Product Guide
Revision A

McAfee Data Loss Prevention Discover
10.0.0

For use with McAfee ePolicy Orchestrator
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 .......................................................................................................................... 5
About this guide ................................................................. 5
Audience ........................................................................... 5
Conventions ................................................................. 5
Find product documentation .............................................. 6

1 Introduction ..................................................................................................... 7
How the software works ................................................................. 8
Types of scans .......................................................................... 9

2 McAfee DLP Discover installation ....................................................... 11
McAfee DLP Discover installation options and considerations ................. 11
System requirements ................................................................ 11
Default ports used by McAfee DLP Discover .............................. 12
Considerations for upgrading McAfee DLP Discover ......................... 13
Install McAfee DLP Discover ....................................................... 13
Install and license the McAfee DLP extension .............................. 14
Install or upgrade the server package using McAfee ePO ................... 14
Install or upgrade the server package manually ............................ 15
Perform post-installation tasks .................................................. 16
Verify the installation ................................................................ 16
Define a rights management server ............................................ 17
Creating evidence folders ......................................................... 17
Configure server settings ......................................................... 17

3 Scan and policy configuration ................................................................. 19
Choosing the scan type ................................................................ 19
How inventory scans work ......................................................... 20
How classification scans work ................................................... 20
How remediation scans work ..................................................... 21
Scan considerations and limitations ............................................. 22
Using definitions and classifications with scans .............................. 23
Using classifications ................................................................... 24
Advanced pattern definitions ................................................. 25
Dictionary definitions .............................................................. 25
Using rules with scans ............................................................... 26
Configure policy for scans .......................................................... 27
Create definitions for scans ...................................................... 27
Create definitions for classifications .......................................... 32
Create classifications ............................................................... 34
Create rules for remediation scans .............................................. 34
Configure a scan ........................................................................... 35
Configure an inventory scan ...................................................... 35
Configure a classification scan .................................................. 36
Configure a remediation scan .................................................... 37
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perform scan operations</td>
<td>38</td>
</tr>
<tr>
<td>Scan behavior</td>
<td>39</td>
</tr>
<tr>
<td>Assigning McAfee DLP permission sets</td>
<td>39</td>
</tr>
<tr>
<td>Create a McAfee DLP permission set</td>
<td>40</td>
</tr>
<tr>
<td>Protecting confidentiality with redaction</td>
<td>41</td>
</tr>
<tr>
<td><strong>4 Analyzing scanned data</strong></td>
<td></td>
</tr>
<tr>
<td>How McAfee DLP Discover uses OLAP</td>
<td>43</td>
</tr>
<tr>
<td>Viewing scan results</td>
<td>43</td>
</tr>
<tr>
<td>Analyze scan results</td>
<td>45</td>
</tr>
<tr>
<td>View inventory results</td>
<td>45</td>
</tr>
<tr>
<td><strong>5 Incidents and operational events</strong></td>
<td></td>
</tr>
<tr>
<td>Monitoring and reporting events</td>
<td>47</td>
</tr>
<tr>
<td>DLP Incident Manager</td>
<td>48</td>
</tr>
<tr>
<td>How the Incident Manager works</td>
<td>48</td>
</tr>
<tr>
<td>Create a Set Reviewer task</td>
<td>50</td>
</tr>
<tr>
<td>Create an Automatic mail Notification task</td>
<td>50</td>
</tr>
<tr>
<td>Create a Purge events task</td>
<td>51</td>
</tr>
<tr>
<td>Edit server tasks</td>
<td>52</td>
</tr>
<tr>
<td>Monitor task results</td>
<td>52</td>
</tr>
<tr>
<td>Working with incidents</td>
<td>52</td>
</tr>
<tr>
<td>View incidents</td>
<td>53</td>
</tr>
<tr>
<td>Sort and filter incidents</td>
<td>53</td>
</tr>
<tr>
<td>Configure column views</td>
<td>53</td>
</tr>
<tr>
<td>Configure incident filters</td>
<td>54</td>
</tr>
<tr>
<td>View incident details</td>
<td>55</td>
</tr>
<tr>
<td>Manage incidents</td>
<td>56</td>
</tr>
<tr>
<td>Update a single incident</td>
<td>56</td>
</tr>
<tr>
<td>Update multiple incidents</td>
<td>57</td>
</tr>
<tr>
<td>Manage labels</td>
<td>57</td>
</tr>
<tr>
<td>Working with cases</td>
<td>58</td>
</tr>
<tr>
<td>Manage cases</td>
<td>59</td>
</tr>
<tr>
<td>Create cases</td>
<td>59</td>
</tr>
<tr>
<td>View case information</td>
<td>59</td>
</tr>
<tr>
<td>Assign incidents to a case</td>
<td>60</td>
</tr>
<tr>
<td>Move or remove incidents from a case</td>
<td>60</td>
</tr>
<tr>
<td>Update cases</td>
<td>61</td>
</tr>
<tr>
<td>Add or remove labels to a case</td>
<td>62</td>
</tr>
<tr>
<td>Delete cases</td>
<td>62</td>
</tr>
</tbody>
</table>

**Index**                                                                 | 63   |
Preface

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

Contents
- About this guide
- Find product documentation

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

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

- **Administrators** — People who implement and enforce the company’s security program.

Conventions
This guide uses these typographical conventions and icons.

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

**Bold**  
Text that is strongly emphasized.

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

*Interface text*  
Words from the product interface like options, menus, buttons, and dialog boxes.

*Hypertext blue*  
A link to a topic or to an external website.

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

**Tip:** Suggestions and recommendations.

**Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.

**Warning:** Critical advice to prevent bodily harm when using a hardware product.
Find product documentation

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

**Task**

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

McAfee® Data Loss Prevention Discover (McAfee DLP Discover) is a software-based network crawler that scans network file systems to identify and protect sensitive files and data.

McAfee DLP Discover runs on designated Microsoft Windows servers and integrates with McAfee® ePolicy Orchestrator® (McAfee ePO®) for configuration, policy management, and scan analysis.

Benefits

McAfee DLP Discover is a scalable, extensible software system that can meet the requirements of any size network. Deploy McAfee DLP Discover software to as many servers throughout the network as needed.

Use McAfee DLP Discover for:

- Detecting and classifying sensitive content
- Moving or copying sensitive content
- Integrating with Microsoft Rights Management Service to apply protection to files
- Automating IT tasks such as finding blank files, determining permissions, and listing files that changed within a specified time range

Supported repositories

McAfee DLP Discover supports these types of repositories:

- Box
- Common Internet File System (CIFS)
- SharePoint 2010 and 2013

SharePoint Enterprise Search Center (ESS) websites are not supported. An ESS website is a consolidation that does not contain files, but only links to the original files. For ESS websites, scan the actual site collections or the entire web application.

Contents

- How the software works
- Types of scans
**How the software works**

McAfee ePO uses McAfee® Agent to install and deploy the McAfee DLP Discover software to a Discover server — a designated Windows Server.

McAfee ePO applies the scan policy to Discover servers. At the scheduled time, the Discover server scans the repository. The data collected and the actions applied to files depend on the scan type and configuration.

Use McAfee ePO to perform configuration and analytics tasks such as:

- Displaying available Discover servers
- Configuring and scheduling scans
- Configuring policy items such as definitions, classifications, and rules
- Reviewing data analytics and inventory results
- Reviewing incidents generated from remediation scans

**Terminology**

These terms have specific definitions to McAfee DLP Discover.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Crawling</strong></td>
<td>Retrieving files or metadata from repositories.</td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>Used to identify and track sensitive content and files.</td>
</tr>
<tr>
<td></td>
<td>Classifications can match content such as text patterns, dictionaries, and</td>
</tr>
<tr>
<td></td>
<td>document properties.</td>
</tr>
<tr>
<td><strong>Definition</strong></td>
<td>A configuration component that makes up a McAfee DLP Discover scan policy.</td>
</tr>
<tr>
<td></td>
<td>Definitions specify items such as scheduled scan times, the repository to scan, and the file metadata to search for.</td>
</tr>
<tr>
<td><strong>Discover server</strong></td>
<td>The Windows Server where the McAfee DLP Discover software is installed.</td>
</tr>
<tr>
<td></td>
<td>You can install multiple Discover servers in your network.</td>
</tr>
<tr>
<td><strong>File information</strong></td>
<td>A definition that can include the file name, owner, size, extension, and date</td>
</tr>
<tr>
<td></td>
<td>created, changed, or accessed.</td>
</tr>
<tr>
<td></td>
<td>Use file information definitions in filters to include or exclude files to scan.</td>
</tr>
<tr>
<td><strong>Path</strong></td>
<td>A UNC name, IP address, or web address.</td>
</tr>
<tr>
<td><strong>Repository</strong></td>
<td>A Box, CIFS, or SharePoint server.</td>
</tr>
<tr>
<td></td>
<td>The repository definition includes the paths and credentials for scanning the server.</td>
</tr>
<tr>
<td><strong>Scheduler</strong></td>
<td>A definition that specifies scan details and the schedule type, such as daily,</td>
</tr>
<tr>
<td></td>
<td>weekly, monthly, once, or immediately.</td>
</tr>
</tbody>
</table>
Types of scans

McAfee DLP Discover supports three scan types — inventory, classification, and remediation.

**Inventory scans**

Inventory scans give you a high-level view of what types of files exist in the repository. This scan collects only metadata — the files are not fetched. McAfee DLP Discover sorts scanned metadata into different content types and analyzes attributes such as file size, location, and file extension. Use this scan to create an overview of your repository or for IT tasks such as locating infrequently used files.

**Classification scans**

Classification scans help you understand the data that exists in the targeted repository. By matching scanned content to classifications such as text patterns or dictionaries, you can analyze data patterns to create optimized remediation scans.

**Remediation scans**

Remediation scans find data that is in violation of a policy. You can monitor, apply a Rights Management policy, copy, or move files to an export location. All actions can produce incidents that are reported to the Incident Manager in McAfee ePO.
Introduction
Types of scans
McAfee DLP Discover installation

McAfee DLP Discover has two components — an extension that provides the user interface in McAfee ePO and a server package for installing the software on the Discover server.

Contents

- McAfee DLP Discover installation options and considerations
- System requirements
- Default ports used by McAfee DLP Discover
- Considerations for upgrading McAfee DLP Discover
- Install McAfee DLP Discover
- Perform post-installation tasks

McAfee DLP Discover installation options and considerations

McAfee DLP Discover can run on physical or virtual servers. You can install one or multiple Discover servers on your network.

Install McAfee DLP Discover on servers through McAfee ePO or manually.

McAfee recommends using McAfee ePO for installation.

Make sure any servers you intend to use for McAfee DLP Discover have McAfee Agent installed and running, are communicating with McAfee ePO, and are added to the McAfee ePO System Tree.

For information on installing and running McAfee Agent, see the McAfee Agent Product Guide.

System requirements

McAfee DLP Discover has different requirements for each of the components.

Table 2-1 McAfee DLP Discover requirements

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO</td>
<td>Version 5.1.3 or later</td>
</tr>
<tr>
<td></td>
<td>Version 5.3.1 or later</td>
</tr>
<tr>
<td>Discover server</td>
<td></td>
</tr>
<tr>
<td>requirements</td>
<td></td>
</tr>
<tr>
<td>Hardware</td>
<td>• CPU — Intel Core 2 64-bit, minimum 2 CPUs</td>
</tr>
<tr>
<td></td>
<td>• RAM — 4 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• Hard disk — 100 GB minimum</td>
</tr>
</tbody>
</table>
Table 2-1 McAfee DLP Discover requirements (continued)

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual servers</td>
<td>• vSphere ESXi 5.0 Update 2 or 6.0</td>
</tr>
<tr>
<td></td>
<td>• vCenter Server 5.0 Update 2 or 6.0</td>
</tr>
<tr>
<td>Operating systems</td>
<td>• Windows Server 2008 R2 Standard Service Pack 1 or later, 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 Standard, 64-bit</td>
</tr>
<tr>
<td></td>
<td>• Windows Server 2012 R2 Standard, 64-bit</td>
</tr>
<tr>
<td></td>
<td>The Discover server installation is not supported on domain controllers or</td>
</tr>
<tr>
<td></td>
<td>workstations.</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>Version 5.0.2 or later</td>
</tr>
</tbody>
</table>

Default ports used by McAfee DLP Discover

McAfee DLP Discover uses several ports for scan communications. Configure any intermediary firewalls or policy-enforcing devices to allow these ports where necessary.

All listed protocols use TCP only, unless noted otherwise.

Table 2-2 Default ports used in scan communications

<table>
<thead>
<tr>
<th>Port, protocol</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>137, 138, 139 — NetBIOS</td>
<td>CIFS scans</td>
</tr>
<tr>
<td>445 — SMB</td>
<td>CIFS scans</td>
</tr>
<tr>
<td>80 — HTTP</td>
<td>SharePoint scans</td>
</tr>
<tr>
<td>443 — SSL</td>
<td>SharePoint servers might be configured to use non-standard HTTP or SSL ports. If needed, configure firewalls to allow the non-standard ports.</td>
</tr>
<tr>
<td>53 — DNS (UDP)</td>
<td>DNS queries</td>
</tr>
<tr>
<td>1801 — TCP</td>
<td>Microsoft Message Queueing (MSMQ)</td>
</tr>
<tr>
<td>135, 2101*, 2103*, 2105 — RPC</td>
<td></td>
</tr>
<tr>
<td>1801, 3527 — UDP</td>
<td></td>
</tr>
</tbody>
</table>

* Indicates that the port numbers might be incremented by 11 depending on the available ports at initialization.

For more information, see Microsoft KB article https://support.microsoft.com/en-us/kb/178517#en-us/kb/178517.
Considerations for upgrading McAfee DLP Discover

The steps for upgrading McAfee DLP Discover are nearly identical to the steps for installing the extension and server package.

1. Upgrade the extension by installing over the existing version.
2. Upgrade the Discover server using one of these options.
   - Use McAfee ePO to deploy the server package.
   - Install the package manually on the server.
3. When upgrading from version 9.4.0, reapply policy due to policy configuration changes.
4. If you plan to use features new to version 10.x, such as Box scans, you must select the appropriate compatibility option.
   In McAfee ePO, select Menu | Data Protection | DLP Settings, then for Backwards Compatibility, select 10.0.0.0 and later.

You must upgrade the extension in McAfee ePO before you upgrade the Discover server. McAfee DLP Discover supports using a later version extension to manage an earlier version server. You can’t manage a later version server with an earlier version extension.

You do not need to relicense the software or re-enter the evidence server path. You might need to restart the Discover server if MSMQ is not enabled after the upgrade or if old data program folders or registry keys were not deleted.

If a restart is required, McAfee DLP Discover generates an operational event.
   - If you installed the server package manually, the server prompts you to restart.
   - If you used McAfee ePO, the prompt might be displayed depending on the McAfee Agent configuration settings.

   In some cases, MSMQ might not be enabled even after a restart and the Discover server sends an operational event. If this happens, you must manually enable MSMQ and start the Discover server service.

For information about the supported upgrade paths, see the McAfee Data Loss Prevention Discover Release Notes.

Do not install the software over an existing installation of the same version.

Install McAfee DLP Discover

Install the McAfee DLP extension and server package.
The server package is deployed to Discover servers and installs McAfee DLP Discover and necessary components such as .NET, postgresQL, AD RMS client 2.1, and C++ redistributables.

Tasks
- Install and license the McAfee DLP extension on page 14
  The extension provides the user interface for configuring McAfee DLP in McAfee ePO.
- Install or upgrade the server package using McAfee ePO on page 14
  McAfee recommends using McAfee ePO to install the server package.
- Install or upgrade the server package manually on page 15
  If you are unable to install the server package through McAfee ePO due to issues such as network connectivity, you can manually install McAfee DLP Discover on the Discover server.
Install and license the McAfee DLP extension
The extension provides the user interface for configuring McAfee DLP in McAfee ePO.

**Before you begin**
- Download the McAfee DLP extension from the McAfee download site.
  
  You can also navigate in McAfee ePO to Menu | Software | Software Manager to view, download, and install the software.

- Verify that the McAfee ePO server name is listed under Trusted Sites in the Internet Explorer security settings.

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

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

2. Browse to the extension .zip file and click OK.
   
   The installation dialog box displays the file parameters to verify that you are installing the correct extension.

3. Click OK. The extension is installed.

4. Install licenses and components to customize the installation.
   
   Installing the license activates the related McAfee ePO components and McAfee ePO Policy Catalog policies. License options are:
   - McAfee Device Control
   - McAfee DLP Endpoint (Includes Device Control)
   - McAfee DLP Discover
   - McAfee DLP network

   McAfee DLP Discover can be installed together with either Device Control or McAfee DLP Endpoint. McAfee DLP network can be installed together with any of the other options.

   a. Select Menu | Data Protection.
   b. Select either DLP Settings or McAfee DLP Discover and click Yes when prompted to enter the license.
   c. In the Key field, enter the license, then click Add.
   d. If needed, add another license.

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

6. Click Save.

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

**Install or upgrade the server package using McAfee ePO**
McAfee recommends using McAfee ePO to install the server package.


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

1. Check in the server package.
   a. In McAfee ePO, select Menu | Software | Master Repository.
   b. Click Check In Package.
   c. Browse to the server package .zip file and click Next.
   d. Click Save.

2. Create a client task.
   a. Select Menu | System Tree.
   b. Select the Discover server and select Actions | Agent | Modify Tasks on a Single System.
   c. Select Actions | New Client Task Assignment.

3. Configure the task assignment.
   a. In the Product area, select McAfee Agent.
   b. In the Task Type area, select Product Deployment.
   c. In the Task Name area, click Create New Task.

4. Configure the task.
   a. In the Target platforms area, select Windows.
   b. From the Product and components menu, select McAfee Discover Server.
   c. From the Action menu, select Install.
   d. Click Save.

5. Select the name of the new task, then click Next.

6. Configure when to run the task, then click Next.

7. Click Save.

**Install or upgrade the server package manually**
If you are unable to install the server package through McAfee ePO due to issues such as network connectivity, you can manually install McAfee DLP Discover on the Discover server.

**Task**
1. Download or transfer the DiscoverServerInstallx64.exe file to the Discover server.
2. Double-click the file and follow the on-screen instructions.
Perform post-installation tasks

Verify the installation

Make sure McAfee DLP Discover is successfully installed and communicating with McAfee ePO.

In the event of an installation failure, McAfee DLP Discover generates an operational event. To view events, select Menu | Data Protection | DLP Operations.

Task

1. If MSMQ is not enabled after the installation or if old data program folders or registry keys were not deleted, restart the Discover server.
   
   If you must restart the server, McAfee DLP Discover generates an operational event.
   
   • If you installed the server package manually, the server will prompt you to restart.
   
   • If you used McAfee ePO, the prompt might display depending on the McAfee Agent configuration settings.

   In some cases, MSMQ might not be enabled even after a restart and the Discover server sends an operational event. If this happens, you must manually enable MSMQ and start the Discover server service.

   For information on enabling MSMQ, see KB87274.

2. In the server operating system, validate that these McAfee DLP Discover services and processes are running:
   
   • McAfee Discover Service
   
   • McAfee Discover Server Postgres service

3. Wake up agents in McAfee ePO or collect and send properties from the Discover server.
   
   • In McAfee ePO, select Menu | System Tree, select the server, and click Wake Up Agents.
   
   • From the Discover server system tray, click the McAfee icon, select McAfee Agent Status Monitor, and click Collect and Send Props.
     
     The Status column displays Enforcing Policies for DISCOVERxxxx.

4. Make sure that the Discover server is detected.
   
   a. In McAfee ePO, select Menu | Data Protection | DLP Discover.

   b. Click the Discover Servers tab.

     A list of detected servers appear.

8. If the server is not listed, select Actions | Detect Servers. This task runs every 10 minutes by default.

5. Best practice: Change the McAfee Agent agent-to-server communication interval to ensure analytical data is up to date.

   a. Select Menu | Policy | Policy Catalog.

   b. From the Product drop-down list, select McAfee Agent.
In the **Category** column, locate the default policy listed as **General** and open it.

On the **General** tab, in the **Agent-to-server communication** area, change the interval to 5.

To uninstall the Discover server, use **Control Panel | Programs and Features** on the Windows server.

---

**Define a rights management server**

You can integrate Microsoft Windows Rights Management Services with McAfee DLP Discover to apply rights management (RM) policies to files.

**Before you begin**

Set up the RM servers and create users and policies. Obtain the policy template URL and password for all servers.

**Task**

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

1. In McAfee ePO, select **Menu | Registered Servers**.
2. Click **New Server**.
3. From the **Server type** drop-down list, select **Microsoft RMS Server**.
4. Type a name for the server configuration, then click **Next**.
5. Fill in the required details. When you have entered the required fields, click **Test Connectivity** to verify the data entered.
6. Click **Save**.

Configure server settings to set the RM service credentials.

**See also**

*Configure server settings on page 17*

**Creating evidence folders**

Evidence folders store evidence information when files match a rule in a remediation scan.

Depending on your McAfee DLP installation, certain folders and network shares must be created, and their properties and security settings must be configured appropriately.

You must configure write permission for the user account that writes to the evidence folder, such as the local system account on the Discover server. In order to view evidence from McAfee ePO, you must allow read access for the local system account of the McAfee ePO server.

**Configure server settings**

Configure McAfee DLP Discover settings such as which evidence share to use.

**Before you begin**

- If you are using a Rights Management server, obtain the domain name, user name, and password.
- If you plan to run remediation scans on SharePoint servers, determine if the SharePoint servers in your enterprise use the recycle bin. Mismatching this setting can lead to errors or unexpected behavior during the remediation scan.
For information about Rights Management or the text extractor, see the McAfee Data Loss Prevention Endpoint Product Guide.

**Task**

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

1. In McAfee ePO, select **Menu | Policy | Policy Catalog**.
2. From the **Product** drop-down list, select **Data Loss Prevention 9.4**.
3. (Optional) From the **Category** drop-down list, select **Server Configuration**.

   All server configurations for McAfee DLP Discover appear.

4. Do one of the following.
   - Select a server configuration to edit.
   - Click **Duplicate** for the **McAfee Default** configuration.

5. On the **Evidence Copy Service** page:
   - Select whether the service is enabled or disabled.
     The evidence copy service allows you to store evidence during remediation scans. If disabled, evidence is not collected and only incidents are generated.
   - Enter the evidence storage share UNC. If you don't want to use the local system account, enter a user name a password to store evidence.
   - **Optional:** Reset the default **Maximum evidence file size** and **Maximum evidence transmission bandwidth** filters.
   - Select whether storing the original file is enabled or disabled.
     Selecting **Disabled** overrides the **Store Original File** setting in individual rules.
   - Set the classification match to abbreviated results or all matches. You can also disable matching with this control.

6. **Optional:** On the **Logging** page, set the log output type and log level.

   **i** McAfee recommends using the default values.

7. On the **Rights Management** page, set the RM service credentials.

8. On the **SharePoint** page, select or deselect **Use Recycle bin when deleting a file**.

   **!** If you enable this setting and the SharePoint server does not use the recycle bin, any Move actions taken on files will fail and will default to Copy. The default setting in SharePoint is to enable the recycle bin.

9. **Optional:** On the **Text Extractor** page, configure the text extractor settings.

   **i** **Best practice:** Use the default values.
   - Set the ANSI fallback code page.
     The default uses the default language of the Discover server.
   - Set the input and output maximum file size, and the timeouts.
Scan and policy configuration

Configure McAfee DLP Discover scans and policy to detect and protect your files.

McAfee DLP Discover and McAfee DLP Endpoint share many configuration components. Depending on your McAfee DLP license, you might see components such as definitions and rules used by either product.

Contents

- Choosing the scan type
- Scan considerations and limitations
- Using definitions and classifications with scans
- Using classifications
- Using rules with scans
- Configure policy for scans
- Configure a scan
- Perform scan operations
- Scan behavior
- Assigning McAfee DLP permission sets

Choosing the scan type

The type of scan you configure determines the amount of information retrieved in a scan, the actions taken during the scan, and the configuration required for the scan.

- Inventory scans retrieve metadata only, providing a base for configuring classification and remediation scans.
- Classification scans retrieve metadata, analyze files, and match policy classifications that you define.
- Remediation scans include classification scan analysis and can take action on files that match configured rules.

The policy components you must configure depend on the scan type.

Table 3-1 Required policy components

<table>
<thead>
<tr>
<th>Scan type</th>
<th>Definitions</th>
<th>Classifications</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inventory</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Classification</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remediation</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Scan results are displayed on the Data Analytics tab. The Data Inventory tab displays the inventory of files from scans that have the File List option enabled.
How inventory scans work

Inventory scans are the fastest scans, retrieving only metadata. Because of this, an inventory scan is a good place to begin planning a data loss prevention strategy.

You can also use inventory scans to help automate IT tasks such as finding empty files or files that have not been modified for a long time.

An inventory scan performs the following:

- Collects metadata but does not download any files
- Returns Online Analytical Processing (OLAP) counters and data inventory (list of files scanned)
- Restores the last access time of files scanned

All scans collect metadata such as the file type, size, date created, and date modified. The type of available metadata depends on the repository type. For example, Box scans retrieve sharing, collaboration, and account name metadata.

The results of inventory scans are displayed on the Data Inventory and Data Analytics tabs.

See also
Configure an inventory scan on page 35

How classification scans work

Use the results of inventory scans to build classification scans.

A classification scan performs the following:

- Collects the same metadata as an inventory scan
- Analyzes the true file type based on the content of the file rather than the extension
- Collects data on files that match the configured classification
- Restores the last access time of files scanned

Classification scans are slower than inventory scans because the text extractor accesses, parses, and analyzes the files to match definitions in the classification specifications. Classifications consist of definitions that can include keywords, dictionaries, text patterns, and document properties. These definitions help identify sensitive content that might require additional protection. By using the OLAP tools to view multidimensional patterns of these parameters, you can create optimized remediation scans.

The results of classification scans are displayed on the Data Inventory and Data Analytics tabs.

Detecting encrypted files

Classification scans detect files with these encryption types:

- Microsoft Rights Management encryption
- Seclore Rights Management encryption
- Unsupported encryption types or password protection
- Not encrypted

Consider these points when scanning encrypted files:
• McAfee DLP Discover can extract and scan files encrypted with Microsoft RMS provided that McAfee DLP Discover has the credentials configured. Other encrypted files cannot be extracted, scanned, or matched to classifications.

• Files encrypted with Adobe Primetime digital rights management (DRM) and McAfee® File and Removable Media Protection (FRP) are detected as Not Encrypted.

• McAfee DLP Discover supports classification criteria options for Microsoft Rights Management Encryption and Not Encrypted.

See also
Create classifications on page 34
Configure a classification scan on page 36

How remediation scans work
Use the results of inventory and classification scans to build remediation scans. Remediation scans apply rules to protect sensitive content in the scanned repository. When a file matches the classification in a remediation scan, McAfee DLP Discover can perform the following:

• Generate an incident
• Store the original file in the evidence share
• Copy the file
• Move the file

Box and SharePoint scans support moving files only to CIFS shares.

• Apply RM policy to the file
• (Box scans only) Modify anonymous share to login required

McAfee DLP Discover cannot prevent Box users from reenabling external sharing on their files.

• Take no action

Moving files or applying RM policy to files is not supported for SharePoint lists. These actions are supported for files attached to SharePoint lists or stored in document libraries. Some file types used for building SharePoint pages, such as .aspx or .js cannot be moved or deleted.

A remediation scan also performs the same tasks as inventory and classification scans. Remediation scans require classifications and rules to determine the action to take on matched files.

The results of remediation scans are displayed on the Data Inventory and Data Analytics tabs. Remediation scans can also generate incidents displayed in the Incident Manager.

See also
Create classifications on page 34
Create rules for remediation scans on page 34
Configure a remediation scan on page 37
Scan considerations and limitations
When planning and configuring your scans, consider these items.

Directory exclusion
To avoid negative performance impacts, exclude McAfee DLP Discover directories and processes from these applications:

- Anti-virus software, including McAfee® VirusScan® Enterprise
- McAfee® Host Intrusion Prevention and other McAfee software
- Firewalls
- Access protection software
- On-access scanning

Table 3-2 McAfee DLP Discover items to exclude

<table>
<thead>
<tr>
<th>Type</th>
<th>Exclude</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processes</td>
<td>• dscrawler.exe&lt;br&gt;• dstex.exe&lt;br&gt;• dseng.exe&lt;br&gt;• dsmsvc.exe&lt;br&gt;• dssvc.exe&lt;br&gt;• dsrm.exe&lt;br&gt;• dsmbroker.exe</td>
</tr>
<tr>
<td>Directories</td>
<td>• c:\programdata\mcafee\discoverserver&lt;br&gt;• c:\program files\mcafee\discoverserver</td>
</tr>
<tr>
<td>Registry keys</td>
<td>• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\DiscoverServer&lt;br&gt;• HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\DiscoverServer&lt;br&gt;• HKEY_LOCAL_MACHINE\SOFTWARE\ODBC.INI\McAfeeDSPostgres</td>
</tr>
</tbody>
</table>

Repository definitions
Configuring repository locations in McAfee ePO has these limitations.

- IP address ranges are supported for Class C addresses only.
- IP address ranges cannot include addresses ending in 0 or 255.

You can define a single IP address ending in 0 or 255.

- IPv6 is not supported.

SharePoint scans
SharePoint scans do not crawl system catalogs, hidden lists, or lists flagged as NoCrawl. Because SharePoint lists are highly customizable, there might be other lists that are not scanned.

Most lists available out-of-the-box with SharePoint 2010 or 2013 can be crawled, such as:

- Announcements
- Contacts
- Discussion boards
- Issue trackers
- Links
- Meetings
• Events
• Tasks
• Generic list

Individual items in a list are combined and grouped together in an XML structure and are scanned as a single XML file. Files attached to list items are scanned as is.

**Box scans**

Configuring the same Box repository on multiple Discover servers is not supported.

Scan ability varies depending on the account used. In order to scan other accounts, contact Box support to enable the as-user functionality.

- The admin account can scan all accounts.
- A co-admin account can scan its own account and user accounts.
- A user account can scan only its own account.

**Setting bandwidth for a scan**

Large scans might take up noticeable bandwidth, especially on networks with low transmission capacities. By default, McAfee DLP Discover does not throttle bandwidth while scanning.

When bandwidth throttling is enabled, McAfee DLP Discover applies it to individual files being fetched rather than as an average across the entire scan. A scan might burst above or below the configured throttle limit. The average throughput measured across the entire scan, however, remains very close to the configured limit. When enabled, the default throttling value is 2000 Kbps.

**Using definitions and classifications with scans**

Use definitions and classifications to configure rules, classification criteria, and scans. All scan types require definitions.

There are two types of definitions used for McAfee DLP Discover.

- Definitions used in scans specify schedules, repositories, and credentials for repositories.
- Definitions used in classifications specify what to match when crawling files, such as the file properties or the data in a file.

<table>
<thead>
<tr>
<th>Definition</th>
<th>Used for</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Pattern*</td>
<td>Classifications</td>
</tr>
<tr>
<td>Dictionary*</td>
<td></td>
</tr>
<tr>
<td>Document Properties</td>
<td></td>
</tr>
<tr>
<td>True File Type*</td>
<td></td>
</tr>
<tr>
<td>File Extension*</td>
<td>Classifications and scans</td>
</tr>
<tr>
<td>File Information</td>
<td></td>
</tr>
<tr>
<td>Credentials</td>
<td>Scans</td>
</tr>
<tr>
<td>Scheduler</td>
<td></td>
</tr>
<tr>
<td>Box</td>
<td></td>
</tr>
</tbody>
</table>
Classification and remediation scans use classifications to identify sensitive files and data.

Classifications use one or more definitions to match file properties and content in a file. You can use classification scans to analyze data patterns in files. Use the results of the classification scans to fine-tune your classifications, which can then be used in remediation scans.

Registered documents and content fingerprinting criteria are not used in McAfee DLP Discover. Classification and remediation scans can detect manually classified files, but McAfee DLP Discover cannot apply manual classifications to files.

### Using classifications

Classification and remediation scans use classifications to identify sensitive files and data.

Classifications match file properties and content in a file using regular expressions and dictionaries. You can use classification scans to analyze data patterns in files. Use the results of the classification scans to fine-tune your classifications, which can then be used in remediation scans.

Classifications are made up of one or more definitions.

#### Table 3-4 Definitions for classifications

<table>
<thead>
<tr>
<th>Classification definition</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Advanced Pattern</strong></td>
<td>Regular expressions or phrases used to match data such as dates or credit card numbers.</td>
</tr>
<tr>
<td><strong>Dictionary</strong></td>
<td>Collections of related keywords and phrases such as profanity or medical terminology.</td>
</tr>
<tr>
<td><strong>Document Properties</strong></td>
<td>Contains these options:</td>
</tr>
<tr>
<td></td>
<td>• Any property</td>
</tr>
<tr>
<td></td>
<td>• Author</td>
</tr>
<tr>
<td></td>
<td>• Category</td>
</tr>
<tr>
<td></td>
<td>• Comments</td>
</tr>
<tr>
<td></td>
<td>• Company</td>
</tr>
<tr>
<td></td>
<td>• Keywords (Tags)</td>
</tr>
<tr>
<td></td>
<td>• Last saved by</td>
</tr>
<tr>
<td></td>
<td>• Manager Name</td>
</tr>
<tr>
<td></td>
<td>• Security</td>
</tr>
<tr>
<td></td>
<td>• Subject</td>
</tr>
<tr>
<td></td>
<td>• Template</td>
</tr>
<tr>
<td></td>
<td>• Title</td>
</tr>
<tr>
<td><strong>File Encryption</strong></td>
<td>McAfee DLP Discover supports these options:</td>
</tr>
<tr>
<td></td>
<td>• Not encrypted</td>
</tr>
<tr>
<td></td>
<td>• Microsoft Rights Management encryption</td>
</tr>
<tr>
<td></td>
<td>• Unsupported encryption types or password protected file</td>
</tr>
<tr>
<td><strong>File Extension</strong></td>
<td>Groups of related file extensions such as graphic files.</td>
</tr>
</tbody>
</table>
Table 3-4 Definitions for classifications (continued)

<table>
<thead>
<tr>
<th>Classification definition</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File Information</strong></td>
<td>Contains these options:</td>
</tr>
<tr>
<td></td>
<td>• Date Accessed (UTC)</td>
</tr>
<tr>
<td></td>
<td>• Date Created (UTC)</td>
</tr>
<tr>
<td></td>
<td>• Date Modified (UTC)</td>
</tr>
<tr>
<td></td>
<td>• File Name</td>
</tr>
<tr>
<td></td>
<td>• File Size</td>
</tr>
<tr>
<td></td>
<td>• File Extension</td>
</tr>
<tr>
<td><strong>Keyword</strong></td>
<td>A string value.</td>
</tr>
<tr>
<td><strong>Location in file</strong></td>
<td>The section of the file the data is located in.</td>
</tr>
<tr>
<td><strong>Proximity</strong></td>
<td>Defines a conjunction between two properties based on their location to each other.</td>
</tr>
<tr>
<td><strong>True File Type</strong></td>
<td>Groups of file types. For example, the built-in Microsoft Excel group includes Excel XLS, XLSX, and XML files, as well as Lotus WK1 and FM3 files, CSV and DIF files, Apple iWork files, and more.</td>
</tr>
</tbody>
</table>

**Advanced pattern definitions**

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

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

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

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

**Dictionary definitions**

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

Classification criteria uses specified dictionaries to classify a document if a defined threshold (total score) is exceeded — that is, if enough words from the dictionary appear in the document.

The difference between a *dictionary* and a string in a *keyword* definition is the assigned score. A dictionary classification gives you more flexibility because you can set a threshold, which makes the classification relative.

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

McAfee DLP software includes several built-in dictionaries with terms commonly used in health, banking, finance, and other industries. In addition, you can create your own dictionaries. Dictionaries can be created (and edited) manually or by copying and pasting from other documents.
Limitations

There are some limitations to using dictionaries. Dictionaries are saved in Unicode (UTF-8) and can be written in any language. The following descriptions apply to dictionaries written in English. The descriptions generally apply to other languages, but there might be unforeseen problems in certain languages.

Dictionary matching has these characteristics:

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

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

Using rules with scans

Remediation scans use rules to detect and take action on sensitive files.

Files crawled by a remediation scan are compared against active discovery rules. If the file matches the repository and classifications defined in a rule, McAfee DLP Discover can take action on the file. These options are available:

- Take no action
- Create an incident
- Store the original file as evidence
- Copy the file
- Move the file
- Apply an RM policy to the file
- (Box scans only) Remove anonymous sharing for the file

Moving files or applying RM policy to files is not supported for SharePoint lists. These actions are supported for files attached to SharePoint lists or stored in document libraries. Some file types used for building SharePoint pages, such as .aspx or .js, cannot be moved or deleted.

Box scans support moving files only to CIFS shares.
Configure policy for scans

Before you set up a scan, create definitions, classifications, and rules for your McAfee DLP Discover policy.

Tasks

• Create definitions for scans on page 27
  Create and configure definitions used in scans and classifications.

• Create definitions for classifications on page 32
  Classifications require one or more definitions to match data and file properties.

Create definitions for scans

Create and configure definitions used in scans and classifications.

Tasks

• Create scan definitions on page 27
  All scans require a definition to specify the repository, credentials, and schedule.

• Create a credentials definition on page 28
  Credentials are required to read and change files in most repositories. If your repositories have the same credentials, you can use a single credentials definition for those repositories.

• Create a CIFS or SharePoint repository definition on page 29
  Configure a CIFS or SharePoint repository for scanning.

• Create a Box repository definition on page 30
  Configure a Box repository for scanning.

• Export or import repository definitions on page 31
  If you have a large number of repositories, it might be easier to manage them as an XML file rather than adding and editing them one by one in McAfee ePO.

• Create a scheduler definition on page 31
  The scan scheduler determines when and how frequently a scan is run.

Create scan definitions

All scans require a definition to specify the repository, credentials, and schedule.

Before you begin

You must have the user name, password, and path for the repository.

Task

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

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

2. Click the Definitions tab.
3 Create a credentials definition.

- In the left pane, select Others | Credentials.
- Select Actions | New and replace the default name with a unique name for the definition.
- Fill in the credentials parameters. Click Save.

4 Create a repository definition.

- In the left pane, under Repositories, select the type of new repository you want to create.
- Select Actions | New, type a unique repository name in the Name field, and fill in the rest of the Type and Definitions information.

- Exclude parameters are optional. At least one Include definition is required.

5 Create a scheduler definition.

- In the left pane, select Others | DLP Scheduler.
- Select Actions | New and fill in the scheduler parameters. Click Save.

- Parameter options depend on which Schedule type you select.

6 Create a file information definition.

- File information definitions are used to define scan filters. Filters allow you to scan repositories in a more granular manner by defining which files are included and which are excluded. File information definitions are optional, but recommended.

- In the left pane, select Data | File Information.
- Select Actions | New and replace the default name with a unique name for the definition.
- Select properties to use as filters and fill in the Comparison and Value details. Click Save.

**Create a credentials definition**

Credentials are required to read and change files in most repositories. If your repositories have the same credentials, you can use a single credentials definition for those repositories.

**Task**

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

1 In McAfee ePO, select Menu | Data Protection | DLP Discover.
2 Click the Definitions tab.
3 In the left pane, select Credentials.
4 Select Actions | New.
Enter a unique name for the definition. The **Description** and **Domain name** are optional fields. All other fields are required.

If the user is a domain user, use the domain suffix for the **Domain name** field. If the user is a workgroup user, use the local computer name.

To crawl all site collections in a SharePoint web application, use a credential which has *Full read* permission on the entire web application.

For Windows domain repositories, click **Test Credential** to verify the user name and password from McAfee ePO.

This does not test the credentials from the Discover server.

There is no verification for credentials that are not part of a Windows domain. If a scan fails due to incorrect credentials, an event is created on the **Operational Event List** page.

**Create a CIFS or SharePoint repository definition**

Configure a CIFS or SharePoint repository for scanning.

You can use regex in Perl syntax when specifying include or exclude parameters for folders, rather than using a specific full path.

- For include entries, specify the path prefix, such as `\server` or `\server\share\folder`. The regular expression must be an exact match of the path suffix.
- For exclude entries, folders that match the path will be skipped entirely from the scan.

**Task**

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

1. In McAfee ePO, select **Menu | Data Protection | DLP Discover**.
2. Click the **Definitions** tab.
3. In the left pane, under **Repositories**, select the type of repository.
4. Select **Actions | New**.
5. Enter a name, select the credentials to use, and configure at least one **Include** definition.
6. (CIFS repositories) Configure at least one **Include** entry.
   a. Select the **Prefix Type**.
   b. In the **Prefix** field, enter the UNC path, single IP address, or IP address range.

   The UNC path can be the fully qualified domain name (FQDN) (`\myserver1.mydomain.com`) or the local computer name (`\myserver1`). You can add both versions to a single definition. Multiple entries are parsed as logical OR.

   c. (Optional) Enter a regular expression for matching folders to scan.
   d. Click **Add**.
7 (SharePoint repositories) Configure at least one Include entry.
   a Select the Include type.
   b Configure one or more URLs.

   The SharePoint Server option uses only one URL. The host name is the NetBIOS name of the server unless Alternate Access Mapping (AAM) is configured on the server. For information about AAM, see the SharePoint documentation from Microsoft.

   • To specify a site — End the URL with a slash (http://SPServer/sites/DLP/).
   • To specify a subsite — Use the subsite ending with a slash (http://SPserver/sites/DLP/Discover/).
   • To specify a web application — Use only the web application name and port in the URL (http://SPServer:port).
   • To specify a list or document library — Use the complete URL up to the default view of the list (http://SPServer/sites/DLP/Share%20Documents/Default.aspx).

   You can look up the default view URL in the list or library settings page. If you do not have privileges to view this, contact your SharePoint administrator.

   c If you configured a Sites list URL, click Add.

8 (Optional) Configure Exclude parameters to exclude folders from being scanned.

9 Click Save.

Create a Box repository definition
Configure a Box repository for scanning.

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

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

2 Click the Definitions tab.

3 In the left pane, under Repositories, select Box.

4 Select Actions | New.

5 Enter the name and optional description.

6 Click the link to the Box website. Follow the instructions on the website to define the Box application and to obtain the client ID and client secret.
   • When defining the application, select the manage enterprise option.
   • For the redirect URI, enter the IP address of the McAfee ePO server.
   • To scan other accounts, contact Box support to enable the as-user functionality.

7 Enter the client ID and client secret, then click Get Token.

8 When prompted on the Box website, grant access for the Discover server.

9 Specify whether to scan all user accounts or specific user accounts.

10 Click Save.
Export or import repository definitions

If you have a large number of repositories, it might be easier to manage them as an XML file rather than adding and editing them one by one in McAfee ePO.

Use the export feature to save existing repository definitions and associated credentials to an XML file. Use this file as a baseline for adding and configuring your repositories in XML format.

When importing an XML file, the repository definitions and credentials are validated and added to the list of entries. If a repository definition exists in McAfee ePO and the XML file, the definition is overwritten with the information in the XML file. The definitions are uniquely identified by the \texttt{id} value in the XML file.

\textbf{Task}

For details about product features, usage, and best practices, click \texttt{?} or \texttt{Help}.

1. In McAfee ePO, select \texttt{Menu \vert Data Protection \vert DLP Discover}.
2. Click the \texttt{Definitions} tab.
3. Select \texttt{File Server (CIFS)} or \texttt{SharePoint}.
4. Perform one of these tasks.
   - To export repositories:
     1. Select \texttt{Actions \vert Export}.
     2. Select whether to open or save the file and click \texttt{OK}.
   - To import repositories:
     1. Select \texttt{Actions \vert Import}.
     2. Browse to the file and click \texttt{OK}.

Create a scheduler definition

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

These schedule types are provided:

- Run immediately
- Once
- Daily
- Weekly
- Monthly

\textbf{Task}

For details about product features, usage, and best practices, click \texttt{?} or \texttt{Help}.

1. In McAfee ePO, select \texttt{Menu \vert Data Protection \vert DLP Discover}.
2. Click the \texttt{Definitions} tab.
3. In the left pane, click \texttt{Scheduler}.
4. Select \texttt{Actions \vert New}.
5. Enter a unique name and select the schedule type.
   
   \textbf{The display changes when you select the schedule type to provide the necessary fields for that type.}

6. Fill in the required options and click \texttt{Save}.
Create definitions for classifications
Classifications require one or more definitions to match data and file properties.

Tasks

- Create a general classification definition on page 32
  Create and configure definitions for use in classifications and rules.

- Create an advanced pattern on page 32
  Advanced patterns are used to define classifications. An advanced pattern definition can consist of a single expression or a combination of expressions and false positive definitions.

- Create or import a dictionary definition on page 33
  A dictionary is a collection of keywords or key phrases where each entry is assigned a score. Scores allow for more granular rule definitions.

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

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

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Select the type of definition to configure, the select Actions | New.
3 Enter a name and configure the options and properties for the definition.

The available options and properties vary depending on the type of definition.

4 Click Save.

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

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

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

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Select the Definitions tab, then select Advanced pattern in the left pane.

The available patterns appear in the right pane.

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

3 Select Actions | New.

The New Advanced pattern definition page appears.

4 Enter a name and optional description.
5 Under **Matched Expressions**, do the following:
   a  Enter an expression in the text box. Add an optional description.

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

   c  Enter a number in the **Score** field.
       This number indicates the weight of the expression in threshold matching. This field is required.

   d  Click **Add**.

6 Under **False Positive**, do the following:
   a  Enter an expression in the text box.

      ![Tip]
      If you have text patterns stored in an external document, you can copy-paste them into the definition with **Import Entries**.

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

   c  Click **Add**.

7 Click **Save**

**Create or import a dictionary definition**

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

**Task**

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

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

2  Click the **Definitions** tab.

3  In the left pane, select **Dictionary**.

4  Select **Actions | New**.

5  Enter a name and optional description.

6  Add entries to the dictionary.
   To import entries:
   a  Click **Import Entries**.

   b  Enter words or phrases, or cut and paste from another document.

      ![Tip]
      The text window is limited to 20,000 lines of 50 characters per line.

   c  Click **OK**.

      ![Tip]
      All entries are assigned a default score of 1.
If needed, updated the default score of 1 by clicking Edit for the entry.

Select the Start With, End With, and Case Sensitive columns as needed. Start With and End With provide substring matching.

To manually create entries:
- Enter the phrase and score.
- Select the Start With, End With, and Case Sensitive columns as needed.
- Click Add.

Click Save.

Create classifications
Classification and remediation scans use classifications to identify sensitive files.

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

1 In McAfee ePO, select Menu | Data Protection | Classification.
2 Click New Classification.
3 Enter a name and optional description.
4 Click OK.
5 Select Actions | New Classification Criteria.
6 Enter the name.
7 Select one or more properties and configure the comparison and value entries.
   The available properties include built-in and user-defined classification definitions.
   - Click < to remove a property.
   - For some properties, click ... to select an existing property or to create a new one.
   - Click + to add values.
   - Click - to remove values.
8 Click Save.

Create rules for remediation scans
Use rules to define the action to take when a remediation scan detects files that match classifications.

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

1 In McAfee ePO, select Menu | Data Protection | DLP Policy Manager.
2 Click the Rule Sets tab.
3 If there are no rule sets configured, create a rule set.
   a Select Actions | New Rule Set.
   b Click the name of a rule set, then if needed, click the Discover tab.
5 Select Actions | New Network Discovery Rule, then select the type of rule.
6 On the Condition tab, configure one or more classifications and repositories.
   • Create an item — Click ...
   • Add additional criteria — Click +.
   • Remove criteria — Click -.
7 (Optional) On the Exceptions tab, specify any exclusions from triggering the rule.
8 On the Reaction tab, configure the reaction.
   The available reactions depend on the repository type.
9 Click Save.

Configure a scan
The amount and type of data that McAfee DLP Discover collects depends on the type of scan configured.

Tasks
• Configure an inventory scan on page 35
  Inventory scans collect metadata only. They are the fastest scans, and thus the usual starting point in determining what scans are needed.
• Configure a classification scan on page 36
  Classification scans collect file data based on defined classifications. They are used to analyze file systems for sensitive data to be protected with a remediation scan.
• Configure a remediation scan on page 37
  Remediation scans apply rules to protect sensitive content in the scanned repository.

Configure an inventory scan
Inventory scans collect metadata only. They are the fastest scans, and thus the usual starting point in determining what scans are needed.
Use inventory scans to plan your data protection strategy. You can create scans or edit and reuse existing ones as required.

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

1 In McAfee ePO, select Menu | Data Protection | DLP Discover.
2 On the Discover Servers tab, select Actions | Detect Servers to refresh the list.
   If the list is long, you can define a filter to display a shorter list.
3 On the Scan Operations tab, select Actions | New Scan and select the repository type.
4. Type a unique name and select **Scan Type: Inventory**. Select a server platform and a schedule.

   > Discover servers must be predefined. You can select a defined schedule or create one.

5. (Optional) Set values for **Files List** or **Error Handling** in place of the default values.

6. Select the repositories to scan.
   a. On the **Repositories** tab, click **Actions | Select Repositories**.
   b. If needed, specify the credentials for each repository from the drop-down list.
      The credentials default to what is configured for that repository.
      > You can create repository and credentials definitions if necessary from the selection window.

7. (Optional) On the **Filters** tab, select **Actions | Select Filters** to specify files to include or exclude.
   By default, all files are scanned.

8. Click **Save**.

9. Click **Apply policy**.

### Configure a classification scan

Classification scans collect file data based on defined classifications. They are used to analyze file systems for sensitive data to be protected with a remediation scan.

**Before you begin**
- Run an inventory scan. Use the inventory data to define classifications.
- Create the required classification definitions before setting up a classification scan. There is no option to create a classification within the configuration setup.

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

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

2. On the **Discover Servers** tab, select **Actions | Detect Servers** to refresh the list.
   > If the list is long, you can define a filter to display a shorter list.

3. On the **Scan Operations** tab, select **Actions | New Scan** and select the repository type.

4. Type a unique name and select **Scan Type: Classification**. Select a server platform and a schedule.
   > Discover servers must be predefined. You can select a defined schedule or create one.

5. (Optional) Set values for **Throttling**, **Files List**, or **Error Handling** in place of the default values.

6. Select the repositories to scan.
   a. On the **Repositories** tab, click **Actions | Select Repositories**.
   b. If needed, specify the credentials for each repository from the drop-down list.
      The credentials default to what is configured for that repository.
      > You can create repository and credentials definitions if necessary from the selection window.
7 (Optional) On the Filters tab, select Actions | Select Filters to specify files to include or exclude.
   By default, all files are scanned.

8 Select the classifications for the scan.
   a On the Classifications tab, click Actions | Select Classifications.
   b Select one or more classifications from the list.

9 Click Save.

10 Click Apply policy.

See also
Create classifications on page 34

Configure a remediation scan
Remediation scans apply rules to protect sensitive content in the scanned repository.

Before you begin
- If the scan is configured to apply RM policy or move files, make sure the credentials for the repository have full control permissions.
- Create the classifications and rules for the scan.

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

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

2 On the Discover Servers tab, select Actions | Detect Servers to refresh the list.
   
   i If the list is long, you can define a filter to display a shorter list.

3 On the Scan Operations tab, select Actions | New Scan and select the repository type.

4 Type a unique name and select Scan Type: Remediation. Select a server platform and a schedule.
   
   i Discover servers must be predefined. You can select a defined schedule or create one.

5 (Optional) Set values for Throttling, Files List, Incident Handling, or Error Handling in place of the default values.

6 Select the repositories to scan.
   a On the Repositories tab, click Actions | Select Repositories.
   b If needed, specify the credentials for each repository from the drop-down list.
      The credentials default to what is configured for that repository.

   i You can create repository and credentials definitions if necessary from the selection window.

7 (Optional) On the Filters tab, select Actions | Select Filters to specify files to include or exclude.
   By default, all files are scanned.
Select the rules for the scan.

a  On the Rules tab, click Actions | Select Rule Sets.

b  Select one or more rule sets from the list.

Click Save.

Click Apply policy.

See also
Create classifications on page 34
Create rules for remediation scans on page 34

Perform scan operations
Manage and view information about configured scans.

Applying policy starts any scans that are scheduled to run immediately. Scans that are currently running are not affected.

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

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

2  Click the Scan Operations tab.
   The tab displays information about configured scans, such as the name, type, state, and overview of the results.

3  To update the configuration for all scans, click Apply policy.

4  To apply a filter to the scan list, select a filter from the Filter drop-down list.

5  To enable or disable a scan:
   a  Select the checkbox for the scans you want to enable or disable.
       The icon in the State column shows if the scan is enabled or disabled.
       •  Solid blue icon — Enabled
       •  Blue and white icon — Disabled
   b  Select Actions | Change State, then select Enabled or Disabled.
   c  Click Apply policy.

6  To change the running state of the scan, click the start, pause, or stop buttons in the Commands column.
   The availability of these options depends on the scan state and if the scan is running or inactive.
7 To clone, delete, or edit a scan:
   a Select the checkbox for the scan.
   b Select Actions, then select Clone Scan, Delete Scan, or Edit Scan.

   To modify the Discover server assigned to the scan, you must disable the scan. You cannot modify the scan type assigned to a scan. To change the type, clone the scan.

8 To refresh the tab, select Actions | Synchronize Data.

---

**Scan behavior**

Changing properties of a scan that is in progress can affect the behavior of the scan.

**Table 3-5 Effect of changing properties during a scan**

<table>
<thead>
<tr>
<th>Change</th>
<th>Effect</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable scan</td>
<td>Scan stops</td>
</tr>
<tr>
<td>Delete scan</td>
<td>Scan stops and is deleted</td>
</tr>
<tr>
<td>Change scan name</td>
<td>Affects only logs on the next scan run</td>
</tr>
<tr>
<td>Change schedule</td>
<td>Affects only the next scan run</td>
</tr>
<tr>
<td>Change throttling</td>
<td>Affects only the next scan run*</td>
</tr>
<tr>
<td>Change file list</td>
<td>Affects only the next scan run*</td>
</tr>
<tr>
<td>Change repository</td>
<td>Affects only the next scan run</td>
</tr>
<tr>
<td>Change filters</td>
<td>Affects only the next scan run</td>
</tr>
<tr>
<td>Change rules</td>
<td>Affects only the next scan run*</td>
</tr>
<tr>
<td>Change classification</td>
<td>Affects only the next scan run*</td>
</tr>
<tr>
<td>Change evidence share</td>
<td>Affects the current scan*</td>
</tr>
<tr>
<td>Change evidence user credentials</td>
<td>Affects the current scan*</td>
</tr>
<tr>
<td>Change remediation user credentials</td>
<td>Affects only the next scan run*</td>
</tr>
<tr>
<td>Upgrade or uninstall the Discover server</td>
<td>Scan stops</td>
</tr>
</tbody>
</table>

* The effect takes place after an agent server communication interval (ASCI) occurs.

---

**Assigning McAfee DLP permission sets**

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

Installing the McAfee DLP server software adds the McAfee ePO permission set Data Loss Prevention. If a previous version of McAfee DLP is installed on the same McAfee ePO server, that permission set also appears.
The permission set covers all sections of the management console. There are three levels of permissions:

- **Use** — The user can see only names of objects (definitions, classifications, and so forth), not details.
  
  *For policies, the minimum permission is no permission.*

- **View and use** — The user can view details of objects, but cannot change them.

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

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

The McAfee DLP Discover permission groups are:

- DLP Discover
- DLP Policy Manager
- Classifications
- Definitions

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

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

**Figure 3-1 McAfee DLP permission sets**

**Create a McAfee DLP permission set**

Permission sets are used to define different administrative and reviewer roles in McAfee DLP software.
Task
For details about product features, usage, and best practices, click ? or Help.

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

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

3 Select a permission set, then click Edit in the Data Loss Prevention section.
   a In the left pane, select a data protection module.
      Incident Management, Operational Events, and Case Management can be selected separately. Other options automatically create predefined groups.
   b Edit the options and override permissions as required.
      Policy Catalog has no options to edit. If you are assigning Policy Catalog to a permission set, you can edit the sub-modules in the Policy Catalog group.
   c Click Save.

Protecting confidentiality with redaction
Data redaction is the obscuring of confidential information to prevent unauthorized viewing. Some countries require redaction practices be followed, and it is considered Best Practice (even when not required by law) to separate incident and operational events reviewing permissions, and to block sensitive data from those not required to view it.

Redacted information is obscured in:
- The DLP Incident Manager display
- The DLP Operations display

As part of redaction, evidence files are not visible until the redaction is released.

To give a user permission to view redacted fields, select Supervisor permission on the Incident Management permissions page.

Use case — redacted fields reviewer
This example requires setting permissions for two reviewers: one to review events and incidents, one to view the redacted fields. Assuming that reviewer roles are separated from policy administrator roles, make the following selections:

- For both reviewers — In the Incidents Reviewer section, select any option. In the Incident Data Redaction section, select Obfuscate sensitive incident data and Supervisor permission.
- For the incident reviewer — In the Incidents Reviewer section, select any option. In the Incident Data Redaction section, select Obfuscate sensitive incident data.
- For the redaction reviewer — In the Incidents Reviewer section, do not select any option. In the Incident Data Redaction section, select Supervisor permission.
Scan and policy configuration
Assigning McAfee DLP permission sets
Analyzing scanned data

McAfee DLP Discover lets you analyze information collected from scanned data in several ways. The basic inventory scan (collection of metadata) is part of all scan types. Classification scans also apply defined classifications, which means that the text extractor parses file content, adding additional information to the stored metadata.

Contents
- How McAfee DLP Discover uses OLAP
- Viewing scan results
- Analyze scan results
- View inventory results

How McAfee DLP Discover uses OLAP

McAfee DLP Discover uses Online Analytical Processing (OLAP), a data model that enables quick processing of metadata from different viewpoints.

Use the McAfee DLP Discover OLAP tools to view multidimensional relationships between data collected from scans. These relationships are known as hypercubes or OLAP cubes.

You can sort and organize scan results based on conditions such as classification, file type, repository, and more. Using the data patterns to estimate potential violations, you can optimize classification and remediation scans to identify and protect data quickly and more effectively.

Viewing scan results

The Data Analytics and Data Inventory tabs display scan results.

These tabs display the results collected from the last time the scan was run.
**Data Analytics tab**

The Data Analytics tab allows you to analyze files from scans. The tab uses an OLAP data model to display up to three categories to expose multidimensional data patterns. Use these patterns to optimize your classification and remediation scans.

---

**Figure 4-1 Configuring data analytics**

1. **Scan Name** — The drop-down list displays available scans for all types. Analysis can only be performed on a single scan.

2. **Analytic Type** — Select from Files or Classifications. For inventory scans, only Files is available. The analytic type determines the available categories.

3. **Show** — Controls how many entries are displayed.

4. **Expand Table/Collapse Table** — Expands the entire page. You can also expand or collapse individual groups.

5. **Category selector** — Drop-down list displays all available categories. You can select from the remaining categories in the second and third selectors to create a three dimensional analysis of data patterns.

6. **Item expansion** — The arrow icon controls expansion/collapse of individual groups to clean up the display.

7. **Count** — Number of files (or classifications) in each group. Click the number to go to the Data Inventory tab and display details for that group.

---

*If the Analytic Type is set to Classifications and any files have more than one associated classification, this number might be larger than the total number of files.*
**Data Inventory tab**

The Data Inventory tab displays the inventory of files from scans that have the File List option enabled. You can define and use filters to adjust the information displayed, which might reveal patterns or potential policy violations.

Classification and File type are not available for inventory scans.

---

**Analyze scan results**

Use the OLAP data model to organize and view relationships between files from scans.

**Task**

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

1. In McAfee ePO, select **Menu | Data Protection | DLP Discover**.
2. Click the **Data Analytics** tab.
3. From the **Scan Name** drop-down list, select the scan to analyze.
4. From the **Analytic Type** drop-down list, select **File** or **Classification**.
5. From the **Show** drop-down list, select the number of top entries to display.
6. Use the category drop-down lists to display files from up to three categories.
7. Use the **Expand Table** and **Collapse Table** options to expand or collapse the amount of information displayed.
8. To view the inventory results of files belonging to a category, click the link that shows the number of files in parentheses.

The link is available only if you selected the **Files List** option in the scan configuration. The link displays the **Data Inventory** page.

---

**View inventory results**

View the inventory of files from all scan types.

**Task**

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

1. In McAfee ePO, select **Menu | Data Protection | DLP Discover**.
2. Click the **Data Inventory** tab.
3. Perform any of these tasks.
   - To view the results of a particular scan, select the scan from the **Scan** drop-down list.
   - To filter the files displayed, select a filter from the **Filter** drop-down list.

Click **Edit** to modify and create filters.
• To group files based on a certain property:
  1. From the **Group By** drop-down list, select a category. The available properties appear in the left pane.
  2. Select the property to group files.

• To configure the displayed columns:
  1. Select **Actions** | **Choose Columns**.
  2. From the **Available Columns** list, click an option to move it to the **Selected Columns** area.
  3. In the **Selected Columns** area, arrange and delete columns as needed.
    • To remove a column, click **x**.
    • To move a column, click the arrow buttons, or drag and drop the column.
  4. Click **Update View**.
Incidents and operational events

McAfee DLP offers different tools for viewing incidents and operational events.

- **Incidents** — The DLP Incident Manager page displays incidents generated from rules.
- **Operational events** — The DLP Operations page displays errors and administrative information.
- **Cases** — The DLP Case Management page contains cases that have been created to group and manage related incidents.

When both McAfee DLP Discover and McAfee DLP Endpoint are installed, the consoles display incidents and events from both applications.

The display for both DLP Incident Manager and DLP Operations can include information on the computer and logged-on user generating the incident/event, client version, operating system, and other information.

Contents
- Monitoring and reporting events
- DLP Incident Manager
- Working with incidents
- View incidents
- Manage incidents
- Working with cases
- Manage cases

Monitoring and reporting events

McAfee DLP divides events into two classes: incidents (that is, policy violations) and administrative events. These events are viewed in the two consoles, DLP Incident Manager and DLP Operations.

When McAfee DLP determines a policy violation has occurred, it generates an event and sends it to the McAfee ePO Event Parser. These events are viewed, filtered, and sorted in the DLP Incident Manager console, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.

As McAfee DLP takes a major role in an enterprise’s effort to comply with all regulation and privacy laws, the DLP Incident Manager presents information about the transmission of sensitive data in an accurate and flexible way. Auditors, signing officers, privacy officials and other key workers can use the DLP Incident Manager to observe suspicious or unauthorized activities and act in accordance with enterprise privacy policy, relevant regulations or other laws.
The DLP Operations console displays:

- **McAfee DLP Discover**: Scan or server errors
- **McAfee DLP Endpoint**: Details on client deployment, policy changes, policy deployment, Safe Mode logons, agent overrides, and other administrative events

## DLP Incident Manager

Use the DLP Incident Manager page in McAfee ePO to view the security events from policy violations. The incident manager has three tabbed sections:

- **Incident List** — The current list of policy violation events.
- **Incident Tasks** — A list of actions you can take on the list or selected parts of it. They include assigning reviewers to incidents, setting automatic email notifications, and purging all or part of the list.
- **Incident History** — A list containing all historic incidents. Purging the incident list does not affect the history.

### How the Incident Manager works

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

Operations you can perform on events include:

- **Case management** — Create cases and add selected incidents to a case
- **Comments** — Add comments to selected incidents
- **Email events** — Send selected events
- **Labels** — Set a label for filtering by label
- **Release redaction** — Remove redaction to view protected fields (requires correct permission)
- **Set properties** — Edit the severity, status, or resolution; assign a user or group for incident review

The DLP Operations page works in an identical manner with administrative events. The events contain information such as why the event was generated and which McAfee DLP product reported the event.

![Figure 5-1 DLP Incident Manager](image)
Incident tasks/Operational Event tasks

Use the Incident Tasks or Operational Event Tasks tab to set criteria for scheduled tasks. Tasks set up on the pages work with the McAfee ePO Server Tasks feature to schedule tasks.

Both tasks tabs are organized by the task type (left pane). The Incident Tasks tab is also organized by incident type, so that it is actually a 4 x 3 matrix, the information displayed depending on which two parameters you select.

<table>
<thead>
<tr>
<th>Task Description</th>
<th>Data in-use/motion</th>
<th>Data at-rest (Endpoint)</th>
<th>Data at-rest (Network)</th>
<th>Data in-use/motion (History)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set Reviewer</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Automatic mail notification</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Purge events</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Use case: Setting properties

Properties are data added to an incident that requires follow-up. You can add the properties from the details pane of the incident or by selecting Actions | Set Properties. The properties are:

- Severity
- Status
- Resolution
- Reviewing Group
- Reviewing User

The reviewer can be any McAfee ePO user. The reason severity can be changed is that if the administrator determines that the status is false positive, then the original severity is no longer meaningful.

Use case: Changing the view

In addition to using filters to change the view, you can also customize the fields and the order of display. Customized views can be saved and reused.

Creating a filter involves the following tasks:

1. To open the view edit window, click Actions | View | Choose Columns.
2. To move columns to the left or right, use the x icon to delete columns, and the arrow icons.
To apply the customized view, click Update View.

To save for future use, click Actions | View | Save View.

When you save the view, you can also save the time and custom filters. Saved views can be chosen from the drop-down list at the top of the page.

Create a Set Reviewer task

You can assign reviewers for different incidents and operational events to divide the workload in large organizations.

Before you begin

In McAfee ePO User Management | Permission Sets, create a reviewer, or designate a group reviewer, with Set Reviewer permissions for DLP Incident Manager and DLP Operations.

The Set Reviewer task assigns a reviewer to incidents/events according to the rule criteria. The task only runs on incidents where a reviewer has not been assigned. You cannot use it to reassign incidents to a different reviewer.

Task

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

1 In McAfee ePO, select Menu | Data Protection | DLP Incident Manager or Menu | Data Protection | DLP Operations.
2 Click the Incident Tasks or Operational Event Tasks tab.
3 Select Data at rest (Network) from the drop-down list (Incident Tasks only), select Set Reviewer in the Task Type pane, then click Actions | New Rule.
4 Enter a name and optional description. Select a reviewer or group, then click Next.
   Rules are enabled by default. You can change this setting to delay running the rule.
5 Click > to add criteria, < to remove them. Set the Comparison and Value parameters. When you have finished defining criteria, click Save.

If there are multiple Set Reviewer rules you can reorder the rules in the list.

The task runs hourly.

After a reviewer is set, it is not possible to override the reviewer through the Set Reviewer task.

Create an Automatic mail Notification task

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

Task

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

1 In McAfee ePO, select Menu | Data Protection | DLP Incident Manager or Menu | Data Protection | DLP Operations.
2 Click the Incident Tasks or Operational Events Tasks tab.
3 Select Data at rest (Network) from the drop-down list (Incident Tasks only), select Automatic mail Notification in the Task Type pane, then click Actions | New Rule.
4 Enter a name and optional description.
   Rules are enabled by default. You can change this setting to delay running the rule.

5 Select the events to process.
   • Process all incidents/events (of the selected incident type).
   • Process incidents/events since the last mail notification run.

6 Select Recipients.
   This field is required. At least one recipient must be selected.

7 Enter a subject for the email.
   This field is required.
   You can insert variables from the drop-down list as required.

8 Enter the body text of the email.
   You can insert variables from the drop-down list as required.

9 (Optional) Select the checkbox to attach evidence information to the email. Click Next.

10 Click > to add criteria, < to remove them. Set the Comparison and Value parameters. When you have finished defining criteria, click Save.

   The task runs hourly.

**Create a Purge events task**

You create incident and event purge tasks to clear the database of data that is no longer needed.

**Task**

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

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

2 Click the Incident Tasks or Operational Event Tasks tab.

3 Select Data at rest (Network) from the drop-down list (Incident Tasks only), select Purge events in the Task Type pane, then click Actions | New Rule.

4 Enter a name and optional description, then click Next.
   Rules are enabled by default. You can change this setting to delay running the rule.

5 Click > to add criteria, < to remove them. Set the Comparison and Value parameters. When you have finished defining criteria, click Save.

   The task runs daily for live data and every Friday at 10:00 PM for historical data.
**Edit server tasks**

McAfee DLP uses the McAfee ePO Server Tasks to run DLP Incident Manager and DLP Operations tasks. Each incident and operational events task is predefined in the server tasks list. The only options available are to enable or disable them or to change the scheduling. The available McAfee DLP server tasks are:

- Detect Discovery Servers
- DLP Purge History of Operational Events and Incidents
- DLP Purge Operational Events and Incidents
- DLP Send Email for Operational Events and Incidents
- DLP Set Reviewer for Operational Events and Incidents

**Task**

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

1. In McAfee ePO, select **Menu | Automation | Server Tasks**.
2. Select the task to edit.

   ![Best practice: Enter DLP in the Quick find field to filter the list.]

3. Select **Actions | Edit**, then click **Schedule**.
4. Edit the schedule as required, then click **Save**.

**Monitor task results**

Monitor the results of incident and operational event tasks.

**Task**

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

1. In McAfee ePO, select **Menu | Automation | Server Task Log**.
2. Locate the completed McAfee DLP tasks.

   ![Enter DLP in the Quick find field or set a custom filter.]

3. Click the name of the task.

   The details of the task appear, including any errors if the task failed.

---

**Working with incidents**

When McAfee DLP receives data that matches parameters defined in a rule, a violation is triggered and McAfee DLP generates an incident.

Using the incident manager in McAfee ePO, you can view, sort, group, and filter incidents to find important violations. You can view details of incidents or delete incidents that are not useful.
View incidents

The incident manager displays all incidents reported by McAfee DLP devices. You can alter the way incidents appear to help you locate important violations more efficiently.

When McAfee DLP processes an object — such as an email message — that triggers multiple rules, the incident manager collates and displays the violations as one incident, rather than separate incidents.

Tasks

- **Sort and filter incidents on page 53**
  Arrange the way incidents appear based on attributes such as time, location, user, or severity.

- **Configure column views on page 53**
  Use views to arrange the type and order of columns displayed in the incident manager.

- **Configure incident filters on page 54**
  Use filters to display incidents that match specified criteria.

- **View incident details on page 55**
  View the information related to an incident.

Sort and filter incidents

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

Task

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

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

2. From the **Present** drop-down list, select **Data at rest (Network)** and if needed, click the **Scan** link to set the scan.

3. Perform any of these tasks.
   - To sort by column, click a column header.
   - To change columns to a custom view, from the **View** drop-down list, select a custom view.
   - To filter by time, from the **Time** drop-down list, select a time frame.
   - To apply a custom filter, from the **Filter** drop-down list, select a custom filter.
   - To group by attribute:
     1. From the **Group By** drop-down list, select an attribute.
        
        A list of available options appears. The list contains up to 250 of the most frequently occurring options.

     2. Select an option from the list. Incidents that match the selection are displayed.

Configure column views

Use views to arrange the type and order of columns displayed in the incident manager.

Task

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

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

2. From the **Present** drop-down list, select **Data at rest (Network)** and if needed, click the **Scan** link to set the scan.
Configure the columns.
   a  From the Available Columns list, click an option to move it to the Selected Columns area.
   b  In the Selected Columns area, arrange and delete columns as needed.
      •  To remove a column, click x.
      •  To move a column, click the arrow buttons, or drag and drop the column.
   c  Click Update View.

Configure the view settings.
   a  Next to the View drop-down list, click Save.
   b  Select one of these options.
      •  Save as new view — Specify a name for the view.
      •  Override existing view — Select the view to save.
   c  Select who can use the view.
      •  Public — Any user can use the view.
      •  Private — Only the user that created the view can use the view.
   d  Specify if you want the current filters or groupings applied to the view.
   e  Click OK.

You can also manage views in the Incident Manager by selecting Actions | View.

Configure incident filters
Use filters to display incidents that match specified criteria.

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

1  In McAfee ePO, select DLP Incident Manager.
2  From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.
3  From the Filter drop-down list, select (no custom filter) and click Edit.
4  Configure the filter parameters.
   a  From the Available Properties list, select a property.
   b  Enter the value for the property.
      To add additional values for the same property, click +.
   c  Select additional properties as needed.
      To remove a property entry, click <.
   d  Click Update Filter.
5 Configure the filter settings.
   a Next to the Filter drop-down list, click Save.
   b Select one of these options.
      • Save as new filter — Specify a name for the filter.
      • Override existing filter — Select the filter to save.
   c Select who can use the filter.
      • Public — Any user can use the filter.
      • Private — Only the user that created the filter can use the filter.
   d Click OK.

You can also manage filters in the incident manager by selecting Actions | Filter.

View incident details
View the information related to an incident.

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

1 In McAfee ePO, select DLP Incident Manager.

2 Do one of the following:
   • For Device Control or McAfee DLP Endpoint incidents: From the Present drop-down list, select Data in-use/motion.
   • For McAfee DLP Endpoint discovery incidents: From the Present drop-down list, select Data at rest (Endpoint).
   • For McAfee DLP Discover incidents: From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.

3 Click an Incident ID.
   In McAfee DLP Endpoint, the page displays general details and source information. Depending on the incident type, destination or device details appear. In McAfee DLP Discover, the page displays general details about the incident.

4 To view additional information, perform any of these tasks.
   • To view user information in McAfee DLP Endpoint, click the user name in the Source area.
   • To view evidence files:
      1 Click the Evidence tab.
      2 Click a file name to open the file with an appropriate program.
      The Evidence tab also displays the Short Match String, which contains up to three hit highlights as a single string.
   • To view rules that triggered the incident, click the Rules tab.
   • To view classifications, click the Classifications tab.

   In McAfee DLP Endpoint, the Classifications tab does not appear for some incident types.
• To view incident history, click the Audit Logs tab.
• To view comments added to the incident, click the Comments tab.
• To email the incident details, including decrypted evidence and hit highlight files, select Actions | Email Selected Events.
• To return to the incident manager, click OK.

Manage incidents

Use the incident manager to update and manage incidents. To delete incidents, configure a task to purge events.

Tasks

• Update a single incident on page 56
  Update incident information such as the severity, status, and reviewer.
• Update multiple incidents on page 57
  Update multiple incidents with the same information simultaneously.
• Manage labels on page 57
  A label is a custom attribute used to identify incidents that share similar traits.

See also
Create a Purge events task on page 51

Update a single incident

Update incident information such as the severity, status, and reviewer.

The Audit Logs tab reports all updates and modifications performed on an incident.

Task

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

1 In McAfee ePO, select DLP Incident Manager.

2 From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.

3 Click an incident.

4 Perform any of these tasks.

• To update the severity, status, or resolution:
  1 From the Severity, Status, or Resolution drop-down lists, select an option.
  2 Click Save.

• To update the reviewer:
  1 Next to the Reviewer field, click ...
  2 Select the group or user and click OK.
  3 Click Save.
To add a comment:

1. Select Actions | Add Comment.
2. Enter a comment, then click OK.

**Update multiple incidents**

Update multiple incidents with the same information simultaneously.

*Example:* You have applied a filter to display all incidents from a particular scan, and you want to change the severity of these incidents to Major.

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

1. In McAfee ePO, select DLP Incident Manager.
2. From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.
3. Select the checkboxes of the incidents to update.

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

4. Perform any of these tasks.
   - To add a comment, select Actions | Add Comment, enter a comment, then click OK.
   - To send the incidents in an email, select Actions | Email Selected Events, enter the information, then click OK.
     
     ![Tip: You can select a template, or create a template by entering the information and clicking Save.]
   - To change the properties, select Actions | Set Properties, change the options, then click OK.

**Manage labels**

A label is a custom attribute used to identify incidents that share similar traits.

You can assign multiple labels to an incident and you can reuse a label on multiple incidents.

*Example:* You have incidents that relate to several projects your company is developing. You can create labels with the name of each project and assign the labels to the respective incidents.

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

1. In McAfee ePO, select DLP Incident Manager.
2. From the Present drop-down list, select Data at rest (Network) and if needed, click the Scan link to set the scan.
3. Select the checkboxes of one or more incidents.

![Tip: To update all incidents displayed by the current filter, click Select all in this page.]
4 Perform any of these tasks.

- To add labels:
  1. Select **Actions** | **Manage Labels** | **Attach**.
  2. To add a new label, enter a name and click **Add**.
  3. Select one or more labels.
  4. Click **OK**.

- To remove labels from an incident:
  1. Select **Actions** | **Manage Labels** | **Detach**.
  2. Select the labels to remove from the incident.
  3. Click **OK**.

- To delete labels:
  1. Select **Actions** | **Manage Labels** | **Delete Labels**.
  2. Select the labels to delete.
  3. Click **OK**.

---

**Working with cases**

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

**Scenario:** Incidents generated from a remediation scan show that many sensitive files were recently added to a publicly accessible repository. Another remediation scan shows that these files have also been added to a different public repository.

Depending on the nature of the violations, you might need to alert the HR or legal teams about these incidents. You can allow members of these teams to work on the case, such as adding comments, changing the priority, or notifying key stakeholders.
Manage cases

Create and maintain cases for incident resolution.

Tasks

- **Create cases on page 59**
  Create a case to group and review related incidents.

- **View case information on page 59**
  View audit logs, user comments, and incidents assigned to a case.

- **Assign incidents to a case on page 60**
  Add related incidents to a new or existing case.

- **Move or remove incidents from a case on page 60**
  If an incident is no longer relevant to a case, you can remove it from the case or move it to another case.

- **Update cases on page 61**
  Update case information such as changing the owner, sending notifications, or adding comments.

- **Add or remove labels to a case on page 62**
  Use labels to distinguish cases by a custom attribute.

- **Delete cases on page 62**
  Delete cases that are no longer needed.

Create cases

Create a case to group and review related incidents.

Task

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

1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Select Actions | New.
3. Enter a title name and configure the options.
4. Click OK.

View case information

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

Task

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

1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Click on a case ID.
3. Perform any of these tasks.
   - To view incidents assigned to the case, click the Incidents tab.
   - To view user comments, click the Comments tab.
   - To view the audit logs, click the Audit Log tab.
4. Click OK.
Assign incidents to a case
Add related incidents to a new or existing case.

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

1. In McAfee ePO, select **Menu | Data Protection | DLP Incident Manager**.
2. From the **Present** drop-down list, select an incident type. For **Data at rest (Network)** click the **Scan** link to set the scan if needed.
3. Select the checkboxes of one or more incidents.
   
   ![Use options such as Filter or Group By to show related incidents. To update all incidents displayed by the current filter, click Select all in this page.]

4. Assign the incidents to a case.
   - To add to a new case, select **Actions | Case Management | Add to new case**, enter a title name, and configure the options.
   - To add to an existing case, select **Actions | Case Management | Add to existing case**, filter by the case ID or title, and select the case.

5. Click **OK**.

Move or remove incidents from a case
If an incident is no longer relevant to a case, you can remove it from the case or move it to another case.

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

1. In McAfee ePO, select **Menu | Data Protection | DLP Case Management**.
2. Click a case ID.
3. Perform any of these tasks.
   - To move incidents from one case to another:
     1. Click the **Incidents** tab and select the incidents.
     2. Select **Actions | Move**, then select whether to move to an existing or new case.
     3. Select the existing case or configure options for a new case, then click **OK**.
   - To remove incidents from the case:
     1. Click the **Incidents** tab and select the incidents.
     2. Select **Actions | Remove**, then click **Yes**.
4. Click **OK**.

You can also move or remove one incident from the **Incidents** tab by clicking **Move** or **Remove** in the **Actions** column.
Update cases
Update case information such as changing the owner, sending notifications, or adding comments. Notifications are sent to the case creator, case owner, and selected users when:

- An email is added or changed.
- Incidents are added to or deleted from the case.
- The case title is changed.
- The owner details are changed.
- The priority is changed.
- The resolution is changed.
- Comments are added.

You can disable automatic email notifications to the case creator and owner from Menu | Configuration | Server Settings | Data Loss Prevention.

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

1 In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2 Click a case ID.
3 Perform any of these tasks.
   - To update the case name, in the Title field, enter a new name, then click Save.
   - To update the owner:
     1 Next to the Owner field, click ...
     2 Select the group or user.
     3 Click OK.
     4 Click Save.
   - To update the Priority, Status, or Resolution options, use the drop-down lists to select the items, then click Save.
   - To send email notifications:
     1 Next to the Send notifications to field, click ...
     2 Select the users to send notifications to.

If no contacts are listed, specify an email server for McAfee ePO and add email addresses for users. Configure the email server from Menu | Configuration | Server Settings | Email Server. Configure users from Menu | User Management | Users.

3 Click Save.
To add a comment to the case:
1. Click the Comments tab.
2. Enter the comment in the text field.
3. Click Add Comment.
4. Click OK.

Add or remove labels to a case
Use labels to distinguish cases by a custom attribute.

Task
For details about product features, usage, and best practices, click ? or Help.
1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Select the checkboxes of one or more cases.
3. Perform any of these tasks.
   - To add labels to the selected cases:
     1. Select Actions | Manage Labels | Attach.
     2. To add a new label, enter a name and click Add.
     3. Select one or more labels.
     4. Click OK.
   - To remove labels from the selected cases:
     1. Select Actions | Manage Labels | Detach.
     2. Select the labels to remove.
     3. Click OK.

See also
Manage labels on page 57

Delete cases
Delete cases that are no longer needed.

Task
For details about product features, usage, and best practices, click ? or Help.
1. In McAfee ePO, select Menu | Data Protection | DLP Case Management.
2. Select the checkboxes of one or more cases.
3. Select Actions | Delete, then click Yes.
**Index**

**A**
- about this guide 5
- advanced patterns
  - creating 32

**B**
- bandwidth 22
- best practices 14

**C**
- cases
  - about 58
  - adding comments 61
  - assigning incidents 60
  - audit logs 59
  - creating 59
  - deleting 62
  - labels 62
  - sending notifications 61
  - updating 61
- classification scans
  - about 20
  - configuring 36
- classifications
  - about 24
  - creating 34
- conventions and icons used in this guide 5
- credentials 28

**D**
- data
  - classifying 25
- default ports 12
- definitions
  - credentials 28
  - dictionaries 25
  - file information 27
  - for classifications 24, 32
  - for scans 27
- McAfee DLP Discover 23
- repositories 29, 30
- scheduler 31
- text pattern 25
- dictionaries
  - about 25
  - creating 33
  - importing entries 33
- DLP data, classifying 25
- DLP Incident Manager 48
  - responding to events 47
- DLP Policy console, installing 14
- documentation
  - audience for this guide 5
  - product-specific, finding 6
  - typographical conventions and icons 5

**E**
- events
  - monitoring 47
- evidence
  - endpoint events 47
  - evidence server 17

**F**
- filters 27

**I**
- incident manager 48
- incident tasks 48, 52
- incidents
  - details 55
  - filtering 53, 54
  - labels 57
  - sorting 53
  - updating 56, 57
  - views 53
- installation 13
- inventory scans
  - about 20
  - configuring 35

**L**
- limitations 22
McAfee Agent 11
McAfee ServicePortal, accessing 6
monitoring 48

OLAP 43
operational event tasks 52
operational events 48

permission sets 39
permission sets, defining 40
policy, configuring 27

redaction
   about 41
remediation scans
   about 21
   configuring 37
repositories 29, 30
rights management 17
role-based access control 40
rules
   about 26
   for remediation scans 34

scans (continued)
   credentials 28
   inventory 20, 35
   remediation 21, 37
   repositories 29, 30
   results 43
   scheduler 31
   types of 9
scheduler 31
server tasks 52
ServicePortal, finding product documentation 6
system requirements 11

technical support, finding product information 6
text patterns
   about 25
throttling 22

upgrading 13

validators 25

Wake Up Agents 16

scans
   classification 20, 36

credentials
   inventory
   remediation
   repositories
   results
   scheduler
   types of

server tasks
ServicePortal, finding product documentation
system requirements