules. Both the user and the system administrator receive messages about the bypass status when its enabled and disabled (the user by a popup message, and the administrator by an event entry in the McAfee DLP Monitor display.)

The agent context-menu is used to request a bypass. When this is done, the McAfee DLP Endpoint software generates a FIPS-compliant 16 digit code. The user communicates this code to the McAfee DLP administrator. The administrator then sets the bypass time limit, generates and 32 digit challenge key, and returns this to the user. The challenge key is entered in the appropriate text box, and the bypass timer starts.

Agent bypass now has a lock-out mechanism. If the user enters an incorrect key three times, the dialog box is locked out for 30 minutes.

Agent uninstall

The McAfee DLP Endpoint plug-in is usually uninstalled through the network using features in ePolicy Orchestrator. Local uninstall with Windows **Add or Remove Programs** is also possible using challenge-response. See the *McAfee Data Loss Prevention Endpoint Installation Guide* for more information.

Quarantine removal

A similar situation occurs when the McAfee DLP Discover crawler quarantines sensitive content on a managed computer. To remove the files from quarantine, the user must request a quarantine remove key from the administrator. The procedure is similar to that of agent bypass and uninstall.

Master release key

The bypass, uninstall, and quarantine release features were designed to solve specific, individual problems. In the case of a system-wide incident affecting hundreds or thousands of users, these features become unworkable. McAfee DLP Endpoint now includes a master release key for such situations.

The master release key is distributed by the DLP administrator to all users affected by the problem, but is time-limited to one hour after release. When the user submits a response key, the McAfee DLP Endpoint agent first tries to validate against a personal challenge key. If there is no match, the agent validates the key as a master response key.

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.

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 In the system tray of the managed computer, click the McAfee Agent icon, click **Manage Features**, click **McAfee DLP Agent** and select **Request Agent Bypass** from the menu.

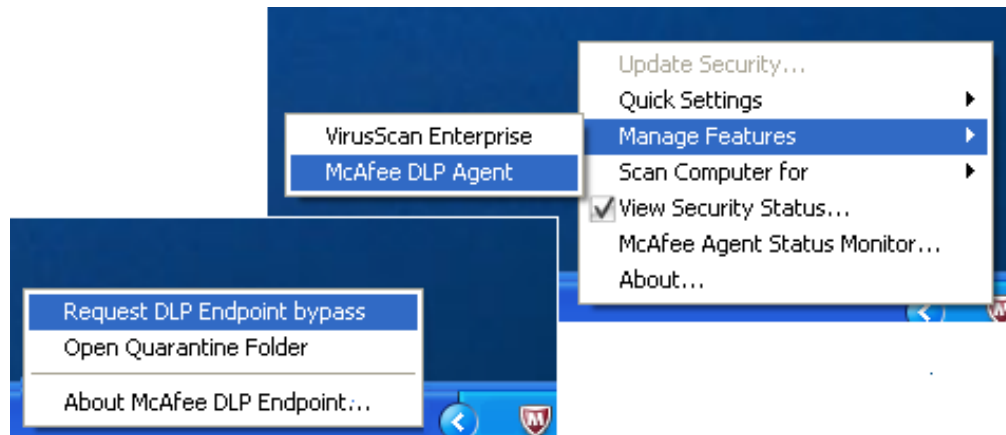


Figure 10-1 Requesting an agent bypass

The release code window appears.



Figure 10-2 Agent bypass release code request

- 2 The user communicates the **Identification Code** to the administrator. 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 **Request Agent Bypass** from the menu a new Identification Code is generated. You must leave the bypass request window open until you receive your matching Release Code.

- 3 Type or paste the **Release Code** into the text box and click **OK**.



The release code is a 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 on the Notification Service tab of the Agent Configuration window, the popup times out for 30 minutes (default setting).

The agent popup displays a verification.

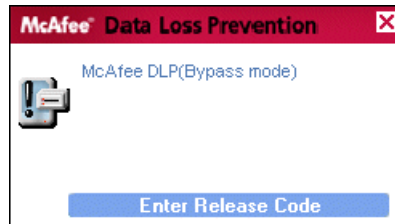


Figure 10-3 Agent popup

Generate an agent override key

An *agent override* is used to create a temporary bypass for DLP policies. When a user requests an override, you can generate an override key for a specified user and a specific period. You can also generate a master release key for problems affecting a large number of users.

This task can be performed in the McAfee DLP Endpoint policy console in ePolicy Orchestrator or using the McAfee DLP Help Desk Tool.

Task

- 1 From the McAfee DLP Endpoint policy console **Tools** menu, select **Generate Agent Override Key**.
- 2 Type the user information in **Step 1**.



All fields are required, and all information is logged to the database.

- 3 Do one of the following in **(Step 2)**:
 - Type the agent override request **Identification Code** generated by the McAfee DLP Endpoint software.
 - Select the **Generate master release code** option.
- 4 Select the length of time to override the system rules. **(Step 3)**
- 5 Type the agent override key password or select **Use password from current policy**. **(Step 4)**
- 6 Click **Generate Key** to create the override code for the user.

This **Release Code** is sent to the user to enter into the request bypass dialog box.

Generate a quarantine release key

File system discovery rules can place files on a managed computer in quarantine if they contain sensitive content. The administrator can release these files for use by creating a quarantine release key. This process is only required once per quarantine folder.

This task can be performed in the McAfee DLP Endpoint policy console in ePolicy Orchestrator or using the McAfee DLP Help Desk Tool.

Task

- 1 From the McAfee DLP Endpoint policy console **Tools** menu, select **Generate Agent Quarantine Release Key**.
- 2 Type the user information in **Step 1**.



All fields are required, and all information is logged to the database.

- 3 Do one of the following in (**Step 2**):
 - Type the agent challenge code.
 - Select the **Generate master release code** option.
- 4 Type the agent override key password or select **Use password from current policy**.
- 5 Click **Generate Key** to create the release key for the user.

This **Release Code** is sent to the user to enter into the request bypass dialog box.

See also

[How McAfee Data Loss Prevention Discover scanning works](#) on page 60

11 Collecting and managing administrative data

The McAfee DLP Monitor software provides the necessary feedback for designing an effective data loss prevention system.

Monitoring the system consists of gathering and reviewing evidence and events, and producing reports. You can use the database administration tools to manage the database and view database statistics.

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

- ▶ *Endpoint events and how they are tracked*
- ▶ *Documenting events with evidence*
- ▶ *Monitoring activity with hit count*
- ▶ *Protecting confidentiality with redaction*
- ▶ *Monitor system events and alerts*
- ▶ *Filter event information*
- ▶ *Use labels to mark events*
- ▶ *Search monitor events by event ID*
- ▶ *Export monitor events*
- ▶ *Print monitor events*
- ▶ *Send monitor events by email*

Endpoint events and how they are tracked

Administrators view security events in McAfee DLP Monitor. The McAfee DLP Monitor software can be installed on multiple servers, or multiple clients connected to the ePolicy Orchestrator server with a browser.

When the McAfee DLP Endpoint 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 can be viewed, filtered, and sorted in McAfee DLP Monitor, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.

The McAfee DLP Monitor software can be installed on multiple ePolicy Orchestrator servers, and specific monitoring permissions are defined during the installation of the DLP Windows Communication Foundation (WCF) Service. It can also be installed on multiple clients that connect to the ePolicy Orchestrator server using a browser.

As McAfee DLP Endpoint takes a major role in a enterprise's effort to comply with all regulation and privacy laws, McAfee DLP Monitor 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

McAfee DLP Monitor 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.

Agent override

Agent override is a temporary suspension of blocking rules. It is applied when a user has permission to send information normally considered sensitive.

Agent override temporarily suspends blocking by the endpoint software. When in override mode, the endpoint software still collects and sends event information to the ePolicy Orchestrator Event Parser. Events are marked with the override flag. The user does not receive visual notification of events while in override mode.

Documenting events with evidence

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

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 software 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 Data Loss Prevention software. 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 McAfee ePolicy Orchestrator. See the *McAfee Data Loss Prevention Installation Guide* for details on setting up the folder and setting access permissions.
- **Evidence service** — The evidence service is enabled on the **Miscellaneous** tab of the Agent Configuration. It is a subentry under **Reporting Service**, which must also be enabled for evidence collection.
- **Evidence replication setting** — A setting on the **Evidence** tab of the Agent Configuration allows you to select evidence collection, hit highlighting, or both.

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. Text patterns find up to 100 hits per expression; dictionaries can display a maximum of 10,000 hits. Display options are set on the **Evidence** tab of the Agent Configuration:

- **Show abbreviated hits** (default) — Displays 1500 characters (5-7 hits) per section.
- **Show all hits** — Displays all hits in all sections.

Rules allowing evidence storage

The following rules have the option of storing evidence:

Table 11-1 Evidence saved by rules

Rule	What is saved
Email protection rules	Copy of the email
File system protection rules	Copy of the file
Printing protection rules	Copy of the file
Removable storage protection rules	Copy of the file
Screen capture protection rules	JPEG of the screen
Web post protection rules	Copy of the email
File System Discovery rules	Copy of the file
Email Storage Discovery rules	Copy of the .msg file

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 McAfee DLP Monitor software 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.

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.

Protecting confidentiality with redaction

Data redaction is the encrypting of confidential information to prevent unauthorized viewing. It is required by law in some countries.

To meet legal demands in some markets, and to protect confidential information in all circumstances, McAfee Data Loss Prevention software offers a *data redaction* feature. When using data redaction, specific fields in the McAfee DLP Monitor display containing confidential information are encrypted to prevent unauthorized viewing, and links to evidence are hidden. Currently, the fields **computer name**, **user name**, and **IP address** are predefined as confidential.

Redacted information is encrypted in:

- the McAfee DLP Monitor display
- RSS feeds

The confidential fields can only be viewed by a user who has **User can reveal sensitive data...** permissions. This can only be done in the presence of a user with **User can partially view DLP Monitor** permissions. The permissions are set up in the Permission Sets section of ePolicy Orchestrator. If you are not using the redaction feature, use the permission **User can view DLP Monitor**, which allows viewing without encryption. See the *McAfee Data Loss Prevention Installation Guide* for details on setting permissions.

For RSS feeds, the enable/disable option is in the WCF setup wizard.

Redaction in ePolicy Orchestrator Reports

In ePolicy Orchestrator reports and the Event Threat log, all DLP events are filtered out of the reports for unauthorized users. A user with the DLP Monitor permission **User can partially view DLP Monitor** can view only the following reports:

- Agent distribution by date
- Agent version
- Bypassed agents
- Enforced device control rules.
- Enforced discovery rules
- Enforced protection rules
- Evidence path distribution
- Policy distribution
- Privileged permissions
- Undefined device classes
- Unmanaged printers
- Unsupported printers

Table 11-2 Summary of McAfee DLP Monitor permissions and their effects

Permission	Description	Effect in DLP Monitor	Effect in ePO Reports	Effect in RSS feeds	Effect in Event Threat log
User cannot view DLP Monitor	User is unauthorized to view the McAfee DLP Monitor display	The McAfee DLP Monitor display is unavailable.	No DLP Reports are authorized.	Available. Confidential fields are encrypted if WCF service was installed with redaction enabled.	Only general information about DLP events is available.
User can partially view DLP Monitor...	User is not authorized to view confidential fields.	The McAfee DLP Monitor display is available, but confidential fields are encrypted and evidence is hidden.	DLP Event Reports are empty. All events are filtered out.		DLP events are filtered out.

Table 11-2 Summary of McAfee DLP Monitor permissions and their effects *(continued)*

Permission	Description	Effect in DLP Monitor	Effect in ePO Reports	Effect in RSS feeds	Effect in Event Threat log
User can reveal sensitive data...	User is not authorized to view DLP events, but can decrypt confidential fields in the presence of a user who can view DLP events.	The McAfee DLP Monitor display is unavailable.	No DLP Reports are authorized.		DLP events are filtered out.
User can view DLP Monitor	User can view all DLP event data.	All the McAfee DLP Monitor display fields are available.	All DLP Reports are authorized.		Only general information about DLP events is available.

View redacted monitor fields

Data redaction is the encrypting of confidential information to prevent unauthorized viewing. It is required by law in some countries.

Before you begin

Create permission sets for viewing and auditing in ePolicy Orchestrator. See the *McAfee Data Loss Prevention Installation Guide* for information.

Task

- 1 Select the events to be viewed.



You can select up to 10 events at one time.

- 2 Right-click, and select **Decrypt Data of Selected Events** from the context menu.

A credentials dialog box appears.

- 3 Enter a user name and password in the Release Redacted Information dialog box and click **OK**.



The permission set in ePolicy Orchestrator for releasing information is different than the permission set for viewing information. An administrator account for viewing the McAfee DLP Monitor (and selecting the events) cannot release the encrypted information. A global administrator account, or one with permission to reveal sensitive data, is required.

The confidential information is revealed.

Monitor system events and alerts


The McAfee DLP Monitor software provides the necessary feedback for designing an effective data loss prevention system.

Task

- 1 In ePolicy Orchestrator, go to **Menu | DLP Monitor**.
- 2 In the **All Events** pane, sort the list by clicking any column. Sort by severity, time of day, user, and so forth.

- 3 Select a single event from the list to display its full details. The event information appears in the **Details** pane.



Click the Hide/Display icon  to hide/display the **Details** pane. To enlarge either of the panes grab the bar between the **All Events** and **Details** panes and drag it.

- 4 If any **Evidence** is available, double-click the attached file to view its content.



When the monitor window is minimized to the taskbar, new event notifications are displayed via the popup tray.

- 5 To view encrypted sensitive text, select the data to view, right-click, and select **Decrypt Data of Selected Events**. 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.



Two administrators are required: one with permission to view the McAfee DLP Monitor display (except sensitive text), the other with permission to view sensitive text. These are separate roles and require separate permission sets. See the *McAfee Data Loss Prevention 9.2 Installation Guide* for information on setting up the permission sets.

Filter event information

When viewing events, 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.

Some typical filters are:

- Critical events.
- Violations of a new rule.
- Events associated with a particular user or computer.



Two standard filters are **Computer Name** and **User Name**. If you are using the redaction feature, these fields are predefined as confidential and are encrypted for users with partial view permission.

Tasks



- [Define filters on page 117](#)
When viewing events in the McAfee DLP Monitor software, 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.
- [Define date filters on page 118](#)
When viewing events in the McAfee DLP Monitor, 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.
- [Add predefined filters on page 118](#)
When viewing events in the McAfee DLP Monitor, 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.
- [Filter the events monitor list on page 118](#)
When viewing events in the McAfee DLP Monitor, 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.

Define filters

When viewing events in the McAfee DLP Monitor software, 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.

For option definitions, press the **F1** key.

Task

- 1 On the McAfee DLP Monitor toolbar, click the Show Filters icon  to display the available filter list.
- 2 Click the Add Filter icon  to add a new filter.
- 3 Type a name for your filter in the **Filter Name** text box.
- 4 Select the filter conditions and properties.

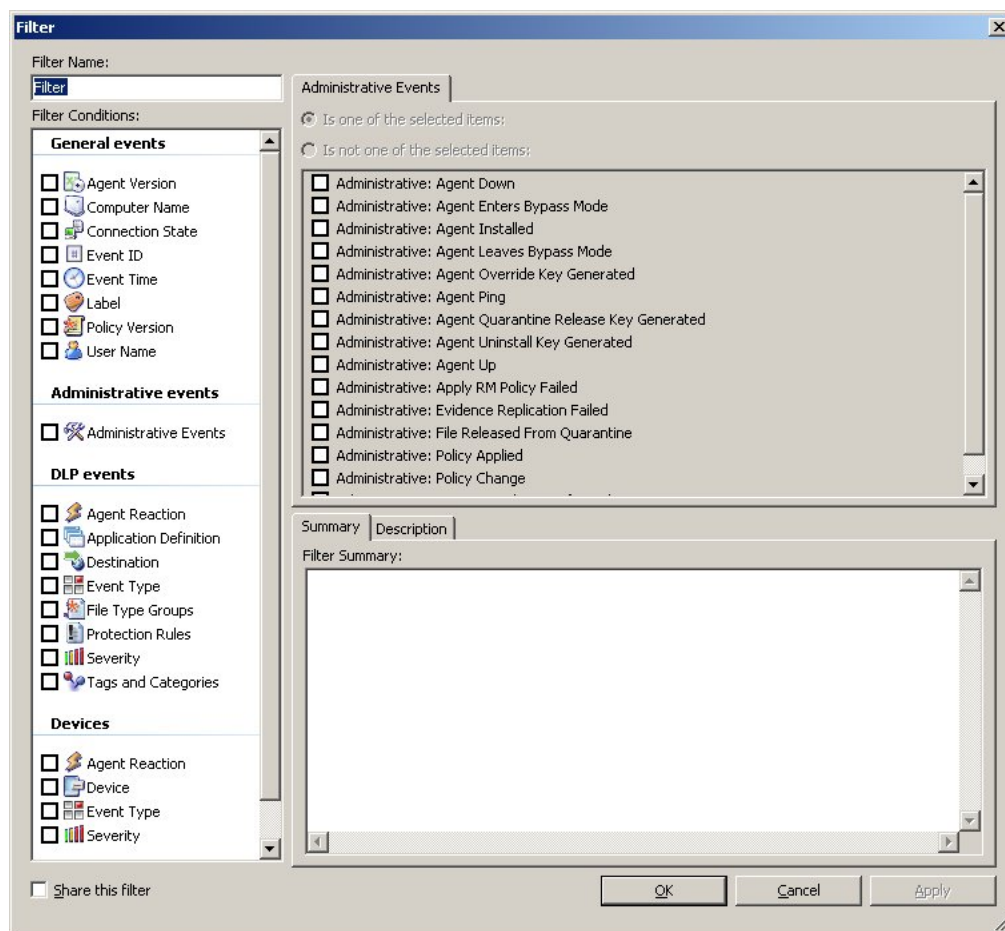


Figure 11-1 McAfee DLP Monitor Filter dialog box

- 5 Click **OK**.

You are prompted to save the filter.



The filter is applied to the events displayed in the events pane even if you click **No** at the prompt. However, you can't use the filter in future monitor sessions if you do not save it.



- 6 In the **Filters** pane, click the Edit button  to modify the filter.

Define date filters

When viewing events in the McAfee DLP Monitor, 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.

For option definitions, press the **F1** key.

Task

- 1 On the McAfee DLP Monitor toolbar, click the Show Filters icon  to display the available filter list.
- 2 Click the Add Filter icon  to add a new filter.
- 3 Type a name for your filter in the **Filter Name** text box.
- 4 Under **Filter Conditions**, select **Event Time**.
 - To set a date range, use the **Date** pull-down list and related calendars.
 - To select a day of the week, select **In** from the **Days** pull-down list, then select the days of the week.
 - To select an hour range, use the **Hours** pull-down menu and related hour lists.
 - To display a relative range, select **Display recent events** in the **Relative** section, select a number in the dial window, and a unit (**Hours**, **Days**, **Months**) in the units window.
- 5 Click **OK**.



You can combine selections from any of the sections to define your date filter. However, you should take care that the definitions are compatible with each other. For example, do not select a relative range with a date that is outside of that range.

Add predefined filters


When viewing events in the McAfee DLP Monitor, 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.

McAfee DLP Endpoint software contains a number of predefined filters that can save you the trouble of creating commonly used filters.

Task

- 1 From the McAfee DLP Monitor **File** menu, select **Load filters from file**. Select the file DefaultFilters.xml and open it.
- 2 Select the filters you want to use and click **OK**.



By default, the Filters pane is hidden. Click the Show Filter icon  on the toolbar to display the selected filters.


The filters appear in the **Filters** window.

Filter the events monitor list


When viewing events in the McAfee DLP Monitor, 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.

For option definitions, press the **F1** key.

Task

- 1 On the McAfee DLP Monitor toolbar, click the Show Filter icon  to display the available filter list.
- 2 In the **Filters** section, select a predefined filter or create a new one.
The title of the event list becomes the name of the filter, and the list displays according to the filter definition.
- 3 Select more filters (optional).
All selected filters display simultaneously.



By default, all administrative events such as agent state (up or down), policy changed, and so forth, are displayed in the event list with all other system events. To exclude administrative events from the list, click the **Hide administrative events** icon  on the toolbar.

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 the McAfee DLP Monitor display, select an event, several events, or a range of events.
- 2 On the McAfee DLP Monitor toolbar, click **Labels | Set Labels**.
- 3 In the **Label Editor**, select a label from the list or create a new label by typing in a name for the label and clicking **New Label**.
- 4 Click **OK** to add the label to the event(s).
The selected label(s) are both applied and saved.
- 5 To remove labels, select the events and click **Labels | Remove Labels**.



You can also use **Set Labels** to remove labels, or to change them. **Set Labels** changes the state of the label according to what is selected. **Add Labels** adds, but doesn't remove or change, a label. **Remove Labels** only removes the selected label(s).

Search monitor events by event ID

The McAfee DLP Monitor software has a search function to help find specific events.

Task

- 1 On the McAfee DLP Monitor toolbar, click the Search icon  to start the search.

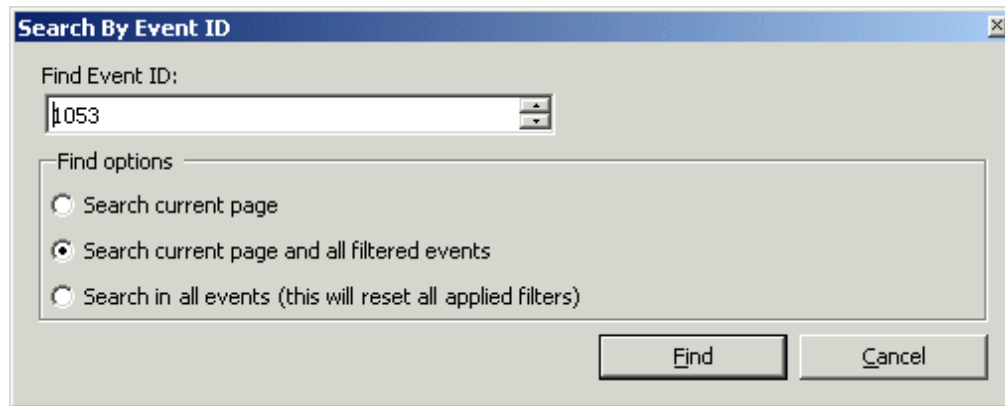


Figure 11-2 McAfee DLP Monitor search dialog box

- 2 Type the event ID and select one of the find options.
- 3 Click Find.

Export monitor events

The McAfee DLP Monitor export feature produces an Excel file that you can use for further analysis or auditing, or as part of an external report.

Task

- 1 From the McAfee DLP Monitor **File** menu, select **Export**.
- 2 Select **Export Events to Excel** to export the complete event list, or **Export Selected Event to Excel** to export a specific event from the list.
- 3 Type a file name and click **Save**.

Print monitor events

Events in the McAfee DLP Monitor can be printed for record keeping or review offline.

Task

- 1 In the McAfee DLP Monitor display, select the event or events you want to print.
- 2 From the **File** menu, select one of the following:
 - To print just the events, select **Print | Selected Events**.
 - To print event details, select **Print | Details**.
 - To print the complete list, select **Print | Event Table**.

Send monitor events by email

Events in the McAfee DLP Monitor can be sent to users or administrators.

Task

- 1 In the McAfee DLP Monitor display, select specific events.
- 2 Right-click and select **Send email report** or **Send email report (Without evidence)**.

An email message with the selected event details appears.

- 3 Add a recipient and click **Send**.

12 Creating reports

McAfee DLP Endpoint software has built-in features for database management and reporting. The database features allow you to remove data that is no longer needed, and to view database statistics.

Reporting

McAfee DLP Endpoint software uses ePolicy Orchestrator reporting features. 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

Nine DLP properties reports are displayed in the **DLP: Status Summary** dashboards. Twelve predefined events queries are provided. All twenty-one 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.

Contents

- [Report options](#)
- [Set up RSS feeds](#)
- [Set up Data Loss Prevention rolled up reports](#)
- [Administer the database](#)
- [View database statistics](#)

Report options

McAfee DLP Endpoint software offers two reporting options to review events: ePolicy Orchestrator Reports and RSS feeds. 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 ePO databases, are supported.

ePolicy Orchestrator Notifications are supported. See the *Sending Notifications* topic in the *McAfee ePolicy Orchestrator Product Guide* for details.

RSS feeds

You can monitor McAfee DLP Endpoint events without being logged on to ePolicy Orchestrator. You can set up any RSS reader that supports authentication to get feeds from the McAfee DLP Monitor. You can use monitor filters to filter results.

ePO Dashboard/ePO Reports

You can view information on DLP product properties on the ePolicy Orchestrator Dashboard. Nine predefined monitors are displayed on the **Dashboards** drop-down list item of the ePolicy Orchestrator Dashboards console. Monitors can be edited and customized, and new monitors can be created. See the McAfee ePolicy Orchestrator documentation for instructions.

DLP Dashboards are created by selecting **Queries** in the Monitor Gallery View drop-down list. Select one of the **Shared Groups - Data Loss Prevention** options from the Monitor Content drop-down list.

The nine dashboard reports and twelve other predefined reports are available by selecting **Menu | Reporting | Queries & Reports**. They are listed under **Shared Groups | Data Loss Prevention**. The six standard reports that are also available as rolled up reports are indicated in the tables.

Predefined dashboards and event reports

The following table describes the predefined McAfee DLP Endpoint dashboards.

Table 12-1 Predefined DLP dashboards (Public Queries)

Name	Description
Agent status	Displays all agents and their status.
Agent to ePO communications distribution	Displays endpoints according to the date of their last communication with ePolicy Orchestrator.
Agent version	Displays the distribution of endpoints in the enterprise. Used to monitor agent deployment progress.
Bypassed agents	Displays how many DLP nodes are in policy bypass mode. This is a real-time view that refreshes when a bypass begins or expires.
Enforced device control rules	Displays the number of computers enforcing each device control rule. Drill down to view which rules are being enforced on which users.
Enforced protection rules	Displays the number of computers enforcing each protection rule.
Evidence path distribution	Displays the different evidence shares used by the agents. Useful when there are several different agent configurations.
Policy distribution	Displays the DLP policy distribution throughout the enterprise. Used to monitor progress when deploying a new policy.
Privileged permissions	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.

The following table describes the predefined McAfee DLP Endpoint event reports.

Table 12-2 Predefined DLP event reports (My Queries)

Name	Description
Agent status (also rolled up report)	Displays all agents and their status.
Agent to ePO communications distribution (also rolled up report)	Displays endpoints according to the date of their last communication with ePolicy Orchestrator.

Table 12-2 Predefined DLP event reports (My Queries) *(continued)*

Name	Description
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 device control rules	Displays the number of computers enforcing each device control rule. Drill down to view which rules are being enforced on which users.
Enforced discovery rules	Displays the number of computers enforcing each discovery rule.
Enforced protection rules	Displays the number of computers enforcing each protection rule.
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.
Evidence path distribution	Displays the different evidence shares used by the agents. Useful when there are several different agent configurations.
Policy distribution (also rolled up report)	Displays the DLP policy distribution throughout the enterprise. Used to monitor progress when deploying a new policy.
Privileged permissions	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.
Undefined device classes	Lists and shows a bar graph of the devices whose device class cannot be determined.
Unmanaged printers	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.
Unsupported printers	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.

Set up RSS feeds

McAfee DLP Endpoint events can be viewed in any RSS reader (feed reader) that supports authentication.

Task

- 1 Open the reader and select the **Add feed** option.
- 2 Specify the DLP RSS URL: `http://<servername>:8731/DLPWCF/DLPRSSFeeder/GetRSS`. The McAfee DLP Monitor software provides a feed of the latest 50 events.



Replace `<servername>` with the name of the ePolicy Orchestrator Event Parser server. For a standard installation, use `localhost`. You might also need to change the port designation, depending on your installation.

- To change the default number of events, change the URL to `.../GetRSSCounted?itemCount=X`.
- To filter the results with an existing McAfee DLP Monitor filter, use `.../GetRSSFiltered?filterName=X`.
- To specify both an event count and a filter, use `.../GetRSSFilteredCounted?filterName=X&itemCount=Y`.

Set up Data Loss Prevention rolled up reports

Roll 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**.
- 3 Type a name for the task, and (optional) notes, then click **Next**.
- 4 In the **Actions** drop-down list, select **Roll Up Data**. In the **Data Type** drop-down list, select one of the McAfee DLP Endpoint report types: **DLP MA Properties** or **DLP Events**.
- 5 Continue with the configuration as required. Click **Next**.
- 6 Set the schedule type, date and time. Click **Next**.
- 7 Review the set-up information, then click **Save**.

Administer the database

Removing unwanted events 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

How to view the database statistics.

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.

13 Configuring system components

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

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

- **Agent configuration** — Sends the agents all relevant information about event storage locations, customized user notifications, whitelisted content limitations and locations, file tracing parameters, Outlook logon settings, and agent module selections
- **System options** — Allows you to set the DLPWCF service path, policy analyzer settings, system logging options, and system report printing options

Contents

- [Agent configuration](#)
- [Configure Safe Mode operation](#)
- [System tools](#)
- [View the system log](#)

Agent configuration

The McAfee DLP Endpoint plug-in 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, use the **Agent Configuration** menu in the McAfee DLP Endpoint policy console. 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.

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.

Managing Agent configuration

After setting the options in the Agent Configuration window, you can use the configuration menu to restore default settings and to save the settings to a file, which can be used as a configuration backup or to load the same agent configuration on other systems.

Use these tasks to work with the global agent configuration policy.

Apply the global agent configuration

The global agent configuration must be applied to ePolicy Orchestrator each time it is modified. The modifications are then scheduled for deployment to the endpoint computers.

- From the McAfee DLP Endpoint policy console **Agent Configuration** menu, select **Apply Global Agent Configuration**. The Agent Configuration progress bar window appears as the configuration is applied to ePolicy Orchestrator.

Import the global agent configuration

Agent configuration is stored in ePolicy Orchestrator. You can recover the old configuration by using the import feature.

Task

- 1 From the McAfee DLP Endpoint policy console **Agent Configuration** menu, select **Import Global Agent Configuration from ePO**.
- 2 Click **Yes** to confirm.

Reset the Agent Configuration values

Agent configuration default values are saved by the system. You can restore them from the **Agent Configuration** menu.

Task

- 1 From the McAfee DLP Endpoint policy console **Agent Configuration** menu, select **Reset Agent Configuration values**.
- 2 Click **Yes** to restore default settings.

Configure Safe Mode operation

Agent protection (WatchDog) can be activated in Safe Mode.

For option definitions, press the **F1** key.

Task

- 1 From the McAfee DLP Endpoint policy console **Agent Configuration** menu, select **Edit Global Agent Configuration**.
- 2 Click the **Advanced Configuration** tab.
- 3 Select **Activate agent self protection in safe mode** and change the setting to **Enabled**.



Due to the risk of permanently locking the computer if the agent fails in Safe Mode, only agent protection now operates when you boot into Safe Mode. The McAfee DLP Endpoint software itself does not run in Safe Mode.

A warning message appears concerning possible system inaccessibility with this option.

- 4 Click **OK**.

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 accessed from the **Tools** menu. Tools are included for:

- Generating an agent bypass key
- Generating an uninstall key
- Generating a quarantine release key
- Analyzing the policy
- Viewing the system log
- Rerunning the initialization wizard
- Setting the tool options

View 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.

- From the McAfee DLP Endpoint policy console **Tools** menu, select **View Log** (or press **F7**). The bottom of the window displays the system log entries.

Index

A

- about this guide [7](#)
- actions/rules matrix (graph) [87](#)
- Adobe LiveCycle Rights Management, See rights management
- agent bypass [107](#), [112](#)
- agent configuration
 - assigning with ePolicy Orchestrator [104](#)
 - global [130](#)
 - resetting [130](#)
- aggregated event behavior [66](#)
- application definitions
 - templates [101](#)
 - about [68](#)
 - creating [69](#)
 - creating from the Enterprise Applications List [70](#)
 - removing [101](#)
 - strategy [14](#)
 - web applications [70](#)
- application definitions, Data Loss Prevention
 - strategy [14](#)
- application strategy [66](#)
- applications, in rules [66](#)
- archiver, application strategy [66](#)
- assignment groups
 - computer [85](#)
 - creating [83](#)
 - definition [10](#)
 - privileged users [85](#)
 - users, including and excluding [83](#)

B

- backward compatibility, errors with [104](#)
- business justification [93](#), [100](#), [106](#)

C

- category catalog [45](#)
- challenge-response [60](#), [65](#), [106](#), [109](#)
- classification rules [10](#), [48](#)
- clipboard protection
 - rules, creating [92](#)
- components, described [13](#)
- computer assignment groups [85](#)
- content categories [43](#), [44](#), [48](#)

- conventions and icons used in this guide [7](#)

D

- dashboard, Data Loss Prevention, report options [123](#)
- dashboards, report options [123](#)
- data
 - classifying [31](#)
 - data-at-rest [60](#)
 - data-in-motion [75](#), [80](#)
 - data-in-use [71](#)
- Data Loss Prevention software, description [9](#)
- database
 - administration [123](#)
 - removing events [126](#)
 - statistics, viewing [127](#)
- date filters, See filters
- definitions
 - device, See device definitions
 - dictionaries [31](#)
 - document properties [32](#), [33](#)
 - email destination [75](#)
 - file extension [32](#), [33](#), [71](#)
 - file server list [72](#)
 - network [73](#)
 - printer [77](#)
 - registered document repository [33](#)
 - registered documents [35](#)
 - removing [101](#)
 - table of [90](#)
 - tags [43](#)
 - text pattern [36](#)
 - web destination [80](#)
 - whitelist [40](#)
- device class
 - creating new [18](#)
 - removing [101](#)
 - status, changing [18](#)
 - types of [17](#)
- device definitions
 - groups [23](#)
 - importing [22](#)
 - importing to existing [22](#)
 - parameter management [19](#)
 - Plug and Play [20](#)

- device definitions (*continued*)
 - removable storage [21](#)
 - device rules
 - about [25](#)
 - definition [10](#)
 - Plug and Play [25](#)
 - removable storage [26](#)
 - devices
 - lists, adding Plug and Play definitions [21](#)
 - management [17](#)
 - parameters, list of [23](#), [28](#)
 - Plug and Play [19](#)
 - removable storage [19](#)
 - whitelisted [19](#)
 - dictionaries
 - about [31](#)
 - creating [32](#)
 - importing entries [32](#)
 - discovery
 - about [60](#)
 - creating a file system discovery rule [61](#)
 - creating an email storage discovery rule [62](#)
 - scheduling [64](#)
 - setup [63](#)
 - DLP Agent, See DLP Endpoint
 - DLP Agent service watch dog [129](#)
 - DLP data, classifying [36](#)
 - DLP Discover [60](#)
 - DLP Endpoint
 - bypass [106](#)
 - defined [13](#)
 - override key, creating [109](#)
 - uninstall [106](#)
 - wake-up call [105](#)
 - DLP Monitor
 - defined [13](#)
 - defining event filters [117](#)
 - responding to events [111](#)
 - system events and alerts [115](#)
 - viewing database statistics [127](#)
 - viewing redacted content [115](#)
 - DLP Policy
 - See also DLP Policy
 - console, illustrated [10](#), [15](#)
 - defined [13](#)
 - DLP repositories, registered document [33](#)
 - DLP rules
 - classification [10](#)
 - device [10](#), [25](#), [26](#)
 - protection [10](#)
 - removable storage file access [27](#)
 - tagging [10](#)
 - DLP system
 - configuring [129](#)
 - document groups
 - registered, creating [35](#)
 - document properties definitions [32](#)
 - documentation
 - audience for this guide [7](#)
 - product-specific, finding [8](#)
 - typographical conventions and icons [7](#)
- ## E
- editor, application strategy [66](#)
 - email
 - protection rules [93](#)
 - sending DLP events by [121](#)
 - email bypass [93](#)
 - email destinations
 - about [75](#)
 - creating [75](#)
 - definitions (table) [90](#)
 - groups [76](#)
 - removing [101](#)
 - encryption [14](#)
 - endpoint configuration
 - about [129](#)
 - Safe Mode [130](#)
 - enterprise applications list
 - about [66](#)
 - importing by scanning [67](#)
 - importing to [67](#)
 - removing applications [68](#)
 - ePO Event Parser [13](#)
 - ePO notifications [123](#)
 - ePO reports [123](#)
 - ePolicy Orchestrator
 - computer assignment groups [85](#)
 - policy template synchronization wizard [103](#)
 - system policy, assigning [104](#)
 - events
 - defining new [117](#)
 - exporting [120](#)
 - monitor list, filtering [118](#)
 - monitoring [111](#)
 - printing [120](#)
 - removing [126](#)
 - RSS feeds for viewing [126](#)
 - search by ID [120](#)
 - sending by email [121](#)
 - viewing [115](#)
 - evidence
 - DLP Monitor [115](#)
 - endpoint events [111](#)
 - storage for encrypted content [112](#)
 - Excel, exporting to [120](#)
 - explorer, application strategy [66](#)

F

- features, described [13](#)
- file access
 - rules, about [25](#)
 - rules, removable storage [27](#)
- file extensions
 - about [71](#)
 - creating [71](#)
 - creating groups [71](#)
 - definitions [32](#)
 - definitions (table) [90](#)
 - removing [101](#)
- file server list
 - about [72](#)
 - adding a server [73](#)
 - creating [72](#)
 - definitions (table) [90](#)
- file system protection rule [94](#)
- filters
 - date, defining [118](#)
 - defining new [117](#)
 - event information, viewing [116](#)
 - events monitor list [118](#)
 - network definitions [73](#)
 - predefined [118](#)

G

- global agent configuration [130](#)
- groups
 - device definitions [23](#)
 - email [76](#)
 - network address range [74](#)
 - text patterns [37, 40](#)

H

- hit count [113](#)
- hit highlighting, events [112](#)

I

- Image Writer, in printing protection rules [97](#)

J

- justification, See business justification

K

- key generator [106, 112](#)

L

- local users [83](#)
- Lotus Notes, email protection rule [93](#)

M

- manual tags [50](#)
- master release key [106](#)
- McAfee Endpoint Encryption for Files and Folders [19](#)
- McAfee Endpoint Encryption for Removable Media [19](#)
- McAfee ServicePortal, accessing [8](#)

N

- network definitions
 - (table) [90](#)
 - about [73](#)
 - address range [73](#)
 - address range group [74](#)
 - port range [74](#)
 - protection rule [95](#)
 - removing [101](#)
- notifications, ePolicy Orchestrator [123](#)

O

- OpenLDAP [83](#)
- override
 - key, generating [109](#)
 - key, requesting [107](#)
 - mode for the DLP Endpoint plug-in [112](#)

P

- parameters, device [23, 28](#)
- PDF writer, in printing protection rules [96](#)
- Plug and Play devices
 - device definitions [20](#)
 - whitelisted [19](#)
 - whitelisted definition, creating [21](#)
- policies
 - applying to [104](#)
 - assigning with [104](#)
 - assignment with [103](#)
 - definition [10](#)
 - editing a description [106](#)
 - refreshing [105](#)
 - user assignment [83](#)
- Policy console
 - console, illustrated [10](#)
- printer list
 - adding printers [78](#)
 - creating [77](#)
 - definitions (table) [90](#)
- printer protection rule [97](#)
- printers
 - about [77](#)
 - unmanaged [77, 78](#)
 - unsupported [77](#)
 - whitelisted [77–79](#)
- privileged users assignment group [85](#)

protection rules

- application file access [91](#)
- clipboard [92](#)
- definition [10](#)
- email [93](#)
- file system [94](#)
- how they work [87](#), [90](#)
- network communication [95](#)
- printer [97](#)
- removable storage [98](#)
- screen capture [99](#)
- web post [100](#)

protection rules, Data Loss Prevention

- how they work [87](#)

Q

quarantine

- release key, generating [109](#)
- removing files [106](#)
- restoring files or email items from [65](#)

R

redaction

- about [113](#)
- viewing content [115](#)
- viewing redacted text [115](#)

registered document repositories [33–35](#)

registered document repositories, using [34](#)

registered documents [33](#)

removable storage

- protection rules [98](#)

reporting [123](#)

repositories, registered document [34](#)

rights management

- setting up the server [56](#), [57](#)
- synchronizing policies [56](#)
- synchronizing templates [57](#)
- users [54](#)
- working with Data Loss Prevention [54](#)

rolled up reports [123](#)

rollup queries [123](#)

RSS feeds

- monitoring events [123](#)
- setting up [126](#)

rules

- classification [48](#)
- removing [101](#)
- tagging [10](#), [46](#)

S

Safe Mode [130](#)

screen capture protection rules [99](#)

ServicePortal, finding product documentation [8](#)

storage devices, removable [19](#)

strategy, See application definitions

strategy, for applications [66](#)

system log, viewing [131](#)

system tools [131](#)

T

tagging rules

- application-based [47](#)
- content-based [49](#)
- creating [46](#)
- definition [10](#)
- dictionary [49](#)
- links to content [46](#)
- location-based [47](#)

tags

- about [43](#)
- content, See content categories
- creating [44](#)
- definitions (table) [90](#)
- linking tags to content [46](#)
- manual [50](#)
- removing [101](#)
- tag groups [45](#)

Technical Support, finding product information [8](#)

templates [101](#), [102](#)

templates, Data Loss Prevention [102](#)

text patterns

- about [36](#)
- creating [37](#)
- definitions (table) [90](#)
- groups [40](#)
- removing [101](#)
- testing [39](#)

trusted, application strategy [66](#)

U

unmanaged printers, See printers, whitelisted

user assignment groups

- creating [83](#)

users

- assignment groups [83](#)
- excluding from a user assignment group [83](#)
- local [83](#)

V

validators [36](#), [39](#)

W

wake-up call [105](#)

WatchDog

- protective service, about [129](#)

WCF service [111](#)

- web destinations
 - about [80](#)
 - creating [80](#)
 - definitions (table) [90](#)
 - groups [80](#)
 - removing [101](#)
- web post protection rules [100](#)
- whitelist
 - adding content [40](#)
 - definition (table) [90](#)
 - deleting content [41](#)
 - printer [77](#)
- whitelisted Plug and Play devices [19](#)
- whitelists
 - about [40](#)
- whitelists (*continued*)
 - application definitions [27](#)
 - Plug and Play definitions, creating [21](#)
 - printers [79](#)
 - unmanaged printers [78](#)
- window titles, in screen capture protection rules [99](#)
- wizards
 - Client Task Builder [35](#)
 - Template Synchronization [102](#)
- wizards, Data Loss Prevention
 - Template Synchronization [102](#)

