McAfee Data Loss Prevention 11.6.x Product Guide

Contents

Product overview

Overview

Data loss occurs when confidential or private information leaves the enterprise as a result of unauthorized communication through channels such as applications, physical devices, or network protocols.

McAfee® Data Loss Prevention (McAfee DLP) is a suite of products that protects against data loss by identifying and securing data within your network and offline. McAfee DLP policies help you understand the types of data on your network, how the data is accessed and transmitted, and if the data contains sensitive or confidential information. Use McAfee DLP to build and implement effective protection policies while reducing the need for extensive trial and error.

Each of this McAfee DLP product protects different types of data in your network.

- **McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) for Windows** — Content-based agent solution that inspects user actions. It scans data-in-use on endpoints and blocks or encrypts unauthorized transfer of data identified as sensitive or confidential. The Endpoint Discovery feature scans local file system and email storage files and applies rules to protect sensitive content.
- **McAfee® Data Loss Prevention Endpoint for Mac (McAfee DLP Endpoint for Mac)** — Offers similar protection for Macintosh computers running macOS operating systems.
- **McAfee® Device Control** — Controls the use of removable media on endpoints. Device Control contains a subset of the protection rules in McAfee DLP Endpoint for Windows and Mac.
- **McAfee® Data Loss Prevention Discover (McAfee DLP Discover)** — Scans network file, Box, SharePoint, and database repositories to identify and protect sensitive data by copying or moving the files, or by applying an RM policy. Registration scans extract fingerprint information from file repositories for file classification and store the signatures in a registered documents database.
- **McAfee® Data Loss Prevention Prevent (McAfee DLP Prevent)** — Works with your web proxy or MTA server to protect web and email traffic.
- **McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor)** — Passively scans unencrypted network traffic for potential data loss incidents.

Key features

McAfee DLP provides comprehensive protection for all potential leaking channels, including removable storage devices, the cloud, email, instant messaging, web, printing, clipboard, screenshot, and file-sharing applications.

Compliance enforcement — Ensure compliance by addressing day-to-day user actions, such as emailing, cloud posting, and downloading to removable media devices.

Advanced protection — Apply fingerprinting, classification, and file tagging to secure sensitive, unstructured data, such as intellectual property and trade secrets.

Scanning and discovery — Scan files and databases stored on local endpoints, shared repositories, or the cloud to identify sensitive data.

User education — Provide real-time feedback through educational pop-up messages to help shape corporate security awareness and culture.

Centralized management — Integrate with McAfee ePO software to streamline policy and incident management.

McAfee Device Control key features

Device Control is a McAfee® Agent plug-in available in Windows and macOS versions.

- Controls what data can be copied to removable devices, or controls the devices themselves. It can block devices completely or make them read-only.
- Provides protection for USB drives, smartphones, Bluetooth devices, and other removable media.
- Prevents executables on removable media from running. Exceptions can be made for required executables such as virus protection. (Windows version only)

McAfee DLP Discover key features

- Detects and classifies sensitive content.
- Creates registered document signature databases.
- Moves or copies sensitive files.
- Integrates with Microsoft Rights Management Service to apply protection to files.
- Automates IT tasks, such as finding blank files, determining permissions, and listing files that changed within a specified time range.
- Supports Optical Character Recognition (OCR) for classification, remediation, and registration scans of file-based repositories.

McAfee Data Loss Prevention Endpoint key features

- McAfee DLP Endpoint includes all Device Control features.
- Classification engine applies definitions and classification criteria that define the content to be protected, and where and when the protection is applied.
- Protection rules apply the classification criteria and other definitions to protect the sensitive content.
- Protects against data loss from:
  - Clipboard software
  - Cloud applications
  - Email
  - Network shares
  - Printers
  - Screenshots
  - Application file access
  - Web posts
  - Removable storage
  - Local file system files

Note

Clipboard, printers, screenshots, and web posts protection are not currently supported on macOS

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

Data Loss Prevention Endpoint for Mac key features

- McAfee DLP Endpoint for Mac includes all Device Control features.
- Classification engine applies definitions and classification criteria that define the content to be protected, and where and when the protection is applied.
- Protects against data loss from:
  - Cloud applications
  - Network shares
  - Removable storage
  - Local file system files
  - Application file access
  - Email (Monitoring only)

Data Loss Prevention Prevent key features

McAfee DLP Prevent interacts with your email and web traffic, generates incidents, and records the incidents in McAfee ePO for subsequent case review.

- Proactively enforces policies for all types of information sent over email or web.
- Enforces policies for the information you know is sensitive and the information you might not know about.
- Filters and controls sensitive information to protect against known and unknown risks.
- Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use.
- Supports Optical Character Recognition (OCR) for scanning images attached to emails. The images can also be .pdf files created by a document scanner.

Data Loss Prevention Monitor key features

- Analyzes the traffic of well-known TCP protocols to identify users or devices that send a high volume of unknown traffic, which might indicate a violation of company policy.
- Analyzes points of data loss without impacting your network to help you plan your data loss prevention strategy.
- Supports protocols that are not proxied by other email or web gateways.
- Monitors network traffic for devices that do not have McAfee DLP installed.
- Provides a wide range of built-in policies and rules for common requirements, including regulatory compliance, intellectual property, and acceptable use.
- Supports Optical Character Recognition (OCR) for scanning images attached to web posts or images found in other network traffic.

McAfee DLP Prevent and McAfee DLP Monitor appliances that have the DLP Capture feature enabled also:

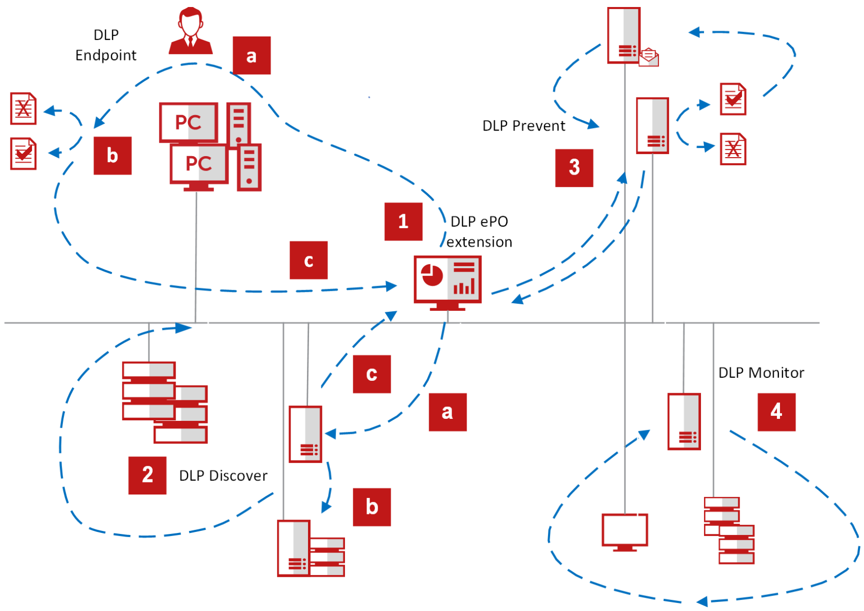
- Capture content to analyze later for keywords, user activity, or file name to identify potential data loss incidents missed by active email protection, web protection, or network communication protection rules.
- Allow complete customization of email, web, or network communication protection rules for testing using the DLP Capture database.

How it works

McAfee DLP products identify sensitive data or user activity, take action on policy violations, and create incidents of violations.

Installing all McAfee DLP products allows you to use the full feature set of the product suite. The following diagram shows a simplified network where all McAfee DLP products and McAfee ePO are deployed.

1. Administrators create policies in McAfee ePO and deploy them to McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac clients.
   a. Users create, save, and copy files or emails.
   b. McAfee DLP Endpoint client applies policies and either blocks or allows user actions.
   c. Applying the policies creates incidents that are sent to DLP Incident Manager for reporting and analysis.
2. McAfee DLP Discover scans files from local or cloud repositories and local databases, collecting file metadata.
   a. McAfee DLP Discover receives classifications and policies from McAfee DLP to apply during classification or remediation scans.
   b. DLP Server software creates registered documents databases for use in policies for McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor.
   c. Incidents from remediation scans are sent to DLP Incident Manager for reporting and analysis.
3. McAfee DLP Prevent receives email from MTA servers and web traffic from web proxy servers. It analyzes the email messages and web traffic, applies the McAfee DLP policies, and sends incidents and evidence to DLP Incident Manager.
4. McAfee DLP Monitor analyzes network traffic, then creates incidents or saves evidence for the supported protocols. It applies network communication protection rules, web protection rules, or email protection rules.



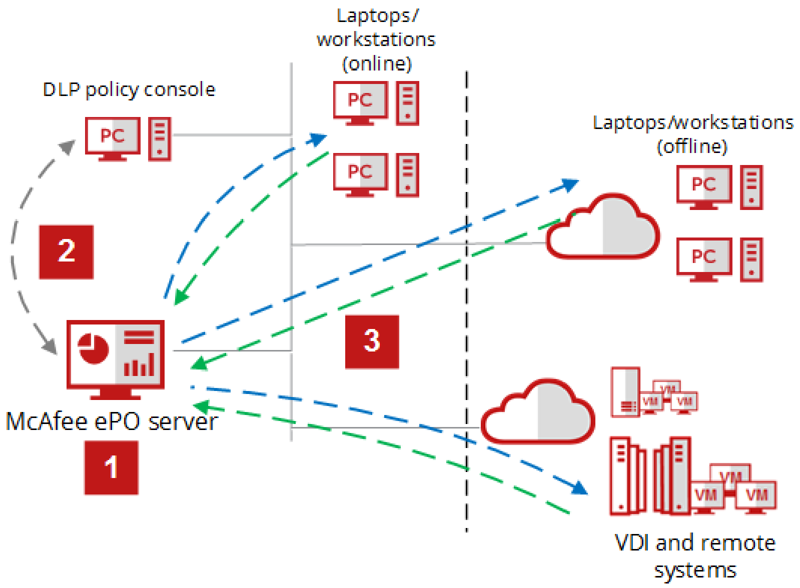
How DLP Endpoint and Device Control protect sensitive content

McAfee Device Control controls sensitive content copied to removable devices. McAfee DLP Endpoint also inspects enterprise users' actions on sensitive content when emailing, using cloud applications, and posting to websites or network shares

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

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

1. Create policies consisting of definitions, classifications, and rule sets (groups of Device Control, Data Protection, and Discovery rules) in the DLP Policy Manager and Classification consoles in McAfee ePO.
2. Deploy the policies to the endpoints.
3. Collect incidents from the endpoints for monitoring and reporting.



McAfee DLP Endpoint for Windows safeguards sensitive enterprise information using four layers of protection:

1. Device Control rules control information copied to external drives.
2. Data protection rules control data as it is used or copied to files and emails.
3. Endpoint discovery scans local file and email repositories for sensitive information.
4. Web application control rules block specified URLs by name or by reputation.

McAfee DLP Endpoint for Mac safeguards sensitive enterprise information using three layers of protection:

1. Device Control rules control information copied to external drives.
2. Data protection rules control data as it is used or copied to files.
3. Endpoint discovery scans local file repositories for sensitive information.

McAfee DLP Endpoint safeguards sensitive enterprise information:

- Applies policies that consist of definitions, classifications, rule sets, endpoint client configurations, and endpoint discovery schedules.
- Monitors the policies and blocks actions on sensitive content, as needed.
- Encrypts sensitive content before allowing the action.
- Creates reports for review and control of the process, and can store sensitive content as evidence.

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

Benefits of protecting Windows endpoints

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

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

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

Job Access With Sound (JAWS), the widely used screen reader software for the visually impaired, is supported on Windows endpoints.

Multiple user sessions

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

Endpoint console

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

The console is activated from the icon in the notification area by selecting **Manage Features** → **DLP Endpoint Console**. It can also be activated by double-clicking **DlpConsoleRunner.exe** in the `C:\Program Files\McAfee\DLP\Agent\Tools\` folder. Fully configured, it has four tabbed pages:

- **Notifications History** — Displays events, including details of aggregated events.
- **Discovery** — Displays details of discovery scans.
- **Tasks** — Generates ID codes and enter release codes for agent bypass and quarantine.
- **About** — Displays information about agent status, active policy, configuration, and computer assignment group, including revision ID numbers.

Benefits of protecting Mac endpoints

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

macOS computers can be protected with either McAfee Device Control or McAfee DLP Endpoint for Mac. Both support removable storage and plug-and-play device rules. McAfee DLP Endpoint for Mac also supports endpoint file discovery and these data protection rules:

- Application file access protection rules
- Cloud protection rules
- Network share protection rules
- Removable storage protection rules
- Email protection rules (monitoring only)

You can identify sensitive content with classifications, as on Windows-based computers, but registered documents and content fingerprinting are not supported.

Other supported features are:

- Manual classification
- Text extraction
- Evidence encryption
- Business justification definitions

Endpoint console

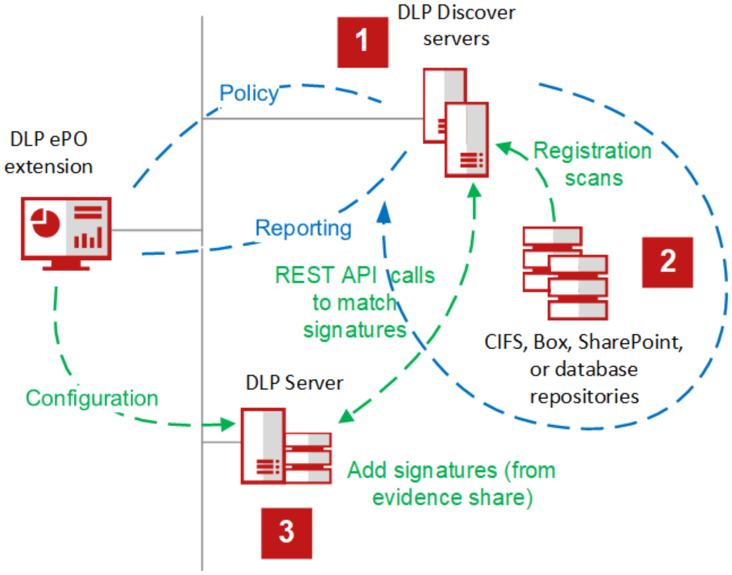
On macOS endpoints, the console is activated from the McAfee menulet on the status bar. The **Dashboard** is integrated with other installed McAfee software such as McAfee® VirusScan® for Mac, and displays an overview of the status of all installed McAfee software. The **Event Log** page displays recent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

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

How McAfee DLP Discover works

McAfee DLP Discover runs on Microsoft Windows servers and scans network file systems and databases to identify and protect sensitive files and data.

1. McAfee ePO applies policies and schedules scans.
2. McAfee DLP Discover runs the scans, collecting results, applying classifications or rules, and reporting back to McAfee DLP.
3. For registration scans, McAfee DLP Discover runs registration scans on repositories. Each scan is stored as a RegDoc package on the network evidence share. The DLP Server loads all of the RegDoc packages. McAfee DLP Discover servers (and McAfee DLP Monitor and McAfee DLP Prevent servers) match fingerprints in the RegDoc packages to rules using REST API calls for classification and remediation scans.


DLP Discover servers
1
Policy
DLP ePO extension
Registration scans
Reporting
REST API calls to match signatures
2
CIFS, Box, SharePoint, or database repositories
Configuration
DLP Server
Add signatures (from evidence share)
3

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.

McAfee ePO uses McAfee Agent to install and deploy the McAfee DLP Discover software to a Discover server — a designated Windows Server. For registration scans, where a registration database is also required, install DLP Server software. For DLP Server system requirements and installation information, see McAfee DLP Discover Installation Guide.

McAfee ePO applies the scan policy to Discover servers, which scan the repository or database at the scheduled time. The data collected and the actions applied to files depend on the scan type and configuration. For database scans, the only actions available are to report the incident and store evidence.

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

Supported repositories

File repositories:

- Box
- File Server — includes the following repository types:
  - Common Internet File System (CIFS)
  - Server Message Block (SMB)
  - Network File System (NFS) 2, 3

- SharePoint 2010, 2013, 2016, and 2019

Note

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.

Databases:

- Microsoft SQL
- MySQL, commercial editions only
- Oracle
- Db2

How different scan types protect your data

McAfee DLP Discover supports four scan types — inventory, classification, remediation, and document registration.

Inventory scans

Use inventory scans to 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. You can run inventory scans on all supported file repositories and databases.

Classification scans

Use classification scans to 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. You can run classification scans on all supported file repositories and databases.

Remediation scans

Use remediation scans to find data that is in violation of a policy. You can run remediation scans on all supported file repositories and databases.

For Box, File Server, and SharePoint scans you can monitor, apply a Rights Management policy, apply automatic classification, copy, move files to an export location, or remove automatic classifications. All actions can produce incidents that are reported to the **DLP Incident Manager** in McAfee ePO. Box scans can also change an anonymous share to one requiring logon.

For database scans, you can monitor, report incidents, and store evidence.

Registration scans

Use document registration scans to extract content from files based on selected fingerprint criteria, and save the data to a signature database.

The registered documents can define classification and remediation scans, or policies for McAfee DLP Prevent and McAfee DLP Monitor. You can run document registration scans only on supported file repositories, not on databases. More than one document registration scan can potentially pick up a particular file. In that case, it is classified based on more than one set of criteria, and its signatures are recorded in more than one registered document.

How McAfee DLP Prevent protects email traffic

McAfee DLP Prevent integrates with any MTA that supports header inspection. It analyzes the email messages and applies McAfee DLP policies.

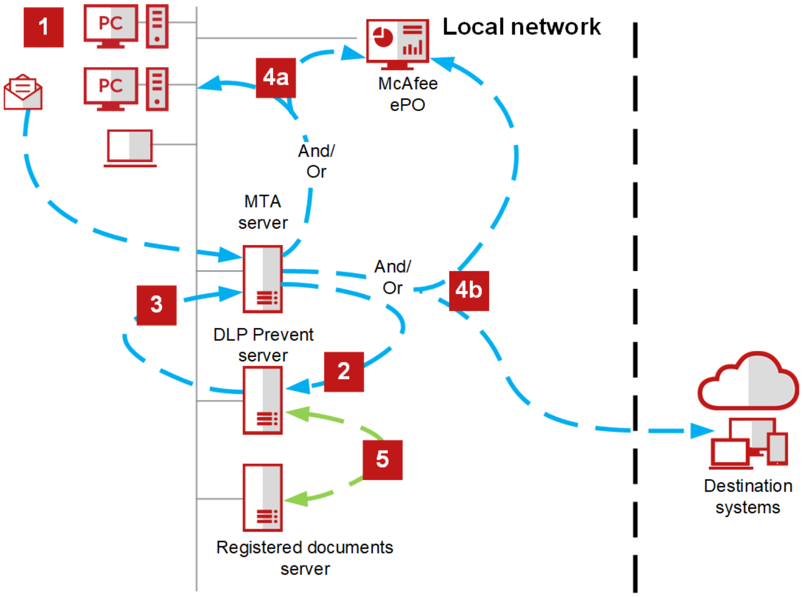
1. **Users** — Incoming or outgoing email messages go to the MTA server.
2. **MTA server** — Forwards the email messages to McAfee DLP Prevent
3. **McAfee DLP Prevent** — Receives SMTP connections from the MTA server and:
    - Decomposes the email message into its component parts
    - Extracts the text for fingerprinting and rule analysis
    - Analyzes the email message to detect policy violations
    - Based on the rule that is set, McAfee DLP Prevent takes one of these actions:
        - Blocks the email message and sends a notification to the Smart Host (MTA server).
        - Adds an X-RCIS-Action header and sends the message to the configured Smart Host (MTA server).

    Note

    > In this example, the configured Smart Host is the original MTA.

4. **MTA server** — Forwards the email message to intended recipient or returns the email message:
    a. When the email message is blocked, Smart Host (MTA server) returns the email message to the sender as an attachment with a notification. Optionally, you can configure to send an incident to McAfee ePO.
    b. When an X-RCIS-Action header is added, based on information it gets from the X-RCIS-Action header, the Smart Host (MTA server) acts on the email message. Optionally, you can configure to send an incident to McAfee ePO.
5. **Registered documents server** — It is a way to define sensitive information, to protect it from being distributed in unauthorized ways.

McAfee DLP Prevent email traffic flow



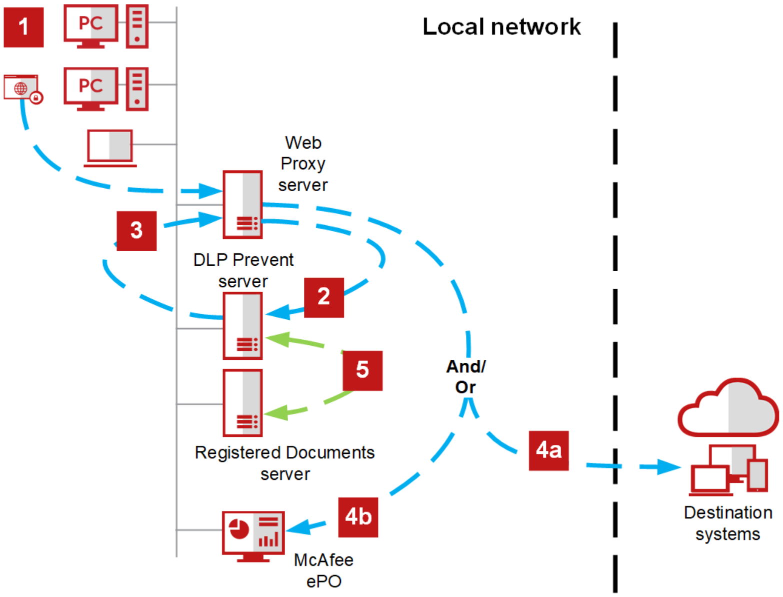
How McAfee DLP Prevent protects web traffic

McAfee DLP Prevent receives ICAP connections from a web proxy server, analyzes the content, and determines if the traffic should be allowed or blocked.

How it works

1. Users send web traffic to the web proxy server.
2. The web proxy server forwards the web traffic to McAfee DLP Prevent.
3. McAfee DLP Prevent inspects the web traffic, and returns a response to the web proxy server to allow the traffic through to the destination server or deny access.
4. 4a/4b — Based on the information from McAfee DLP Prevent, the Web Proxy server:
   - Sends or delivers the inspected web traffic to the appropriate destinations.
   - Blocks the web traffic and sends an event to McAfee ePO.
5. Registered documents server defines sensitive information, to protect it from being distributed in unauthorized ways.

McAfee DLP Prevent web traffic flow

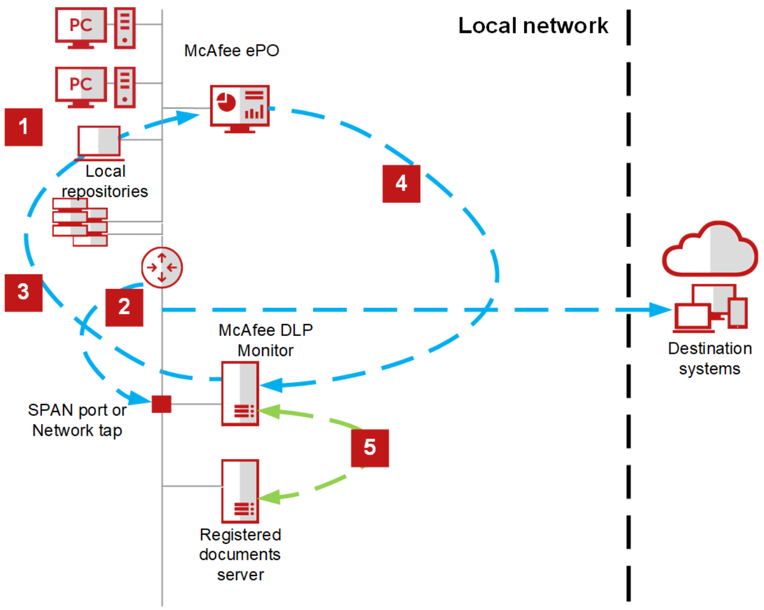


How McAfee DLP Monitor inspects live network traffic

Use McAfee DLP Monitor to learn about the quantity and types of data transferred across the network. McAfee DLP Monitor does not block or change network traffic, so you can integrate it into a production environment without impacting live traffic.

1. The router receives network packets from internal users and servers.
2. McAfee DLP Monitor connects to either a Switched Port Analyzer (SPAN) port or a network tap to passively monitor live traffic received from the router.
3. McAfee DLP Monitor receives copies of network packets and analyzes them. Sends incidents to McAfee ePO.
4. McAfee ePO sends policy to McAfee DLP Monitor.
5. Registered documents server defines sensitive information to protect it from being distributed in unauthorized ways.

McAfee DLP Monitor network analysis flow



Types of protection rules

McAfee DLP Monitor can apply one of these McAfee DLP protection rules to your network traffic.

- **Email Protection** — By default, McAfee DLP Monitor inspects SMTP traffic using email protection rules, which incorporate protocol-specific information such as sender and recipient email addresses.
- **Web Protection** — By default, McAfee DLP Monitor inspects HTTP and FTP traffic using web protection rules, which incorporate protocol-specific information such as the URL.
- **Network Communication Protection** — McAfee DLP Monitor can inspect all supported traffic using network communication protection rules, which do not incorporate any protocol-specific information.

If you don't want to analyze SMTP, HTTP, or FTP traffic with email and web protection rules, you can configure McAfee DLP Monitor to use network communication protection rules. To disable the analysis of SMTP, HTTP, or FTP traffic, go to **Menu** → **Policy Catalog** → **DLP Appliance Management** → **McAfee DLP Monitor Settings** and deselect the options in the **Protocol Rule Application** field.

Note

Using **Email Protection** and **Web Protection** rules allows you to share rules with McAfee DLP Prevent.

Supported protocols

- SMTP*
- IMAP*
- POP3*
- HTTP
- LDAP
- Telnet

- FTP
- IRC
- SMB**

McAfee DLP Monitor can also analyze traffic that is encapsulated in SOCKS.

* These protocols support STARTTLS (plain text initial connection converted to TLS/SSL after STARTTLS command). McAfee DLP Monitor treats these protocols as encrypted and does not analyze them if STARTTLS is used.

** Data transferred using SMB might be encrypted depending on the version of the protocol and your configuration.

Note

> McAfee DLP Monitor does not analyze the content of encrypted connections directly. You can use a dedicated gateway (for example, the SSL Tap feature in Web Gateway), to intercept the encrypted connection and send the decrypted data to McAfee DLP Monitor for analysis. See the documentation for your gateway for information. If McAfee DLP Monitor can't classify a connection as a known protocol, it shows the connection as unknown.

McAfee DLP and data vectors

Each McAfee DLP product collects data and categorizes it by vectors — *Data in Motion*, *Data at Rest*, and *Data in Use*.

Data vector	Description	Products
Data in Use	The actions of users on endpoints, such as copying data and files to removable media, printing files to a local printer, and taking screen captures.	• McAfee DLP Endpoint • McAfee Device Control
Data in Motion	Live traffic on your network. Traffic is analyzed, categorized, and stored in the McAfee ePO database.	• McAfee DLP Prevent • McAfee DLP Monitor
Data at Rest	Data residing in file shares, databases, and repositories. McAfee DLP can scan, track, and perform remedial actions on Data at Rest.	• McAfee DLP Discover • McAfee DLP Endpoint discovery

How DLP interacts with other McAfee products

McAfee DLP integrates with other McAfee products, increasing the functionality of the product suite.

McAfee ePO — All McAfee DLP products integrate with McAfee ePO for configuration, management, monitoring, and reporting.

McAfee® File and Removable Media Protection (FRP) — Integrates with McAfee DLP Endpoint for Windows to encrypt sensitive files.

McAfee® Logon Collector — Integrates with McAfee DLP Monitor and McAfee DLP Prevent for user authentication information.

McAfee® Web Gateway — Integrates with McAfee DLP Prevent to provide web protection.

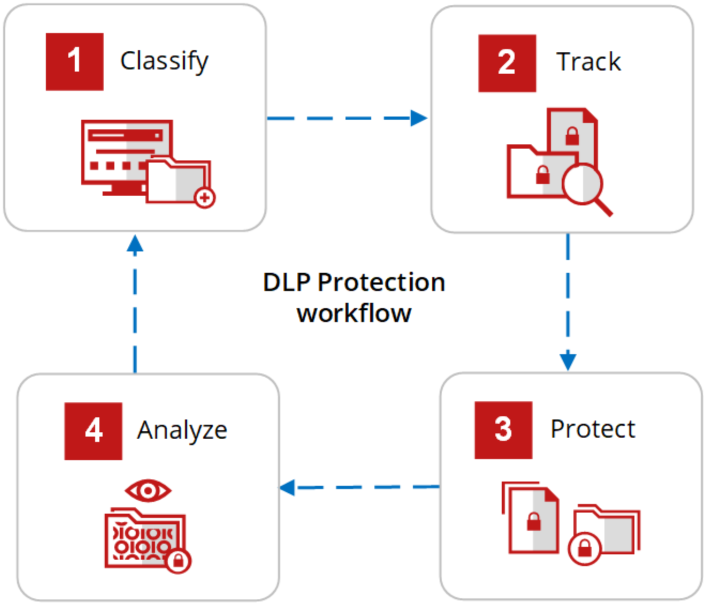
McAfee® MVISION Cloud — Synchronizes classifications with MVISION Cloud, pulls incidents to the DLP Incident Manager.

How data protection works

Workflow for protecting sensitive data with McAfee DLP

McAfee DLP features and policy components make up a protection process that fits into this overall workflow.

The McAfee DLP protection process



Use McAfee DLP to monitor the data and user actions on the network. You can use predefined rules or create a basic policy.

1. Create classifications from the **Classification** console.

   Classify and define sensitive data by configuring classifications and definitions. For more information, see Classifying your data

2. Track how and where the files containing sensitive content are used with tags or registered documents. For more information, see Tracking how and when sensitive content is used.
3. Protect sensitive data by applying rules with **DLP Policy Manager**.

   Protect data with scans and rules. Configure the action to take when sensitive data is discovered, accessed, or transmitted. For more information, see Protecting sensitive data with rules and policies.

4. Analyze the McAfee DLP incidents from **DLP Incident Manager**.

   Review incidents and analyze scan results to see potential policy violations. Use this information to begin creating an effective policy. You can manage the incidents by grouping and working with incidents, which can be escalated to other departments, such as legal or Human Resources. You can also create reports with dashboards and queries. For more information, see Reviewing and managing incidents to fine-tune your policies.

Getting Started with DLP — The **DLP Getting Started** feature enables you to configure any of the McAfee DLP products quickly and run the policies immediately after installation. This option allows you to add license and shared network location details, and create your first McAfee DLP rule and policy.

For more information, see *Getting started with DLP* in the Installation Guide.

Classifying your data

To protect sensitive content, start by defining and classifying sensitive information that needs to be protected.

Content is classified by defining classifications and classification criteria. Classification criteria defines the conditions on how data is classified. Methods to define criteria include:

- **Advanced patterns** — Regular expressions combined with validation algorithms, used to match patterns such as credit card numbers. Advanced patterns are ranked according to a score, meaning, the number of times the sensitive expressions need to appear in the content for the rule to be triggered. The Classifications editor includes several built-in advanced patterns for ensuring compliance with government regulations and simplifying detection of personal information. You can also create your own advanced patterns.
- **Dictionaries** — Lists of specific words or terms, such as medical terms for detecting possible HIPAA violations.
- **Keywords** — A string value that defines sensitive data. You can add multiple keywords for content classifications. Keywords are not consistent across classifications. If you need to use consistent keywords across classifications, use a dictionary.
- **File size** — The size of the file to detect the sensitive data. You can also define a file size range.
- **True file types** — The true file type to determine which files to identify the sensitive data. True file type helps detect attachment violations when file extensions are renamed and sent as attachments. For example, a .cpp file saved as a .txt file can be detected using the true file type classification criteria.
- **File extension** — The file types to detect the sensitive data, such as MP3 and PDF.
- **Source or destination location** — URLs, network shares, or the application or user that created or received the content.
- **Location in file** — The section of the file to look for the sensitive content; Header, Footer, Body or within the first characters. Specifying the number of characters for the **within first (characters)** option in a classification looks for the sensitive content in the Header, that is, in the first part of the first page in a document.
-
    - Microsoft Word documents - Header, body and footer is identified.
    - PowerPoint documents - WordArt is considered Header, everything else is identified as Body.
    - Other documents - Only Body is applicable.

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

Tracking how and when sensitive content is used

McAfee DLP can track content based on storage location or the application used to create it.

The mechanisms used to track content are:

- Content fingerprinting — Supported on McAfee DLP Endpoint for Windows and McAfee DLP appliances.
- Registered documents — Supported on all McAfee DLP products except McAfee DLP Endpoint for Mac.

Note

> Only Manual registration, performed in the **Classification** module, is supported on McAfee DLP Endpoint for Windows, McAfee DLP Prevent, and McAfee DLP Monitor.
> Automatic registration, performed by McAfee DLP Discover registration scans, is supported on McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor.

- Manual classifications — Created by McAfee DLP Endpoint and McAfee DLP Endpoint for Mac users, but supported on all McAfee DLP products.

Content fingerprinting

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

Support for persistent fingerprint information

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

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

Note

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

Registered documents

The registered documents feature is based on pre-scanning all files in specified repositories (such as the engineering SharePoint) and creating signatures of fragments of each file in these repositories. McAfee DLP Endpoint and the network McAfee DLP products use registered documents, but differ in the way the signatures of files are distributed.

Manual registration in McAfee DLP Endpoint for Windows — Signatures of the files are uploaded to McAfee ePO from when you manually upload files and create a package. These signatures are made available and downloaded by the endpoints from the shared location. The McAfee DLP Endpoint client is then able to track any content copied from one of these documents and classify it according to the classification of the registered document signature.

Manual registration in McAfee DLP network products — Signatures of the files are uploaded to McAfee ePO from McAfee DLP when you manually upload files and create a package. A package of these signatures of files is saved in an evidence share. These signatures are made available and downloaded by the appliances from the shared location. The appliance is then able to track any content copied from one of these documents and classify it according to the classification of the registered document signature.

Automatic registration in McAfee DLP network products — McAfee DLP Discover runs registration scans on file repositories. The signatures created are stored in signature databases on servers designated as **DLP Servers**. McAfee DLP Discover uses them to create classification and remediation scans. McAfee DLP Prevent and McAfee DLP Monitor use them to define rules.

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

Tip

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

Manual classification

When working with manual classification, you have the option of applying content fingerprints or content classifications to files. Manually applied content fingerprinting is identical to the automatically applied fingerprinting described previously.

Manually applied content classifications embed a physical tag in the file which can be used to track the file wherever it is copied, but do not create signatures. Content copied from these files into other files can't be tracked.

Manual classification is supported on Microsoft Windows and macOS computers. If you try to classify a file type that doesn't support tagging (for example, TXT files), an error message displays.

Protecting sensitive data with rules and policies

Create rules to identify sensitive data and take appropriate action.

Rules and rule sets

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

-

Data Protection rules — Data protection rules are used to prevent unauthorized distribution of classified data. When you try to copy classified data, or attach it to an email, McAfee DLP intercepts the attempt and uses the data protection rules to determine which action to take. For example, if the rule action requires a business justification, McAfee DLP Endpoint halts the attempt and displays a dialog box. When the user inputs the justification for the attempt, processing continues.

- McAfee DLP Endpoint uses several rules to inspect user actions. It scans data-in-use on endpoints and blocks unauthorized transfer of data identified as sensitive or confidential.
- McAfee DLP Prevent uses web and email protection rules to monitor and take action on communication from an MTA server or web proxy server.
- McAfee DLP Monitor can apply the network communication protection, email protection, or web protection rules to analyze supported traffic on your network.
- McAfee Device Control uses only removable storage data protection rules.

-

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

-

Application control rules — Application control rules block the application rather than blocking the content. For example, a web application control rule blocks a specified URL by name or by reputation.

-

Discovery rules — **Discovery** rules are used for file and data scanning. **Endpoint Discovery** is a crawler that runs on managed computers. It scans the local endpoint file system and the local email (cached) inbox and PST files. Local file system discovery rules define whether the content is to be quarantined, encrypted, content fingerprinted, or have an RM policy or classification applied. Local emails can be quarantined or content fingerprinted. These rules can also define whether an incident is reported, and whether to store the file or email as evidence included in the incident.

Note

File system scans are not supported on server operating systems.

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

Policies

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

Reviewing and managing incidents to fine-tune your policies

You can review, analyze, and manage incidents for policy violations that have occurred. These functions include:

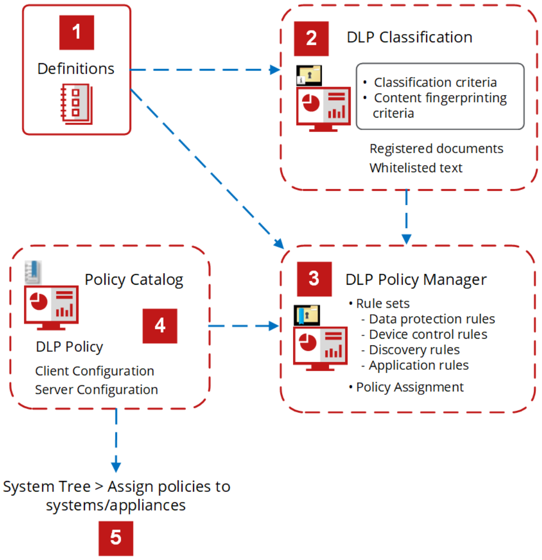
- **Incident management** — Incidents are sent to the McAfee ePO Event Parser and stored in a database. Incidents contain the details about the violation, and can optionally include evidence information. You can view incidents and evidence as they are received in the **DLP Incident Manager** console.
- **Case management** — Group-related incidents into cases for further review in the **DLP Case Management** console.
- **Operational events** — View errors and administrative events in the **DLP Operations** console.
- **Evidence collection** — For rules that are configured to collect evidence, a copy of the data or file is saved and linked to the specific incident. This information can help determine the severity or exposure of the event. Evidence is encrypted using the AES-256 algorithm before being saved.
- **Hit highlighting** — Evidence can be saved with highlighting of the text that caused the incident. Highlighted evidence is stored as a separate encrypted HTML file.
- **Reports** — Reports, charts, and trends are created in McAfee ePO dashboards.

Policy workflow to protect sensitive data

McAfee DLP products use a similar workflow for creating policies. A policy consists of rules, grouped into rule sets. Rules use classifications and definitions to specify what McAfee DLP detects. Rule reactions determine the action to take when data matches the rule.

Use this workflow for creating and applying policies:

How policy components make up a policy



1	**Create definitions** — Used to create classifications and rules.
2	**Create a classification** — Define categories of sensitive data by creating classifications. Classifications are used by rule sets to define the data protection rule. • Content fingerprinting criteria and whitelisted text — Supported in McAfee DLP Endpoint for Windows only. • Registered documents — Created in the Classification console (manual registration) for McAfee DLP Endpoint for Windows clients and McAfee DLP appliances. • Classification criteria — Used to create definitions to identify sensitive text patterns, dictionaries, and keywords. Not supported with McAfee Device Control.
3	**Create a rule set** and **Create a rule** — Rule sets can combine multiple data protection rules for improved coverage of data protection. Create a rule and its actions and add it to a rule set.
4	**Assign rule sets to policies** — A policy can have multiple rule sets. Before you apply rule sets to a policy, activate the rule sets. Assign the rule sets to the policy and then apply the required rule sets to the policy.
5	**Assign and push a policy to a system** — McAfee DLP policies are assigned to endpoints and McAfee DLP appliances from **System Tree**. You can use the **Wake Up Agents** option or the **Break inheritance and assign the policy and settings below** option to push a policy to a system.

The options and availability for these components vary depending on which McAfee DLP product you use.

Use case: Data loss prevention policy workflow to block email attachments with sensitive data

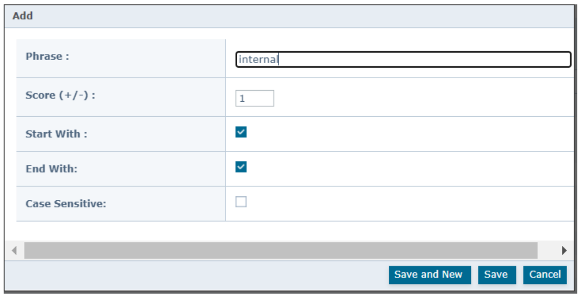
This section describes all step-by-step tasks that you need to perform to create and apply a policy to block email attachments with sensitive data. McAfee DLP Prevent can use file extension or true file type in classification criteria to block email attachments with sensitive data. You can also use these classifications to block attachments sent in web posts or network.

Consider that you have some architecture and planning diagrams of your business solution in Autocad and Visio formats, which you have saved in a shared location. The administrator wants to block all Autocad or Visio attachments with sensitive data from going outside the network. You can use these steps to block attachments for these specific extensions and prevent any data loss.

1. Create a definition or choose a built-in definition. (See Step 1 in the following task)
2. Create a classification and classification criteria. (See Step 2 in the following task)
3. Create a rule set and rules. (See Step 3 in the following task)
4. Assign rule sets to policy. (See Step 4 in the following task)
5. Assign and push policy to system. (See Step 5 in the following task)

Task

1. Choose a built-in definition or create a definition to include phrases that must be tracked.
   a. In McAfee ePO, go to **Menu** → **Data Protection** → **Classification** and select **Definitions**.
   b. Select **Dictionary**, click **Action** → **New Item**, give the dictionary definition a name and an optional description, then click **Action** → **Add**. You can also use an existing dictionary.
   c. In **Phrase**, type the word `internal`, then set the Score as `1` and select **Case Sensitive** to only match on the keyword when it is lowercase. To add multiple phrases, you can click **Save and New**.



Add

Phrase : internal

Score (+/-) : 1

Start With : ☑

End With: ☑

Case Sensitive: ☐

   d. Click **Save**.
2. Create a classification and classification criteria. You can also edit an existing classification.
   a. Select **Classification**.
   b. Click **Actions**, then click **New Classification** and type a unique name and an optional description. Select **Save Classification** in the **Actions** menu.
   c. In the right pane, click **Actions**, then select **New Content Classification Criteria** and type the classification criteria name.
   d. In the **Data conditions** properties, click to select **Dictionary** and add the dictionary that you created.
   e. In the **File conditions** properties, click to select **File Extensions** and **True File Type**.
      Classification criteria with true file type helps detect attachment violations when file extensions are renamed and sent as attachments. For example, a .cpp file saved as .txt file can be detected using the true file type classification criteria.
   f. For the **File Extensions** property, click the select icon (...) to open the **Choose from existing values** window. Choose all file types that you want to block. To add more values, click **+**.
   g. For the **True File Type** property, click the select icon (...) to open the **Choose from existing values** window. Choose all file types that you want to block. To add more values, click **+**.
   h. Click **Save**.
3. Create a rule set that includes an **Email Protection** rule and add the classification criteria that you created.
   a. Go to **Menu** → **Data Protection** → **DLP Policy Manager**.
   b. Click **Actions** → **New Rule Set**. Enter a name for the rule set and provide a description for your reference. Click **OK**.
      A new rule set is created. Click the rule set and then create a new rule.
   c. Click **Actions** → **New Rule** → **Email Protection** rule.
   d. Type the rule name and optionally enter the description. Select the state as **Enabled** and click the checkbox to select **McAfee Network DLP** to enforce the policy on.
   e. In the **Conditions** tab, in **Classification of**, select **one of the attachments (*)** and **contains one of (OR)**, and then select the classification criteria you created.
   f. Set the **Recipient** to any recipient (ALL).

   g. In the **Reactions** tab, set the reaction you want to take when the rule gets triggered. Set the **Action** to **Block and return email to sender**, then select the appropriate **User Notification**. Click **Save**.

4. Assign rule sets to a policy. Before you assign rule sets to a policy, activate the rule set.
   a. Go to **Menu** → **Policy** → **Policy Catalog**.
   b. In the **Product** drop down list, select **Data Loss Prevention <version>** and select **DLP Policy**.
   c. Click the **Edit** link of the policy you want to update.
   d. In the policy page, go to **Active Rule Sets** → **Actions**, then click **Activate Rule Set**.
      The **Activate Rule Set** window opens.
   e. Select the checkboxes of one or more rule sets that you want to apply to the policy.
   f. Click **OK** and click **Apply Policy**.
      McAfee DLP displays the status of the policy applied.
5. Assign and push the policy to McAfee DLP appliances.
   a. Go to **Menu** → **Systems** → **System Tree**.
   b. Select the checkbox of one or more McAfee DLP Prevent appliances (target system) that you want to assign the policy to.
   c. Click **Wake Up Agents** to push the policy to McAfee DLP appliances immediately.
      The **Wake Up McAfee Agent** window opens.
   d. Next to **Wake-up call type**, select whether to send an **Agent Wake-Up Call** or a **SuperAgent Wake-Up Call**.
   e. Accept the default **Randomization** (0–60 minutes) or type a different value.
      If you type 0, agents respond immediately.
   f. Click **OK** to send the wake-up call to the target appliances.

   Alternatively, you can use the **Break inheritance and assign the policy and settings below** option to push the policy. For information, see Assign and push a policy to a system.

Results

The appliance is now set with policy to block email attachments with sensitive data.

Configuring system components

Participating in the McAfee DLP appliances Product Improvement Program

The Product Improvement Program (PIP) capability or the secure product telemetry framework, when enabled allows McAfee to collect data. You can choose to participate in the McAfee DLP appliance product improvement program and allow McAfee to collect data through McAfee Agent.

Purpose

McAfee uses the McAfee DLP appliances data that is collected through McAfee Agent. The data collected is:

- Analyzed by McAfee to improve product features and customers' experience with the product.
- Used by McAfee Technical Support for troubleshooting.

Privacy protection

The McAfee DLP appliances data collected by McAfee Agent is only for product improvement and Technical Support. The system-specific data is filtered or used in aggregate form, unless it is needed for Technical Support. For details about McAfee Privacy Notice, see https://www.mcafee.com/enterprise/en-us/about/legal/privacy.html.

Enable Product Improvement Program on McAfee ePO to collect data

You can configure the McAfee ePO server settings to enable Product Improvement Program capability.

Task

1. Click **Menu** → **Configuration** → **Server Settings**, select **Product Improvement Program** from the **Setting Categories**, then click **Edit**.
2. Select **Yes** to allow McAfee to collect anonymous diagnostic and usage data.
3. Click **Save**.

Results

Enforce policy to enable the PIP capability on McAfee DLP appliances

You can manage Product Improvement Program (PIP) on McAfee DLP appliances using the McAfee Agent PIP policy.

Before you begin

Make sure you enable the Product Improvement Program server settings before enforcing the policies.

Task

1. Click **Menu** → **Systems** → **System Tree**, then select a group in the **System Tree**.
   All systems within this group (but not its subgroups) appear in the details pane.
2. Select the needed appliances, then click **Actions** → **Agent** → **Set Policy & Inheritance**.
3. Select **McAfee Agent** as the **Product**, **Product Improvement Program** as the **Category**, then select the required policy.
4. Select whether to **Reset inheritance** or **Break inheritance**, then click **Save**.

Configurations and policies in Policy Catalog for McAfee DLP

McAfee DLP products use the Policy Catalog in McAfee ePO to store policies and client configurations.

Policies are assigned to endpoints in the McAfee ePO **System Tree**.

- **DLP Policy** — Contains **Active Rule Sets** assigned to the policy, scheduled **Endpoint Discovery** scans, **Settings** for application strategy, device class overrides, and privileged users, and **Policy Validation**.
- **Server Configuration** — Contains the McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor configurations. Allows you to set the evidence copy service and logging options, Rights Management and SharePoint settings, and text extractor options.

Note

> You must create separate server configurations for each of your McAfee DLP products. The server configuration appears only if a McAfee DLP Discover, McAfee DLP Prevent, or McAfee DLP Monitor license is registered.

McAfee DLP Prevent and McAfee DLP Monitor use only the **Shared Storage and Evidence** and **OCR** section of the server configuration.

McAfee DLP Discover uses all sections except **ActiveSync Proxy**.

- **Client Configurations** — Separate configurations for Microsoft Windows and macOS computers contain the configuration settings for the McAfee DLP Endpoint clients. The settings determine how clients apply McAfee DLP policies on the endpoints. Enable the **Evidence Copy Service** for McAfee DLP Endpoint products in the client configuration.

Note

> Client configurations appear only if a license for McAfee DLP Endpoint is registered.

Windows client configuration

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

Note

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

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

Client Service WatchDog

Note

> The Client Service WatchDog is not supported on McAfee DLP Endpoint for Mac.

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

Whitelists in the client configuration

Whitelists in the client configuration exclude the listed processes, extensions, or URLs from rules.

Setting	Whitelist	Description
Clipboard Protection Applies to Windows clients only	Whitelisted Processes	McAfee DLP Endpoint ignores clipboard operations performed by the listed applications
Content Tracking Applies to both Windows and macOS clients	Whitelisted Processes	McAfee DLP Endpoint ignores access to files performed by the listed applications
Printing Protection Applies to Windows clients only	Whitelisted Processes	McAfee DLP Endpoint ignores printing actions performed by the listed applications
Web Protection Applies to Windows clients only	Whitelisted URLs	Lists URLs excluded by the browser plug-in from all web protection rules. You can add multiple whitelists by domain or IP address range.

Client configuration settings

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

Tip

To verify that the client configuration settings continue to meet your requirements, review them at regular intervals.

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

Endpoint configuration

Setting	Details	Description
Advanced Configuration	**Run DLP client in Safe Mode** Applies to Windows clients only	Disabled by default. When enabled, McAfee DLP Endpoint is fully functional when the computer is started in Safe Mode. A recovery mechanism exists in case the McAfee DLP Endpoint client causes a boot failure.
	DLP access protection	When enabled, activates the DLP data access protection features. **Default:** Enabled in both Device Control and full McAfee DLP Endpoint.
	Show challenge response on upgrade Applies to both Windows and macOS clients	When enabled, activates the challenge/response pop-up window on upgrade.
	Show challenge response on uninstall	When enabled, activates the challenge/response pop-up window on uninstall.
	Run DLP client watch dog Applies to both Windows and macOS clients	When enabled, monitors the endpoint processes and restarts them if closed. Changing this setting requires a client computer restart.
	Run DLP client service watch dog Applies to both Windows and macOS clients	When enabled, monitors the watch dog and restarts it if it closes. Changing this setting requires a client computer restart.

Setting	Details	Description
	Agent Bypass Applies to both Windows and macOS clients	Stops the agent bypass when a new client configuration is loaded. Deselected by default.
Content Tracking Applies to both Windows and macOS clients	**Use the following fallback ANSI code page**	If no language is set, the fallback is the default language of the endpoint computer.
Corporate connectivity Applies to both Windows and macOS clients	**Corporate Network Detection** **Corporate VPN Detection**	You can apply different prevent actions to endpoint computers in the corporate network or outside the network. For some rules, you can apply different prevent actions when connected by VPN. To use the VPN option, or to determine network connectivity by corporate server rather than by connection to McAfee ePO, set the server IP address in the relevant section.
Device Control	**iPhone Protection Mode**	Allows or prevents charging iPhones when the device rule action is **Block**.
	Device Control Settings	Allows the administrator to choose whether to apply Device Control policies immediately when the policy is applied, or to apply them only when the computer is restarted or the device is physically or logically enabled or disabled.
Debugging and Logging	**Log DLP events to external HTTP server**	Use these settings to configure the server receiving raw data from the McAfee DLP Endpoint client.
	Syslog Server Settings	Stores the Syslog server path. Syslog can be used for logging certain types of McAfee DLP events.
Email Protection Applies to Windows clients only	**Email Caching**	Stores tag signatures from emails to disk to eliminate re-parsing emails.
	Email recipients	Sets the maximum number of email recipients to report. Default is 10.

Setting	Details	Description
	Email Handling API	Outgoing email is handled by either Outlook Object Model (OOM) or Messaging Application Programming Interface (MAPI). OOM is the default API, but some configurations require MAPI.
	Outlook 3rd party add-in integration	Sets integration with either Titus or Bolden James email classification software.
	Outlook Background Processing (Only for McAfee DLP Endpoint 11.6 or later)	Enable background processing of emails to reduce user impact when sending emails using Microsoft Outlook. Set the maximum amount of time allowed to analyze the emails. • Maximum time allowed to analyze - 600 seconds • Maximum time allowed to analyze in foreground - 120 seconds Enable a pop-up message that allows the end-user to either review a blocked email or to discard it. Enabling this pop-up message overrides the notification configurations defined in the Email Protection rule. Set the action taken to either send the email or to block it if the analyzing time exceeds.
	Email Timeout Strategy (Applicable for McAfee DLP Endpoint lower than 11.6 when Outlook Background Processing is enabled.)	Sets the maximum time to analyze an email and the action if the time is exceeded.
	Outgoing Email User Notification (Applicable for McAfee DLP Endpoint lower than 11.6 when Outlook Background Processing is enabled.)	Sets the end user notification message and when it is displayed.

Setting	Details	Description
Shared Storage and Evidence Applies to both Windows and macOS clients	**Shared Storage**	Replace the example text with the evidence storage share. Specify this path to store: • Evidence files • File with classification matches • Registered document fingerprints For Manual Registered Document, the fingerprints are copied to all available evidence share. (Applicable only to McAfee DLP Endpoint for Windows.) • Package containing ignored texts. (Applicable only to McAfee DLP Endpoint for Windows.) • Endpoint discovery scan summary in CSV file format
	Client Settings	You can change the way hit highlighting is displayed by setting classification matches to all matches or abbreviated results.
	Incident Information	You can hide or display the short match string in the incident details. The setting works in real time, that is, if you change the setting, it only affects the display for incidents collected from that point forward.
Operational Mode and Modules Applies to both Windows and macOS clients	**Operational Mode**	Set Device Control or full McAfee DLP Endpoint mode. Reset this parameter if you upgrade or downgrade licensing.
	Data Protection Modules	Activate required modules. **Tip:** To improve performance, deselect modules you are not using.
Operational Mode and Modules Applies to Windows clients only	**Browsers**	Enables the browsers you want to block or monitor data upload when using **Web Protection** rules. Supported browsers are Microsoft Internet Explorer, Google Chrome, Microsoft Edge (Chromium-based), and Mozilla Firefox. Default: All browsers are selected.

Setting	Details	Description
		Note: We recommend not allowing Chrome guest and incognito mode to end-users. If either of these options are allowed, the active web URL on the endpoint might be unavailable to the McAfee DLP client.
	Browser Address Bar URL detection	This feature is used to control a major cause of high CPU utilization. The default is to enable browser address bar URL detection. If high CPU utilization is encountered, you can disable the feature.
Plug and Play Applies to Windows clients only	**iPhone Protection Mode**	Selects whether or not a blocked iPhone can be charged. This setting applies to plug and play device rules.
Web Protection Applies to Windows clients only	**Web protection evaluation**	Select inputs for web request evaluation when matching web protection rules. These settings allow blocking requests sent by AJAX to a different URL from the one displayed in the address bar. At least one option must be selected.
	Process HTTP GET requests	GET requests are disabled by default because they are resource-intensive. Use this option with caution.
	Web Timeout strategy	Sets the web post analysis timeout, action to perform if timeout is exceeded, and optional user message.
	Whitelisted URLs	Create URL whitelists and select which list to exclude from web post protection rules.

Troubleshooting guidance for McAfee DLP Endpoint

Use the **Troubleshooting** page in Windows client configuration for tips and guidance on actions that you can take to troubleshoot performance issues and tune policies in McAfee DLP Endpoint.

Configure Outlook background processing time for Email Protection

You can enable background processing of emails to reduce user impact when sending emails using Microsoft Outlook. Set the maximum amount of time allowed to analyze the emails.

Note

Currently background processing is applicable when the end-user clicks **New Email** in Outlook to send an email. When an end-user sends an email from quick menus, My Tasks, Invitations, etc., these emails are only processed in the foreground according to the time set in **Windows Client Configuration** → **Email Protection** → **Email Timeout Strategy** → **Email analysis maximum time (sec)**. The action for the end-user to take if the email processing time is exceeded is set from **Windows Client Configuration** → **Email Protection** → **Outlook Background Processing** → **Action performed if maximum time is exceeded**.

The Outlook background processing feature is supported in McAfee DLP Endpoint for Windows 11.6 or later.

Task

1. In McAfee ePO, select **Menu** → **Policy** → **Policy Catalog**
2. Select **Data Loss Prevention <version>** and select the **Windows Client Configuration** to edit.
3. On the **Email Protection** page, select **Enable Background Processing**.
4. Select the maximum amount of time, in seconds, the emails are analyzed. Use the slider to determine how much of the time selected is for analyzing emails in the foreground and the background.
   We recommend analyzing emails in the foreground for 3–5 seconds. If email processing is not completed in the foreground, analysis is moved to the background and end-users can continue working in Outlook. Only set foreground analysis time to zero if all your Email Protection rules are set with **No Action**.
5. Enable a pop-up message where end-users can choose to either review an email that is blocked or to discard it.
   Enabling this pop-up message overrides the notification configurations defined in the Email Protection rule.
6. If the email processing time is exceeded, you can set to either allow this email to be sent or to block the email. If you select to block the email, end-users receive a pop-up message that email analysis exceeded maximum time and the email is blocked. You can edit this message, if needed.

Support for client configuration parameters

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

Debugging and Logging page

Parameter	Operating system support
Administrative events reported by the clients	The filter settings that apply to both McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac are: • **Client Enters Bypass Mode** • **Client Leaves Bypass Mode**

Parameter	Operating system support
	- **Client Installed** All other settings apply to McAfee DLP Endpoint for Windows only.
Logging	Supported on both McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac.

User Interface Components page

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

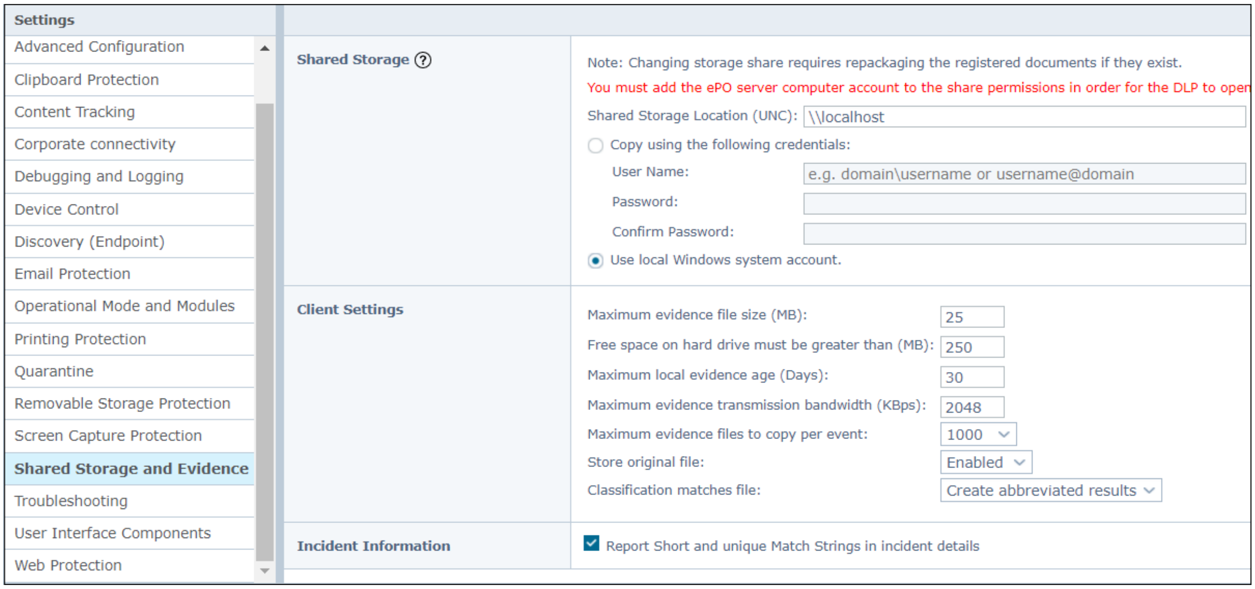
Configure client settings

Configure settings for McAfee DLP Endpoint.

Task

1. In McAfee ePO, select **Menu** → **Policy** → **Policy Catalog**.
2. On McAfee ePO 5.10, select **Data Loss Prevention <version>**.
    - On McAfee ePO 5.9 and earlier, from the **Product** drop-down list, select **Data Loss Prevention <version>**.

3. On McAfee ePO 5.10, select **Windows Client Configuration** or **Mac OS X Client Configuration**.
   - (Optional) On McAfee ePO 5.9 and earlier, from the **Category** drop-down list, select **Windows Client Configuration** or **Mac OS X Client Configuration**.
4. Select a configuration to edit or click **Duplicate** for the **McAfee Default** configuration.
5. On the **Shared Storage and Evidence** page, enter the storage share and credentials.
6. Update the settings on the other pages as needed.
7. Click **Apply Policy**.



Shared Storage

Note: Changing storage share requires repackaging the registered documents if they exist.

You must add the ePO server computer account to the share permissions in order for the DLP to open

Shared Storage Location (UNC): \\localhost

○ Copy using the following credentials:

User Name: e.g. domain\username or username@domain

Password:

Confirm Password:

● Use local Windows system account.

Client Settings

Maximum evidence file size (MB): 25

Free space on hard drive must be greater than (MB): 250

Maximum local evidence age (Days): 30

Maximum evidence transmission bandwidth (KBps): 2048

Maximum evidence files to copy per event: 1000

Store original file: Enabled

Classification matches file: Create abbreviated results

Incident Information

☑ Report Short and unique Match Strings in incident details

Configure server settings

Configure settings for McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor.

Before you begin

For McAfee DLP Discover server settings:

- 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.
- If you plan to use the OCR feature, install the OCR package on top of McAfee DLP Discover server software. After updating McAfee DLP Discover server software, add the OCR license details and enable the OCR checkbox in the server configuration settings.

Note

- McAfee DLP Prevent and McAfee DLP Monitor use only the **Shared Storage and Evidence** and **Optical Character Recognition (OCR)** settings.
- McAfee DLP Discover can use all server setting options except **ActiveSync Proxy**, though some are optional.

Task

1. In McAfee ePO , select **Menu** → **Policy** → **Policy Catalog**.
2. On McAfee ePO 5.10, select **Data Loss Prevention <version>**.
   - On McAfee ePO 5.9 and earlier, from the **Product** drop-down list, select **Data Loss Prevention <version>**.
3. On McAfee ePO 5.10, select **Server Configuration**.
   - (Optional) On McAfee ePO 5.9 and earlier, from the **Category** drop-down list, select **Server Configuration**.
4. Do one of the following.
   - Click an existing policy to edit.
   - Click **Duplicate** on the **McAfee Default** configuration to create a copy of the default policy and update the policy.
5. (Optional, McAfee DLP Discover only) On the **Box** page, verify the options for trash and version history.
6. On the **Shared Storage and Evidence** page, enter the evidence storage server details for McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor:
   a. Enter the storage share and credentials and test the credentials.
   For McAfee DLP Prevent and McAfee DLP Monitor, do not select the local system account option.

   Tip

   Use the default values for **Server Settings**. McAfee DLP Prevent and McAfee DLP Monitor ignore the evidence transmission bandwidth setting.

   b. Enter the server settings, or accept the defaults.
   c. If the policy must comply with privacy regulations such as GDPR, deselect the **Report short and unique match string** checkbox.
7. If you are configuring an evidence server outside your firewall or if your appliance is in a demilitarized zone, select the **Enable Evidence Storage HTTP service** checkbox.
   DLP Server can act as an HTTP proxy for McAfee DLP Prevent and McAfee DLP Monitor for saving evidence files and capture search evidences to storage share that they can't access directly. DLP Server, McAfee DLP Prevent and McAfee DLP Monitor must use the same settings for the evidence share location and credentials. If not, DLP Server will not store the files and returns an operation error. The Active Directory account lockouts can also occur when the same settings are not configured.
   You can configure a DLP Server for evidence copy by creating or editing a policy from **Policy Catalog** → **DLP Appliance Management** → **General**. For more information, see Connect to an evidence server outside your firewall.

Note

> If both CIFS and DLP Server are configured for evidence copy, McAfee DLP Prevent and McAfee DLP Monitor always use only the DLP Server even if it fails and doesn't use the CIFS share.

8. (Optional, McAfee DLP Discover only) On the **Debugging and Logging** page:
   a. Set the log output type and log level.

   Tip

   > Use the default values.

   b. Select on which McAfee DLP Discover process to run an Automatic Memory Dump for storing contents of memory. Contents can be analyzed for system issues, such as a system crash.

   Note

   > Analyzing the contents of a memory dump requires knowledge of developments tools, such as Microsoft Visual Studio.

9. On the **Registered Documents** page:
   a. (McAfee DLP Discover only) Verify the **Shared Storage** (set on the **DLP Settings** → **General** page).
   b. (McAfee DLP Discover and McAfee Network DLP) Verify that the **Documents engine** is enabled, and enter the IP address of the DLP Server.
   The documents engine uses REST API to match fingerprints stored on the specified DLP Server. If you are not using registered documents, you can disable the documents engine.
   c. (DLP Server only) Enter the name, UNC storage share, and user name for the evidence shares to upload registered document packages to the DLP Server.
10. (McAfee DLP Discover only) On the **Rights Management** page, set the RM service credentials.
11. (McAfee DLP Discover only) On the **SharePoint** page, select, or deselect, **Use Recycle bin when deleting a file**.

    Caution

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

12. (Optional, McAfee DLP Discover only) On the **Text Extractor** page, configure the text extractor settings.

    Tip

    > Use the default values.

    a. Set the ANSI fallback code page.
    The default uses the default language of the Discover server.
    b. Set the input and output maximum file size, and the timeouts.
13. Select the **Optical Character Recognition (OCR)** checkbox if you want to extract text from image files.

Note

OCR is resource-intensive. It can significantly increase the scan time if you are scanning numerous images. Deselect the checkbox when you don't need OCR scanning.

14. Click **Apply Policy**.

Reset the Shared Password

As a mandatory security requirement, reset the default **Shared Password** in **DLP Settings**. The default shared password can affect both the Identification Code (*challenge key*) generated from the Diagnostic tool and the DLP Release Code (*response key*) generated from the console as the shared password is needed to generate these codes.

Resetting the shared password also prevents a compromise between two different McAfee ePO servers or a compromise between two different policies on the same McAfee ePO server. You can follow these steps before applying the **My Default DLP Policy**:

1. Reset the shared password as needed.
2. Duplicate or create the **My Default DLP Policy** and apply the newly created policy.

For example, if you duplicate the **My Default DLP Policy** in the **Policy Catalog** and send it out to endpoints, McAfee DLP Appliances, or McAfee DLP Discover servers, any McAfee ePO server can bypass the policy. When you apply the bypass code from the other McAfee ePO server, the response code allows the bypass. This happens because the challenge-response codes for **My Default DLP Policy** are the same across all McAfee ePO installs. Any other McAfee ePO administrator can bypass any DLP policy that is based on **My Default DLP Policy**. So, it is mandatory to reset the shared password or create a policy that is anything other than **My Default DLP Policy** to prevent bypassing the systems not associated with the McAfee ePO server you are working on.

To reset the **Shared Password**:

Task

1. In McAfee ePO, go to **Menu** → **Data Protection** → **DLP Settings** → **General**.
2. Update the **Shared Password** as needed and maintain the password in confidence.
3. You are prompted to save the changes when you try to navigate to a different page, click **Yes** to save the changes.

Protecting files with rights management

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

McAfee DLP Endpoint and McAfee DLP Discover supports applying policies with Microsoft RMS on-premises, Azure RMS and Seclore.

Important

- When using Microsoft RMS on-premise, with McAfee DLP Endpoint 10.x and 11.x, you must install Active Directory Rights Management Services Client 2.1 build 1.0.2004.0 on each endpoint using RM services.
- When using Azure RMS, you must install Azure Information Protection 2.6.111 on each endpoint using RM services.

The **Apply RM** command does not work without this version of the RM client.

- McAfee DLP Prevent and McAfee DLP Monitor can identify if an email or an attachment has RM protection applied to it, but, they do not support applying RM policies.

You can apply an RM policy reaction to these data protection and discovery rules:

- Cloud protection
- Endpoint file system discovery
- Removable storage protection
- (For McAfee DLP Discover only) Network share protection, including
  - Box protection
  - File Server protection
  - SharePoint protection

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

How McAfee DLP works with rights management

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

RM workflow

1. Create and apply a data protection or a discovery rule with a reaction to apply RM policy. The reaction requires an RM server, and an RM policy entry.
2. When a file triggers the rule, McAfee DLP encrypts the file using the selected RM server.
3. The RM server applies protections based on the specified policy, such as encrypting the file, limiting the users allowed to access or decrypt the file, limiting the users allowed to read or access labeled files, and limiting the conditions in which the file can be accessed.
4. The RM server sends the file back to the source with the applied protections.
5. If you have configured a classification for the file, McAfee DLP can monitor the file.

Limitations

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

Supported RM servers

McAfee DLP Endpoint supports Microsoft Windows Rights Management Services (Microsoft RMS) including on-premise and Azure RMS, and Seclore FileSecure™ information rights management (IRM). McAfee DLP Discover supports Microsoft RMS on-premises and Azure RMS.

Microsoft RMS

McAfee DLP supports Microsoft RMS on Windows Server 2003 and Active Directory RMS (AD-RMS) on Windows Servers 2008 and 2012. McAfee DLP also supports Azure RMS and Office 365. You can apply Windows Rights Management Services protection to the following applications.

Document type	Version
Microsoft Word	2010, 2013, 2016, and 2019
Microsoft Excel	
Microsoft PowerPoint	
SharePoint	2007
Exchange Server	

With Microsoft RMS, McAfee DLP can inspect the content of protected files by document properties, or by the Azure Information Protection labels that are applied, if the current user has view permissions

For more information on Microsoft RMS, go to http://technet.microsoft.com/en-us/library/cc772403.aspx.

Seclore IRM

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

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

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

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

Documenting events with evidence

Using evidence and evidence storage

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

McAfee DLP Endpoint stores evidence in a temporary location on the client between agent-server communication intervals. When McAfee Agent passes information to the server, the folder is purged and the evidence is stored in the server evidence folder. You can specify the maximum size and age of local evidence storage when the computer is offline.

Prerequisites for evidence storage

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

- **Evidence storage folder** — Creating a network evidence storage folder and specifying the UNC path to the folder are requirements for applying a policy to McAfee ePO. Specify the default path on the **DLP Settings** → **General** page.
- **Evidence copy service** — The default UNC path is copied to the **Shared Storage and Evidence** page in the Policy Catalog. For McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor, the **Shared Storage and Evidence** page is in the Server configuration. For McAfee DLP Endpoint, it is in the Windows and macOS client configurations. You can specify different evidence storage folders in the configurations.

Note

> If your McAfee DLP appliance is in a DMZ, you can specify an evidence server outside your firewall in the **General** page in the **DLP Appliance Management** policy catalog.

- **Reporting Service** — For McAfee DLP Endpoint for Windows, you must also activate the **Reporting Service** and **Evidence Copy Service** options in the **Operational Modes and Modules** page of the client configuration to enable evidence collection.

Evidence storage and memory

Evidence is stored in evidence folders on the network. You can specify a different storage share for each McAfee DLP product.

The number of evidence files stored per event has implications for storage volume, event parser performance, and the screen rendering (and thus user experience) of the **DLP Incident Manager** and **DLP Operations** pages.

Most rules allow the option of storing evidence. When this option is selected, an encrypted copy of the content is stored in the predefined evidence folder. Multiple evidence files are created for an event when possible. For example, if an Email Protection rule is triggered, the email, the body text, and the attachments are all saved as evidence files.

Note

If a classification occurs in the email headers, no separate evidence is written because it can be found in the message itself. The matched text is included in the hit highlights for the body evidence.

To handle different evidence requirements, McAfee DLP software does the following:

- The UNC storage share and the maximum number of evidence files to store per event are set on the **Evidence Copy Service** page. Each instance of Windows client configuration, macOS client configuration, and server configuration can have different values for these parameters.
- The DLP Incident Manager field **Total Match Count** displays the total evidence count.
- If the evidence storage becomes critically full, McAfee DLP Prevent temporarily rejects the message with an SMTP error. An event is listed in the **Client Events** page, and an alert appears in the **Appliance Management** dashboard.

Purging evidence files

Evidence can contain information covered by policies or laws that regulate the storage of private information.

To optimize system performance, McAfee DLP purges incidents from the live incidents list table and moves them to the **Incident History** view when a million incidents are reached, starting with the oldest incidents.

The server task **DLP Purge History of Operational Events and Incidents** deletes events and incidents from the history database tables and marks evidence files for deletion. If the event or incident are still in the live incidents and operational events list tables, this task will delete them from the live tables. By default, this server task runs weekly. Evidence files are held for two calendar months, and if not required by another incident or operational event in the database, the files are deleted with the **DLP purge evidences** server task. By default, this server task runs weekly on Friday at 23:30.

Tip

Don't run **DLP purge evidences** when more than one McAfee ePO instance shares an evidence storage path.

Hit highlighting

The hit highlighting option helps administrators identify exactly which sensitive content caused an event.

When selected, it stores an encrypted XML evidence file with extracted text.

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

For McAfee DLP Endpoint and McAfee DLP Endpoint for Mac, display options are set on the **Evidence Copy Service** page of the client configuration policy in the **Classification matches file** field. For McAfee DLP Discover, display options are set on the **Evidence Copy Service** page of the server configuration policy in the **Classification matches file** field:

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

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

In the **Incident Information** field, you can choose to display the **Short Match String** on the incident details page. Short match strings contain up to three hit highlights as a single string. Short match strings, like other hit highlights, are saved as encrypted files.

Rules allowing evidence storage

These rules have the option of storing evidence.

Evidence saved by McAfee DLP Monitor or McAfee DLP Prevent rules

Rule	What is saved
Email Protection Rule	Copy of the email
Network Communication Protection Rule	Copy of the content
Web Protection Rule	Copy of the web post

Evidence saved by McAfee DLP Endpoint rules

Rule	What is saved
Application File Access Protection Rule	Copy of the file
Clipboard Protection Rule	Copy of the clipboard
Cloud Protection Rule	Copy of the file
Email Protection Rule	Copy of the email

Rule	What is saved
Network Share Protection Rule	Copy of the file
Printer Protection Rule	Copy of the file
Removable Storage Protection Rule	Copy of the file
Screen Capture Protection Rule	JPEG of the screen
File System Discovery Rule	Copy of the file
Email Storage Discovery Rule	Copy of the .msg file
Web Protection Rule	Copy of the web post

Evidence saved by McAfee DLP Discover rules

Rule	What is saved
Box Protection Rule	Copy of the file
File Server Protection Rule	Copy of the file
SharePoint Protection Rule	Copy of the file
Database Protection Rule	Copy of the table

Creating evidence folders

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

Evidence folder paths are set in different locations in the McAfee DLP products. When more than one McAfee DLP product is installed in McAfee ePO, the UNC paths for the evidence folders are synchronized.

Note

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

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

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

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

Enable permissions to download evidence files when evidence share is on a different domain

When McAfee ePO and evidence server are not on the same domain, you must configure the group policy settings on Windows to download evidence files from **Incident Manager**.

1. On your evidence server, open the **Local Group Policy Editor**.
2. Go to **Computer Configuration** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options** and configure these options:
   - **Network access: Let Everyone permissions apply to anonymous users**: Enabled
   - **Network access: Shares that can be accessed anonymously**: <evidence_share_folder>

Shared Storage and Evidence page

Use this page to configure the client **Shared Storage and Evidence** for McAfee DLP Endpoint for Windows.

Option definitions

Category	Option	Definition
Shared Storage	**Shared Storage Location**	The UNC path to the location on the server where evidence is saved. To collect evidence, specify a folder for evidence collection in this text box. You can specify these paths: Specify this path to store: • Evidence files • File with classification matches • Registered document fingerprints For Manual Registered Document, the fingerprints are copied to all available evidence share

Category	Option	Definition
		• Package containing ignored texts • Endpoint discovery scan summary in CSV file format
	Use local Windows system account	You can use the local system account to copy evidence. Not supported by McAfee DLP Endpoint for Mac or McAfee DLP Prevent.
	Copy files using the following credentials	When selected, uses the specified user and password to copy evidence. Fill in the **User Name**, **Password**, and **Confirm Password** text boxes to specify a user.
	Test Credential	Tests the connection to the storage share. You can save the configuration even if the test is unsuccessful.
Client Settings	**Maximum evidence file size (MB)**	The maximum size of an evidence file. **Range:** 10–2,575 **Default:** 25
	Free space on hard drive must be greater than (MB)	The minimum free space on the managed computer including the evidence storage space. **Default:** 250
	Maximum local evidence age (Days)	The maximum number of days that evidence remains on the managed computer before it is deleted. **Default:** 30
	Maximum evidence transmission bandwidth (KBps)	The network bandwidth available between the managed computer and the server. **Default:** 2048
	Maximum evidence files to copy per event	Sets the maximum number of evidence files copied. Select options from 100–10000. **Default:** 1000
	Store original file	Select from the drop-down list. **Default:** Enabled
	Classification matches file	Sets the hit highlighting display option. **Default:** Create abbreviated results
Incident Information	**Report short match string in incident details**	When selected, displays the short match string on the **Evidence** tab of the incident details page.

Administrative and end users in McAfee DLP

McAfee DLP has two categories of users: administrative users and end users.

McAfee DLP accesses Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) servers to create both types of user definitions. User definitions can consist of users, user groups, or organizational units (OU), allowing the administrator to choose an appropriate model. Enterprises organized on an OU model can continue using that model, while others can use groups or individual users as needed.

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

User definitions are set up in DLP Policy Manager on the **Definitions** → **End-user Group** page. Administrative users are assigned permissions in McAfee ePO **Permissions Sets**. Data protection, discovery, and application control rules can apply to specific end users or groups by specifying them in the rule **Conditions**. Additional granularity can be obtained by exempting specific users or groups on the **Exceptions** tab of the rule definition. In addition, *privileged users* can be named in the Policy Catalog on the **Settings** page of the DLP Policy. Privileged users are only monitored if they trigger a rule. They are not blocked by any rule in the policy.

Create user definitions

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Definitions** tab.
3. Select **Source/Destination** → **End-User Group**, then **Actions** → **New Item**.
4. In the **New End-User Group** page, enter a unique name and optional description.
5. Select the method of identifying objects (SID or name).
6. Click one of the **Add** buttons (**Add Users**, **Add Groups**, **Add OU**).
   The selection window displays the selected type of information.

   The display might take a few seconds if the list is long. If no information appears, select **Container and children** from the **Preset** drop-down list.

7. Select names and click **OK** to add them to the definition.
   Repeat the operation as needed to add users, groups, or organizational users.
8. Click **Save**.

Controlling assignments with users and permission sets

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

Tip

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

System Tree filtering permissions support

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

Tip

If you use **Group Administrators** in **Data Loss Prevention** permission sets, give **Group Administrators**:

- **View "System Tree" tab** permission (under **Systems**)
- **System Tree access** permissions at the appropriate level

Sensitive data redaction and the McAfee ePO permission sets

To meet the legal demand in some markets to protect confidential information in all circumstances, McAfee DLP software offers

a data redaction feature. Fields in the **DLP Incident Manager** and **DLP Operations** consoles with confidential information can be redacted to prevent unauthorized viewing. Redaction can be controlled by choosing specific sensitive incidents data fields. Links to sensitive evidence are hidden. The feature is designed with a "double key" release. Thus, to use the feature, you must create *two permission sets*: one to view the incidents and events and another to view the redacted fields (supervisor permission). Both roles can be assigned to the same user.

REST API for importing definitions and applying policies

McAfee DLP uses REST (REpresentational State Transfer) architecture for certain functions to reduce bandwidth.

You can use McAfee DLP REST API calls to create policies in certain circumstances, to decrypt evidence files, and to import definitions. You can also use REST API calls to import user information from a CSV file.

To use the McAfee DLP REST API feature, the McAfee DLP administrators must be valid McAfee ePO users with permissions that allow them to perform the actions invoked by the APIs.

You can create McAfee DLP REST API calls in the programming language of your preference. See KB87855 for sample Java source code that shows how to use the REST API.

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 sets cover all sections of the management console. There are three levels of permissions:

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

Note

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 Endpoint permission groups are:

Group I	Group II	Group III
• **Policy Catalog** • **DLP Policy Manager** • **Classifications** • **Definitions**	• **DLP Policy Manager** • **Classifications** • **Definitions**	• **Classifications** • **Definitions**

The McAfee DLP Discover permission group is:

- **DLP Discover**
- **DLP Policy Manager**
- **Classifications**
- **Definitions**

The DLP Capture permission group is:

- **Capture**
- **Classifications**
- **Definitions**

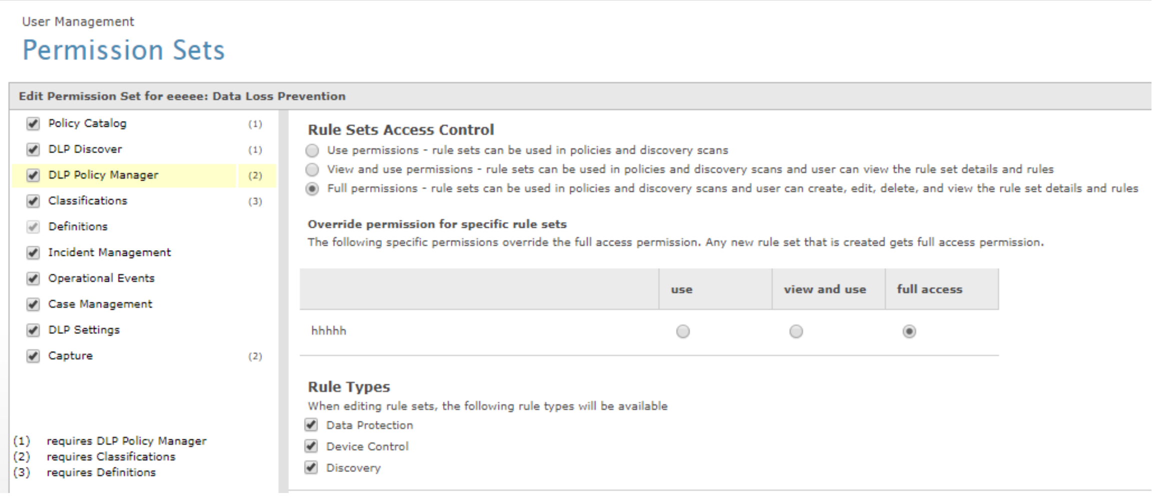
Incident Management, **Operational Events**, **Case Management**, **DLP Settings**, and **Capture** permissions can be selected separately.

Note

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

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

McAfee DLP permission sets



User Management

Permission Sets

Edit Permission Set for eeeee: Data Loss Prevention

- ☑ Policy Catalog (1)
- ☑ DLP Discover (1)
- ☑ DLP Policy Manager (2)
- ☑ Classifications (3)
- ☑ Definitions
- ☑ Incident Management
- ☑ Operational Events
- ☑ Case Management
- ☑ DLP Settings
- ☑ Capture (2)

(1) requires DLP Policy Manager
(2) requires Classifications
(3) requires Definitions

Rule Sets Access Control

○ Use permissions - rule sets can be used in policies and discovery scans
○ View and use permissions - rule sets can be used in policies and discovery scans and user can view the rule set details and rules
● Full permissions - rule sets can be used in policies and discovery scans and user can create, edit, delete, and view the rule set details and rules

Override permission for specific rule sets

The following specific permissions override the full access permission. Any new rule set that is created gets full access permission.

	use	view and use	full access
hhhhh	○	○	●

Rule Types

When editing rule sets, the following rule types will be available

- ☑ Data Protection
- ☑ Device Control
- ☑ Discovery

Create a user

You can add and manage users from McAfee ePO.

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Users**.
2. Click **New User** and type a user name.
3. Select whether to enable or disable the logon status of this account.

Tip

Disable the account if you are setting up a user who has not yet started working for the company.

4. Select an authentication method for this account, and provide the required credentials.
    - Windows authentication
    - Certificate-Based Authentication
5. (Optional) Provide the user's full name, email address, phone number, and a description in the **Notes** text box.
6. Choose to make the user an administrator, or select the appropriate permission sets.
7. Click **Save** to return to the **Users** tab.

Results

The new user appears in the **Users** list on the **User Management** page.

Create a McAfee DLP permission set

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

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Select a predefined permission set, click **New Permission Set** to create a permission set, or **Import** to import a permission set.
3. In the **Data Loss Prevention** section, click **Edit**.
    a. In the left pane, select a data protection module.
       Incident Management, **Operational Events**, and **Case Management** can be activated separately. Other options automatically create predefined groups.
    b. Edit the options and override permissions as needed.
       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**.

Use case: DLP administrator permissions

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

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Click **New Permission Set** to create a permission set.
   a. Type a name for the set and select users.
      To edit a policy, the user must be the policy owner or a member of the global administrator permission set.
   b. Click **Save**.
3. In the **Data Loss Prevention** permissions set, select **Policy Catalog**.

   Note

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

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

Results

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

Use case: Limit DLP Incident Manager viewing with redaction permissions

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

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

Note

The fields **computer name** and **user name** are predefined as private.

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

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Create permission sets for regular reviewers and for the redaction reviewer.
   a. Click **New Permission Set**.
   b. Enter a name for the group such as `DLPE Incident Reviewer` or `Redaction Reviewer`.

Note

> You can assign different types of incidents to different reviewer groups. You must create the groups in **Permission Sets** before you can assign incidents to them.

   c. Assign users to the group, either from available McAfee ePO users or by mapping Active Directory users or groups to the permission set. Click **Save**.

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

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

      Selecting this option activates the redaction feature. Leaving it deselected displays all data fields in clear text.
   d. In the **Incident Tasks** section, select or deselect tasks as required.
   e. Click **Save**.
4. Select the redaction reviewer permission set, then click **Edit** in the **Data Loss Prevention** section.
   a. In the left pane, select **Incident Management**.
   b. In the **Incidents Reviewer** section, select **User can view all incidents**.

      Note

      > In this example, we assume a single redaction reviewer for all incidents. You can also assign different redaction reviewers for different sets of incidents.

   c. In the **Incidents Data Redaction** section, select both the **Supervisor permission** and the **Obfuscate sensitive incidents data** option.
   d. In the **Incident Tasks** section, deselect all tasks.

      Note

      > Redaction reviewers do not normally have other reviewer tasks. This is optional according to your specific requirements.

   e. Click **Save**.
5. Control redaction from **DLP Settings** → **Incident Management**.
   a. In the **Redaction Fields** section, click **Edit**.
   b. Choose specific fields you want redacted from the DLP Incident Manager display.
   c. Click **OK**.

Create a DLP Help Desk permission set

Assign Help Desk permissions to a permission set group.

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Select a predefined permission set, click **New Permission Set** to create a permission set, or **Import** to import a permission set.
3. In the **DLP Help Desk Actions** section, click **Edit**.
4. Select the key or keys the administrator is allowed to generate.
   The **Generate master response key** option becomes available when at least one other key is selected.
5. Click **Save**.

Control access to McAfee DLP appliance features

Use McAfee ePO **Permission Sets** to control what roles in your organization have access to McAfee DLP appliance and Appliance Management policies and settings.

Restrict users from viewing appliances in the System Tree

Use the **No permissions** option to restrict users from viewing appliances in the **System Tree** and viewing or editing the policies.

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Select the permission set whose roles you want to edit.
3. Select **No permissions**, and click **Save**.

Allow users to edit the Appliance Management policies

Configure the role to allow users to view and change the policy and task settings.

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Select the permission set whose roles you want to edit.
3. Select **View and change policy and task settings**, and click **Save**.

Results

The selected users can view and change the McAfee DLP **Appliance Management** policy settings.

Control access to Appliance Management features

For McAfee DLP appliances, you can apply two roles to access the **Appliance Management** features.

- **Appliance Management Common Policy** — Controls who can view or change the **Common Appliance Management** policy in the **Policy Catalog**.
- **Appliance Management** — Controls who can view appliance management statistics and tasks, and who can create and run database tasks.

Allow users to view Appliance Management statistics

Allow users in a selected permission set to view system health and statistics in the **Appliance Management** dashboard (**Systems** → **Appliance Management**).

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Select the permission set for the roles you want to edit.
3. Select the **Appliance Management** role, and click **Edit**.
4. In **Appliance Health and Statistics**, select **View health and statistics**, and click **Save**.

Results

The selected users can view the Appliance system health and statistics in the **Appliance Management** dashboard.

Restrict users from viewing the Common Appliance Management settings

The **Common Appliance Management** policy settings enable users to set the appliance date and time, add DNS servers and static routes, allow remote logon using SSH, and add one or more remote logging servers.

Task

1. In McAfee ePO, **Menu** → **User Management** → **Permission Sets**.
2. Select the permission set for the roles you want to edit.
3. Click **Edit** next to the **Appliance Management Common Policy**.
4. Select **No permissions**, and click **Save**.

Results

The view permissions for the selected users are removed.

McAfee ePO features

McAfee DLP uses these McAfee ePO features.

ⓘ **Important**

You must have appropriate permissions to access most features.

McAfee ePO feature	Addition
Actions	Actions that you can perform from the **System Tree** or use to customize automatic responses.
Client tasks	(McAfee DLP Endpoint only) Client tasks that you can use to automate management and maintenance on client systems.
Dashboards	Dashboards and monitors that you can use to keep watch on your environment.
Events and responses	• Events for which you can configure automatic responses. • Event groups and event types that you can use to customize automatic responses.
Managed system properties	Properties that you can review in the **System Tree** or use to customize queries.
Permissions sets	Available in all existing permission sets: • **Data Loss Prevention** • **DLP Appliance Management Policy** • **DLP Help Desk Actions**
Policies	**DLP Policy**, **Windows Client Configuration**, and **Mac OS X Client Configuration** for McAfee DLP Endpoint, and **Server Configuration** for McAfee DLP Discover and McAfee DLP appliance policy categories in the **Data Loss Prevention <version>** product group.

McAfee ePO feature	Addition
Queries and reports	• Default queries that you can use to run reports. • Custom property groups based on managed system properties that you can use to build your own queries and reports.
Server tasks	Server tasks for McAfee DLP Endpoint include DLP Incident Manager and DLP Operations. Use the **Roll UP Data** task to roll up McAfee DLP incidents, operational events, or endpoint discovery data from selected McAfee ePO servers to produce a single report. Use the **Detect Discovery Servers** task with McAfee DLP Discover, and the **LdapSync** task with McAfee DLP appliances.
Data Protection	Used to configure, manage, and monitor McAfee DLP.

For information about these features, see the McAfee ePO documentation.

Classifying sensitive content

Identifying and tracking content with classifications

McAfee DLP uses user-defined classifications to identify and track sensitive content and files in data protection and discovery rules.

McAfee DLP uses two mechanisms and two modes to classify sensitive content.

The two modes are automatic and manual classification.

- Automatic classifications are defined in McAfee DLP and distributed by McAfee ePO in the deployed policies. They can then be applied to content with data protection rules or discovery rules.
- Manual classifications are applied by authorized users to files and emails on their computers.

  The manual classification dialog is supported on McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac.

  Note

  McAfee DLP Prevent and McAfee DLP Monitor can enforce data protection rules based on manual classifications, but cannot set or view them.

The two mechanisms are content classifications and content fingerprinting.

Note

McAfee DLP Endpoint only supports content classifications.

- Content classifications are applied differently for manual and automatic classifications
  - For automatic classification, the classification criteria are compared to the content each time a rule is triggered.
  - For manual classification, the classification is embedded as a physical tag inside the file or email.
- Content fingerprint signatures are stored in a file's extended file attributes (EA), alternate data stream (ADS), or in a hidden folder (ODB$).

All McAfee DLP products support content classifications, that is, can apply them by assigning them to data protection or discovery rules.

On deployment, McAfee DLP displays many predefined classifications. Predefined classifications include, amongst others, classifications for personal data specific to different European Union countries, that can be used for detection accuracy, specifically when scanning for personal data for European Union Citizens.

You can use predefined classifications as is in protection rules, but if you want to customize a classification you must duplicate it first. The classifications reduce false positives.

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

The module provides these features:

- **Manual Classification** — Configures the user groups allowed to manually classify or fingerprint content.
- **Definitions** — Defines the content, properties, and location of files for classification.
- **Classification** — Creates classifications and defines content classification and fingerprinting criteria.
- **Classification Tester** - Tests classifications by checking if a phase or file triggers the classifications.
- **Register Documents** — Uploads files containing known sensitive content for distribution to endpoints; displays McAfee DLP Discover registration scan information.
- **Whitelisted Text** — Uploads files containing whitelisted text for distribution to endpoints.

Content classification

Content classifications include data and file conditions that define sensitive content. For automatic classification, the classification criteria are compared to the content each time a data protection, endpoint discovery, or McAfee DLP Discover rule is triggered. For manual classification, the classification is embedded as a physical tag inside the file or email. Manual content classifications are persistent, and remain in the file when copied to storage, attached to an email, or uploaded to a website such as SharePoint.

Automatic content classifications are supported on all McAfee DLP products. Data protection rules based on manual classifications are enforced on all McAfee DLP products but only McAfee DLP Endpoint (both Windows and Mac versions) have the manual classification dialog that allows users to classify files.

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

Content fingerprints

Content fingerprints are used by McAfee DLP products in the following ways:

- McAfee DLP Endpoint for Windows can apply content fingerprints to data protection rules and enforce the rules.
- McAfee DLP Prevent and McAfee DLP Monitor can enforce content fingerprints in rules but can't apply them to content.
- McAfee DLP Discover can use Location, SharePoint, or Box content fingerprint classification criteria in registration scans, but can't use or apply them in classification or remediation scans.

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

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

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

Content fingerprint signatures are stored in a file's extended file attributes (EA), alternate data stream (ADS), or in a hidden folder (ODB$). You can select the preferred technology on the Windows client configuration **Content Tracking** page. They are applied to a file when the file is saved. The mechanism is the same for automatic and manual content fingerprints. If a user copies or moves fingerprinted content to another file, the fingerprint criteria are applied to that file. If the fingerprinted content is removed from the file, the content fingerprint signatures are also removed. If the file is copied to a system that doesn't support EA or ADS (such as SharePoint), the fingerprint criteria are lost.

Note

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

Applying classification criteria

McAfee DLP applies criteria to a file, email, or web request in one of the following ways:

- McAfee DLP Prevent applies criteria when an email or web request matches a configured classification.
- McAfee DLP Monitor applies criteria when network traffic matches a configured classification.
- McAfee DLP Endpoint applies criteria when:
  - The file matches a configured classification.
  - The file or sensitive content is moved or copied to a new location.
  - A file is matched during a discovery scan.
  - An email or a web request matches a configured classification.
- A user with permission manually applies criteria to a file.

How applications are categorized

How McAfee DLP categorizes applications used in classifications and rule sets can affect system performance.

Note

Categorization is not supported on McAfee DLP Endpoint for Mac.

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

The strategies, in order of decreasing security, are:

- **Editor** — Any application that can modify file content. This includes “classic” editors like Microsoft Word and Microsoft Excel, as well as browsers, graphics software, accounting software, and so forth. Most applications are editors. McAfee DLP Endpoint client always analyzes files opened or created by editors.
- **Explorer** — An application that copies or moves files without changing them, such as Microsoft Windows Explorer or certain shell applications.

- **Trusted** — An application that needs unrestricted access to files for scanning purposes. Examples are McAfee® VirusScan® Enterprise or backup software. Use the trusted strategy when you want to make sure that the McAfee DLP Endpoint client doesn't analyze files opened or created by the application.
- **Archiver** — An application that can reprocess files. Examples are compression software such as WinZip, and encryption applications such as McAfee Endpoint Encryption software or PGP.

How to work with DLP strategies

Application strategies are set on the **Application Template** page in **DLP Policy Manager** → **Definitions**. Use the built-in templates, or create your own custom templates.

Note

> You can't edit strategies in the built-in templates. You can create overrides on the **DLP Policy** → **Settings** → **Application Strategy** page. Create and remove overrides as needed to experiment with fine-tuning the policy.

Change the strategy as needed to optimize performance. For example, the high level of observation that an editor application receives is not consistent with the frequent processing of backup software. The performance penalty is high and the risk of a data leak from such an application is low, so we don't recommend using the trusted strategy with these applications.

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

Trusted strategy vs whitelisted processes

McAfee DLP uses two mechanisms to bypass processing files when no analysis is needed.

Trusted strategy is the general mechanism to use when you want to make sure that files opened or created by the application are not analyzed by the McAfee DLP Endpoint client. Use this mechanism for applications that always need unrestricted access to files.

Whitelisted processes are used to create exceptions to rules. Whitelisted URLs create exceptions for web protection rules. You can whitelist applications to create exceptions to clipboard and printer protection rules, and to define exceptions for content tracking when creating content fingerprints.

Classifying by file destination

In addition to classifying content by its originating location, you can classify and control where content is being sent. In data loss prevention parlance, this is known as data-in-motion.

File protection rules controlling destinations include:

- **Cloud Protection** rules

- **Email Protection** rules
- **Network Communication Protection** rules (outgoing)

Note

Data Network Communication Protection rules can be incoming or outgoing or both. For classifying by destination only outgoing rules are relevant.

- **Printer Protection** rules
- **Removable Storage Protection** rules
- **Web Protection** rules

Protecting email content with classifications

McAfee DLP Endpoint protects sensitive data in email headers, body, or attachments when emails are sent. Email storage discovery detects emails with sensitive data in OST or PST files and either tags or quarantines them.

McAfee DLP Endpoint protects sensitive content in email by adding content classifications to content and blocking emails with sensitive content from being sent. The email protection policy can specify different rules for different users and email destinations, or for emails protected with encryption or Rights Management. Rules can be enabled for McAfee DLP Endpoint for Windows, McAfee DLP Prevent, or both. Manual classifications added by McAfee DLP Endpoint for Windows users are supported by McAfee DLP appliances.

Monitor or block sensitive emails

McAfee DLP Endpoint protects sensitive data in email headers, body, or attachments when emails are sent. Email storage discovery detects emails with sensitive data in OST or PST files and either tags or quarantines them.

McAfee DLP Endpoint protects sensitive content in email by adding content classifications to content and blocking emails with sensitive content from being sent. The email protection policy can specify different rules for different users and email destinations, or for emails protected with encryption or Rights Management. Rules can be enabled for McAfee DLP Endpoint for Windows, McAfee DLP Prevent, or both. Manual classifications added by McAfee DLP Endpoint for Windows users are supported by McAfee DLP appliances.

Define network parameters

Network definitions serve as filter criteria in network protection rules.

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

- **Network Share** definitions specify shared network folders in network share protection rules. You can include or exclude defined shares.

Working with printers

Printer protection rules manage both local and network printers, and either block or monitor the printing of confidential material.

Printer protection rules in McAfee DLP Endpoint support advanced mode and V4 printers. Defined printers and end-users can be included or excluded from a rule. Image printers and PDF printers can be included in the rule.

Printer protection rules can include application definitions. You can define whitelisted processes that are exempted from printer protection rules on the **Printing Protection** page in the **Windows Client Configuration**.

Controlling information uploaded to websites

Web addresses are used in web protection rules and web application control rules.

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

Classifying by file location

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

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

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

Text extraction

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

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

Text extraction with McAfee DLP Endpoint

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

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

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

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

Classifying content with dictionary definitions

A dictionary is a collection of keywords or key phrases where each entry is assigned a score. Sensitive content is compared to the dictionary entries and ranked according to the score.

Content classification and content fingerprinting criteria use specified dictionaries to classify a document if a defined threshold (total score) is exceeded — that is, if enough words from the dictionary appear in the document. The assigned scores can be negative or positive, allowing you to look for words or phrases in the presence of other words or phrases.

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

- A keyword classification always tags the document if the phrase is present.
- A dictionary classification gives you more flexibility because you can set a threshold when you apply the definition, making the classification relative. The threshold can be up to 1000. You can also choose how matches are counted: **Count multiple occurrences** increases the count with each match, **Count each match string only one time** counts how many dictionary entries match the document.

McAfee DLP software includes several built-in dictionaries with terms commonly used in health, banking, finance, and other industries. You can also create your own dictionaries and edit them manually or copy and paste 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, be careful when entering short words because of the potential for false positives. For example, a dictionary entry of "cat" would flag "**cat**aracts" and "dupli**cat**e." 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.

Classifying content with advanced pattern definitions

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

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

To ensure compliance with recent government regulations and simplify detection of personal information, more built-in advanced pattern definitions have been added. In addition, many validation algorithms have also been added.

ⓘ **Important**

When working with older McAfee DLP products, evaluating an advanced pattern with a regular expression might result in a false-positive. When the older McAfee DLP product doesn't support the new validation algorithm, the validation algorithm is ignored. If the regular expression matches but the value isn't valid based on the validation algorithm, the positive match reported is a false positive.

When defining an advanced pattern, you can choose how matches are counted: **Count multiple occurrences** increases the count with each match, **Count each match string only one time** counts how many defined patterns give an exact match in the document.

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

Note

If both a 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.

Classifying content with document properties or file information

Document property definitions classify content by predefined metadata values. File information definitions classify content by file metadata.

Document properties

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

There are three types of document properties:

- **Predefined properties** — Standard properties such as *author* and *title*.
- **Custom properties** — Some applications, such as Microsoft Word, allow custom properties to be added to the document metadata. A custom property can also reference a standard document property that is not on the predefined properties list, but cannot duplicate a property that is on the list.
- **Any property** — Allows defining a property by value alone. This feature is useful in cases where the keyword has been entered in the wrong property parameter or when the property name is unknown. For example, adding the value *Secret* to the **Any property** parameter classifies all documents that have the word *Secret* in at least one property.

File information

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

Note

The **Date Accessed**, **Date Created**, **Date Modified**, and **File Owner** file conditions are not embedded in the file so they cannot be detected. The conditions are lost when the file is in-motion or uploaded to the cloud or a website.

Benefits of using templates to define content fingerprinting criteria

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

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

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

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

- **Command line** — Allows command-line arguments, for example: `java-jar`, that can control previously uncontrollable applications.
- **Executable directory** — The directory where the executable is located. One use of this parameter is to control U3 applications.
- **Executable file hash** — The application display name, with an identifying SHA-2 hash.
- **Executable file name** — Normally the same as the display name (minus the SHA-2 hash), but could be different if the file is renamed.
- **Original executable file name** — Identical to the executable file name, unless the file has been renamed.
- **Product name** — The generic name of the product, for example, Microsoft Office 2012, if listed in the executable file's properties.
- **Vendor name** — The company name, if listed in the executable file's properties.
- **Window title** — A dynamic value that changes at runtime to include the active file name.

All parameters except the SHA-2 application name and the executable directory accept substring matches.

Application templates for macOS can use any of the following parameters:

- **Command line**
- **Executable directory**
- **Executable file hash**
- **Executable file name**

Classifying files manually

Users can manually apply or remove classifications or content fingerprinting to files.

The manual classification feature applies file classification. That is, the classifications applied do not need to be related to content. For example, a user can place a PCI classification on any file. The file does not have to contain credit card numbers. Manual classification is embedded in the file. In Microsoft Office files, the classification is stored as a document property. In other supported files, it is stored as an XMP property. For email, it is added as markup text.

When setting up manual classification, you can also allow a user to manually apply content fingerprints.

Support for manual classification is as follows:

- McAfee DLP Endpoint users (on both Windows and Mac endpoints) can manually classify files.
- McAfee DLP Endpoint clients (on both Windows and Mac endpoints), McAfee DLP Prevent, and McAfee DLP Monitor can detect manually classified files (in email attachments, for example) and take appropriate action based on the classification.
- McAfee DLP Discover can detect manual classifications in classification and remediation scans, and can take appropriate action in remediation scans.

By default, users do not have permission to view, add, or remove classifications, but you can assign specific classifications to specific user groups, or to **Everyone**. The assigned users can then apply the classification to files as they work. Manual classification can also allow you to maintain your organization's classification policy even in special cases of sensitive or unique information that the system does not process automatically.

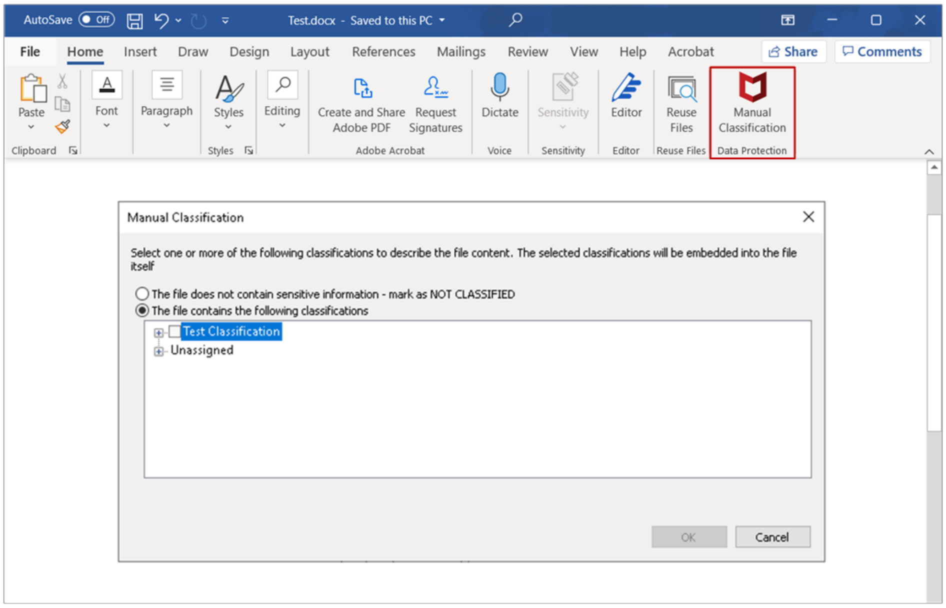
When setting up permission for manual classification, you have the option of allowing content classifications, content fingerprints, or both to be applied manually.

Support for manual classification

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

Microsoft Office applications (Word, Excel, and PowerPoint) and Microsoft Outlook are supported at the file creation level. Users can choose to classify files by clicking the manual classification icon. You can also set options to force users to classify files by activating the manual classification pop-up when files are saved, or Outlook emails sent.

Manual classification of an email is relevant for a specific thread only. If you send the same email twice in different threads, you have to classify it twice. For emails, information added to the header or footer (set on the manual classification **General Settings** page) is added as clear text.



Manual Classification

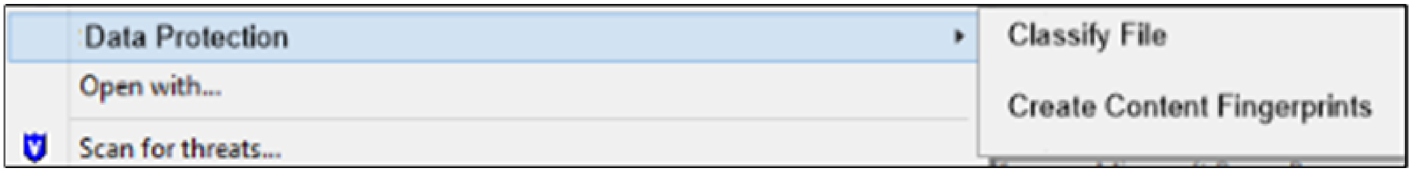
Select one or more of the following classifications to describe the file content. The selected classifications will be embedded into the file itself

○ The file does not contain sensitive information - mark as NOT CLASSIFIED

● The file contains the following classifications

- ☐ Test Classification
- Unassigned

All supported file types can be classified from Windows Explorer or Mac Finder using the right-click (Mac Ctrl-click) menu.



Embedding properties for third-party integration

Properties embedded when using manual classification allow third-party applications to integrate with McAfee DLP classified documents.

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

Document type	True file type	Method
Microsoft Word	DOC, DOCX, DOCM, DOT, DOTX, DOTM	document property
Microsoft PowerPoint	PPT, PPTX, PPS, PPSX, PPSM, PPTM, POT, POTM, POTX	
Microsoft Excel	XLS, XLSX, XLSM, XLSB, XLT, XLTX, XLTM	
XPS document	XPS	
Portable Document Format	PDF	XMP property
Audio and video formats	AIF, AIFF, AVI, MOV, MP2, MP3, MP4, MPA, MPG, MPEG, SWF, WAV, WMA, WMV	
Graphic and image formats	PNG, JPG, JPEG, TIF, TIFF, DNG, WMF, PSD	

The following table lists the internal properties.

Classification	Property name
Manual file classification	DLPManualFileClassification
File classification last modified by	DLPManualFileClassificationLastModifiedBy
File classification last modification date	DLPManualFileClassificationLastModificationDate
File classification version	DLPManualFileClassificationVersion
Endpoint discovery automatic classification	DLPAutomaticFileClassification

Classification	Property name
Endpoint discovery automatic classification version	DLPAutomaticFileClassificationVersion

Configure manual classification

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

Manual classification allows McAfee DLP Endpoint for Windows end-users to add classifications to files from the Windows Explorer right-click menu. For Microsoft Office applications and Outlook, manual classifications can be applied when saving files or sending emails. All McAfee DLP products can apply rules based on manual classifications.

Task

1. In McAfee ePO select **Menu** → **Data Protection** → **Classification**.
2. Click **Manual Classification**.
3. From the **View** drop-down list, select **General Settings**.
4. Select or deselect options to optimize to your enterprise requirements.
5. (Optional) Select additional information to add to the email by clicking ... and selecting a notification definition or creating one.
   The notifications support the **Locales** feature for all supported languages. Language support also applies to added email comments.

Registered documents and whitelisted text

The registered documents feature is an extension of location-based content fingerprinting. It gives administrators another way to define sensitive information, to protect it from being distributed in unauthorized ways. Whitelisted text is text that McAfee DLP ignores when processing file content.

To create registered documents, McAfee DLP categorizes and fingerprints the contents of files predefined as sensitive. For example, sales estimate spreadsheets for the upcoming quarter. It uses the fingerprints to create signatures that are stored as registered documents. The signatures created are language-agnostic, that is, the process works for all languages.

McAfee DLP supports two types of registered documents, manual and automatic.

Manual registration

Create manually registered documents by uploading files in the **Classification** module on the **Register Documents** page. Then create packages from the uploaded files, to create signatures. These signatures are made available to and downloaded by the endpoints from the shared location, and used in rules enforced on the endpoints.

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

McAfee DLP appliances also use manual registration. Signatures of the files are uploaded to McAfee ePO from McAfee DLP when you manually upload files and create a package. These signatures are made available to and downloaded by the appliances from the shared location. The appliance is then able to track any content copied from one of these documents and classify it according to the classification of the registered document signature.

Whitelisted Text — Upload whitelisted text files on the **Whitelisted Text** page. Whitelisted text does not cause content to be classified, even if parts of it match content classification or content fingerprinting criteria. Use whitelisting for text that commonly appears in files, such as boilerplates, legal disclaimers, and copyright information. Whitelisted text packages are created separately from the registered documents packages, and are distributed to the endpoints in a similar manner.

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

Automatic registration

Create automatically registered documents by running McAfee DLP Discover document registration scans. Use them to define classification and remediation scans, or protection rules for McAfee DLP Prevent and McAfee DLP Monitor.

McAfee DLP Discover registration scans create signature files that are stored as registered documents packages on the network, typically in the evidence storage share. A DLP Server assigned to act as the signature database loads the signatures from all storage shares. Each server configuration in the Policy Catalog can specify a DLP Server to distribute registered documents packages, so there can be more than one DLP Server in a network. In such a case, we recommend configuring each DLP Server to load signatures from all storage shares, as the signature databases are no longer synchronized. When a McAfee DLP Discover scan wants to match fingerprints, or McAfee DLP Monitor or McAfee DLP Prevent need to access the database to create a policy, they send an HTTP call using REST API. For DLP Server system requirements and installation information, see McAfee DLP Discover Installation Guide.

You can run registration scans on File Server, SharePoint, or Box repositories. Assign a classification to the registered documents on the **Scan Details** page when setting up the scan. You can view the scans on the **Register Documents** page when you select **Type: Automatic Registration**.

Viewing registered documents data

The default **Statistics** view displays totals for number of files, file size, number of signatures, and so forth, in the left pane, and statistics per file in the right pane. Use this data to remove less important packages if the signature limit is approached.

The **Group by** view for manual registration allows grouping by classification or type/extension. It displays uploaded files per classification or type. You can filter the data by classification or with a custom filter. Information about last package creation and changes to the file list are displayed in the upper right.

For automatic registration, **Group by** allows grouping by classification, repository server, scan, or True File type. You can filter the data by scan, classification, or with a custom filter.

Exact data matching

The Exact Data Matching (EDM) feature enables you to protect sensitive database records by only matching the actual values from the original records. Employee records, customer records, and patient medical records are typical examples of sensitive information that needs protection. Although you can protect such records by matching patterns and dictionary terms, these methods of data matching require complex condition and rule logic, which are prone to false matching.

Matching individual fields of a sensitive record (such as, name, social security number, date of birth, telephone number) might not be useful and can easily result in a false match. But matching two or more fields of the same sensitive record (for example, both name and social security number) within the same text (such as, an email or a document) indicates that meaningful related information is present.

EDM enables associative matching of multiple fields from the same record, allowing rules based on:

- Number of field matches that constitute a record match
- Required proximity of field matches
- Number of record matches that constitute an EDM classification criteria match

The workflow requires you to:

1. Prepare the sensitive data in a CSV file format.
2. Upload the CSV file directly into McAfee ePO. For large data sets that contain for than 100,000 rows, upload the CSV file using the CSV2Fingerprints.exe utility. These upload options are available when you click **Upload file** in the **Classification** → **Registered Documents** page.

   The CSV data is converted into an opaque hashed fingerprint format.

3. After you upload the CSV file into McAfee ePO, define classification criteria using the associative matching criteria.

Example

Consider you have this data record in a CSV file that has to be protected:

First Name	Last Name	Credit Card Number	Social Security Number	Phone number
John	Doe	1111222233334444	12345678	+1 9876543210

In the **Exact Data Fingerprints Match Criteria** page, try to match using "if at least 5 cell values out of 5 cell values... ". If a user sends an email with "Doe John CCN is 1111222233334444...", this will not match the CSV row because there is a need to match at least 5 columns. The email doesn't get blocked; but the CCN gets leaked.

In this CSV example, consider you want to prevent an individual's credit card number and social security numbers being leaked and you use the criteria "if at least 2 cell values out of 4 cell values...", without considering the "Phone number" column. In this case, you can potentially get many false EDM triggers for different combinations of data triggered from columns 1, 2, 3, and 4.

When defining the EDM criteria, we recommend you carefully analyze how many columns to match on and make the criteria as tight as possible. For example, use the criteria "if at least 3 cell values out of 4 cell values..." to protect data containing first name, last name, and CCN, or first name, last name, and SSN without causing false triggers.

Creating CSV file and fingerprinting CSV file

We recommend not to use common values in a CSV file. The values must be unique to get the best results while using EDM. Analyze the data that you want to protect (match) and make sure it is a meaningful match value. All values in the CSV file are indexed in the fingerprint file, regardless of the definition you use in classifications.

Fingerprint files are created automatically by uploading CSV files to McAfee ePO or for large data sets with more than 100,000 rows, upload the CSV file using the CSV2Fingerprints.exe utility and using the **Create package** feature. A fingerprint file is created and the hash of the CSV cell is added to a fingerprint file. This file is copied to the evidence network storage share folder, where McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor pick it up to use in classification and remediation scans.

Note

In scenarios where there is a difference between the available fingerprint files on the appliance and the expected fingerprint files as defined in the policy, the policy push gets temporarily rejected. This can happen if the .zip file containing new fingerprints is still being downloaded and processed, and a new policy is pushed by McAfee ePO containing references to fingerprint files that are not yet processed. After the fingerprint file processing is complete, the next policy push succeeds (unless you add new fingerprints and policy, in which case the policy push gets temporarily rejected again). The **Appliance Management** dashboard shows it as a corrupt policy. This is a temporary issue until the next push of the policy.

How to specify special characters in a CSV file?

The text containing special characters, such as backslash (\), double quotes (""), and comma (,), which are used as CSV values, must be entered in the CSV file as shown in these examples:

Description	Example	Entry in the CSV file
Text containing comma — include the text in double-quotes	Virgin Islands, British	"Virgin Islands, British"
Text containing double quotes — include the backslash character as an escape character for the quotes	"Hello"	\"Hello\"
Text containing backslash character — include the backslash character as an escape character for the backslash character itself	\\share\file	\\\\share\\file

Creating EDM classification criteria

The input for creating an EDM classification can have the following values:

- **Exact Data Fingerprints Records** — Matches the specific CSV file
- **Single record match criteria** — Matches a record in a file, for example, "at least X out of Y cell values appear in the text, in any order, less than Z characters apart"
- **Number of records to match** — For example, "find at least X records in the analyzed text"

Supported languages

EDM can scan traffic in all languages except languages that do not use whitespace characters or punctuation marks for breaking words. For example, Chinese and Japanese.

Limitations

- The first line of the CSV file must be a header of column names.
- Fingerprints can be uploaded as CSV or .zip files only. CSV files must be comma delimited and can't contain more than 100,000 records or rows (excluding the header) when invoking the utility from the UI.

Note

Automatic fingerprint creation is limited to files with less than 100,000 records. For larger CSV files, download the utility and create files manually using a command line or by drag-and-drop on the utility.

- Fingerprints are not created for cells with fewer than three characters.
- A column name can't contain more than 100 characters.
- Phone numbers in the fingerprint file only match identical numbers in text files. For example, a phone number entered in the CSV without a country code doesn't trigger a match with the same number in the text file if it includes the country code.
- The first and last names in a single column only match if they are in the same order. If the CSV column contains first name - last name, and the text file contains last name - first name, it doesn't trigger a match.

Note

You can avoid this limitation by placing first and last names in separate columns.

Backward compatibility

A classification with an EDM condition sent to any McAfee DLP product version earlier than McAfee DLP Discover version 11.1 or McAfee DLP appliances version 11.4 is ignored.

- If the criterion contains multiple conditions — for example Advanced Patterns AND Dictionaries AND EDM — it is evaluated based on the conditions that are recognized, and EDM is ignored.
- If the criterion contains only EDM, the criterion is considered empty and is evaluated as false, that is — as a non-match.

Find an exact match in a data file

You can protect sensitive data using the Exact data matching (EDM) feature. Sensitive data or data records you want to protect must be saved in the form of .csv file and used as classifications to match data for any violation.

The feature in McAfee DLP Discover supports exact data matching on File Server, SharePoint, Box, and Database repositories.

McAfee DLP Prevent appliances support scanning emails and web posts with EDM. McAfee DLP Monitor appliances support scanning emails, web posts, and network traffic with EDM.

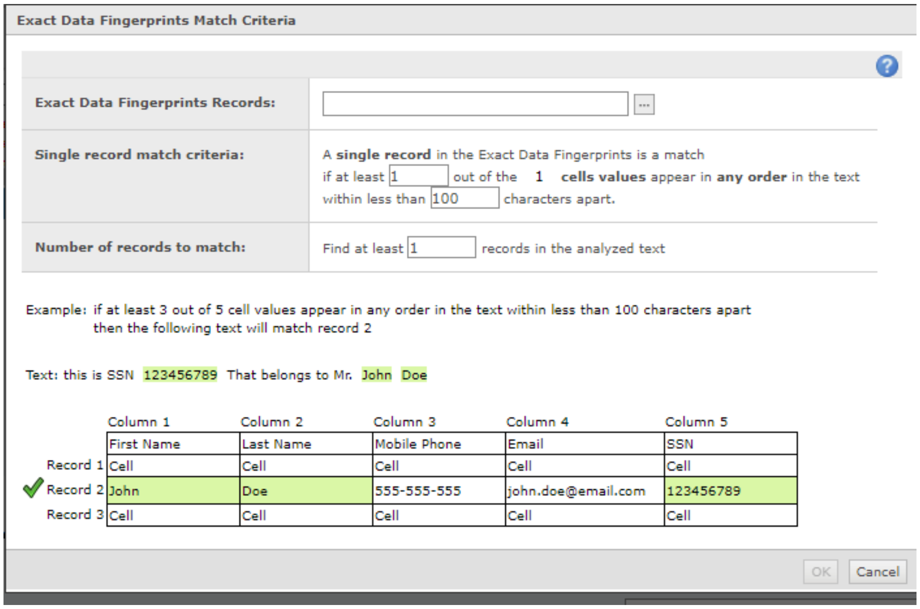
Data records are stored in CSV files as rows of data where the cells in each row are related, for example:

First name	Last name	Phone	Email
John	Doe	871-555-5555	j.doe@google.com

When you add an exact data match condition to a classification definition, apply that classification to the uploaded files and create an EDM package. McAfee DLP makes the EDM package available for classification and remediation scans.

Task

1. Upload CSV files with the data records that you want to protect from being leaked.
    a. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
    b. On the **Register Documents** tab, select **Exact Data Fingerprints** from the **Type** drop-down list.
    c. Click **Upload file**, select a CSV or .zip file to upload, then click **OK**.
    d. For uploads with more than 100,000 records, click the **executable** link to open the **CSV2Fingerprints.exe** utility.
2. Create or add an exact data match condition.
    a. In McAfee ePO, select **Menu** → **Data Protection** → **Classification.**
    b. Optional: Create a classification — select **Actions** → **New Classification** in the classifications list.
    You can also add an EDM condition to an existing classification.
    c. Select **Actions** → **New Content Classification Criteria**.
    d. From the **Data conditions** list, select **Exact Data Matching**.
    e. Click the choose icon (...) next to the **Value** field.
    The **Exact Data Fingerprints Match Criteria** page appears.



Exact Data Fingerprints Match Criteria

Exact Data Fingerprints Records:	
Single record match criteria:	A **single record** in the Exact Data Fingerprints is a match if at least 1 out of the 1 **cells values** appear in **any order** in the text within less than 100 characters apart.
Number of records to match:	Find at least 1 records in the analyzed text

Example: if at least 3 out of 5 cell values appear in any order in the text within less than 100 characters apart then the following text will match record 2

Text: this is SSN 123456789 That belongs to Mr. John Doe

	Column 1	Column 2	Column 3	Column 4	Column 5
	First Name	Last Name	Mobile Phone	Email	SSN
Record 1	Cell	Cell	Cell	Cell	Cell
✓ Record 2	John	Doe	555-555-555	john.doe@email.com	123456789
Record 3	Cell	Cell	Cell	Cell	Cell

f. Click the choose icon and select a CSV file from the list of files you uploaded. Fill in the match criteria and number of records to match. Click **OK**.

3. Create the package. On the **Register Documents** tab, select **Exact Data Fingerprints** from the **Type** drop-down list, then click **Create package**.

   All uploaded documents are added to the package, and the package is copied to the network evidence share folder.

4. (For McAfee DLP Discover only.) Create a network discovery rule.
   a. In the DLP Policy Manager, open a rule set or create one.
   b. On the **Discovery** tab, select **Actions** → **New Network Discovery Rule**, then select one of the repository types supported by the feature (File Server, SharePoint, Box, or Database).
   c. Select the classification you created in Step 2 and a repository that matches the type selected in Substep b. Fill in the rest of the fields, and click **Save**.
5. (For McAfee DLP Discover only.) Run the scan.
   a. In McAfee DLP Discover, on the **Scan Operations** page, select **Actions** → **New Scan** then select the appropriate repository type.
   b. Select the scan type (**Classification** or **Remediation**) and fill in the other fields as needed.
   c. On the **Repositories** tab, select a repository.
   d. On the **Rules** tab, select the rule set that includes the rule created in Step 4.
   e. Click **Save**.

Exact Data Fingerprints Match Criteria page

Use this screen to set up an exact data fingerprints match.

Option definitions

Option	Definition
Exact Data Fingerprints Records	Opens a window with a list of exact data fingerprints to select from.
Single record match criteria	Contains two text fields to specify the match criteria: The first field specifies the number of cell values to match. The second specifies the proximity.
Number of records to match	Text field to enter the number of matches.

Scanning image files with OCR

Optical character recognition (OCR) scans extract text from image files.

You can use the OCR feature for extracting text from image files. The extracted text is matched with classification definitions to classify or remediate files.

In McAfee DLP Discover, you can use the OCR feature when scanning any file-based repository. Database scans are not supported.

In McAfee DLP appliances, you can use the OCR feature when scanning images attached to emails, uploaded in web posts, or found in other network traffic.

Note

The OCR feature is supported in McAfee DLP Discover 11.1.100 and later and in McAfee DLP appliances 11.4.0 and later.

OCR is part of the text extraction feature. When the text extractor comes across an image file, a second pass is made with OCR to extract text and classify, remediate, or register the file according to the relevant rules. The feature also works with images saved as a .pdf file. If a .pdf file contains both text and images, it is scanned as a text file in the usual way. For example, McAfee DLP appliances monitor a hardcopy sensitive document scanned and sent in an email as a .pdf attachment. OCR scanning works with all McAfee DLP-supported languages, and most Western and Asian languages.

For information about installing and updating the OCR package in McAfee DLP Discover, see the *McAfee Data Loss Prevention Discover Installation Guide* and KB91046.

No additional software installation is needed on the McAfee DLP appliances to run the OCR feature.

Supported image formats

McAfee DLP Discover and McAfee DLP appliances support scanning of images of these formats:

- BMP*

- GIF
- JPEG
- PCX
- PDF
- PNG
- TIFF

* Although BMP files can be scanned, 32-bit BMP files (8 bits per color channel and 8-bit alpha channel) are not supported.

The following image formats are not supported on McAfee DLP appliances, but are supported on McAfee DLP Discover:

- TIFF-FX (Fax eXtended)
- WMP (Windows Media Photo)
- XPS (XML Paper Specification)

Unscannable images with McAfee DLP appliances

OCR scanning might fail on certain images because of:

- Image size greater than 8400 pixels
- Resolution is less than 75 dpi or more than 2400 dpi.
- OCR scanning time exceeding the timeout period of 5 minutes for an individual image
- File corruption that renders the file unreadable

On McAfee DLP Prevent appliances, OCR scan failure results in the entire email or web post being treated as unscannable. If there is no higher priority action set, such as BLOCK, the UNSCANNABLE action is executed. The McAfee DLP Prevent appliance adds **X-RCIS-Action: SCANFAIL** header to such unscannable emails received by the Smart Host.

For web posts, the web proxy receives a 400 Bad Request ICAP status. Any other detections in the email or web post still result in DLP incidents.

Limitations

OCR is resource-intensive, and significantly increases the scan time if there are many image files in the repository.

For this reason, in McAfee DLP Discover, it can be disabled with a checkbox on the **Text Extractor** page of the Server Configuration if it is not needed.

Creating and configuring classifications

Create a classification

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

Task

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

Create classification groups

Classifications are managed by placing them into logical groups.

Existing built-in classifications are grouped into logical groups, while new classifications are categorized into the **Unassigned** group until assigned a group.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Click **New Classification Group** from the **Actions** menu.
3. Enter a name for the group and an optional description.
4. Click **Save and New** to save the Group Name and enter another new classification group. Or click **Save** to exit the window.
5. To manage classifications in a group, select the group name and click **Manage Classifications**.
   The **Choose classifications** window opens.
6. Select one or more classifications from the list and click **Save**.
   The selected classifications are added to the group.

Results

Classification list is now grouped into logical categories for more efficient management.

Create classification criteria

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

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

Task

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

Create document properties

Create a classification based on document properties.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Click **New Classification**, type a unique name and an optional description.
3. Click **Actions**, then select **New Content Classification Criteria** or click the **Edit** link to change an existing classification criteria.
4. Click **Document Properties** , then click **...** and select **New item**.
5. Select the property you want, then click **Save**.

Upload registered or whitelisted documents

Select and create package of files to create signatures. These signatures are made available to the appliances and endpoints to track and classify content.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Click the **Register Documents** tab, and select **Type: Manual Registration**.
3. Click **File Upload**.

   The **Choose File** window appears.
4. Browse to the file, select it, then select whether to replace the file if the file name exists and which classification to apply to the file.

   File Upload processes a single file. To upload multiple documents, create a .zip file.
5. Click **OK**.

   The file is uploaded and processed, and statistics are displayed on the page.
6. Click **Create Package** when the file list is complete.

   When files are deleted, remove them from the list and create a new package to apply the changes.
7. To upload whitelisted documents, repeat this procedure on the **Classification** → **Whitelisted Text** tab.

   For whitelisted text, only the replace file option appears in the **Choose File** window.

Results

Signature packages of all registered documents and all whitelisted documents are loaded to the McAfee ePO database for distribution to the endpoints.

Note

From McAfee DLP 11.5 and onwards, creating the package applies all client configurations and the version number is incremented.

Test classifications

Check if a phrase or file is triggered with your classifications by running the classification tester.

Classifications with the following conditions can't be tested:

- Exact Data Matching
- Third-party tags
- Registered documents
- Whitelisted text
- Content fingerprinting
- Manual classifications

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**. Click the **Classification Tester** tab.

2. In the Classifications List area, select the classifications you want to test. Classifications that can't be tested appear as grayed out.
3. To enter text, either click **Browse** to select a file from your network, or select **Plain Text** to enter text manually. Maximum file size for upload is 50 MB.

   Note

   > The **Plain Text** field has a limit of 1024 characters. If the text containing sensitive content appears beyond this limit, the text gets truncated and the classification doesn't show any match.

4. In **Time-out test after**, select the amount of time the classification tester attempts to provide results.
5. Click **Start Test**.

Results

The results of the test appear in the **Test Results** area. Text that is triggered is highlighted.

Classification tester page

Use this page to test classifications by checking if a phase or file triggers the classifications.

Option definitions

Category	Option	Definition
Classifications List	**Select classifications for testing.**	Lists all your classifications, including built-in and customized. Use the search box to search for classifications from the list. Use the expand button to view the classifications in groups and select classifications by clicking the checkboxes.
Test Data	**Select a file, or enter text to test your classifications.**	Options for adding text. • **Browse** — When option is selected, the browse button is enabled, and you can browse your network to upload a file. Maximum file size for upload is 50 MB. • **Plain Text** — When option is selected, you can enter text manually. **Note:** The **Plain Text** field has a limit of 1024 characters. If the text containing sensitive content appears beyond this limit, the text gets truncated and the classification doesn't show any match.

Category	Option	Definition
	Run test.	• **Time-out test after** — Use the menu to select the amount of time the classification tester attempts to provide results. • **Start Test** — Starts testing the selected classifications and text.
Test Results		Displays the results of the classification test.

Check classification usage in rules

You can check which rules are using a specific classification.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. In the **Classification** list, select the classification you want to check usage in rules.
3. Select **Actions** → **Classification Usage**.
   The **Classification Usage** window displays a list of all rules that use the selected classification. You can click a rule to make changes, if needed.

   Note

   If you delete a classification that is in use with other rules, the **Classification Usage** window opens automatically.

Configuring classification components for McAfee DLP

Create content fingerprinting criteria

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

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Select the classification to add the criteria to.
3. Select **Actions** → **New Content Fingerprinting Criteria**, then select the type of fingerprinting criteria.
4. Enter the name and specify additional information based on the type of fingerprinting criteria.
   - **Application** — Click **...** to select one or more applications.

- **Location** — Click **...** to select one or more network shares. If needed, specify the type of removable media.
- **Web application** — Click **...** to select one or more URL lists.

5. (Optional) Select one or more properties and configure the comparison and value entries.
   - To remove a property, click **<**.
   - For some properties, click **...** to select an existing property or to create a new one.
   - To add additional values to a property, click **+**.
   - To remove values, click **–**.
6. Click **Save**.

Assign manual classification permissions

Configure users allowed to manually classify files.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Click the **Manual Classification** tab.
3. From the **View** drop-down list, select either **Group by classifications** or **Group by end-user groups**.
   You can assign classifications to end-user groups or end-user groups to classifications, which ever is more convenient. The **View** list controls the display.
4. If you are grouping by classifications:
   a. Select a classification from the displayed list.
   b. In the **Classifications** section, select the classification type.
      Reduce the list by typing a string in the **Filter list** text box if the list is very long.
   c. Select **Actions** → **Select End-User Groups**.
   d. In the **Choose from existing values** window, select user groups or click **New Item** to create a new group. Click **OK**.
5. If you are grouping by end-user groups:
   a. Select a user group from the displayed list.
   b. Select **Actions** → **Select Classifications**.
   c. In the **Choose from existing values** window, select classifications. Click **OK**.

How end users can classify their own files

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

Users working on Windows or Mac computers with McAfee DLP Endpoint can classify files manually. Files classified manually are supported by McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor rules.

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

Task

1. Create a user group or groups for workers who create or edit patient records.
   a. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
   b. On the **Definitions** tab, select **Source/Destination** → **End User Group**.
   c. Select **Actions** → **New Item**, replace the default name with a meaningful name such as `PHI User Group`, and add users or groups to the definition.
   d. Click **Save**.
2. Create a PHI (Protected Health Information) classification.
   a. In the **Classification** module, on the **Classification** tab, select **[Sample] PHI [built-in]** in the left pane, then select **Actions** → **Duplicate Classification**.
      An editable copy of the sample classification appears.
   b. Edit the **Name**, **Description**, and **Classification Criteria** fields as required.
   c. In the **Manual Classification** field, click **Edit**.
   d. In the **Additional Actions** section, select the classification type.
      By default, **Manual classification** only is selected.
   e. Select **Actions** → **Select End-User Groups**.
   f. In the **Choose from existing values** window, select the group or groups you created previously, then click **OK**.
   g. Go back to the **Classification** tab and select **Actions** → **Save Classification**.

Results

Workers who are members of the assigned groups can now classify the patient records as they are created. To do so, right-click on the file, select **Data Protection**, and select the appropriate option.

Note

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

Creating classification definitions

Create a general classification definition

Create and configure definitions for use in classifications and rules.

Task

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

   The available options and properties depend on the type of definition.
4. Click **Save**.

Create or import a dictionary definition

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

You can create a dictionary definition by importing a dictionary file in CSV format. You can also import items with a script containing REST API calls. The administrator running the script must be a valid McAfee ePO user who has permissions in McAfee ePO **Permission Sets** to perform the actions that are invoked by the APIs.

Tip

Dictionary CSV files can use multiple columns. Export a dictionary to understand how the columns are populated before creating a file for import.

Task

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 Item**.
5. Enter a name and optional description.
6. Add entries to the dictionary.

   To import entries:

   a. Click **Import Entries**.

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

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

   c. Click **OK**.

      All entries are assigned a default score of 1.

   d. If needed, update the default score of 1 by clicking **Edit** for the entry.

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

      Start With and **End With** provide substring matching.

   To manually create entries:

   a. Click **Actions** → **Add**.

   b. Enter the phrase and score.
   c. Select the **Start With**, **End With**, and **Case Sensitive** columns as needed.
   d. Click **Save** or to add another entry click **Save and New**.
7. Click **Save**.

Use case: Create a keyword-based dictionary definition

Create a dictionary definition based on a lowercase keyword and add it to a classification.

Task

1. In McAfee ePO, go to **Classification** → **Definitions** → **Dictionary** and click **Actions** → **New Item**.
2. Give the dictionary definition a name and an optional description, then click **Actions** → **Add**.
3. In **Phrase**, type the word `security`, then set the **Score** as 1 and select **Case Sensitive** to only match on the keyword when it is lowercase.
4. Click **Add**, then click **Save**.
5. Select **Classification** → **New Classification**. Give the classification a name, add an optional description, and click **OK**.
6. Select the newly created classification and click **Action** → **New Content Classification Criteria**.
7. Select the dictionary and use the comparison (OR/AND/NOT).
8. Click **(...)** and select the dictionary definition you recently created, give it a threshold of 10 and click **OK**.
9. Assign the classification to a rule to trigger the classification.

Create a definition based on 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).

Note

There is no equivalent to the **Percentage match** and **Number of bytes from the beginning** options in McAfee DLP Appliances.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Select the **Definitions** tab, then select **Advanced pattern** in the left pane.
   To view only the user-defined advanced patterns, deselect **Include Built-in items**. User-defined patterns are the only patterns that can be edited.
   The available patterns appear in the right pane.

3. Select **Actions** → **New Item**.
4. Enter a name and optional description.
5. Under **Matched Expressions**:
    a. Enter an expression in the text box and add an optional description.
    b. Select a validator from the drop-down list or if validation is not appropriate for the expression, select **No Validation**. A validator is the same as algorithm in McAfee DLP 9.3.x. Use it to minimize false positives.
    c. Enter a number in the **Score** field to indicate the weight of the expression in threshold matching.
    d. Click **Add**.
6. Under **Ignored Expressions**:
    a. Enter an expression in the text box.
       If you have text patterns stored in an external document, copy 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. Keyword expressions can also be added using **Import Keywords**, entering keywords separated by a new line.
    c. Click **Add**.
7. Add the count to the concept:
    a. Give all the expressions a score of 1.
    b. When you assign the dictionary to the classification, give the threshold the same value that the count setting had in McAfee DLP 9.3.x.
    c. Select **count multiple occurrence of each match string** if the score must be added for multiple occurrence of a single expression in a document.
    d. Select **count each match string only one time** if the score should not be added and should be one even when multiple occurrences of a single expression are present in a document.
    e. Select **start with** and **end with** to see if the document starts or ends with the expression, or select both options to find the expression anywhere in the document.
    f. To match on the number of lines from the beginning of the document, you can create a new regular expression using conditions such as less than, equals, or greater than.
8. Click **Save**.

Create a URL list definition

URL list definitions are used to define web protection rules and web content fingerprinting classification criteria. They are added to rules and classifications as **Web address (URL)** conditions.

You can create a URL list definition by importing the list in CSV format. You can also import items with a script containing REST API calls. The administrator running the script must be a valid McAfee ePO user who has permissions in McAfee ePO **Permission Sets** to perform the actions that are invoked by the APIs.

Tip

URL list CSV files can use multiple columns. Export a URL list to understand how the columns are populated before creating a file for import.

Perform these steps for each URL required.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select URL List, then select **Actions** → **New Item**.
3. Enter a unique **Name** and optional **Definition**.
4. Do one of the following:
   - Enter the **Protocol**, **Host**, **Port**, and **Path** information in the text boxes, then click **Add**.

     Note

     You can also add an optional query string.

   - Paste a URL in the **Paste URL** text box, then click **Parse**, then click **Add**.

   The URL fields are filled in by the software.
5. When all required URLs are added to the definition, click **Save**.

Classify sensitive content using Boldon James and Titus labels

Create classifications using Titus and Boldon James classification labels.

Before you begin

1. Install the third-party API on the endpoints.
2. In the **Policy Catalog**, open the current Windows Client Configuration. Select **Settings** → **Operational Modes and Modules**. Verify that **Outlook Add-ins** → **Activate 3rd Party Add-in Integration** is selected.
3. In **Settings** → **Email Protection**, in the **Outlook 3rd Party Add-in Integration** section, select **Titus**, or **Boldon James** from the **Vendor Name** drop-down list.

Note

These settings affect the use of third-party tags with email only. You can use third-party tags with files without changing client configuration settings.

Titus and Boldon James are popular solutions for classifying and protectively labeling files and emails. McAfee DLP Endpoint can integrate with these applications by calling the third-party API to identify tagged files and determine the tags. You can apply classifications created with third-party tags to email and to all protection and discovery rules that inspect files.

Note

Boldon James limitations:

- Boldon James classifications are only supported on NTFS file systems.
- Classifications must be in rules that use file information.
- In screen capture protection rules, Boldon James only supports fingerprint classifications.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Click **New Classification**.
3. Type a unique name and an optional description.
4. Click **Actions**, then select either **New Content Classification Criteria** or **New Content Fingerprinting Criteria**.
5. Select the **Third Party tags** property.
6. Select the classification labels as needed.
    - Enter the Titus tag name and a value. Define the value string by selecting a value from the drop-down list and typing in a value. Define the value string entered for Titus tag names as:
        - **equals one of**
        - **equals all of**
        - **contains one of**
        - **contains all of**
    - Enter the Boldon James selector name and the value. Define the value string by selecting a value from the drop-down list and typing in a value. Define the value string entered for Boldon James tag names as:
        - **equals one of**
        - **equals all of**
        - **contains one of**
        - **contains all of**
7. (Optional) Click **+** and add another name or value pair.
8. Click **Save**.

Classify sensitive content using Microsoft RMS or Azure Information Protection labels

You can use the third party tags option to identify and track sensitive content for documents maintained using third party tools. Microsoft RMS templates or Azure Information Protection labels can be used for these classifications.

Before you begin

Make sure that your server is defined in **Registered Servers** in McAfee ePO. For more information about registering third-party servers, see McAfee DLP Endpoint Installation Guide.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Click **New Classification**.
3. Type a unique name and an optional description.
4. Click **Actions**, then select either **New Content Classification Criteria** or **New Content Fingerprinting Criteria**.
5. Select the **Third Party tags** property.
6. Select the classification labels as needed.
   - Select the Microsoft RMS server name from the **Value** drop-down list and select a template for that server. To select a template, click picker and select the template from the pop-up window.
   - Select the Azure RMS server name from the **Value** drop-down list and provide a label. To select a label, click picker and select the label from the pop-up window.
7. (Optional) Click **+** and add another name / value pair.
8. Click **Save**.

Results

The selected tags are applied to the classification.

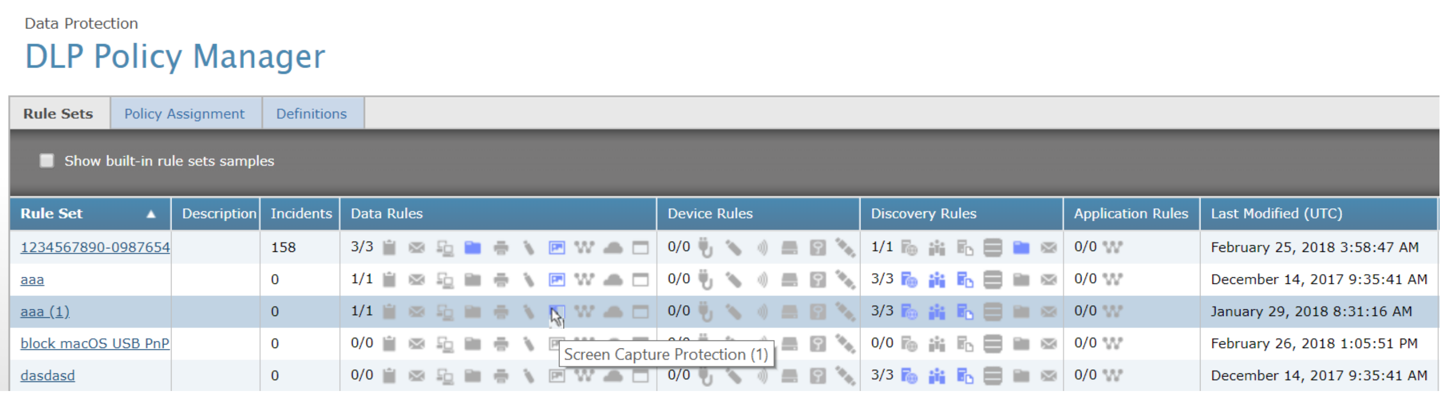
Using rules and policies to protect sensitive content

Creating policies with rule sets

Rule sets define McAfee DLP policies. A rule set can contain a combination of data protection, device control, discovery rules, and application control rules. Rule definitions apply to all rule sets.

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

Rule Sets page showing tooltip information



Data Protection

DLP Policy Manager

☐ Show built-in rule sets samples

Rule Set ▲	Description	Incidents	Data Rules	Device Rules	Discovery Rules	Application Rules	Last Modified (UTC)
1234567890-0987654		158	3/3	0/0	1/1	0/0	February 25, 2018 3:58:47 AM
aaa		0	1/1	0/0	3/3	0/0	December 14, 2017 9:35:41 AM
aaa (1)		0	1/1	0/0	3/3	0/0	January 29, 2018 8:31:16 AM
block macOS USB PnP		0	0/0	0/0	0/0	0/0	February 26, 2018 1:05:51 PM
dasdasd		0	0/0	0/0	3/3	0/0	December 14, 2017 9:35:41 AM

In Rule set *aaa (1)*, one data protection rule is defined, and it is enabled (*1/1* at the left of the **Data Rules** section). The blue icons show which types of rules are defined. The tooltip shows one of these is a screen capture protection rule. To view which rules are defined but disabled, open the rule for editing.

Create a network port range

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

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select **Network Port**, then click **Actions** → **New**.
   You can also edit the built-in definitions.
3. Enter a unique name and optional description.
4. Enter the port numbers, separated by commas, and optional description, then click **Add**.
5. When you have added all required ports, click **Save**.

Create a network address range

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

For each required definition, perform steps 1–4:

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select **Network Address (IP address)**, then click **Actions** → **New**.
3. Enter a unique name for the definition and an optional description.
4. Enter an address, a range, or a subnet in the text box. Click **Add**.
   Correctly formatted examples are displayed on the page.

   Note

   > Only IPv4 addresses are supported. If you enter an IPv6 address, the message says `IP address is invalid` rather than saying that it isn't supported.

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

Create an email address list definition

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

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

Tip

> For combinations of operators that you use frequently, add multiple entries to one email address list definition.

You can import email address lists in CSV format.

You can also import items with a script containing REST API calls. The administrator running the script must be a valid McAfee ePO user who has permissions in McAfee ePO **Permission Sets** to perform the actions that are invoked by the APIs.

Tip

> Email address list CSV files use multiple columns. Export an address list to understand how the columns are populated before creating a file for import.

Email value definitions support wildcards, and can define conditions. An example of a condition defined with a wildcard is *@mcafee.com. Combining an address list condition with a user group in a rule increases granularity.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select **Email Address List**, then **Actions** → **New**.
3. Enter a **Name** and optional **Description**.
4. Select an **Operator** from the drop-down list.

   Operators defined using the **Email Addresses** option support wildcards in the **Value** field.
5. Enter a value, then click **Add**.
6. Click **Save** when you have finished adding email addresses.

Create a network printer definition

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

Before you begin

Obtain the UNC path of the printer in the network.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left panel, select **Network Printer**, then select **Actions** → **New Item**.
3. Enter a unique **Name** and optional **Description**.
4. Enter the **UNC** path.

   All other fields are optional.
5. Click **Save**.

Create a URL list definition

URL list definitions are used to define web protection rules and web content fingerprinting classification criteria. They are added to rules and classifications as **Web address (URL)** conditions.

You can create a URL list definition by importing the list in CSV format.

You can also import items with a script containing REST API calls. The administrator running the script must be a valid McAfee ePO user who has permissions in McAfee ePO **Permission Sets** to perform the actions that are invoked by the APIs.

Tip

> URL list CSV files can use multiple columns. Export a URL list to understand how the columns are populated before creating a file for import.

Perform these steps for each URL required.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select URL List, then select **Actions** → **New Item**.
3. Enter a unique **Name** and optional **Description**.
4. Do one of the following:
    - Enter the **Protocol**, **Host**, **Port**, and **Path** information in the text boxes, then click **Add**.

      Note

      You can also add an optional query string.

    - Paste a URL in the **Paste URL** text box, then click **Parse**, then click **Add**.

   The URL fields are filled in by the software.
5. When all required URLs are added to the definition, click **Save**.

Defining rules to protect sensitive content

Rules define the action taken when an attempt is made to transfer or transmit sensitive data.

Rule sets can contain four types of rules, data protection, device control, discovery, and application control, though not all rule types are supported by all McAfee DLP products.

Product	Data Protection	Device Control	Discovery	Application Control
McAfee Device Control	No **Note:** If you have installed Device Control with content aware removable storage protection, removable storage protection rules are supported.	(Same as full endpoint products for Mac and Windows)	No	No
McAfee DLP Endpoint for Windows	All except mobile protection rules	All	Endpoint discovery rules	All

Product	Data Protection	Device Control	Discovery	Application Control
McAfee DLP Endpoint for Mac	Application file access, cloud, network share, email (monitoring only)and removable storage protection rules	Plug and play and removable storage protection rules	Endpoint file discovery rules	No
McAfee DLP Monitor	Email, web, and network communication protection rules	No	No	No
McAfee DLP Prevent	Email and web protection rules	No	No	No

A rule has three parts in addition to the basic rule definition. The basic definition includes the **Rule Name**, optional **Description**, drop-down lists to define the **State** (enabled or disabled) and **Severity**, and check boxes to define which McAfee DLP product the rule supports. The three parts of the rule — **Condition**, **Exceptions**, and **Reaction** — are defined on separate tabs in the rule definition.

Condition

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

Exceptions

Exceptions define parameters excluded from the rule. Exceptions have a separate setting to enable or disable them, allowing you to turn the exception on or off when you test rules. Creating an exception definition is optional.

For example, a cloud protection rule can allow specified users and classifications to upload data to the specified cloud services. At the same time, the rule can also block users and classifications defined in the condition section of the rule.

Exception definitions for data protection and discovery rules are similar to condition definitions. The available parameters for exclusion are a subset of the parameters for defining the condition.

Exception definitions for data protection rules are similar to condition definitions. The available parameters for exclusion are a subset of the parameters for defining the condition.

For device control rules, the exception is defined by selecting whitelisted device templates from a list. The available whitelisted templates depend on the type of device rule.

Reaction

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

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

Defining rules by reputation

Use a Threat Intelligence Exchange file and certificate security reputations to define rules.

You can define certain rules using reputations from Threat Intelligence Exchange.

McAfee® Threat Intelligence Exchange (TIE) software determines and distributes file and certificate security reputations. McAfee DLP communicates with the McAfee® Data Exchange Layer (DXL) in TIE to share information about file type and certificate threat levels. You can define the **Applications** field in application file access protection rules according to TIE reputation.

Protecting data-in-use

Data protection rules monitor and control user content and activity.

Data protection rules must specify at least one classification. The classification identifies the content as sensitive or not, and determines accordingly what can be done with the content. Other definitions in the rule act as filters to determine which files are monitored.

Data protection rules are supported differently by the different McAfee DLP applications.

- McAfee DLP Endpoint for Windows supports all data protection rules.
- McAfee DLP Endpoint for Mac supports application file access, network share, removable storage protection rules, and email protection rules.
- McAfee DLP Prevent supports email and web protection rules.
- McAfee DLP Monitor supports email, web, and network communication protection rules.

Note

McAfee DLP Monitor is a passive device that reports on detected incidents but does not block or modify the data.

How data protection rules work

Protecting content by application

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

To limit the rule to specific applications, select an application or URL definition. You can also specify a TIE reputation.

Note

URL definitions are not supported on McAfee DLP Endpoint for Mac.

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

Controlling copy-paste

Clipboard protection rules manage content copied with the Windows clipboard. They are supported on McAfee DLP Endpoint for Windows only.

Clipboard protection rules are used to block or request justification for copying sensitive content from one application to another. The rule can define both the application copied from and the application copied to, or you can write a general rule specifying any application for either source or destination. Supported browsers can be specified as applications. The rule can be filtered with an end-user definition to limit it to specific users. As with other data protection rules, exceptions to the rule are defined on the **Exceptions** tab.

By default, copying sensitive content from one Microsoft Office application to another is allowed. If you want to block copying within Microsoft Office, disable the Microsoft Office clipboard in the Windows client configuration.

Protecting cloud uploads

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

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

The McAfee DLP Endpoint **Cloud Protection Rule** supports:

- Box Sync
- Dropbox
- GoogleDrive
- iCloud
- OneDrive (personal)

- OneDrive for business (groove.exe)
- Syncplicity

Note

iCloud and Syncplicity are not supported on McAfee DLP Endpoint for Mac.

To improve scanning speed, you can specify the top-level subfolders included or excluded in the rule.

Protecting email content and attachments

Email protection rules monitor or block email sent to specific destinations or users. They are supported on McAfee DLP Endpoint for Windows , McAfee DLP Endpoint for Mac (supports monitoring emails only), McAfee DLP Monitor, McAfee DLP Prevent, and McAfee® MVISION Cloud.

Email protection rules enforced on McAfee DLP Monitor and McAfee DLP Prevent can be saved as DLP Capture searches so you can tune the settings without affecting the live rule analysis.

Email protection rules can block emails according to the following parameters:

- **Classification** definitions limit the rule to specific content fingerprinting or content classification criteria. You can apply classifications to the whole email, or just the subject, body, email headers, or attachments.

  From McAfee DLP 11.1, the **one of the email elements** option does not include email headers other than **subject** for email protection rules used by the McAfee DLP appliances. You must add other email headers separately.

- **Sender** definitions limit the rule to specific user groups or email address lists. User group information can be obtained from registered LDAP servers. You can also limit the rule to local or non-LDAP users.
- The **Email Envelope** field specifies the email is protected by RMS permissions, PGP encryption, digital signature, or S/MIME encryption. This option is typically used to define exceptions.

  Note

  When the envelope is S/MIME and there is no S/MIME certificate for the recipient, the Outlook pop up allowing the email to be sent unencrypted appears. But, if there is a matching rule to block the email, McAfee DLP Prevent blocks the email.

- The **Recipient** list includes email address list definitions. The definitions can use wildcards in the operator field.

Messages that cannot be analyzed

If McAfee DLP Prevent is unable to extract text from a message to analyze it because, for example, the message is corrupt, it takes the following action:

- Rejects the email and returns it to the MTA.
- The MTA keeps trying to deliver the message to McAfee DLP Prevent.

- When McAfee DLP Prevent identifies that it cannot analyze the message, it adds the X-RCIS-Action header with the SCANFAIL value to the message.
- McAfee DLP Prevent sends the message with the modified X-RCIS-Action header to one of the configured smart hosts.

Note

McAfee DLP Prevent makes no other change to the message.

If the message contains an encrypted, corrupt, or password-protected attachment, the message is analyzed for data loss triggers, but the attachment is not analyzed. The SCANFAIL value is not added because the message contents were partially analyzed.

Notifying an email sender of policy violations

McAfee DLP Prevent enables you to actively block an email message and return the message to the sender with a notification when there is a policy violation.

You can configure McAfee DLP Prevent to block an email that violates policy and send a notification to the configured Smart Host.

The Smart Host returns the original email to the sender as an attachment to a notification. An additional details file in HTML format is also attached to this notification. This additional details file includes information about the incident type, severity level, blocked status, date and time about when the incident occurred, sender, and recipient details. The file also shows the evidence details, rules that triggered the incident, and the classification details.

Important

The block and return email to sender reaction always takes priority over the add X-RCIS-Action header reaction.

You can choose the predefined **User Notification** definition as the notification message or create a customized notification using the placeholder values in the **User Notification definition** page. You can also choose to send an incident about the bounced message.

If the notification email delivery to the sender fails due to a temporary failure code (4xx), the incident is not generated. The original mail remains in the temporary failed state and is queued on the sending Smart Host. The Smart Host retries sending the email message.

If the notification email delivery to the sender is rejected due to a permanent error (5xx), an incident is generated. The original mail gets rejected with the 5xx error code.

Note

When a notification email delivery fails because of 5xx error code, the original email message from the sender gets blocked. The email message is not returned to the sender and the **Incident Manager** shows this email message as blocked.

McAfee DLP Prevent X-RCIS-Action header behavior

You can take several actions on the email messages that are sent to the Smart Host. You can use the **Add header to X-RCIS-Action** reaction to add values to the email message headers. The Smart Host implements the action that is indicated in the X-RCIS-Action header.

X-RCIS-Action header values

Priority	Value	Indicates
1	BYPASS	Added to messages that are bypassed from scanning.
2	SCANFAIL	Messages that cannot be analyzed. The appliance generates the SCANFAIL header value automatically. So the header value cannot be configured as an action within a rule.
3	BLOCK	Blocks the message.
4	QUART	Quarantines the message.
5	ENCRYPT	Encrypts the message.
6	BOUNCE	Issues a Non-Delivery Receipt (NDR) message to the sender.
7	REDIR	Redirects the message.
8	NOTIFY	Notifies supervisory staff.
9	ALLOW	Allows the message through. The Allow value is added automatically to all messages that do not contain any matched contents.

When not monitoring, McAfee DLP Prevent always delivers an email to a configured Smart Host. The Smart Host implements the action that is indicated in the X-RCIS-Action header.

If the message triggers multiple rules, the highest priority value is inserted into the X-RCIS-Action header (where 1 is the highest priority). If no rules are triggered, the ALLOW value is inserted.

If another appliance analyzes a message and adds an X-RCIS header, McAfee DLP Prevent replaces the existing header with its own header.

Adding BYPASS value to the X-RCIS-Action header

You can configure the McAfee DLP appliance to bypass scanning of emails sent from the specified email addresses. To these bypassed emails, you can choose to add the BYPASS value to the X-RCIS-Action header or not add a header in the message sent to the configured Smart Host.

X-MFE-PREVENT: SCANFAIL ICAP header behavior

McAfee DLP Prevent adds the **X-MFE-PREVENT: SCANFAIL** header in its ICAP response when it detects unscannable content or for ICAP requests that exceed the maximum configured file size for scan.

McAfee DLP Prevent categorizes content as unscannable when it can't be analyzed. Examples of unscannable content include corrupt files, files that exceed the maximum analysis size or time, and files that exceed maximum depth if there are nested files. The appliance allows an ICAP request with unscannable content and sends a 2xx ICAP response back to the web proxy server. In addition, the appliance adds the **X-MFE-PREVENT: SCANFAIL** header in its ICAP response when it detects unscannable content.

By default, the McAfee DLP Prevent appliance sends a 4xx ICAP response back to the web proxy server for ICAP requests that exceed the maximum configured file size for scan. You can configure the McAfee DLP Prevent appliance to allow these ICAP requests with a 2xx response. When the configuration is enabled, the appliance sends the 2xx ICAP response back to the web proxy server and also adds the **X-MFE-PREVENT: SCANFAIL** header with information about the cause of the ICAP response. For information about how to configure to allow ICAP requests that exceed the maximum configured file size for scan with a 2xx response, see KB91550.

Controlling network traffic

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

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

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

Note

> Network communication protection rules on McAfee DLP Endpoint for Windows do not check content classification criteria. Use content fingerprinting criteria when defining classifications used with network communication protection rules.

Protecting network shares

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

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

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

Protecting sensitive content sent to printers

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

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

Protecting content written to removable devices

Removable storage protection rules monitor or block data from being written to or from removable storage devices. They are supported on McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac. On McAfee DLP Endpoint for Mac, CD and DVD devices are not supported.

Removable storage protection rules control CD and DVD devices, removable storage devices, or both. They can block copying to or from the device, or both. Limit the rule with content fingerprinting or content classification criteria in classifications (required). You can also define the rule with specified users, applications, or web URLs.

Note

> Removable storage protection rules for McAfee DLP Endpoint for Mac only support control of removable storage devices. They do not support CD/DVD devices.

Use classifications to limit the rule. You can also limit the rule by specifying users, or the applications copying the file.

Controlling screen captures

Screen capture protection rules control data copied and pasted from a screen. They are supported on McAfee DLP Endpoint for Windows only.

Use classification definitions to limit the rule to specific content fingerprinting criteria. You can also limit the rule to local users or to specified user groups, or by applications visible on the screen.

Note

> Screen capture protection rules do not check content classification criteria. Use content fingerprinting criteria when defining classifications used with screen capture rules.

To block screen captures from the Windows Explorer preview pane, disable the pane in the client configuration (**Policy Catalog** → **Windows Client Configuration** → **Screen Capture Protection**).

Controlling content posted to websites

Web protection rules monitor or block data from being posted to websites, including web-based email sites. They are supported on McAfee DLP Endpoint for Windows and McAfee DLP Prevent. McAfee DLP Monitor also supports web protection rules, but can't block data.

Web protection rules enforced on McAfee DLP Monitor and McAfee DLP Prevent can be saved as DLP Capture searches so you can tune the settings without affecting the live rule analysis.

Four conditions define web protection rules:

- Classification
- End User
- Web address (URL)
- Upload type

Define the rule by adding **URL List** definitions to the web address condition. You can use built-in **URL List** definitions as is or with changes that you define. Internet Explorer, Firefox, Chrome and Microsoft Edge (Chromium-based) support whitelisted URLs in web protection rules. Enter the URLs you want to whitelist on the **Web Protection** page of the client configuration.

Note

For more information about URL list definitions, see KB90846.

Use the upload type **is file upload** to limit the rule to files only. This option allows other data types, such as webmail or web forms, to be uploaded without inspection.

Web protection rules aggregate repeat incidents. If you try to upload the same file to a website several times, or if the website automatically tries repeated uploads, it produces a single incident in the DLP Incident Manager.

Working with Chrome and Microsoft Edge browsers

McAfee DLP web post protection rules can block file uploads posted with Chrome and Microsoft Edge (Chromium-based) browsers. The web protection rule evaluates the Web Address (URL) condition with the browser address bar URL.

For text posts, the web protection rule evaluates the Web Address (URL) condition with the HTTP request URL. Because HTTP requests rely on the Chrome browser extensions, text posts can only be monitored.

Note

We recommend disabling Chrome guest and incognito mode in the Windows Client Configuration. If either of these are enabled, the active web URL on the endpoint might be unavailable.

One alternative to blocking web posts at the endpoint is to apply McAfee DLP web protection rules by enforcing the same web post protection rules on McAfee DLP Prevent. You can also use McAfee Web Gateway, which has native DLP capabilities.

Device control rules

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

Device control rules can monitor or block devices attached to enterprise-managed computers.

McAfee DLP Endpoint for Windows supports the following types of rules:

- **Citrix XenApp Device Rule**
- **Fixed Hard Drive Rule**
- **Plug And Play Device Rule**
- **Removable Storage Device Rule**
- **Removable Storage File Access Device Rule**
- **TrueCrypt Device Rule**

McAfee DLP Endpoint for Mac supports the following types of rules:

- **Plug And Play Device Rule** (USB devices only)
- **Removable Storage Device Rule**

Device control rules are described in detail in **Protecting sensitive data from being copied to storage devices**.

Endpoint and network discovery rules

McAfee DLP Endpoint and McAfee DLP Discover use discovery rules to scan files and repositories.

Data vector descriptions

Product	Discovery rule
McAfee DLP Endpoint	**Local Email (OST, PST)**
	Local File System
McAfee DLP Discover	**Box Protection**
	Database Protection
	File Server Protection

Product	Discovery rule
	SharePoint Protection

Application control rules

Application control rules monitor or block user access to websites. They are enforced on McAfee DLP Endpoint for Windows.

Web application control rules are similar to web protection rules, but do not analyze data, and do not include a classification. Rather than blocking content uploaded to specified websites, they block all GET requests to the specified web applications. The rule checks the browser address bar, post-URL, and the HTTP referer header. If any of them matches the URL definition specified in the rule condition, the rule is triggered.

Whitelists

Whitelists are collections of items that you want the system to ignore.

You can whitelist content, devices, processes, and user groups.

Whitelists in data protection rules

You can specify whitelisted processes for clipboard and printer protection rules in the **Policy Catalog** Windows client configuration on their respective pages. You can specify whitelisted URLs on the **Web Protection** page. Because these whitelists are applied at the client, they work with all clipboard, printer, and web protection rules. Clipboard and printer protection rules ignore content produced by whitelisted processes. Web protection rules are not enforced on whitelisted URLs.

You can specify whitelisted processes for text extraction on the **Content Tracking** page. Depending on the definition, the text extractor does not analyze files or content fingerprinting opened by the specified application, or does not create dynamic fingerprints for web upload. The definition can specify specific folders and extensions, allowing granular control what is whitelisted. If no folder is named, the process is not monitored by application file access rules.

Whitelists in device rules

You can create whitelisted plug-and-play items in the **Definitions** → **Device Control** → **Device Templates** page in the **DLP Policy Manager**.

Some plug-and-play devices do not handle device management well. Trying to manage them might cause the system to stop responding or cause other serious problems. Whitelisted plug-and-play devices are automatically excluded when a policy is applied.

Note

Whitelisted plug-and-play definitions are not applicable on macOS operating systems.

The **Exceptions** tab in device control rules is defined by whitelists that are specific to the rule that contains them. The whitelists exclude the specified definitions from the rule.

- **Excluded Users** — Used in all device rules
- **Excluded Device Definitions** — Used in all device rules except Citrix and TrueCrypt
- **Excluded Processes** — Used in plug and play and removable storage rules
- **Excluded Serial Number & User Pairs** — Used in plug and play and removable storage rules
- **Excluded File names** — Used in removable storage file access rules to exempt files such as antivirus applications

Customizing end-user messages

McAfee DLP Endpoint sends two types of messages to communicate with end users: notifications and user justification messages.

Notifications support Rich Text (HTML) messages. Notification and justification definitions can specify **Locales** (languages), and add placeholders that are replaced by their real values. When locales are defined, the messages and option buttons (for business justifications) appear in the default language of the endpoint computer. The following locales are supported:

- English (US)
- English (UK)
- French
- German
- Spanish
- Polish
- Portuguese
- Russian
- Japanese
- Korean
- Chinese (simplified)
- Chinese (traditional)

English (US) is the standard default locale, but any supported locale can be set as the default in the definition. The default locale is used when other defined locales are not available as the endpoint computer default language. McAfee DLP Prevent attempts to detect the user's preferred language from request headers.

Note

McAfee DLP Prevent does not fully support Korean, Russian, or Chinese (Simplified) locales.

User notification

McAfee DLP Endpoint user notifications are pop-up messages that notify the user of a policy violation.

Note

When a rule triggers multiple events, the pop-up message states: *There are new DLP events in your DLP console*, rather than displaying multiple messages.

You can include Rich Text in the pop-up by including HTML tags embedded in a <DIV>.

When McAfee DLP Prevent blocks a web request, it sends the user notification as an HTML document that appears in the user's browser. The notification text that you configure can contain embedded HTML tags, such as <p>, <ul>, or <li>. The alert that the user sees also shows **Access Denied**.

Business justification

(For McAfee DLP Endpoint only) Business justification is a form of policy bypass. When **Request Justification** is specified as the action in a rule, the user can enter the justification to continue without being blocked.

Placeholders

Placeholders are a way of entering variable text in messages, based on what triggered the end-user message. The available placeholders are:

- `%c` for classifications
- `%r` for rule-set name
- `%v` for vector (for example, **Email Protection**, **Web Protection**, **DLP Prevent**)
- `%a` for action (for example, **Block**)
- `%s` for context value (for example, file name, device name, email subject, URL)
- `%f` for context value in McAfee DLP Prevent for Email (for example, file name, email subject, email body), for context value in McAfee DLP Prevent for Web and McAfee DLP Endpoint (for example, full path, URL)

Create and configure rules and rules sets

Create a rule set

Rule sets combine multiple device protection, data protection, and discovery scan rules.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Rule Sets** tab.
3. Select **Actions** → **New Rule Set**.
4. Enter the name and optional description, then click **OK**.

Create a rule

Use the generic steps in this process to create a rule and its actions, and add it to a rule set. The steps can apply to all rule types.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Rule Sets** tab.
3. Click the name of a rule set and if needed, select the appropriate tab for the **Data Protection**, **Device Control**, **Discovery**, or **Application Control** rule.
4. Select **Actions** → **New Rule**, then select the type of rule.
5. On the **Condition** tab, enter the information.
    - For some conditions, such as classifications or device template items, click **...** to select an existing item or create an item.
    - To add additional criteria, click **+**.
    - To remove criteria, click **–**.
6. (Optional) To add exceptions to the rule, click the **Exceptions** tab.
    a. Select **Actions** → **Add Rule Exception**.
    Device rules do not display an **Actions** button. To add exceptions to device rules, select an entry from the displayed list.
    b. Fill in the fields as needed.
7. Depending on your product, configure the **Action**, **User Notification**, and **Report Incident** options on the **Reaction** tab.
Rules can have different actions, depending on whether the endpoint computer is in the corporate network. Some rules can also have a different action when connected to the corporate network by VPN.
8. Click **Save**.

Assign rule sets to policies

Before being assigned to endpoint computers or appliances, rule sets are assigned to policies and the policies are saved to the McAfee ePO database.

Before you begin

Make sure you create rule sets and activate them before assigning the rule sets to policies.

To activate rule sets, from the **Policy Catalog** page, edit the required **DLP policy**. On the selected policy page, go to **Active Rule Sets** tab and select **Actions** → **Activate Rule Set**, then click **OK**.

Note

On the **Active Rule Sets** page, you can click **Apply Policy** to apply the selected rule set to the policy. This is an alternate method of assigning rule sets to a selected policy.

Task

1. On the **DLP Policy Manager** → **Policy Assignment** page, do one of the following:

- Select **Actions** → **Assign a Rule Set to policies**. In the assignment window, select a rule set from the drop-down list and select the policies to assign it to. Click **OK**.
- Select **Actions** → **Assign Rule Sets to a policy**. In the assignment window, select a policy from the drop-down list and select the rule sets to assign it to. Click **OK**.

Note

If you deselect a rule set or policy previously selected, the rule set is deleted from the policy.

2. Select **Actions** → **Apply selected policies**. In the assignment window, select the policies to save to the McAfee ePO database. Click **OK**.
   Only policies not yet saved to the database appear in the selection window. If you change a rule set assignment, or a rule in an assigned rule set, the policy appears and the revised policy is applied in place of the previous policy.

Enable, disable, or delete rules

You can delete or change the state of multiple rules at once.

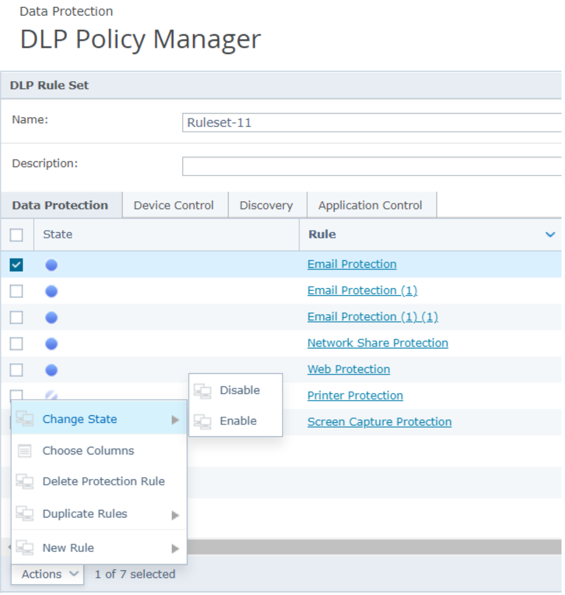
Note

For built-in rules, you can only duplicate a rule and make changes in the duplicated rule.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Rule Sets** tab.
3. Click the name of a rule set and if needed, click the appropriate tab for the **Data Protection**, **Device Control**, **Discovery**, or **Application Control** rule.
4. Select one or more rules.
5. Update or delete the selected rules.
   - To enable the rules, select **Actions** → **Change State** → **Enable**.
   - To disable the rules, select **Actions** → **Change State** → **Disable**.

- To delete the rules, select **Actions** → **Delete Protection Rule**.



Data Protection

DLP Policy Manager

DLP Rule Set

Name: Ruleset-11

Description:

☐	State	Rule
☑	●	Email Protection
☐	●	Email Protection (1)
☐	●	Email Protection (1) (1)
☐	●	Network Share Protection
☐	●	Web Protection
☐		Printer Protection
		Screen Capture Protection

1 of 7 selected

Back up and restore policy

You can back up policies, including rules and classifications, from McAfee ePO and restore them to McAfee ePO server.

Make sure there is a license key added before restoring the file. If you restore the file without a license, all rules become disabled, and you must enable rules before applying policy.

For McAfee DLP Discover, you must reassign Discover servers to scans before applying policy.

Task

1. In McAfee ePO, select **Data Protection** → **DLP Settings** → **Backup & Restore**.
2. Enter an encryption password for the backup file.
3. Click **Backup to file** and save the file in a place such as a USB drive or a shared folder.
4. On another McAfee ePO account, select **Data Protection** → **DLP Settings** → **Backup & Restore**.
5. Enter the password for decrypting the file.
6. Click **Restore from file** and select the file you saved earlier.

Configure rule or rule set columns

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

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Rule Sets** tab.

3. Access the **Select the Columns to Display** page.
   - **Rule sets** — Select **Actions** → **Choose Columns**.
   - **Rules** — Select a rule set, then select **Actions** → **Choose Columns**.
4. Modify the columns.
   - In the **Available Columns** pane, click items to add columns.
   - In the **Selected Columns** pane, click the arrows or **x** to move or delete columns.
   - Click **Use Defaults** to restore the columns to the default configuration.
5. Click **Save**.

Create a justification definition

For McAfee DLP Endpoint, business justification definitions define parameters for the justification prevent action in rules.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Definitions** tab, then select **Notification** → **Justification**.
3. Select **Actions** → **New**.
4. Enter a unique name and optional description.
5. To create justification definitions in more than one language, select **Locale Actions** → **New Locale**. For each required locale, select a locale from the drop-down list.
   The selected locales are added to the list.
6. For each locale, do the following:
   a. In the left pane, select the locale to edit. Enter text in the text boxes and select checkboxes as required.
   Show Match Strings provides a link on the pop up to display the hit-highlighted content. **More Info** provides a link to a document or intranet page for information.

   Note

   > When entering a locale definition, checkboxes and actions are not available. You can only enter button labels, overview, and title. In the **Justification Options** section, you can replace the default definitions with the locale version by using the **Edit** feature in the **Actions** column.

   b. Enter a **Justification Overview** and optional **Dialog Title**.
   The overview is a general instruction for the user, for example: *This action requires a business justification.* Maximum entry is 500 characters.

   c. Enter text for button labels and select button actions. Select the **Hide button** checkbox to create a two-button definition.
   Button actions must match the prevent actions available for the type of rule that uses the definition. For example, network share protection rules can have only **No Action**, or **Request Justification** for prevent actions. If you select **Block** for one of the button actions, and attempt to use the definition in a network share protection rule definition, an error message appears.

   d. Enter text in the text box and click **Add** to add to the list of **Justification Options**. Select the **Show justifications options** checkbox if you want the end user to view the list.
      You can use placeholders to customize the text, indicating what caused the pop up to trigger.

7. When all locales are complete, click **Save**.

Create a notification definition

With McAfee DLP Endpoint, user notifications appear in pop-ups or the end-user console when user actions violate policies.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Definitions** tab, then select **Notification** → **User Notification**.
3. Select **Actions** → **New**.
4. Enter a unique name and optional description. Select the dialog size and position.
5. To create user notification definitions in more than one language, select **Locale Actions** → **New Locale**. For each required locale, select a locale from the drop-down list.
   The selected locales are added to the list.
6. For each locale, do the following:
   a. In the left pane, select the locale to edit.

      Note

      > You can set any locale to be the default by selecting the **Default locale** checkbox.

   b. Enter text in the text box.
      You can use placeholders to customize the text, indicating what caused the pop-up to trigger. The available placeholders are listed to the right of the text box.
      To use Rich Text, place the text inside an HTML <DIV> element. Add HTML element tags as required.
      The text input `<div><b>Sensitive content was found in file %s</b></div>` produces the output **Sensitive content was found in file %s**, where %s is the short display name.
   c. (Optional) Select the **Show link to more information** checkbox and enter a URL to provide more detailed information.

      Note

      > The information is available only in the default locale.

7. When all locales are complete, click **Save**.

Create and assign policies

Create a policy

Create a new version of a **DLP Policy**.

Task

1. Click **Menu** → **Policy** → **Policy Catalog**, select the **DLP Policy** category, and click **New Policy**.
2. Select the policy you want to duplicate, type a name for the new policy and click **OK**.
   The policy appears in the **Policy Catalog**.
3. Select the name of the new policy to open the **Policy Settings** wizard.
4. Edit the policy settings and click **Save**.

Assign and push a policy to a system

Add an existing policy to McAfee DLP.

Before you begin

You must create and activate a rule set for the policy. For information about activating a rule set, see Assign rule sets to policies.

Task

1. In McAfee ePO, click **Menu** → **Systems** → **System Tree** → **Assigned Policies**, then select a group from the **System Tree**.
2. Select the product as **Data Loss Prevention <version>**.
   All assigned policies, organized by product, appear in the details pane.
3. Click the **Edit Assignment** link for the **DLP Policy** category.
4. Select **Break inheritance and assign the policy and settings below** and change the assigned policy to the policy you created, then click **Save**.

   Note

   You can also click **Wake Up Agents** to push the policy to McAfee DLP appliances immediately.

Results

The policy is assigned to the selected systems.

Assign and push a policy to configure a McAfee DLP appliance

Add an existing policy to a McAfee DLP appliance.

Before you begin

- Create and activate a rule set for the policy. For information about how to activate rule sets, see Assign rule sets to policies.
- Set up an appliance policy that is assigned to a rule set.

Task

1. In McAfee ePO, click **Menu** → **Systems** → **System Tree** → **Policies**, then select a group from the **System Tree**.
2. Select the product as **DLP Appliance Management**.
   All assigned policies, organized by product, appear in the details pane.
3. Click the **Edit Assignment** link for the **DLP Policy** category.
4. Select **Break inheritance and assign the policy and settings below** and change the assigned policy to the policy you created.

   Note

   You can also click **Wake Up Agents** to push the policy to McAfee DLP appliances immediately.

5. Click **Save**.

Results

The policy is assigned to the selected appliances.

Rule use cases

Use case: Removable storage file access device rule with a whitelisted process

You can whitelist file names as an exception to a removable storage blocking rule.

Removable storage file access device rules are used to block applications from acting on the removable device. Whitelisted file names are defined as processes that are not blocked. In this example, we block SanDisk removable storage devices, but allow antivirus software to scan the device to remove detected files.

Note

This feature is supported only for Windows-based computers.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. On the **Definitions** tab, locate the built-in device template **All Sandisk removable storage devices (Windows)**, and click **Duplicate**.
   The template uses the SanDisk vendor ID `0781`.

   Tip

   Duplicate the built-in templates to customize a template. For example, you can add other vendor IDs to the duplicated SanDisk* template to add other brands of removable devices.

3. On the **Rule Sets** tab, select or create a rule set.
4. On the rule set **Device Control** tab, select **Actions** → **New Rule** → **Removable Storage File Access Device Rule**.
5. Enter a name for the rule and select **State** → **Enabled**.
6. On the **Conditions** tab, select an **End-User** or leave the default (**is any user**). In the **Removable Storage** field, select the device template item you created in step 2. Leave the default settings for **True File Type** and **File Extension**.
7. On the **Exceptions** tab, select **Excluded File Names**.
8. In the **File Name** field, add the built-in **McAfee AV** definition.
   As with the removable storage device template item, you can duplicate this template and customize it.
9. On the **Reaction** tab, select **Action** → **Block**. You can optionally add a user notification, select the **Report Incident** option, or select a different action when disconnected from the corporate network.
10. Click **Save**, then click **Close**.

Use case: Set a removable device as read-only

Removable storage device protection rules, unlike plug-and-play device rules, have a read-only option.

By setting removable devices to read-only, you can allow users to use their personal devices as MP3 players while preventing their use as storage devices.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. On the **Definitions** tab, on **Device Templates** page, create a removable storage device template item.

   Note

   Removable storage device templates must be categorized as Windows or Mac templates. Start by duplicating one of the built-in templates for Windows or Mac and customize it. The **Bus Type** can include USB, Bluetooth, and any other bus type you expect to be used. Identify devices with vendor IDs or device names.

3. On the **Rule Sets** tab, select or create a rule set.
4. On the **Device Control** tab, select **Actions** → **New Rule** → **Removable Storage Device Rule**.
5. Enter a name for the rule and select **State** → **Enabled**. In the **Conditions** section, in the **Removable Storage** field, select the device template item you created in step 2.
6. On the **Reaction** tab, select **Action** → **Read-only**. You can optionally add a user notification, select the **Report Incident** option, or select a different action when the user is disconnected from the corporate network.
7. Click **Save**, then click **Close**.

Use case: Block and charge an iPhone with a plug-and-play device rule

Apple iPhones can be blocked from use as storage devices while being charged from the computer.

This use case creates a rule that blocks a user from using the iPhone as a mass storage device. A plug-and-play device protection rule is used because it allows iPhones to charge no matter how the rule is specified. This feature is not supported for other smartphones, or other Apple mobile devices. It does not prevent an iPhone from charging from the computer.

To define a plug-and-play device rule for specific devices, you create a device definition with the vendor and product ID codes (VID/PID). You can find this information from the Windows **Device Manager** when the device is plugged in. Because this example only requires a VID, you can use the built-in device definition **All Apple devices** rather than looking up the information.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. On the **Rule Sets** tab, select a rule set (or create one). Click the **Device Control** tab, and create a plug-and-play device rule. Use the built-in device definition **All Apple devices** as the included (**is one of (OR)**) definition.
3. On the **Reaction** tab, set the **Action** to **Block**.
4. Click **Save**, then click **Close**.

Use case: Prevent copying sensitive information to disk

Application file access protection rules can be used to block the use of CD and DVD burners for copying classified information.

Before you begin

Create a classification to identify the classified content. Use parameters that are relevant to your environment — keyword, text pattern, file information, and so forth.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. On the **Rule Sets** tab, select a current rule set or select **Actions** → **New Rule Set** and define a rule set.

3. On the **Data Protection** tab, select **Actions** → **New Rule** → **Application File Access Protection**.
4. (Optional) Enter a name in the **Rule Name** field (required). Select options for the **State** and **Severity** fields.
5. On the **Condition** tab, in the **Classification** field, select the classification you created for your sensitive content.
6. In the **End-User** field, select user groups (optional).

   Adding users or groups to the rule limits the rule to specific users.
7. In the **Applications** field, select **Media Burner Application [built-in]** from the available application definitions list.

   You can create your own media burner definition by editing the built-in definition. Editing a built-in definition automatically creates a copy of the original definition.
8. (Optional) On the **Exceptions** tab, create exceptions to the rule.

   Exception definitions can include any field that is in a condition definition. You can define multiple exceptions to use in different situations. One example is to define "privileged users" who are exempt from the rule.
9. On the **Reaction** tab, set the **Action** to **Block**. Select a **User Notification** (optional). Click **Save**, then **Close**.

   Other options are to change the default incident reporting and prevent action when the computer is disconnected from the network.
10. On the **Policy Assignment** tab, assign the rule set to a policy or policies:
    a. Select **Actions** → **Assign a Rule Set to policies**.
    b. Select the appropriate rule set from the drop-down list.
    c. Select the policy or policies to assign it to.
11. Select **Actions** → **Apply Selected Policies**. Select policies to apply to the McAfee DLP Endpoint database, and click **OK**.

Use case: Block outbound messages with confidential content unless they are sent to a specified domain

Outbound messages are blocked if they contain the word *Confidential*, unless the recipient is exempt from the rule.

Expected behavior

Email contents	Recipient	Expected result
Body: Confidential	external_user@external.com	The message is blocked because it contains the word Confidential.
Body: Confidential	internal_user@example.com	The message is not blocked because the exception settings mean that confidential material can be sent to people at example.com.
Body: Attachment: Confidential	external_user@external.com internal_user@example.com	The message is blocked because one of the recipients is not allowed to receive it.

Task

1. Create an email address list definition for a domain that is exempt from the rule.
   a. In the **Data Protection** section in McAfee ePO, select **DLP Policy Manager** and click **Definitions**.
   b. Select the **Email Address List** definition and create a duplicate copy of the built-in **My organization email domain**.
   c. Select the email address list definition you created, and click **Edit**.
   d. In **Operator**, select **Domain name is** and set the value to `example.com`.
   e. Click **Save**.
2. Create a rule set with an **Email Protection** rule.
   a. Click **Rule Sets**, then select **Actions** → **New Rule Set**.
   b. Name the rule set `Block Confidential in email`.
   c. Create a duplicate copy of the built-in **Confidential** classification.
      An editable copy of the classification appears.
   d. Click **Actions** → **New Rule** → **Email Protection Rule**.
   e. Name the new rule **Block Confidential** and enable it.
   f. Enforce the rule on **McAfee DLP Endpoint for Windows**.
   g. Select the classification you created and add it to the rule.
   h. Set the **Recipient** to **any recipient (ALL)**.
      Leave the other settings on the **Condition** tab with the default settings.
3. Add exceptions to the rule.
   a. Click **Exceptions**, then select **Actions** → **Add Rule Exception**.
   b. Type a name for the exception and enable it.
   c. Set the classification to *Confidential*.
   d. Set **Recipient** to **at least one recipient belongs to all groups (AND)**, then select the email address list definition you created.
4. Configure the reaction to messages that contain the word *Confidential*.
   a. Click **Reaction**.
   b. Set the **Action** to **Block** for computers connected to and disconnected from the corporate network.
5. Save and apply the policy.

Use case: Block email message and return to the sender

Outbound email messages are blocked if they contain the word *Confidential*. The email message is not sent to the recipient from the Smart Host. A notification mail with the original email as an attachment is sent back to the sender. You can choose a predefined user notification or customize the definition. In addition, more details about the blocked email message are attached to the notification in HTML file format.

Task

1. Create a rule set with an **Email Protection** rule.

   a. In McAfee ePO, select **Data Protection** → **DLP Policy Manager**.
   b. Click **Rule Sets**, then select **Actions** → **New Rule Set**.
   c. Name the rule set `Block email and return to sender`.
   d. Create a duplicate copy of the in-built **Confidential** classification.
      An editable copy of the classification appears.
   e. Click **Actions** → **New Rule** → **Email Protection Rule**.
   f. Name the new rule **Bounce email** and enable it.
   g. Enforce the rule on **DLP Prevent**.
   h. Select the classification you created and add it to the rule.
      Leave the other settings on the **Condition** tab with the default settings.
2. Configure the reaction to messages that contain the word *Confidential*.
   a. Click **Reaction**.
   b. In **DLP Prevent**, select **Actions** → **Block and return email to sender**.
   c. Select the notification that has to be sent from **User Notification**.
3. (Optional) To report an incident, about the bounced email message, select the **Report Incident** checkbox. To save the evidence, select the **Store original email as evidence** checkbox.
4. Save and apply the policy.
5. Set the sender email address for the bounced email messages.
   a. Open the **Policy Catalog**.
   b. Select the **DLP Appliance Management** product, select the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
   c. Specify the sender email address in the **Bounce Messages Sender** field. It must be a generic email address.
   d. Click **Save**.

Use case: Allow a specified user group to send credit information

Allow people in the human resources user group to send messages that contain personal credit information by obtaining information from your Active Directory.

Before you begin

Register an Active Directory server with McAfee ePO. Use the **Registered Servers** features in McAfee ePO to add details of the server.

Follow these high-level steps to:

1. (Optional for McAfee DLP Prevent only) Select an LDAP server to get the user group from.
2. Create a personal credit information classification.
3. Create a rule set and a rule that acts on the new classification.
4. Make the human resources user group exempt from the rule.
5. Block messages that contain personal credit information.

6. Apply the policy.

Tip

To ensure that your rules identify potential data loss incidents with minimal false positive results, create your rules using the **No action** setting. Monitor the **DLP Incident Manager**. until you are satisfied that the rule identifies incidents correctly, then change the **Action** to **Block**.

Task

1. Select the LDAP server that you want to get the user group from.
   a. In McAfee ePO, open the **Policy Catalog**.
   b. Select the **McAfee DLP Prevent Server** policy.
   c. Open the **Users and Groups** category and open the policy that you want to edit.
   d. Select the Active Directory servers that you want to use.
   e. Click **Save**.
2. From the McAfee ePO menu, select **Classification**, and create a duplicate **PCI** classification.
3. Create the rule set and exceptions to it.
   a. Open the **DLP Policy Manager**.
   b. In **Rule Sets**, create a rule set called `Block PCI for DLP Prevent and Endpoint`.
   c. Open the rule set you created, select **Action** → **New Rule** → **Email Protection**, and type a name for the rule.
   d. In **Enforce On** select **DLP Endpoint for Windows** and **DLP Prevent**.
   e. In **Classification of**, select the classification you created.
   f. Leave **Sender**, **Email Envelope**, and **Recipient** with the default settings.
4. Specify the user group that you want to exclude from the rule.
   a. Select **Exceptions**, click **Actions** → **Add Rule Exception**, and name it `Human resource group exception`.
   b. Set the **State** to **Enabled**.
   c. In **Classification of**, select **contains any data (ALL)**.
   d. In **Sender** select **Belongs to one of end-user groups (OR)**.
   e. Select **New Item**, and create an end-user group called `HR`.
   f. Click **Add Groups**, select the group, and click **OK**.
5. Set the action you want to take if the rule triggers.
   a. Select the group you created and click **OK**.
   b. Select the **Reaction** tab.
   c. In the **DLP Endpoint** section, set the **Action** to **Block**.

      If **DLP Endpoint** is selected, you must set a reaction.
   d. In the **DLP Prevent** section, set the X-RCIS-Action header value to **Block**.

      Note

      If you want to test the rule, you can keep the **Action** as **No Action** until you are satisfied that it triggers as expected.

   e. Select **Report Incident**.
   f. Save the rule and click **Close**.

6. Apply the rule.
   a. In the **DLP Policy Manager**, select **Policy Assignment**.

      Note

      Pending Changes, shows **Yes**.

   b. Select **Actions** → **Assign Rule Sets to a policy**.
   c. Select the rule set you created.
   d. Select **Actions** → **Apply Selected Policies**.
   e. Click **Apply policy**.
      Pending Changes shows **No**.

Use case: Classify attachments as NEED-TO-SHARE based on their destination

Create classifications that allow NEED-TO-SHARE attachments to be sent to employees in the United States, Germany, and Israel.

Before you begin

1. Use the **Registered Servers** features in McAfee ePO to add details of the LDAP servers. For more information about registering servers, see the *McAfee ePO Product Guide*.
2. Use the **LDAP Settings** feature in the **Users and Groups** policy category to push group information to the McAfee DLP Prevent appliance.

Follow these high-level steps:

- Create a NEED-TO-SHARE classification.
- Create a United States classification.
- Create an Israel classification.
- Create email address list definitions.
- Create a rule set and a rule that classifies attachments as NEED-TO-SHARE.
- Specify exceptions to the rule.

The example classifications in the table show how the classifications behave with different classification triggers and recipients.

Expected behavior

Classification	Recipient	Expected result
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser1@example1.com	Allow — example1.com is allowed to receive all NEED-TO-SHARE attachments
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser2@example2.com	Allow — example2.com is allowed to receive all NEED-TO-SHARE attachments
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser2@example2.com exampleuser1@example1.com	Allow — example1.com and example2.com are allowed to receive both attachments
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser3@gov.il	Allow — gov.il is allowed for both attachments
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser4@gov.us	Block — exampleuser4 is not allowed to receive Attachment2
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser3@gov.il exampleuser4@gov.us	Block — exampleuser4 is not allowed to receive Attachment2
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us)	exampleuser1@example1.com exampleuser4@gov.us	Block — exampleuser4 is not allowed to receive Attachment2

Classification	Recipient	Expected result
Attachment2 — NEED-TO-SHARE, Israel (.il) and Germany (.de)		
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser3@gov.il exampleuser1@example1.com	Allow — exampleuser1 and exampleuser3 are allowed to receive both attachments
Attachment1 — NEED-TO-SHARE, Israel (.il) and United States (.us) **Attachment2** — NEED-TO-SHARE, Israel (.il) and Germany (.de)	exampleuser2@example2.com exampleuser1@example1.com exampleuser4@gov.us	Block — exampleuser4 cannot receive Attachment2

Task

1. Create an email address list definition for the domains that are exempt from the rule.
   a. In the **Data Protection** section in McAfee ePO, select **DLP Policy Manager** and click **Definitions**.
   b. Select the **Email Address List** definition and create a duplicate copy of the built-in **My organization email domain**.
   c. Select the email address list definition you created, and click **Edit**.
   d. In **Operator**, select **Domain name equals** and set the value to example1.com.
   e. Create an entry for `example2.com`.
   f. Click **Save**.
   g. Repeat these steps to create a definition for gov.il.
   h. Repeat the steps again to create a definition for gov.us.
2. Create a rule set that includes an **Email Protection** rule.
   a. Click **Rule Sets**, then select **Actions** → **New Rule Set**.
   b. Name the rule set `Allow NEED-TO-SHARE email to Israel and United States`.
3. Create a rule and add the NEED-TO-SHARE classification criteria.
   a. Click **Actions** → **New Rule** → **Email Protection Rule**.
   b. Name the rule `NEED-TO-SHARE`, enable it, and enforce it on **DLP Endpoint for Windows** and **DLP Prevent**.
   c. Set **Classification of** to **one of the attachments (*)**.
   d. Select **contains one of (OR)**, and select the **NEED-TO-SHARE** classification criteria.
   e. Set the **Recipient** to **any recipient (ALL)**.
   f. Leave the other settings on the **Condition** tab with the default settings.
4. Add exceptions to the rule, and enable each exception.
   - Exception 1

    - Set **Classification of** to **matched attachment**.
    - Select **contains one of (OR)**, and select the **NEED-TO-SHARE** classification criteria.
    - Set the **Recipient** to **matched recipient belongs to one of groups (OR)**, and select the email address definition that includes example.com and example2.com that you created.
  - Exception 2
    - Set **Classification of** to **matched attachment**.
    - Select **contains all of (AND)**, and select the **NEED-TO-SHARE** and **.il (Israel)** classification criteria.
    - Set the **Recipient** to **matched recipient belongs to one of groups (OR)**, and select **gov.il**.
  - Exception 3
    - Set **Classification of** to **matched attachment**.
    - Select **contains all of (AND)**, and select the **NEED-TO-SHARE** and **.us (United States)** classification criteria.
    - Set the **Recipient** to **matched recipient belongs to one of groups (OR)**, and select **gov.us**.

5. Set the reaction you want to take if the rule triggers.
   a. In **DLP Endpoint**, set the **Action** to **Block**.
   b. In **DLP Prevent**, set the **Action** to **Add header X-RCIS-Action**, and select the **BLOCK** value.
6. Click **Save**.
7. Apply the policy.

Use Case: Prevent data leaks on removable devices

An organization wants to block all removable devices in the company, while maintaining a list of specific devices that are trusted. Also, specific content needs to be blocked on all devices, including the trusted ones.

An administrator needs to perform these tasks.

Task

1. Block all removable devices in the organization with the Removable Storage Device Rule.
   a. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager.**
   b. On the **Rule Sets** tab, select or create a rule set. For new rule sets, make sure to assign a policy.
   c. On the **Device Control** tab, select **Actions** → **New Rule** → **Removable Storage Device Rule.**
   d. Enter a name for the rule and select **State** → **Enabled.**
   e. In the **Conditions** section, select the built-in **Removable storage devices (Windows)** value in the **Removable Storage** field.
   f. On the **Reaction** tab, select **Action** → **Blocked.** Select the **Report Incident** option.
   g. From the **User Notification** list, select **Default device management user notification** and click **OK**.
   h. Click **Save**, then click **Close**.
2. Identify trusted devices and create a device template.
   a. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Incident Manager** and click the Incidents list.
   b. In the **Filter By** pane, under **Incident Type**, select **Device Plug**.
   c. Click the Incident ID of a device you want to set as trusted to verify **Endpoint Details** and **Additional Information** about the device. From here you can obtain specific details about the device, such as the serial number.

  d. Click **OK** to return to the Incidents list.
  e. Select the checkbox next to the incident and select **Create Device Template → Removable Storage Device.**
  f. Enter a name for the device template and click **Save**. Repeat steps **e** and **f** for each of your trusted devices.
  g. Select **DLP Policy Manager → Definitions.**
  h. In the left pane, select **Device Control → Device Templates.**
  i. Select **Actions → New Group → Removable Storage Device Group.**
  j. Enter a name for the group, such as, Trusted devices. Add one or more device templates created in steps **e** and **f** and click **Save**.

3. Add trusted devices to the Removable Storage Device Rule created in **step 1**.
   a. Select **DLP Policy Manager**.
   b. On the **Rule Sets** tab, select **Device Control** tab and then the rule set created in **step 1**.
   c. On the **Exceptions** tab, select **Excluded Device Templates (Disabled)** and then select the device template group created in **step 2**.
   d. Select **State → Enabled.**
4. Assign rule sets to policies.
   a. Select **DLP Policy Manager → Policy Assignment**
   b. Select the policy name and select **Actions → Apply selected policies.**
   c. Make sure the revision is incremented and there are no pending changes.

Use Case: Prevent data from being leaked to the web from your cloud-based applications

Your organization wants to block all content from leaking to the web from cloud services, such as Dropbox and Google Drive. The Sales team needs access and copy rights to their shared folder on Google Drive.

An administrator needs to perform these tasks.

Task

1. Block Dropbox and Google Drive services with the Cloud Protection Rule.
   a. In McAfee ePO, select **Menu → Data Protection → DLP Policy Manager.**
   b. On the **Rule Sets** tab, select or create a rule set. For new rule sets, you must assign a policy.
   c. On the **Data Protection** tab, select **Actions → New Rule → Cloud Protection Rule.**
   d. Enter a name for the rule and select **State → Enabled.**
   e. On the **Condition** tab, in the **Classification** field, select the classification you created for your confidential content.
   f. In the **Cloud Services** field, select Dropbox and GoogleDrive.
2. Specify the user group and folder that you want to exclude from the rule.
   a. Select **Exceptions**, click **Actions → Add Rule Exception**, and name it `Sales`.
   b. Set the **State** to **Enabled**.
   c. In **Classification of**, select **contains any data (ALL)**.
   d. In **End-User**, select **Belongs to one of end-user groups (OR)**.
   e. Select **New Item**, and create an end-user group called `Sales team`.

   f. Click the add group button, select Sales team, and click **OK**.
   g. In the **top-level Subfolder name**, select **equals**, and type the name of the folder (for example, Sales pitch).
3. Add the Google Drive URL you want to block content from leaking.
   a. Select **Menu** → **Data Protection** → **DLP Policy Manager.** → **Definitions.**
   b. In the left pane, select **URL List**, then select **Actions** → **New**.
   c. Name the URL `Google Drive URL`.
   d. Enter the **Host** details, and optionally, the **Protocol**, **Port**, and **Path**, then click **Add**.
   e. Click **Save**.
4. Block Dropbox and Google Drive from leaking to the web with the Web Protection Rule.
   a. On the Data Protection tab of your rule set, select **Actions** → **New Rule** → **Web Protection Rule.**
   b. Enter a name for the rule and select **State** → **Enabled.**
   c. On the **Condition** tab, in the **Classification** field, select the classification you created for your confidential content. This must be the same classification selected for the Cloud Protection Rule.
   d. In the **Web address (URL)** field, select **is one of (OR)** and choose **Dropbox (built-in)** and **Google Drive URL**, created in previous step.
   e. On the **Reaction** tab, set the **Action** to **Block.**
   f. In the **User Notification** field, select **Default web protection user notification**.
   g. Click **OK**, then **Save**.

Use case: Block GDPR data leaks

Your organization wants to block General Data Protection Regulation (GDPR) related data from leaving the organization.

McAfee DLP includes built-in rule set, rules, and classifications for GDPR-related data. Use the built-in **Block GDPR** rule set and classifications samples to set up your policies for GDPR-related data.

Task

1. Create a duplicate copy of the built-in GDPR rule set.
   a. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager.**
   b. On the **Rule Sets** tab, select **Show built-in rule sets samples**.
   c. In the **Actions** column of **[Sample] Block GDPR Content [built-in]**, click **Duplicate**.

   The new rule set **Block GDPR Content** is added to the rule sets list.
2. Edit the **Block GDPR Content** rule set.
   a. On the **Rule Sets** tab, select the **Block GDPR Content** rule set.
   b. Edit the description as needed.
   c. On the **Data Protection** tab, select the **Block GDPR content copied to removable storage** rule.
   d. On the **Condition** tab, leave or remove the PII classifications for specific countries as needed for your organization.
   e. Select each of the remaining rules to remove PII classifications as needed.
   f. Leave the remaining defaults.
   g. Click **Save**.
3. Assign the **Block GDPR Content** rule set to a policy.

a. Select **DLP Policy Manager** → **Policy Assignment**.
b. Select **Actions** → **Apply rule set to a policy.**
c. Select a policy to assign the rule set and select **Block GDPR Content** rule set.
d. Click **OK**. Make sure there are no pending changes and that the revision is incremented.

Protecting removable devices

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

Device Control can monitor or block devices attached to enterprise-managed computers, allowing you to monitor and control their use in the distribution of sensitive information. Devices such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or plug-and-play devices can all be controlled. McAfee Device Control is a component of McAfee DLP Endpoint that is sold as a separate product. While the term Device Control is used throughout this section, all features and descriptions apply to McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac as well.

Device Control terminology

Device template — A list of device properties used to identify or group devices.

Device group — A list of device templates grouped into a single template. Used to simplify rules while maintaining granularity.

Device property — A property such as bus type, vendor ID, or product ID that can be used to define a device.

Device rule — Defines the action taken when a user tries to use a device that has a matching device definition in the policy. The rule is applied to the hardware, either at the device driver level or the file system level. Device rules can be assigned to specific users.

Removable storage device rule — Used to block or monitor a device, or set it as read-only.

Removable storage protection rule — Defines the action taken when a user tries to copy content labeled as sensitive to a managed device.

Device class* — A collection of devices that have similar characteristics and can be managed in a similar manner. Device classes have the status Managed, Unmanaged, or Whitelisted.

Managed device * — A device class status indicating that Device Control manages the devices in that class.

Unmanaged device* — A device class status indicating that Device Control does not manage the devices in that class.

Whitelisted device* — A device class status indicating that Device Control can't manage the devices in that class because attempts to manage them can affect the managed computer, system health, or efficiency.

* Windows only

Protecting content on removable devices

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

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

McAfee Device Control protection is built in three layers:

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

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

Removable storage protection rules

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

Note

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

Benefits of device classes in managing devices

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

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

Note

Device classes are not applicable to macOS devices.

How device classes are organized

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

- *Managed* devices are specific plug-and-play or removable storage devices that Device Control manages.
- *Unmanaged* devices are devices Device Control doesn't manage in the default configuration.
- *Whitelisted* devices are devices that Device Control doesn't try to control, such as battery devices or processors.

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

Tip

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

Overrides can be used for testing user-defined changes before creating a permanent class, and troubleshooting Device Control problems.

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

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

Define a device class

Create a GUID

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

Some hardware devices install their own new device class. If a suitable device class does not exist on the predefined list, or is not created automatically when new hardware is installed, you can create a device class in the DLP Policy Manager. To control the behavior of plug-and-play hardware devices that define their own device class, you must first add a new device class to the **Managed** status in the **Device Classes** list.

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

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Incident Manager** → **Incident List**.
2. Click **Edit** next to the **Filter** drop-down list to edit the filter criteria.
3. In the **Available Properties** list (left pane), select **Incident Type**.

4. Verify that the **Comparison** drop-down list value is **Equals**.
5. From the **Values** drop-down list, select **Device New Class Found**.
6. Click **Update Filter**.
   The **Incident List** displays the new device classes found on all endpoint computers.
7. To view the name and GUID of a specific device, double-click the item to display the incident details.

Create a device class

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

Before you begin

Obtain the device GUID before beginning this task.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select **Device Control** → **Device Class**.
3. Do one of the following:
   - Select **Actions** → **New Item**.
   - Locate a similar device class on the built-in device class list, then click **Duplicate** in the **Actions** column. Click **Edit** for the duplicated device class.
4. Enter a unique **Name** and optional **Description**.
5. Verify the **Status** and **Filter Type** required.
6. Enter the GUID, then click **Add**.
   The GUID must be in the correct format. You are prompted if you enter it incorrectly.
7. Click **Save**.

Organizing devices with device templates

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

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

Available device template types are:

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

- *Whitelisted plug and play devices* are mostly the devices that do not interact with device management properly and might cause the system to stop responding or cause other serious problems.

  Note

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

- McAfee DLP Endpoint for Windows and McAfee DLP Endpoint for Mac
  - *Plug and play devices* are added to the managed computer without any configuration or manual installation of DLLs and drivers. Plug-and-play devices include most Microsoft Windows devices. On McAfee DLP Endpoint for Mac, they are supported for USB only.
  - *Removable storage devices* are external devices containing a file system that appear on the managed computer as drives.

You can also create device group templates, which are collections of previously defined device templates. Device groups must specify only one operating system, either Microsoft Windows or macOS.

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

Tip

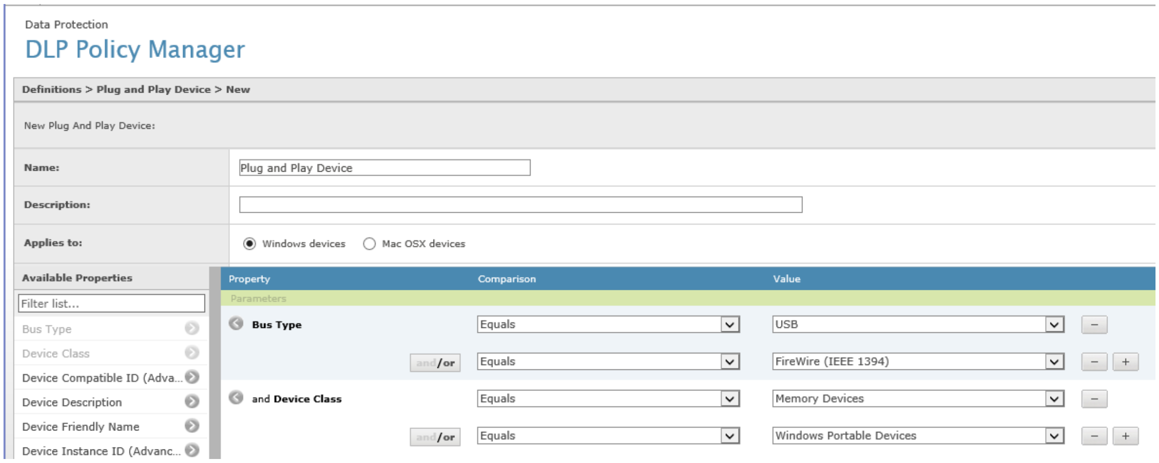
Use the removable storage device templates and rules to control devices that can be classified as either, such as USB mass storage devices.

Benefits of device templates in defining device parameters

You can add multiple parameters to a single device template. The available properties list and values varies depending on the type of device.

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

For example, the following parameter selection:



Data Protection

DLP Policy Manager

Definitions > Plug and Play Device > New

New Plug And Play Device:

Name:	Plug and Play Device
Description:	
Applies to:	● Windows devices ○ Mac OSX devices

Available Properties

Filter list...

- Bus Type
- Device Class
- Device Compatible ID (Adva...
- Device Description
- Device Friendly Name
- Device Instance ID (Advanc...

Parameters

Property		Comparison	Value
Bus Type		Equals	USB
	and/or	Equals	FireWire (IEEE 1394)
and Device Class		Equals	Memory Devices
	and/or	Equals	Windows Portable Devices

Creates this template:

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

Create a device template

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

Device templates can be created as described below, by importing from a CSV file, from a device plug incident in the **DLP Incident Manager**, or with a script containing REST API calls. The administrator running the script must be a valid McAfee ePO user who has permissions in McAfee ePO **Permission Sets** to perform the actions that are invoked by the APIs.

Tip

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

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select **Device Control** → **Device Templates**.
3. Select **Actions** → **New Item**, then select the type of definition.
4. Enter a unique **Name** and optional **Description**.
5. (Plug and Play and Removable Storage devices only) Select the **Applies to** option for Microsoft Windows or OS X devices. The **Available Properties** list changes to match properties for the operating system selected.
6. Select properties for the device.

Note

The available properties list varies depending on the type of device.

- To add a property, click **>**.
- To remove a property, click **<**.
- To add another value for the property, click **+**.

Values are added as logical *OR* by default. Click the **and/or** button to change it to *AND*.

- To remove properties, click **-**.

7. Click **Save**.

Create a device group

Device groups simplify rules while maintaining granularity by combining several device templates into one group.

Device groups can be created as described below, or with a script containing REST API calls. The administrator running the script must be a valid McAfee ePO user who has permissions in McAfee ePO **Permission Sets** to perform the actions that are invoked by the APIs.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the **Device Templates** pane, select **Actions** → **New Group**, then select the type of group.
   Three device group types are supported: **Fixed Hard Drive**, **Plug and Play Device**, or **Removable Storage Device**.
3. Enter a unique **Name** for the group and optional **Description**.
4. Select the **Applies to** option for Microsoft Windows or macOS devices.
   This field is not available for fixed hard drive device groups.
5. Using the check boxes, select the items to add to the group.
   You can filter long device template lists by typing some text in the **Filter items** text box and clicking **Go**.
6. Click **Save**.

Create a removable storage device template

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

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select **Device Control** → **Device Templates**, then select **Actions** → **New Item** → **Removable Storage Device Template**.
3. Enter a unique **Name** and optional **Description**.
4. Select the **Applies to** option for Microsoft Windows or macOS devices.
   The **Available Properties** list changes to match properties for the operating system selected.
5. Select properties for the device.
   - To add a property, click **>**.
   - To remove a property, click **<**.
   - To add additional values for the property, click **+**.

   Values are added as logical *OR* by default. Click the **and/or** button to change it to *AND*.

   - To remove properties, click **-**.
6. Click **Save**.

Create a whitelisted plug and play template

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

Whitelisted plug-and-play devices are added to plug-and-play device rules automatically and are hidden. They are never managed, even if their parent device class is managed.

Tip

To avoid compatibility problems, add devices that do not handle device management well to the whitelisted device list.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Definitions**.
2. In the left pane, select **Device Control** → **Device Templates**, then select **Actions** → **New Item** → **Whitelisted Plug and Play Device Template**.
3. Enter a unique **Name** and optional **Description**.
4. Select properties for the device.
   - To add a property, click **>**.
   - To remove a property, click **<**.
   - To add additional values for the property, click **+**.

Values are added as logical *OR* by default. Click the **and/or** button to change it to *AND*.

- To remove properties, click **-**.

5. Click **Save**.

Create a serial number and user pair definition

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

Before you begin

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

You can create a serial number and user pair definition by importing the information in CSV format. You can also export existing definitions in CSV format.

Tip

Serial number and user pair CSV files use multiple columns. Export a definition to understand how the columns are populated before creating a file for import.

Note

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

Task

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

Device control rules

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

Note

Device control rules trigger ONLY when a device is plugged in. The notification sent (block, read-only, report incident) is based on the rule action. User actions on a plugged-in device don't cause more incidents to be logged or notifications to be sent.

Removable Storage Device Rule

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

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

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

Note

Device rules have an **Enforce on** parameter that applies the rule to either Windows or macOS or both. Device templates used in device rules have an **Applies to** parameter that specifies either **Windows devices** or **macOS devices**. When selecting device templates, match the operating system in the template and the rule. The McAfee DLP Endpoint clients for both operating systems ignore properties that do not apply to that system. But you can’t save a rule that, for example, enforces on Windows only but contains macOS device templates.

Plug-and-play Device Rule

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

A plug-and-play device is a device that can be added to the managed computer without any configuration or manual installation of DLLs and drivers.

For plug-and-play device rules to control Microsoft Windows hardware devices, the device classes specified in device templates used by the rule must be set to **Managed** status.

Important

Device rules have an **Enforce on** parameter that applies the rule to either Windows or macOS or both. Device templates used in device rules have an **Applies to** parameter that specifies either **Windows devices** or **macOS devices**. When selecting device templates, match the operating system in the template and the rule. The McAfee DLP Endpoint clients for both operating systems ignore properties that do not apply to that system, but you can’t save a rule that, for example, enforces on Windows only but contains macOS device templates.

Removable Storage File Access Rule

Use removable storage file access rules to block executables on plug-in devices from running. They are supported on McAfee DLP Endpoint for Windows.

Fixed Hard Drive Rule

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

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

Citrix XenApp Device Rule

Use Citrix device rules to block Citrix devices mapped to shared desktop sessions. They are supported on McAfee DLP Endpoint for Windows.

McAfee DLP Endpoint software can block Citrix devices mapped to shared desktop sessions. Floppy disk, fixed, CD, removable, and network drives can all be blocked, as well as printers and clipboard redirection. You can assign the rule to specific users.

TrueCrypt Device Rule

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

TrueCrypt device rules are a subset of removable storage device rules. TrueCrypt encrypted virtual devices can be protected with TrueCrypt device rules or with removable storage protection rules.

- Use a device rule if you want to block or monitor a TrueCrypt volume, or make it read-only.
- Use a protection rule if you want content-aware protection of TrueCrypt volumes.

Note

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

Create a device rule

Follow these general rules for creating the different types of device rules.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager** → **Rule Sets**.
2. Select **Actions** → **New Rule Set**, or edit an existing rule set.
3. Click the rule set name to open the rule set for editing. Click the **Device Control** tab.

4. Select **Actions** → **New Rule** and select the type of rule you want to create.
5. Enter a unique **Rule Name**.
6. (Optional) Change the status and select a severity.
7. (Removable storage and plug-and-play device rules only) Deselect the **McAfee DLP Endpoint for Windows** or **McAfee DLP Endpoint for Mac OS X** checkbox if the rule applies to only one operating system.
8. On the **Condition** tab, select one or more items or groups.

   Some device rules allow you to optionally assign user groups or a **Process Name**. Citrix rules have resources rather than items. TrueCrypt rules only have optional user groups.

   Note

   When saving the rule, the device template used to create the items or groups is validated against the operating systems selected in the **Enforce on** field. If they don't match, an error message appears. You must correct the error by deleting templates or changing the selected **Enforce on** operating system selected before you can save the rule.

9. (Optional) On the **Exceptions** tab, fill in the required fields.

   For some rules you have to select a whitelist template, then fill in the details.
10. On the **Reaction** tab, select an **Action**. Optional: add a **User Notification**, and **Report Incident**.

    If you don't select **Report Incident**, there is no record of the incident in the DLP Incident Manager.
11. (Optional) Select a different action when the user is working outside the corporate network.
12. Click **Save**.

Removable storage file access rules

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

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

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

Note

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

Synchronizing DLP policies with MVISION

Integrating DLP policies with McAfee MVISION Cloud

Support for McAfee DLP Classifications is available to customers of both McAfee DLP and MVISION Cloud.

Note

> For instructions on enabling the MVISION Cloud integration feature and configuring the server connections, see the McAfee DLP Endpoint 11.x.x Installation Guide.

MVISION Cloud is a cloud access security broker (CASB) that can detect user behavior and apply protection rules in the cloud.

You can apply policies created in McAfee DLP to cloud content with MVISION Cloud in two ways.

- To enforce consistent classification behavior in on-premises and cloud policies, apply McAfee DLP Classifications to MVISION Cloud policies

  Tip

  > Classifications can be applied to protect content uploaded to selected cloud services such as Box Sync or Microsoft OneDrive.

- To enforce consistent Email Protection rule behavior for on-premises and cloud email, apply the McAfee DLP policy directly.

  Tip

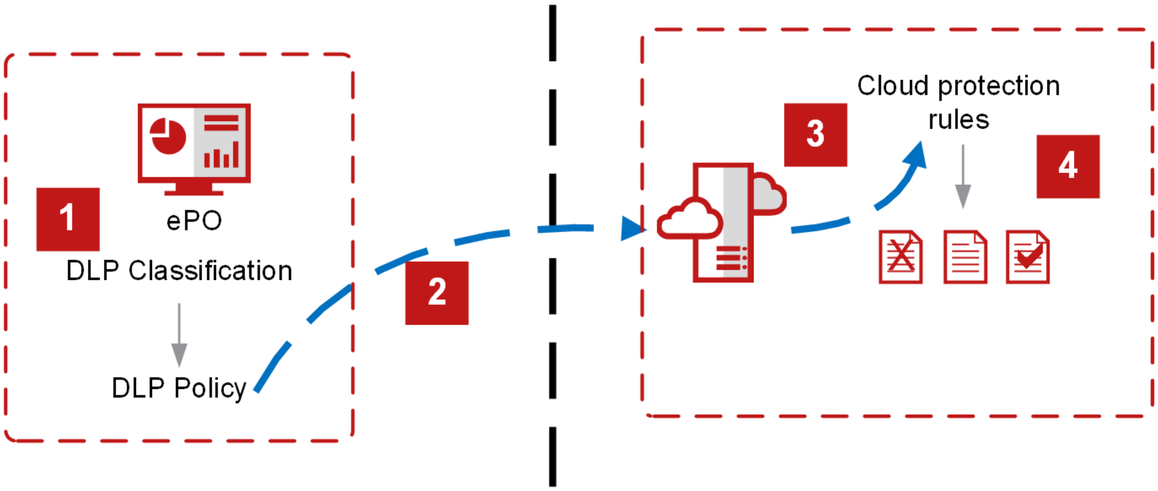
  > Email Protection rules that include the **Enforce on McAfee Cloud DLP** option extend support to supported cloud email services such as Microsoft Exchange Online.

The incidents reported in MVISION Cloud can be used for analysis and reporting in the DLP Incident Manager, giving a merged view of DLP incidents occurring in both on-premises and cloud enforcement points.

Use the following workflow to add McAfee DLP classifications to MVISION Cloud protection rules:

1. The McAfee DLP administrator creates classification definitions, and adds them to a policy.
2. The McAfee DLP administrator applies the McAfee DLP policy to MVISION Cloud.
3. The MVISION Cloud administrator enables using DLP classifications in the MVISION Cloud UI and adds DLP classifications to MVISION Cloud protection rules.
4. The MVISION Cloud protection rules are applied to content in the customer's protected cloud service accounts.

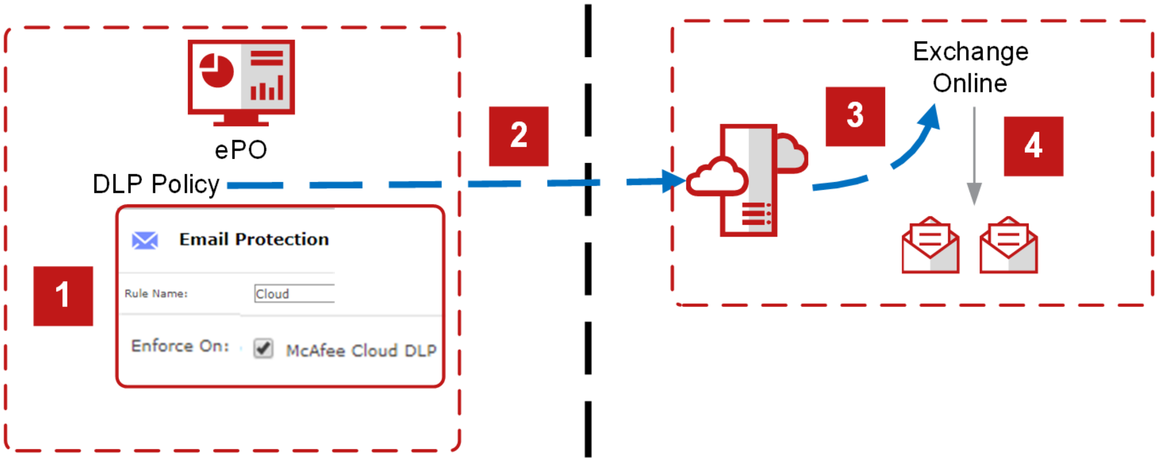
Workflow for MVISION Cloud protection rules



Use the following workflow to apply a MVISION Cloud policy to Exchange Online:

1. The McAfee DLP administrator creates a DLP policy with email rules and associated MVISION Cloud reactions
2. The McAfee DLP administrator applies the McAfee DLP policy to MVISION Cloud.
3. The MVISION Cloud administrator enables DLP policy for Exchange Online within the MVISION Cloud UI.
4. The DLP Policy is applied to Exchange Online content in the customers connected account.

Workflow for McAfee DLP policy applied to Exchange Online



Email Protection

Rule Name: Cloud

Enforce On: ☑ McAfee Cloud DLP

How MVISION Cloud incidents are reported in McAfee DLP

McAfee DLP pulls incidents periodically from MVISION Cloud and displays them in the DLP Incident Manager. Some of the MVISION Cloud incident properties have different names than the incident properties in DLP Incident Manager. These incident properties are mapped to their equivalent terms in DLP Incident Manager to guarantee consistency across all incident reports, regardless of their source.

To enable Evidence Copy from MVISION Cloud, go to **Policy Settings** → **Send evidence files to ePO Enable**. Evidence files are downloaded by McAfee DLP and copied to the on-premises DLP evidence storage.

Evidence files that are pulled from MVISION Cloud can be opened via the McAfee DLP Incident Manager, with hit highlighting also displayed.

Note

> Evidence Copy is only supported for MVISION Cloud Classification Policy incidents.

For more detailed information about how each MVISION Cloud incident property is mapped to the equivalent term in DLP Incident Manager see KB 90962

Use case: Import MVISION Cloud incidents to McAfee DLP

McAfee DLP pulls incidents periodically from MVISION Cloud and displays them in the **DLP Incident Manager**. To manually import incidents MVISION Cloud, you can run the **DLP Import MVision Cloud Events Task** server task.

Task

1. Configure number of incidents in **MVISION Cloud Server**.
   a. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Settings** → **MVISION Cloud Server**.
   b. Select **Connect to McAfee MVISION Cloud** to enable the fields needed to configure the settings for MVISION Cloud incidents and policies.
   c. Provide the MVISION Cloud server details and credentials.
   d. To **Pull incidents from MVISION Cloud**, select the number of incidents that you want to import in a server task.

      Note

      > The default number of incidents that you can import from MVISION Cloud is 1000.

   e. To **Push DLP policy to MVISION Cloud**, select the policy name.
2. Run the server task to import MVISION Cloud incidents.
   a. In McAfee ePO, select **Menu** → **Automation** → **Server Tasks**.
   b. Select the checkbox next to **DLP Import MVision Cloud Events**, then select **Actions** → **Run**.

Results

After the server task is complete, the specified number of incidents can be viewed in **DLP Incident Manager**.

Policy violations in McAfee ePO and MVISION Cloud

When there is a violation of a McAfee DLP policy that uses synchronized classifications fromMcAfee DLP, an incident is created in MVISION Cloud. Additionally, this incident is synchronized back to McAfee ePO because McAfee ePO allows you to view and manage all McAfee DLP incidents (both on-premise and in the cloud).

Policy limitations

- If there is a need to perform further manual remediation actions on the incidents generated (for example, releasing a file from quarantine), these actions need to be taken from the MVISION Cloud interface.

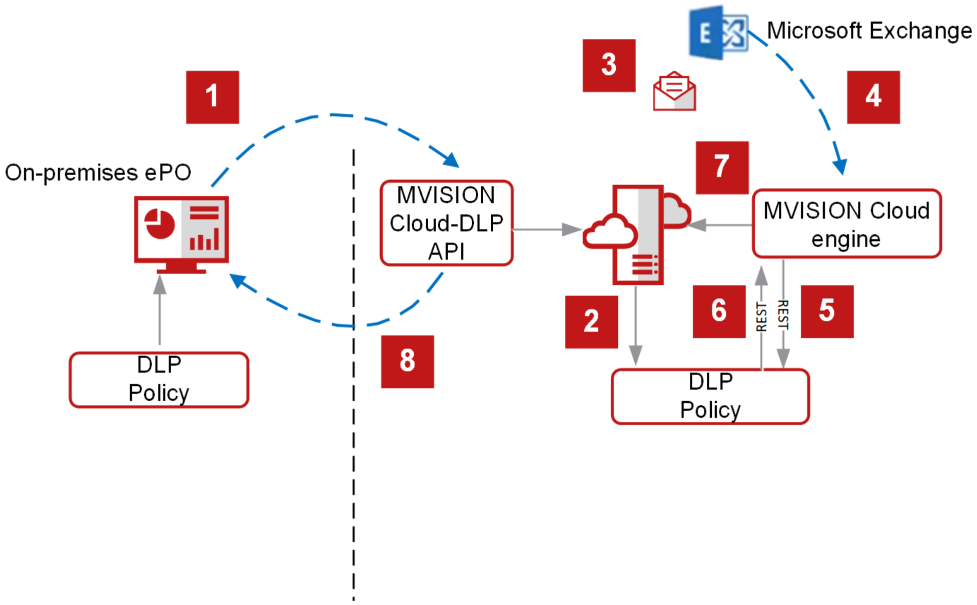
Working with DLP policies in MVISION

Using McAfee DLP policies in MVISION Cloud

Push McAfee DLP policies to MVISION Cloud and apply them to emails

The following diagram describes the high-level process of pushing a McAfee DLP policy to MVISION Cloud.

1. Push the McAfee DLP policy to MVISION Cloud with the **Apply Selected Policies** command in the DLP Policy Manager.
2. MVISION Cloud loads the policy.
3. A user sends an email from the cloud.
4. MVISION Cloud receives the email.
5. MVISION Cloud send the email information to the DLP policy.
6. The DLP service returns the expected action and event metadata.
7. MVISION Cloud performs the action and saves the incident to its database.
8. McAfee DLP pulls incidents to DLP Incident Manager with a frequently scheduled McAfee ePO server task.



Enforcing email protection rules on MVISION Cloud

You can apply email protection rules to Microsoft Exchange Online emails by pushing the policy containing the rule to MVISION Cloud. The **Business Requirements** setting in MVISION Cloud determines how the policy is applied: inline mode or passive mode. Inline mode includes the ability to block emails. Passive mode can't block emails. Depending on the settings in MVISION Cloud, it can monitor, delete, or quarantine.

Create a classification policy in MVISION Cloud

When MVISION Cloud integration is enabled, a MVISION Cloud DLP policy rule called **McAfee Classification** appears.

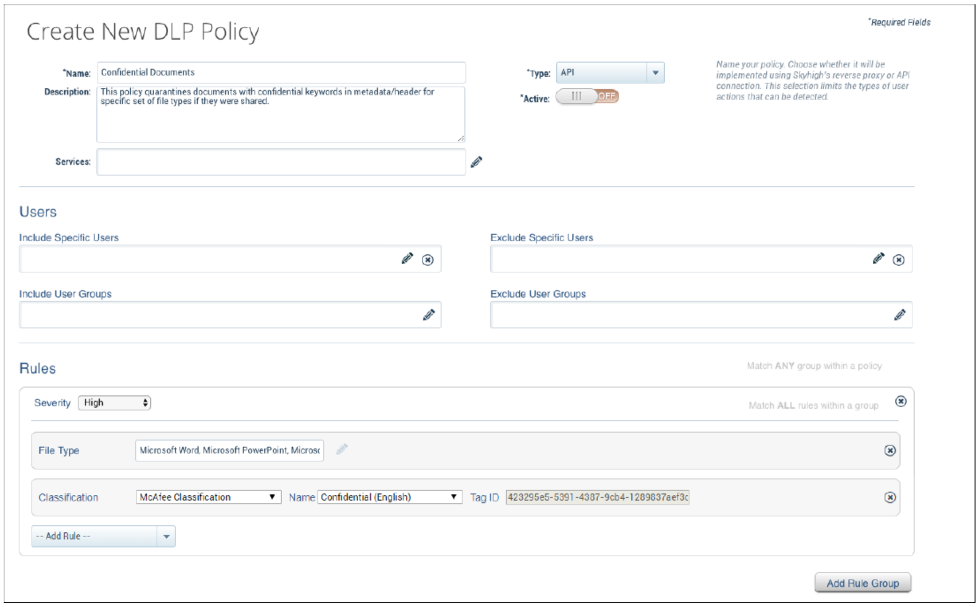
Before you begin

Configure integration with MVISION Cloud on the **DLP Settings** → **MVision Cloud Server** page.

Task

1. Select **Policy** → **Create Policy** or **Edit Policy**.
2. Enter a name and optional description.
3. Under **Rules**, select **Add Rule** → **McAfee Classification**.
4. In the **Name** field, enter the name of the imported classification you want to include in the policy.
5. Fill in the remaining fields, then click **Save**.

Results



Create New DLP Policy

*Required Fields

*Name: Confidential Documents

Description: This policy quarantines documents with confidential keywords in metadata/header for specific set of file types if they were shared.

Services:

*Type: API

*Active: OFF

Name your policy. Choose whether it will be implemented using Skyhigh's reverse proxy or API connection. This selection limits the types of user actions that can be detected.

Users

Include Specific Users

Exclude Specific Users

Include User Groups

Exclude User Groups

Rules

Match **ANY** group within a policy

Severity: High

Match **ALL** rules within a group

File Type: Microsoft Word, Microsoft PowerPoint, Microsc

Classification: McAfee Classification | Name: Confidential (English) | Tag ID: 423295e5-5391-4387-9cb4-1289837aef3c

Configuring MVISION Cloud to use McAfee DLP on-premise classifications

In MVISION Cloud, you can choose to use the McAfee DLP on-premise classifications, because the content rules for your **Cloud DLP** policies. With this option, you do not have to recreate the content rules in the MVISION Cloud tenant, but rather simply synchronize the classifications already created in McAfee ePO.

Task

1. Select **Policy** → **Policy Settings**.
2. Click **On Premise DLP** and then click **McAfee DLP**.
3. Click **On** under **Use Policies** defined in **On Premise McAfee DLP**.
4. Click **Select Services** and then choose the cloud services for which you'd like to use McAfee classifications as the content rules. This gives you the ability to use McAfee classification rules for some services, and MVISION Cloud rules for other services.
   For example, you might want to use McAfee classifications for O365 services like SharePoint and OneDrive, but use native MVISION Cloud rules for Slack.

   Important

   Do *not* select Exchange Online as one of the services to use on-premise McAfee DLP classifications.

5. Click **Save**.

Creating McAfee DLP policies using classifications from on-prem McAfee DLP

Once you've configured MVISION Cloud to synchronize classifications from McAfee DLP, you can create policies using those classifications .

Task

1. Go to **Policy** → **DLP Policies** and select **Create a new DLP Policy** from the **Action** menu.
2. For **Type**, choose **API**.
3. For **Content**, choose **McAfee On Prem DLP**.

   Important

   When you choose **McAfee On Prem DLP** for **Content Rule**, the rules you use in policies can only be classification rules or collaboration rules.

If you are looking for content matches only (for example, looking for documents with 10 or more social security numbers), then use the classifications rules. If you are looking for content matches, combined with a cloud context (for example, looking for documents with 10 or more social security numbers that are being shared with external users), then use the classifications rules, combined with collaboration rules

4. For **Services**, select one or more of the cloud services you selected to use On Prem DLP Classifications.
5. Define the rest of the policy, including any response actions, and click **Save**.

Protecting email - using McAfee DLP policies in McAfee MVISION Cloud

About Inline Email DLP

Inline Email DLP extends MVISION Cloud DLP to the messages sent from your organization's mailboxes.

When using Inline Email DLP, Exchange Online remediation actions occur in real time so data never leaves your organization through Exchange Online email messages.

Components

The following components are required for this feature:

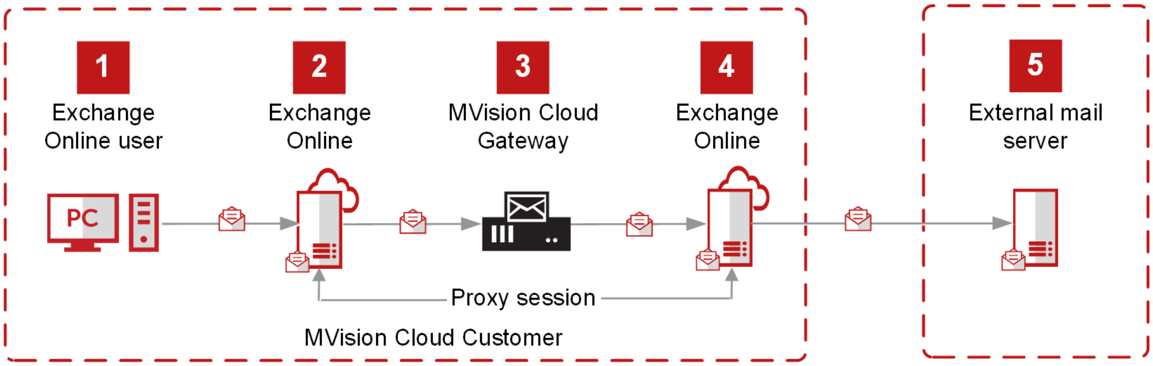
- Exchange Online mail routing (connectors and rules)
- MVISION Cloud Gateway (mail is routed from Office 365 to MVISION Cloud Gateway proxy)
- MVISION Cloud Link (API) connection to Exchange Online for quarantine and delete remediation actions

Email flow

Office 365 is configured to send messages through MVISION Cloud Gateway so it can inspect the contents of the message. MVISION Cloud Gateway acts as an SMTP proxy and as such never stores or queues messages. Messages are processed in real time and require an active inbound and outbound SMTP session to proxy both legs.

The email flow is as follows:

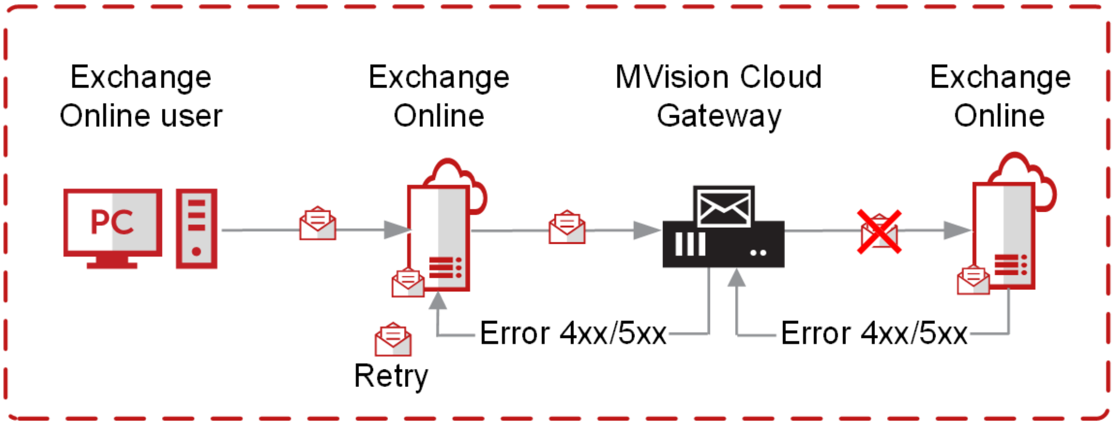
1. A user in your organization sends a message.
2. Based on mail routing rules configured in Exchange Online, messages are forwarded to the MVISION Cloud Gateway SMTP server.
3. The MVISION Cloud Gateway SMTP server proxies the connection from Exchange Online server (2), performs DLP inspection, and proxies back the connection to Exchange Online server (4).
4. Exchange Online receives the message.
5. Exchange Online forwards the message onto one or more original destinations.



Message Transport Error Handling

As the MVISION Cloud Gateway acts as an SMTP proxy, it never accepts the SMTP connection unless the outbound leg can be established. MVISION Cloud Gateway never queues or stores messages so both legs of the connection must be up for messages to flow. This ensures that Exchange Online handles any issues with connections. If a connection fails, the sending Exchange Online will re-queue the message and try again.

Error messages received from the receiving SMTP gateway are relayed back to the sending SMTP gateway so the sending gateway can re-queue the message for transport.



Remediation Options

Because Inline DLP is done in real-time, it requires the API-based MVISION Cloud Gateway integration. MVISION Cloud Gateway ensures that emails are blocked, deleted, or quarantined before they ever leave a sender's email account. For example, if you set up a DLP policy that deletes emails containing sensitive keywords, any message containing a specified word is deleted from a sender's mailbox. With MVISION Cloud Gateway you can choose from the following options:

Block — When an email is blocked, the email remains in the sender's **Sent** folder, but the intended recipient does not receive the message. The MVISION Cloud administrator does not receive a copy of the email in the **Quarantined** folder. The email does not leave the sender's account.

Delete — When an email is deleted, the email is removed from the sender's **Sent** folder, and the intended recipient does not get the email. The MVISION Cloud administrator does not receive the email in the **Quarantined** folder.

Quarantine — When an email is quarantined, the email is removed from the sender's **Sent** folder, and the intended recipient does not receive the email. The MVISION Cloud administrator receives the email in the **Quarantined** folder. Emails are quarantined in real-time, 8031 API.

Notifications — You can choose to notify users and MVISION Cloud administrators by email when messages are blocked, deleted, or quarantined.

Inline Email DLP Prerequisites

To configure Inline DLP, you need the following:

- MVISION Cloud tenant
- A Microsoft Office 365 account with global admin permissions
- An Exchange Online email account

Make sure that you've confirmed that you can send and receive emails before proceeding.

Integrate Inline Email DLP with McAfee ePO

Task

1. In MVISION Cloud, select **Settings** → **Integrations** → **McAfee**.
2. Click **Enable** to begin to use McAfee ePO Exchange Online policies instead of any policies in MVISION Cloud.
3. Click **Edit Users** to add a user account associated with the Service Account that will have the ePO Connector Role.
4. In McAfee ePO, connect to MVISION Cloud. Then return to MVISION Cloud and click **I Did This**.
5. In McAfee ePO, extend rules to MVISION Cloud. Then in MVISION Cloud click **I Did This**.

Enabling inline DLP

1. Set up Exchange Online in MVISION Cloud

There are five steps to enabling Inline DLP: set up Exchange Online in MVISION Cloud, route email from Office 365 to MVISION Cloud, route email back after scanning, create a mail routing rule in Office 365, and test the setup.

Before you begin

To allow the proper flow of email traffic set up a new connector in Office 365. You can learn more about connectors at Configure mail flow using connectors in Office 365.

Task

1. Select **Settings** → **Service Management**.
2. Click **Microsoft Exchange Online**.
3. If Exchange Online has been configured, click **Default**. Otherwise click **New Instance**.
4. Click **Setup**, then click **Configure**.
5. On the Business Requirements screen, select **Inline Only**. Click **Next**.
6. Review the prerequisites, then select **I have reviewed all prerequisites** and click **Next**.
7. Now add domains that are used for McAfee DLP. Add the Microsoft Exchange Online domain(s), then the email domain associated with your McAfee ePO deployment. Next, enter a value for **Host Name** and the **Port**. Make sure that the automatically-generated MVision Cloud Email Server Domain is correct. Click **Next**.
8. For **Quarantine Settings**, you can enter an optional email address where quarantined files are sent. To enable this option, select **Quarantine Emails and Attachments**, then type the email address. Click **Next**.
9. On the **Summary** screen, make sure all settings are correct. Click **Done**.

2. Create mail connectors — route email from Office 365

Create two mail connectors. The first connector sends emails from Office 365 to MVISION Cloud for inspection, and the second accepts emails after they are scanned by MVISION Cloud.

Before you begin

Create a Security Group. To limit the impact of enabling Inline DLP, it's wise to set up a security group in Office 365 with a few email addresses that you can use to test. Once you're happy with the performance, you can then either add additional security groups, or use Inline DLP with all email addresses in your organization. See Manage mail-enabled security groups for instructions.

Make sure to set the following:

- **Type**: Mail-enabled security group
- **Name**: MVisionCloudEmailDLP
- **Allow people outside of my organization to send email to this distribution group**: OFF

If you're unfamiliar with setting up connectors in Office 365, you can find information here.

Task

1. Log on to Office 365 as a Global Admin and navigate to the **Exchange Admin** center.
2. Select **Mail flow**, then **connectors**.
3. Add a connector. Follow the instructions found here: Set up connectors to route mail between Office 365 and your own email server. Make sure to set the following options:

a. Name the new connector `Office 365 to MVision Cloud Email DLP`.

b. Make sure to select **Only when I have a transport rule set up that redirects messages to this connector** when setting up the new connector.

c. Make sure to select **Always use TLS** and **Any digital certificate**, including self-signed when asked how to connect Office 365 to your partner's email server.

3. Create mail connectors — route email back after scanning

Task

1. Return to **Mail flow**, then **connectors**.
2. Add a new **connector**.
3. Under **Select your mail flow scenario**, set the following:
   - **From**: Your organization's email server
   - **To**: Office 365
4. Click **Next**.
5. On the **New connector** screen, enter the following:
   - **Name**: MVISION Cloud Email DLP to Office 365
   - **Description**: Receives email after they are scanned by MVISION Cloud DLP
6. Under What do you want to do after connector is saved, select both of the following:
   - Turn it on
   - Retain internal Exchange email headers
7. Click Next.
8. On the **Edit Connector** screen, under **How should Office 365 identify email from your email server**, select **By verifying that the IP address of the sending server matches one of these IP addresses that belong to your organization**. Then type a list of all Source IP addresses.
9. Click **Next**.

Results

You should now have two connectors, one configured in each direction.

4. Create a mail routing rule in Office 365

Task

1. Log in to Office 365 as a Global Admin and navigate to the **Exchange Admin** center.
2. Select **Mail flow**, then **rules**.
3. Configure a new rule as follows:
   - **Name**: Send to MVISION Cloud Email DLP for inspection
   - **Apply this rule if**: The sender is a member of the [security group you created earlier in Step 2]
4. Click **More options**.
5. From the **Do the following** drop down, choose **Redirect the message to** then choose **the following connector**.
6. Select the **Office 365 to Skyhigh Cloud Email DLP** connector. Click **OK**.
7. On the **new rule** screen, add an exception. Under **Except if**, choose **A message header matches**, then pick**matches these text patterns**. Click **Enter text** then type `X-SHN-DLP-SCAN` . Click **OK**.
8. Type `success` in the text box, then click **OK**.
9. Deselect **Audit this rule with severity level**, then click **Save** to save the rule.

5. Test the setup

Task

1. Test outbound email:
   a. Log in to your Office 365 account using a user that is a member of the security group you created in Step 2.
   b. Send a test email to your work email address and confirm it is received.
2. Confirm the test message was relayed by MVISION Cloud Email DLP. Use the message trace in the Microsoft Exchange admin center to verify that Inline DLP is functioning.
   a. Use a custom date range to filter out noise as required.
   b. Create a policy that will trigger low (log only), medium (quarantine) and high (delete).
   c. Find the message you sent to yourself earlier, and double-click to review details.
   d. Review the message trace and confirm the email was sent out using the connector.

Working with appliance policies

Using policies to define how your McAfee DLP appliances work

Use **DLP Appliance Management**, **Data Loss Prevention**, and **Common Appliance Management** in the **Policy Catalog** to define McAfee DLP appliance settings.

DLP Appliance Management

Use the options in the **DLP Appliance Management** category with McAfee DLP appliances to set policies. You can perform tasks such as specifying a Smart Host or ICAP clients, enabling authenticated email submission, or specifying McAfee DLP Monitor and McAfee DLP Prevent, or enabling the **McAfee DLP Capture** settings. You can also set up load balancing and timeout settings, and the LDAP servers that you want to get user information from.

Data Loss Prevention

Use the **Server Configuration** policy category to edit the **Evidence Copy Service** and OCR settings to work with McAfee DLP appliances.

The **Maximum evidence transmission bandwidth (KBps)** option in **Client Settings** doesn't apply to McAfee DLP appliances.

Common Appliance Management

Specify DNS settings, static route settings, and remote logging servers. You can also edit the appliance date and time and enable SNMP alerts and monitoring.

Set up a cluster of McAfee DLP Prevent appliances

To load balance incoming traffic and ensure high availability, you can create clusters of McAfee DLP Prevent appliances.

Before you begin

Configure two or more McAfee DLP Prevent appliances with LAN 1 connected to the same network segment.

All appliances in a cluster must be in the same subnet or network.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **General** category, and open the policy that you want to edit.
3. In **Load Balancing**, select **Enable**.
4. In **Cluster ID**, use the arrows to select a number to identify the cluster.
5. In **Virtual IP**, enter a virtual IP address so that packets for the virtual IP address are sent to the cluster master.

The appliances in the cluster use the netmask assigned to the physical IP address. The virtual IP address must be in the same subnet or network as the other McAfee DLP Prevent appliances, and cannot be the same IP address as any other appliance in the cluster.

6. Click **Save**.

Results

McAfee ePO pushes the configuration to all appliances in the cluster when you apply the changes. It takes about five minutes for the cluster to stabilize and identify the cluster master and cluster scanners. The appliance descriptions then change accordingly in **Appliance Management**.

Set up a cluster of McAfee DLP Monitor appliances

To load balance the analysis of incoming traffic, you can set up a cluster of McAfee DLP Monitor appliances.

Before you begin

- Configure the McAfee DLP Monitor appliance for a cluster role from the Setup Wizard during installation.
- Configure two or more McAfee DLP Monitor appliances with LAN 1 connected to the same network segment.
- All appliances in a cluster must be in the same subnet or network.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management <version>** product, choose the **General** category, and open the policy that you want to edit.
3. In **Load Balancing**, select **Enable**.
4. In **Cluster ID**, use the arrows to select a number to identify the cluster.
5. In **Virtual IP**, enter a virtual IP address so that packets for the virtual IP address are sent to the cluster master.
   The appliances in the cluster use the netmask assigned to the physical IP address. The virtual IP address must be in the same subnet or network as the other McAfee DLP Monitor appliances, and cannot be the same IP address as any other appliance in the cluster.

   Caution

   > The cluster ID and virtual IP address must be same for all members of a cluster.

6. Click **Save**.

Results

McAfee ePO pushes the configuration to all appliances in the cluster when you apply the changes. It takes about five minutes for the cluster to stabilize and identify the cluster master and cluster scanners. The appliance descriptions then change accordingly in **Appliance Management**.

Enable FIPS 140-2 mode

Configure the McAfee DLP appliance to perform cryptographic operations in a way that is compliant with FIPS 140-2.

Due to the nature of FIPS 140-2, enabling this feature will decrease your appliance's throughput.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **General** category, and open the policy that you want to edit.
3. In **Security mode**, select **Enable FIPS 140-2** mode and click **Save**.

Set connection timeout settings

Change the number of seconds that McAfee DLP Prevent appliance tries to connect with an MTA.

By default, McAfee DLP Prevent appliance tries to connect for 20 seconds. If a connection can't be made in that time, there is an issue with either the network or the MTA that must be investigated.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
3. In **Connection Settings** → **Onward connection**, type the number of seconds that McAfee DLP Prevent appliance can spend trying to connect to an MTA.
4. Click **Save**.

Add an evidence server to store incidents

Some incidents have evidence items associated with them. You can store the evidence on an evidence server.

Before you begin

The evidence server must be a CIFS share with read/write permissions.

Perform this task to configure the default shared evidence storage settings. The settings entered here are reflected in the policies configured in the **Policy Catalog** → **Data Loss Prevention <version>** → **Server Configuration**, **Policy Catalog** → **Data Loss Prevention <version>** → **Windows Client Configuration**, and **Policy Catalog** → **Data Loss Prevention <version>** → **Mac OS X Client Configuration** pages. You can update the settings for the McAfee DLP Discover, McAfee DLP Prevent, McAfee DLP Monitor, and DLP Server in the **Server Configuration** policy.

Task

1. In McAfee ePO, select **Menu** → **DLP Settings** → **General**.
2. Enter the path to the evidence server in **Shared Storage** to save the settings and activate the software.
   The evidence storage path must be a network path, that is `\\[server]\[share]`.
3. Provide the user name and password to access the server, and click **Save**.

Connect to an evidence server outside your firewall

If your McAfee DLP appliance is in a demilitarized zone (DMZ), you can securely copy the evidence files, despite no network access to the evidence file share. McAfee DLP allows you to copy the evidence files to the evidence file share via the McAfee DLP server.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **General** category, and open the policy that you want to edit.
3. In **McAfee DLP Server for Evidence Copy**, click + to add the host name or IP address of the McAfee DLP servers you want the McAfee DLP appliance to connect to.
4. Click **Update**, then save the changes.

What to do next

After you add the DLP Server for evidence copy, edit the **Policy Catalog** → **Data Loss Prevention <version>** → **Server Configuration** policy applied to the DLP Server and enable evidence storage HTTP service.

Specify the server for registered documents

Specify a McAfee DLP Discover server in the Policy Catalog to use registered documents in McAfee DLP appliance policies.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **General** category, and open the policy that you want to edit.

3. In **McAfee DLP Server for Registered Documents**, click the add button (**+**) to enter IP addresses or host names of the McAfee DLP Discover servers with the registered documents databases you want to use.
   Registered documents database servers are McAfee DLP Discover servers with the McAfee DLP Server role. The server port is predefined as 6379.
4. (Optional) Select the **Use TLS** checkbox to specify a secure connection.
5. Click **Save**.

Customize the appliance console banner text

You can customize the text that appears at the top of the appliance console logon screen and when you connect using SSH.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **General** category, and open the policy that you want to edit.
3. In **Custom Logon Banner**, select **Display a custom banner** and click **Save**.
   You must use plain text.

Results

The next time you log on to the appliance console, or connect to it using SSH, your text is displayed after you provide your user credentials.

Disable access to management ports through the traffic interface

You can separate management traffic from client traffic to improve security.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **General** category, and open the policy that you want to edit.
3. In **Out-of-Band Management**, select **Disable in-band access to management ports**.
   The listed ports are only accessible through the management interface.
4. Add or remove management ports from the list as needed, and click **Save**.

Specify a maximum level of nesting of archived attachments

To protect the appliance from denial-of-service attacks, set the maximum level of nesting of archived attachments that it attempts to analyze before it times out.

Note

An example of a nested attachment is a .zip file in another .zip file.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **General** category, and open the policy that you want to edit.
3. In **Analysis Settings** → **Maximum nesting depth**, set the maximum level of nested archive attachments.
4. Click **Save**.

Enable authenticated email submission

You can configure the McAfee DLP Prevent appliance for authenticated email submission in scenarios where network policies do not allow email communication on port 25. You can also use this configuration when it is mandatory to use authenticated mail submission.

Before you begin

- Make sure that the configured Smart Host supports LOGIN mechanism for authentication.
- The default port for authenticated mail submission is 587.
- If the Smart Host configuration includes a port number, make sure that the configured port supports LOGIN mechanism for authentication. For example, in 1.2.3.4:50, port 50 must support LOGIN mechanism.

When this feature is enabled, the McAfee DLP Prevent appliance listens on port 587 to accept emails using the supported authentication mechanisms. McAfee DLP Prevent appliance currently supports only the LOGIN mechanism for SMTP AUTH.

For emails received on port 587, the McAfee DLP Prevent appliance expects the inbound MTA to use LOGIN mechanism to provide the user name and password details. McAfee DLP Prevent appliance then connects to port 587 or the port specified in the Smart Host configuration of the outbound MTA (Smart Host). It then uses these logon credentials (via LOGIN mechanism) while delivering the email.

The authentication of user name and password sent by the inbound MTA typically happens in the Smart Host when the appliance delivers the email to the Smart Host. The McAfee DLP Prevent appliance doesn't store the user name and password details.

Note

McAfee DLP Prevent appliance implicitly mandates Transport Layer Security (TLS) for both inbound and outbound communication when authenticated email submission is enabled. The Transport Layer Security settings in **DLP Appliance Management <version> → McAfee DLP Prevent Email Settings** are not used for authenticated email submission.

Task

1. In McAfee ePO, select **Menu → Policy → Policy Catalog**.
2. In **Product → DLP Appliance Management**, select the **McAfee DLP Prevent Email Settings** category, and open the policy you want to edit.
3. In the **SMTP** field, select the **Enable Authenticated Mail Submission (Uses SMTP AUTH over TLS on port 587)** checkbox.
4. Click **Save**.

Close the McAfee DLP Prevent appliance SMTP ports

To improve performance and security on McAfee DLP Prevent appliances dedicated to analyzing web traffic, close the SMTP ports.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, select the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
3. In the **SMTP** field, deselect **Enable SMTP** and **Enable Authenticated Mail Submission (Uses SMTP AUTH over TLS on port 587)**.
4. Click **Save**.

Add more MTAs that can deliver email

McAfee DLP Prevent delivers email messages using the configured Smart Host. You can add more MTAs that McAfee DLP Prevent deliver email messages in addition to the Smart Host.

Before you begin

Make sure that you have the IP addresses or host names of the Smart Hosts.

McAfee DLP Prevent accepts email messages from more than one MTA, but forwards the inspected email messages to only one of the configured Smart Hosts.

Task

1. In McAfee ePO, open the **Policy Catalog**.

2. Select the **DLP Appliance Management** product, choose the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
3. In the **Smart Hosts** field, add the details of the MTAs that you want to use.
4. Click **Update** and click **Save**.

Deliver emails using a round-robin approach

Configure McAfee DLP Prevent appliance to deliver to multiple email servers by distributing the email messages among them.

Before you begin

Ensure that you have the IP addresses or host names of the Smart Hosts.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
3. In **Smart Hosts**, select the **Round-robin** checkbox. Click **+** to add an MTA. Add the details of the MTAs and click **Update**.
4. Click **Save**.

Limit connections to specified hosts or networks

By default McAfee DLP Prevent appliance accepts messages from any host. Specify the hosts that can send messages to McAfee DLP Prevent so that only legitimate source MTAs can relay email though the appliance.

Before you begin

Specify the Smart Hosts that can send messages.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
3. In **Permitted Hosts**, select **Accept mail from these hosts only**.
4. Type the details of a host that the McAfee DLP Prevent appliance can receive messages from.
   Add the host information using its IP address and subnet, domain names, or wildcard domain name.
5. Click **Update** to add the details to the list of permitted hosts.
   You can create groups of relay hosts using subnets or wildcard domains. To add more than one subnet, you must create separate entries for each.
6. Click **Save**.

Bypass scanning of emails

You can configure the McAfee DLP Prevent appliance to bypass scanning of emails sent from the specified email addresses.

Before you begin

Specify the Smart Hosts that can send messages.

Note

> The bypassed emails are not reported in incidents. The appliances also don't generate evidence or capture data from the bypassed emails.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management <version>** product, choose the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
3. In the **DLP Scan Bypass** field, type the sender email address that you want to bypass from scanning. Use the **is** format to specify the actual email address. Use the **matches** format to specify multiple email addresses using *@domain_name.com. Click **Update** after typing each email address or domain name.
    - To add an email address, click **+**.
    - To remove an email address, click **–**.
4. From **Actions**, choose the action header that you want to include in the message sent to the configured Smart Host. By default, you can select **Add header X-RCIS-Action (BYPASS)**
   Selecting **Add header X-RCIS-Action (BYPASS)** adds the BYPASS value to the X-RCIS-Action header in the message sent to the configured Smart Host. Selecting **No Action** doesn't add any header value in the message sent to configured Smart Host.
5. Click **Save**.

Enable TLS on incoming or outgoing messages

You can specify whether McAfee DLP Prevent uses TLS to protect incoming and outgoing messages, or only uses TLS when it is available (known as **Opportunistic**). A minimum protocol version of TLS 1.1 is used.

McAfee DLP Prevent can perform cryptographic operations in a way that is compliant with FIPS 140-2. This means that incoming and outgoing TLS connections use high-strength cryptographic algorithms.

Important

> Using FIPS 140-2 can impact performance when analyzing SMTP content.

The option to enable FIPS 140-2 is located in the **General** category of the **DLP Appliance Management** product in the **Policy Catalog**. Due to the nature of FIPS 140-2, enabling this feature decreases your appliance's throughput.

TLS works by communicating a set of parameters — known as a handshake — at the start of a connection between participating servers. When these parameters are defined, communications between the servers become secure so that servers that did not participate in the handshake can't decode them.

The handshake process

- The appliance requests a secure connection to the receiving email server and presents it with a list of cipher suites.
- The receiving server selects the strongest supported cipher from the list, and gives the details to the appliance.
- The servers use the Public Key Infrastructure (PKI) to establish authenticity by exchanging digital certificates.
- Using the server's public key, the appliance generates a random number as a session key and sends it to the receiving email server. The receiving server decrypts the key using the private key.
- Both the appliance and the receiving email server use the encrypted key to set up communications and complete the handshake process.

Once the handshake is complete, the secure connection is used to transfer the email messages. The connection remains secure until the connection is closed.

Note

If you select the **Always** option for outbound communications, but the Smart Host is not configured to use TLS, McAfee DLP Prevent sends a **550 x.x.x.x: Denied by policy. TLS conversation required** error.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **McAfee DLP Prevent Email Settings** category, and open the policy that you want to edit.
3. In **Transport Layer Security**, select either **Always** or **Opportunistic** for inbound communications.
   Opportunistic is the default setting.
4. Select either **Always** or **Opportunistic** for outbound communications.
   Opportunistic is the default setting.
5. Click **Save**.

Configure McAfee DLP Prevent to scan encrypted ICAP traffic only

To improve security, you can stop the McAfee DLP Prevent appliance from analyzing unencrypted ICAP traffic.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, select the **McAfee DLP Prevent Web Settings** category, and open the policy you want to edit.
3. In **Web Settings**, deselect **Unencrypted ICAP (port 1344)**.
4. Click **Save**.

Close the McAfee DLP Prevent appliance ICAP ports

To improve security and performance on a McAfee DLP Prevent appliance dedicated to analyzing email traffic, you can close the ICAP ports.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, select the **McAfee DLP Prevent Web Settings** category, and open the policy that you want to edit.
3. In **Web Settings**, deselect both the ICAP service options.
4. Click **Save**.

Enable a McAfee DLP Prevent appliance to process response requests

You can configure a McAfee DLP Prevent appliance to analyze requests made to your web servers from external users.

Note

A common McAfee DLP Prevent appliance deployment is to have the McAfee DLP Prevent appliance inside your network and the web server outside your network. Enabling RESPMOD analysis can impact performance because it takes longer to get responses from the appliance, which causes a slower user experience.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, select the **McAfee DLP Prevent Web Settings** category, and open the policy you want to edit.
3. In **Web Settings**, select **RESPMOD**.
4. Click **Save**.

Using external authentication servers

McAfee DLP appliances can work with registered LDAP servers and McAfee Logon Collector to retrieve user information and logon data. The data helps identify users responsible for data loss incidents using their name, group, department, city, or country.

McAfee DLP appliances can:

- Get information from Active Directory servers and OpenLDAP directory servers that are registered with McAfee ePO.
- Communicate with registered LDAP servers over SSL.
- Synchronize with LDAP servers daily at the configured time.
- Act on email and web protection rules which apply to specific users and groups.
- Act on network communication protection rules which apply to specific users and groups (McAfee DLP Monitor).
- Connect to **Global Catalog** ports instead of standard LDAP ports to retrieve user and group information when querying Active Directory.
- Include user information in incidents so that you can see all incidents generated by a user, regardless of the McAfee DLP product that detected them.

McAfee Logon Collector records Windows user logon events and communicates the information to McAfee DLP appliances. McAfee DLP appliances can map an IP address to a Windows user name if no other authentication information is available.

What happens if the LDAP server is unavailable?

McAfee DLP appliances cache LDAP information. The cache updates every 24 hours, so temporary unavailability of the LDAP server does not affect McAfee DLP appliances service availability. If the cache update fails, McAfee DLP appliances use the previous cache. If a previous cache is not available, it performs an LDAP lookup to get the information.

Note

If the McAfee DLP appliances can't reach or communicate with a newly configured LDAP server, the domain-based lookup and the policy push fail. Policy push also fails if you have configured domain-based users or groups in policies and not selected the corresponding LDAP server for the appliance.

When McAfee DLP Prevent needs LDAP group information to evaluate rules for a request or message, and LDAP is not configured or the server is unavailable:

- For SMTP traffic — A temporary failure code (451) is returned so the message is queued on the sending server and retried.
- For ICAP traffic — An ICAP status 500 code is returned that indicates the server encountered an error and was unable to analyze the request. You can configure your web gateway to fail open or closed when it receives an error from the McAfee DLP Prevent server.

For McAfee DLP Monitor, if McAfee Logon Collector or the LDAP information is unavailable, rules which refer to user and group information can't be matched and incidents are not created. Your traffic flow is unaffected.

OpenLDAP and Active Directory servers

- OpenLDAP and Active Directory produce different user schemas. Active Directory has a constrained set of parameters, but OpenLDAP is customizable.
- OpenLDAP and Active Directory servers identify users by using different means of identification. Active Directory uses sAMAccountName, and OpenLDAP uses UID. LDAP queries for sAMAccountName are handled by using the UID property on OpenLDAP systems.
- OpenLDAP and Active Directory servers also identify user classes by using different user attributes. Instead of the User object class, OpenLDAP uses inetOrgPerson, which does not support country or memberOf attributes.

Additional web protection authentication

When applying web protection rules, McAfee DLP Prevent can get *user* information from:

- X-Authenticated-User ICAP request header sent from the web gateway.
- McAfee Logon Collector

If a user name is supplied in the X-Authenticated-User ICAP header, it is used in preference to data from McAfee Logon Collector.

Tip

Using the X-Authenticated-User header is the recommended authentication method because it indicates that the web gateway has positively authenticated the user. To set it up, you must perform some additional configuration on the web gateway. For more information, see your web gateway product documentation.

If the X-Authenticated-User header is not available, you can configure McAfee Logon Collector to provide additional authentication. McAfee Logon Collector is another McAfee product that monitors Windows logon events and maps an IP address to a Security Identifier (SID). To use McAfee Logon Collector, you must have at least one LDAP server configured: The McAfee DLP appliance can query it to convert a SID to a user name.

When applying email or web protection rules, McAfee DLP Prevent evaluates *group* information from the *user* information. It ignores any X-Authenticated-Groups header value from the web gateway.

To select rules based on users and groups for McAfee DLP Monitor, you must configure McAfee Logon Collector.

Important

To obtain user or group information, you must have at least one LDAP server configured. The McAfee DLP appliance queries LDAP servers to get the required attributes. For example, for McAfee Logon Collector, the McAfee DLP appliance uses the LDAP server to convert the SID to a user DN.

Supported authentication schemes

The McAfee DLP Prevent appliance supports the WINNT, NTLM, KERBEROS, LOCAL, and LDAP authentication schemes to process the X-Authenticated-User header from the web gateway.

The McAfee DLP Prevent appliance expects the format for the X-Authenticated-User header to be in one of these formats for Active Directory:

- NTLM — NTLM://<*NetBIOS_name/sAMAccountName*>
- WINNT — WINNT://<*NetBIOS_name/sAMAccountName*>
- KERBEROS — Kerberos://<*Realm-Name*>/<*sAMAccountName*>
- LOCAL — Local://UPN, where UPN is the Active Directory User Principal Name in the <*user_name@internet.domain.com*> format.

Note

OpenLDAP is not supported with Kerberos, NTLM, and LOCAL.

With LDAP, McAfee DLP Prevent expects the X-Authenticated-User header to be in the format LDAP://<*LDAP_servername/distinguished-name*> for Active Directory and OpenLDAP.

Note

McAfee DLP Prevent uses the distinguished-name LDAP attribute to retrieve user details for web protection rules. Verify that your LDAP server exposes this attribute to make sure that the LDAP authentication scheme works correctly.

Use case

You want to configure a web protection rule that blocks uploads of PCI data for all users in a department apart from one.

1. Register an Active Directory server with McAfee ePO that contains the user account of the employee that you suspect.
2. Set up McAfee Logon Collector.
3. Create a web protection rule that looks for web requests from users in the group **GROUPNAME** matching a classification.
4. Create an exception for user **USERNAME**.
5. Set the reaction to **Block**.
6. Monitor the **DLP Incident Manager** for incidents sent by the user that contain the component name.

Register an LDAP server

You must have a registered LDAP server to use Policy Assignment rules, to enable dynamically-assigned permission sets, and to enable Active Directory User Login.

Task

1. Select **Menu** → **Configuration** → **Registered Servers**, then click **New Server**.
2. Select **LDAP Server** from the **Server type** menu, then specify a unique name and optional description and click **Next**.
3. Select an OpenLDAP or Active Directory server from the **LDAP server type** list.
4. Specify a domain name or a specific server name.
   Use DNS-style domain names (such as `internaldomain.com`), or fully-qualified domain names or IP addresses for servers (such as `server1.internaldomain.com` or `192.168.75.101`). OpenLDAP servers can only use server names. They cannot be specified by domain.
5. Specify whether to use the Global Catalog (not available for OpenLDAP servers).

Select it only if the registered domain is the parent of only local domains to avoid potential network traffic, which can impact performance.

6. If you don't use the Global Catalog, select whether to chase referrals.
   Chasing referrals can generate non-local network traffic.
7. Choose whether to use SSL to communicate with this server.
8. If you are configuring an OpenLDAP server, enter the port.
9. Enter a user name and password for an admin account on the server.
   - Active Directory servers — Use the format `domain\username`
   - OpenLDAP servers — Use the format `cn=User,dc=realm,dc=com`
10. Enter a **Site** name for the server, and click **Test Connection** to verify the connection, then click **Save** to complete the registration.

Retrieve and synchronize information from registered LDAP servers

McAfee DLP appliances can get user and group information from LDAP servers that are registered with McAfee ePO. You need to select the registered LDAP servers that you want McAfee DLP appliances to get information from.

Before you begin

Make sure that the LDAP servers are registered with McAfee ePO.

User and groups details are used when evaluating the **Sender** information. The McAfee DLP appliance can:

- Connect to OpenLDAP and Active Directory servers.
- Communicate with a registered LDAP server over SSL.
- Configure or set the daily synchronization time of appliances with LDAP servers as synchronizing multiple appliances with LDAP servers at the same time can overload the LDAP servers.
- Connect to **Global Catalog** ports instead of standard LDAP ports to retrieve user and group information when querying Active Directory.
  If you configured Active Directory to use **Global Catalog** ports, make sure that at least one of these attributes is replicated to the **Global Catalog** server from the domains in the forest:
  - proxyAddresses
  - mail

  If a McAfee DLP appliance needs to use NTLM or WINNT authentication for analyzing web protection rules, these LDAP attributes must also be replicated:
  - configurationNamingContext
  - netbiosname
  - msDS-PrincipalName

Messages are temporarily rejected with a 451 status code when both of these conditions are met:

- McAfee DLP Prevent uses rules that specify the sender is a member of a particular LDAP user group.
- McAfee DLP Prevent is not configured to receive information from the LDAP server that contains the specified user group.

Events are sent to the **Client Events** page if synchronization with the LDAP server or an LDAP query fails.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, choose the **Users and groups** category, and open the policy that you want to edit.
3. In **LDAP Servers**, select at least one valid LDAP server to enable synchronization configuration.
4. In the **Initiate daily synchronization at** field, set the daily synchronization time. The default synchronization start time is set to 3 a.m.
   The synchronization of the appliance with LDAP servers happens daily at the configured time.
5. (Optional) Select and update the **Delay synchronization start by up to (hours)** field to configure the delay between the synchronization start of appliances. The default synchronization delay between appliances is set to two hours. You can configure the random delay synchronization start interval between 1–10 hours.
6. Click **Save**.

Add a McAfee Logon Collector server and certificate to a McAfee DLP appliance

To start using McAfee Logon Collector with McAfee DLP appliance, you must add a McAfee Logon Collector certificate to an appliance and then add a McAfee DLP appliance certificate to McAfee Logon Collector.

Before you begin

- Have at least one McAfee Logon Collector server configured.
- Do these web proxy changes to ensure a smooth communication between McAfee Logon Collector and McAfee DLP appliance:
  -

    The web proxy must be configured to send the **X-Client-IP** header. This is usually the IP of the host running the browser or the web client.
  - The web proxy must not send the **X-Authenticated-User** header.

Task

1. To download the certificate from the McAfee DLP appliance, go to https://*<APPLIANCE>*:10443/certificates, then select **[Hostname.domain.crt]**
2. In McAfee Logon Collector, select **Menu** → **Trusted CAs** → **New Authority** → **Choose File**, select the certificate you downloaded, and click **Save**.
3. In McAfee ePO, open the **Policy Catalog**.
4. Select the **DLP Appliance Management** product, choose the **Users and groups** category, and open the policy that you want to edit.
5. Add the McAfee Logon Collector server details to the McAfee DLP appliance.
   a. In the **McAfee Logon Collector** section, select **Identify users making web requests**.
   b. Click **+** to open the **Add** dialog box.
   c. Type an IPv4 address or host name of a McAfee Logon Collector server you want to connect to.
   d. Edit the McAfee Logon Collector port if needed.
6. Get the certificate text from McAfee Logon Collector.
   a. In McAfee Logon Collector, select **Menu** → **Server Settings**.
   b. Click **Identity Replication Certificate**.
   c. Select the certificate text in the **Base 64** field and copy it to the clipboard or into a file.
7. Return to the **Add** dialog box and select either **Import from file** or **Paste from clipboard** to add the certificate text.
8. Click **OK** to complete the McAfee Logon Collector authentication.
   [Optional] Add more McAfee Logon Collector servers.
   The **McAfee Logon Collector** server is added to the list of servers.

Web proxy changes needed for integration with McAfee Logon Collector

You must configure the web proxy servers to enable smooth communication between McAfee DLP appliances and McAfee Logon Collector.

Web proxy server configurations include:

-

  The web proxy must be configured to send the **X-Client-IP** header. This is usually the IP of the host running the browser or the web client.

- The web proxy must not send the **X-Authenticated-User** header.

Apply network communication protection rules to FTP, HTTP, or SMTP traffic

You can configure McAfee DLP Monitor to apply network communication protection rules to SMTP, HTTP, or FTP traffic. By default, email and web protection rules are applied.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, select the **McAfee DLP Monitor Settings** category, and open the policy that you want to edit.
3. In **Protocol Rule Application**, deselect the options as required and click **Save**.

Create a traffic filtering rule

By default, McAfee DLP Monitor analyzes all protocol traffic. You can create extra rules that filter the protocol traffic in priority order. This improves performance and stops incidents being created for protocols that are not relevant to your requirements.

McAfee DLP Monitor analyzes the traffic rules in a top-down priority order. The analysis stops when it finds a match, and takes the corresponding action.

If there is an HTTP conversation between a client 1.2.3.4 and a server 2.3.4.5, there are two transactions over the same TCP connection. As a result, the traffic filtering rules are evaluated separately. For example:

- The HTTP request (source 1.2.3.4:9999, destination 2.3.4.5:80)
- The HTTP response (source 2.3.4.5:80, destination 1.2.3.4:9999)

Tip

If your organization's network range is, for example, 192.168.0.0/16:

- Filter out protocols or hosts that you do not want to analyze.
- Analyze all traffic where the source address is in the range 192.168.0.0/16.
- Do not analyze the remaining traffic.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, select the **McAfee DLP Monitor Settings** category, and open the policy that you want to edit.
3. In the **Traffic Rules** section, click + to open the **Define Rule** dialog box.
4. Type a name for the rule, then click + to specify the network attributes you want the rule to filter on.
   Each attribute can only be added once to a rule.
   - **Source IP Address** — Specify an IP address or an IP address and netmask.
   - **Destination IP Address** — Specify an IP address or an IP address and netmask.
   - **Source Port** — Specify a port in the range of 0-65535.

- **Destination Port** — Specify a port in the range 0-65535.
- **VLAN ID** — Specify the VLAN tag ID. Untagged traffic uses the default 4095 ID.
- **Transport Protocol** — Choose from TCP or UDP.
- **Application Protocol** — Select the protocol you want the rule to match on.
- **SOCKS Encapsulation** — Select whether the traffic is encapsulated.
- **Sender Email Address** — Specify the sender email address to match against.
- **Recipient Email Address List** — Specify the recipient email address to match against.
- **URL** — Specify the HTTP URL.

5. Select the match operator and select or type the value for the attribute you are adding, then click **Update**.
6. Add more criteria as needed and click **OK** to return to **DLP Monitor Settings**.
   The rule is added to the top of the list.
7. Use the arrows to position the new rule where you want it in the priority order and optionally select **Scan Traffic**.

Integrating McAfee DLP Prevent in your web environment to secure your web environment

The McAfee DLP Prevent appliance works with your web proxy to protect web traffic.

McAfee DLP Prevent appliance uses ICAP or ICAPS (ICAP over TLS) to process web traffic, which uses these ports:

- **ICAP** — 1344
- **ICAPS** — 11344

Use this workflow to configure your environment for web protection.

1. Configure endpoint clients to send web traffic to the web proxy.
2. Configure the web proxy to forward HTTP traffic to McAfee DLP Prevent via ICAP.
3. Configure policy on the McAfee DLP Prevent appliance to specify the action to take based on the content of the traffic.

   Example: Configure a rule to allow or block traffic from particular users that contains credit card numbers.

After the McAfee DLP Prevent appliance analyzes the traffic, it performs one of these actions:

- Allows the traffic and informs the web proxy.
- Denies the traffic and supplies a block page, which is presented to the user.

Integrate with Web Gateway

You can configure Web Gateway to forward HTTP traffic using ICAP to McAfee DLP Prevent for analysis. McAfee DLP Prevent returns a response to Web Gateway, allowing or denying the page.

Note

All versions of Web Gateway are supported, but these steps are applicable only for version 7.8.1. The steps can differ slightly for older or newer versions. For the detailed steps in the version of Web Gateway that you have installed, see the Web Gateway documentation.

Task

1. In Web Gateway, select **Policy**.
2. Add the rule set:
   a. Click the **Rule Sets** tab.
   b. Select **Add** → **Rule Set from Library**.
   c. From the **ICAP Client** rule set library, select **ICAP Client**, then click **OK**.
   d. Click **Unlock View**, then click **Yes**.
   e. Deselect **Responses**.
3. (Optional) If you want the generated incidents to contain the destination IP address, edit the REQMOD settings.
   a. On the **Rule Sets** tab, expand the **ICAP Client** rule set and select **ReqMod**.
   b. Select **Add X-Server-IP header**.
4. Follow these steps to set the appliance as an ICAP client:
   a. Click the **Lists** tab, expand ICAP Server and select **ReqMod Server**.
   b. Select **1** and click **Edit**.
   c. Type the IP address or the fully qualified domain name of the McAfee DLP Prevent appliance, followed by the ICAP mode in the **URI** field. Optionally, you can add a port. If you add no port, the default port 1344 is configured.

      The syntax for specifying this information is displayed above the field. For example, you can use one of these formats:

      ```
      icap://xx.xxx.xxx.xx/reqmod
      ```

      ```
      icap://xx.xxx.xxx.xx:1346/reqmod
      ```

      ```
      icap://test-icap.micmwg.com/reqmod
      ```

      ```
      icap://test-icap.micmwg.com:1346/reqmod
      ```

   d. Click **OK**.
5. Enable the rule.
   a. On the **Rule Sets** tab, select the **ICAP Client** rule.
   b. Select **Enable**.
6. Click **Save Changes**.

Enable secure ICAP connections

Appliance port 11344 is the only port that receives SSL traffic for ICAP. For communication to happen in the SSL mode, you can enable the secure ICAP port. To use this mode, you also have to import the appliance certificate.

Task

1. Import the appliance certificate for ICAP connections by uploading the certificate to /home/admin/upload/cert.
   The appliance uses this certificate for ICAP and SMTP traffic. If you have already imported a certificate for SMTP traffic over TLS, you can skip this step.
   The certificate is automatically picked up from this location and imported by the appliance. When negotiating TLS for ICAPS, the appliance presents this certificate. Make sure you have a valid Common Name (CN), Subject Alternative Name, or both.
2. Enable secure ICAP:
   a. In McAfee ePO, open **Policy Catalog**.
   b. Select the **DLP Appliance Management <version>** product, select the **McAfee DLP Prevent Web Settings** category, and open the policy you want to edit.
   c. Select the **Secure ICAP (port 11344)** and **Unencrypted ICAP (port 1344)** checkboxes.
   d. Click **Save**.
   To use only secure ICAP, deselect the **Unencrypted ICAP (port 1344)** checkbox and configure the web proxy to send traffic to only port 11344.

Appliance Management General policy settings

Use the **Policy Catalog** → **Common Appliance Management** → **General** → **<policy name>** → **General** page to configure settings to be applied to appliances managed from McAfee ePO.

Benefits of using general policy settings

Configuring commonly used settings from one page simplifies the process for adding new or re-imaged appliances to your network.

When configuring several appliances or clusters of appliances on a network, some common settings are applied to each appliance. Examples of these settings include:

- Time zones and time and date information
- Lists of DNS servers
- Static routing information
- Secure Shell (SSH) remote logon settings
- System logging settings

By defining and storing these settings in McAfee ePO, you can quickly configure new or re-imaged appliances with relevant settings.

Configure general settings

Configure settings to be applied to several appliances from one location.

Note

You must configure at least one DNS server. The **Save** button is not enabled until you enter a DNS server address. You do not need to configure all other areas of this page; set up only the settings that you want applied to your appliances.

Task

1. From **Policy Catalog** → **Common Appliance Management** → **General** → **<policy name>**, configure **Date and Time**:
    a. Select your required time zone from the drop-down list.
    b. Select **Enable NTP**.
    c. To define a Network Time Protocol (NTP) server, click the + icon.
    d. Enter the server details.
    e. Click **Update**.
2. Configure DNS settings:
    a. To enter DNS server details, click the + icon.
    b. Enter the server details.
    c. Click **Update**.
3. Configure static routing settings:
    a. To enter static routing information, click the + icon.
    b. Enter the route details.
    c. Click **Update**.
4. Configure SSH settings:
    a. Select your required option from the drop-down list.
    b. If you select **Allow remote login from these hosts only**, click the + icon.
    c. Enter the host address.
    d. Click **Update**.
5. Configure logging settings:
    a. To enable remote logging, select **Store log data remotely**.
    b. To define a syslog server, click the + icon.
    c. Enter the syslog server address or domain.
    d. Select the protocol information.
    e. Enter the port.
    f. Click **Update**.
6. Click **Save** to add the configured settings to the **Policy Catalog** in McAfee ePO.

SNMP policy settings

Use the **Policy Catalog** → **Common Appliance Management <version>** → **General** → **<policy name>** → **SNMP** tab to configure the SNMP settings to be applied to appliances managed from McAfee ePO.

Benefits of using SNMP settings

Configuring Simple Network Management Protocol (SNMP) from a single page simplifies the process for adding new or reimaged appliances or clusters of appliances to your network.

Defining common SNMP settings enables these settings to be applied to multiple appliances or clusters of appliances on your network.

- SNMP Alert Settings — SNMP alerts from your appliances provide alert messages directly to a specified trap destination.
- SNMP Monitor Settings — SNMP monitor settings enable other devices to access your appliances or clusters of appliances. You can allow queries from all devices in your network, or restrict access to specific devices.

By defining and storing these settings in McAfee ePO, you can quickly configure new or reimaged appliances with relevant settings.

Configure SNMP settings

Configure the SNMP settings to be applied to your appliances and clusters of appliances.

Before you begin

Make sure that your SNMP management system is configured and tested before configuring the SNMP settings for your appliances.

Task

1. From **Policy Catalog** → **Common Appliance Management** → **General** → **<policy name>** → **SNMP**, configure SNMP Alerts:
   a. Enable **SNMP alerts**.
   b. Enter the address or host name for your **Trap destination**.
   c. Enter the **Community name** you have set up for your SNMP management system.
   d. Select the required version of the SNMP protocol to use.
   e. (Optional) Click the + icon and repeat steps b through d to add more than one trap destination.
2. Configure SNMP Monitor:
   a. Enable **SNMP monitor**.
   b. Select the version of the SNMP protocol used by your SNMP management system.
3. For SNMP versions v1 or v2c:
   a. Enter the community name you have set up for your SNMP management system.
4. For SNMP version v3:
   a. Enter the user name that you have configured for your SNMP management system.
   b. Enter your required authentication protocol. This can be either **MD5 Protocol** or **SHA Protocol**.
   c. Enter your required privacy protocol. This can be either **DES Protocol** or **AES Protocol**.
   d. Enter the authentication passphrase.
   e. Enter the privacy passphrase.
5. Select either **Allow SNMP monitor for all hosts**, or **Allow SNMP monitor for these hosts only**.

If you selected **Allow SNMP monitor for these hosts only**, you must configure at least one host before you can save the SNMP settings.

6. Click **Save** to save these changes, or **Duplicate** to create a policy using these settings.

Download MIBs and SMI files

Download MIB and SMI files to view the SNMP traps and counters that are available on the appliance.

Task

1. Go to https://<APPLIANCE>:10443/mibs.
2. Download the MCAFEE-SMI.txt and MCAFEE-DLP-PREVENT-MIB.txt files in the language you want to view the information in.
3. Download the MCAFEE-SMI.txt and MCAFEE-DLP-MONITOR-MIB.txt files in the language you want to view the information in.
4. Import the MIB and SMI files into your network monitoring software.

Scanning local files with DLP Endpoint discovery

Protecting files with discovery rules

Discovery rules define the content that McAfee DLP searches for when scanning repositories and determine the action taken when matching content is found. Discovery rules can be defined for McAfee DLP Discover or for McAfee DLP Endpoint discovery.

Depending on the type of rule, files matching a scan can be copied, moved, classified, encrypted, quarantined, content fingerprinted, or have a rights management policy applied. All discovery rule conditions include a classification.

Note

When using email storage discovery rules with the **Quarantine** prevent action, verify that the Outlook Add-in is enabled (**Policy Catalog** → **Data Loss Prevention 10** → **Client Configuration** → **Operational Modes and Modules**). You cannot release emails from quarantine when the Outlook Add-in is disabled.

Available discovery rules

Rule type	Product	Controls files discovered from...
Local File System	McAfee DLP Endpoint	Local file system scans.
Local Email (OST, PST)	McAfee DLP Endpoint	Email storage system scans.
File Server Protection	McAfee DLP Discover	File server scans.
SharePoint Protection	McAfee DLP Discover	SharePoint server scans.
Box Protection	McAfee DLP Discover	Box scans
Database Protection	McAfee DLP Discover	Database scans – Oracle, Microsoft SQL, MySQL, DB2

Note

McAfee DLP Discover rules also require a repository. See the chapter *Scanning data with McAfee DLP Discover* for information on configuring rules and scans.

End-user initiated scans

When activated in the DLP Policy local file system scan configuration, end-users can run enabled scans and can view self-remediation actions. Every scan must have an assigned schedule, and the scan runs according to the schedule whether or not the user chooses to run a scan, but when the user interaction option is enabled, the end-users can also run scans at their convenience. If the self-remediation option is also selected, end-users and also perform remediation actions.

Local file system automatic classification

When the **Classify File** action is chosen for local file system discovery rules, the rule applies automatic classification, and embeds the classification Tag ID into the file format. The ID is added to all Microsoft Office and PDF files, and to audio, video, and image file formats. The classification ID can be detected by all McAfee DLP products and 3rd-party products.

How discovery scanning works

Use endpoint discovery scans to locate local file system or email storage files with sensitive content and tag or quarantine them.

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

Note

To use endpoint discovery, you must activate the **Discovery** modules on the **Policy Catalog** → **Client configuration** → **Operational Mode and Modules** page.

At the end of each discovery scan, the McAfee DLP Endpoint client sends a discovery summary event to the **DLP Incident Manager** console in McAfee ePO to log the details of the scan. The event includes an evidence file that lists the files that could not be scanned and the reason for not scanning each of these files. There is also an evidence file with files matching the classification and the action taken.

When can you search?

Schedule discovery scans on the **Policy Catalog** → **DLP Policy** → **Endpoint Discovery** page. You can run a scan at a specific time daily, or on specified days of the week or month. You can specify start and stop dates, or run a scan when the McAfee DLP Endpoint configuration is enforced. You can suspend a scan when the computer's CPU or RAM exceed a specified limit.

If you change the discovery policy while an endpoint scan is running, rules and schedule parameters will change immediately. Changes to which parameters are enabled or disabled will take effect with the next scan. If the computer is restarted while a scan is running, the scan continues where it left off.

What content can be discovered?

You define discovery rules with a classification. Any file property or data condition that can be added to classification criteria can be used to discover content.

What happens to discovered files with sensitive content?

You can quarantine or tag email files. You can encrypt, quarantine, tag, or apply an RM policy to local file system files. You can store evidence for both file types.

Find content with the discovery crawler

There are four steps to running the McAfee DLP Endpoint discovery crawler.

1. Create and define classifications to identify the sensitive content.
2. Create and define a discovery rule. The discovery rule includes the classification as part of the definition.
3. Create a schedule definition.
4. Set up the scan parameters. The scan definition includes the schedule as one of the parameters.

Create and define a discovery rule

Discovery rules define the content the crawler searches for, and what to do when this content is found.

Discovery rules can define endpoint (local email, local file system) or network (Box, File Server, SharePoint, Database) discovery rules.

Changes to a discovery rule take effect when the policy is deployed. If a scan is in progress when a rule is changed, the change takes effect the next time the scan runs.

For email storage (PST, mapped PST, and OST) scans, the crawler scans email items (body and attachments), calendar items, and tasks. It does not scan public folders or sticky notes.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. On the **Rule Sets** page, select **Actions** → **New Rule Set**. Enter a name and click **OK**.
   You can also add discovery rules to an existing rule set.
3. On the **Discovery** tab do one of the following:
   - Select **Actions** → **New Endpoint Discovery Rule**, then select either **Local Email** or **Local File System**.
   - select **Actions** → **New Network Discovery Rule**, then select the rule type: **Box Protection**, **Database Protection**, **File Server Protection**, or **SharePoint Protection**.

   The appropriate page appears.
4. (Optional) On the **Exceptions** tab, specify any exclusions from triggering the rule.
   - For McAfee DLP Endpoint, enter a rule name and configure one or more classifications.
   - For McAfee DLP Discover, enter a rule name and configure one or more classifications and repositories.

   Note

   > For Box protection rules, you also configure the **File Sharing**.
5. On the **Reaction** tab, select an **Action** from the drop-down list.
   For McAfee DLP Discover, the available reactions depend on the repository type.

6. (Optional) Select **Report Incident** options, set the **State** to **Enabled**, and select a **Severity** designation from the drop-down list.
7. Click **Save**.

Create a scheduler definition

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

Five schedule types are provided:

- **Run immediately**
- **Once**
- **Daily**
- **Weekly**
- **Monthly**

Task

1. In McAfee ePO do one of the following:
   a. Select **Menu** → **Data Protection** → **DLP Policy Manager**.
   b. select **Menu** → **Data Protection** → **DLP Discover**.
2. Click the **Definitions** tab.
3. In the left pane, click **Scheduler**.
   If both McAfee DLP Discover and McAfee DLP Endpoint are installed, the displayed list of existing schedules includes schedules for both.
4. Select **Actions** → **New Item**.
   The **New Scheduler** page appears.
5. Enter a unique **Name**, and select the **Schedule type** from the drop-down list.
   The screen changes when you select the schedule type to provide the fields needed for that type.
6. Fill in the required options and click **Save**.

Set up a scan

Discovery scans crawl the local file system or mailboxes for sensitive content.

Before you begin

Verify that the rule sets you want to apply to the scans have been applied to the **DLP Policy**. This information is displayed on the **DLP Policy** → **Rule Sets** tab.

Changes in discovery setting parameters take effect on the next scan. They are not applied to scans already in progress.

Task

1. In McAfee ePO, select **Menu** → **Policy** → **Policy Catalog**.
2. Select **Product** → **Data Loss Prevention <version>**, then select the active DLP Policy.
3. On the **Endpoint Discovery** tab, select **Actions** → **New Endpoint Scan**, then select either **Local Email** or **Local File System**.

   Note

   McAfee DLP Endpoint for Mac only supports local file system scans.

4. Enter a name for the scan, then select a schedule from the drop-down list.
5. (Optional) Change the **Incident Handling** and **Error Handling** defaults. Set the **State** to **Enabled**.
   Error handling determines what to report when text cannot be extracted.
6. (Optional) For local file system scans, select the checkbox in the **User Interaction** field to allow the user to run enabled scans before they are scheduled. You can also enable the user to perform remediation actions from the McAfee DLP Endpoint client console.
7. On the **Folders** tab, do one of the following:
   - For file system scans, select **Actions** → **Select Folders**. Select a defined folder definition or click **New Item** to create one. Define the folder as **Include** or **Exclude**.
   - For email scans, select the file types (OST, PST) and the mailboxes to be scanned.

   Note

   McAfee DLP Endpoint for Mac only supports local file system scans.

8. (Optional) On the **Filters** tab (file system scans only) select **Actions** → **Select Filters**. Select a file information definition or click **New Item** to create one. Define the filter as **Include** or **Exclude**. Click **OK**.
   The default is **All Files**. Defining a filter makes the scan more efficient.
9. On the **Rules** tab, verify the rules that apply.
   All discovery rules from rule sets applied to the policy are run.

Use case: Restore quarantined files or email items

When McAfee DLP Endpoint discovery finds sensitive content, it moves the affected files or email items into a quarantine folder, replacing them with placeholders that notify users that their files or emails have been quarantined. The quarantined files and email items are also encrypted to prevent unauthorized use.

Before you begin

To display the McAfee DLP icon in Microsoft Outlook, the **Show Release from Quarantine Controls in Outlook** option must be enabled in **Policy Catalog** → **Client Policy** → **Operational Mode and Modules**. When disabled, both the icon and the right-click option for viewing quarantined emails are blocked, and you cannot release emails from quarantine.

When you set a file system discovery rule to **Quarantine** and the crawler finds sensitive content, it moves the affected files into a quarantine folder, replacing them with placeholders that notify users that their files have been quarantined. The quarantined files are encrypted to prevent unauthorized use.

For quarantined email items, McAfee DLP Endpoint discovery attaches a prefix to the Outlook **Subject** to indicate to users that their emails have been quarantined. Both the email body and any attachments are quarantined.

Note

The mechanism has been changed from previous McAfee DLP Endpoint versions, which could encrypt either the body or attachments, to prevent signature corruption when working with the email signing system.

Microsoft Outlook calendar items and tasks can also be quarantined.

Important

Quarantined files are deleted after the policy defined number of days (max 30 days storage).

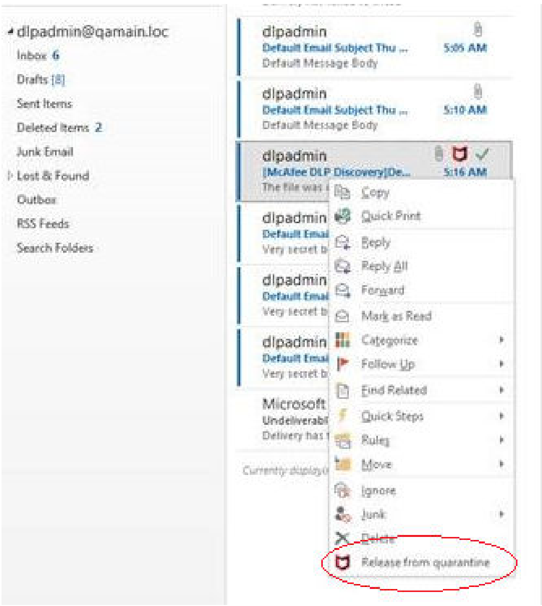
Task

1. To restore quarantined files:
   a. In the system tray of the managed computer, click the **McAfee Agent** icon, and select **Manage Features** → **DLP Endpoint Console**.
      The DLP Endpoint Console opens.
   b. On the **Tasks** tab, select **Open Quarantine Folder**.
      The quarantine folder opens.
   c. Select the files to be restored. Right-click and select **Release from Quarantine**.

      Note

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

      The **Release Code** pop-up window appears.
2. To restore quarantined email items, select **Release from Quarantine**.
   a. In Microsoft Outlook, right-click the email or other item to be restored.
   b. Click the **Release from Quarantine** icon.
      The **Release Code** pop-up window appears.



3. Copy the challenge ID code from the pop-up window and send it to the DLP administrator.
4. The administrator generates a response code and sends it to the user. (This also creates an operational event recording all the details.)
5. The user enters the release code in the **Release Code** pop-up window and clicks **OK**.

   The decrypted files are restored to their original location. If the release code lockout policy has been activated (in the **Agent Configuration** → **Notification Service** tab) and you enter the code incorrectly three times, the pop-up window times out for 30 minutes (default setting).

   Note

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

Scanning data with McAfee DLP Discover

Getting started with network discovery

First steps to using McAfee DLP Discover in a new environment.

1. To collect metadata from the files in your organization's repositories, run an inventory scan. The scan results help you understand which files reside in the repositories.
2. Configure classifications to detect classified or sensitive information. Use these classifications to define and run a classification scan.
3. Use the results of the classification scan to see where sensitive information resides.
4. Configure a remediation scan to encrypt sensitive files or move them to a more secure repository.
5. Continue to run scans regularly, monitoring scan results and any incidents generated. Refine scans based on the results or changes in your organization's policy.
6. Registered documents have a significant RAM impact. Run registration scans only on the most sensitive repositories.

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 needed 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 enforce rules on files.

Note

For database scans, remediation scans can only report an incident and store evidence.

- Registration scans fingerprint the content in sensitive files and store the fingerprints as registered documents on the DLP Server.

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

Required policy components

Scan type	Definitions	Classifications	Rules	Fingerprint criteria
Inventory	X			
Classification	X	X		

Scan type	Definitions	Classifications	Rules	Fingerprint criteria
Remediation	X	X	X	
Registration	X			X

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.

An inventory scan performs the following:

Action	When scanning a file repository	When scanning a database
Collects metadata but does not download any files/tables	x	x
Returns Online Analytical Processing (OLAP) counters and data inventory (list of files/tables scanned)	x	x
Restores the last access time of files scanned	x	

Inventory scans on file repositories 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. Inventory scans on databases collect metadata such as the schema name, table name, number of records, size, and owner.

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

Note

You can also use inventory scans to help automate IT tasks such as:

- Finding empty files
- Finding files that have not been modified for a long time
- Extracting database table formatting

How classification scans work

Use the results of inventory scans to build classification scans.

A classification scan performs the following:

Action	When scanning a file repository	When scanning a database
Collects the same metadata as an inventory scan	x	x
Analyzes the true file type based on the content of the file rather than the extension	x	
Collects data on files/tables that match the configured classification	x	x
Restores the last access time of files scanned	x	

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 extra 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

File repository classification scans detect data with these encryption types:

- Microsoft Rights Management encryption
- Azure RMS 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 as long as McAfee DLP Discover has the credentials configured. Other encrypted files can't 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**.

Classify content with Azure Rights Management encryption criteria

When creating a classification for files that are encrypted with Azure, you can select and assign the Azure Rights Management Encryption criteria to that classification. With this criteria, you can exclude or include scanning of Azure-protected files.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **Classification**.
2. Select the classification to add the criteria to, then select **Actions** → **New Content Classification Criteria** or **New Content Fingerprinting Criteria**.
3. Enter a name for the classification criteria.
4. From the **Available Properties** panel, select **File Encryption**.
5. Select comparison as **is equals to** and value as **Azure Rights Management Encryption**.
6. Click **Save**.

Results

The**Azure Rights Management Encryption**criteria is created and assigned to the selected classification.

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 data matches the classification in a remediation scan, McAfee DLP Discover can perform the following:

Action	When scanning a file repository	When scanning a database
Generate an incident.	x	x
Store the original file/table in the evidence share.	x	x

Action	When scanning a file repository	When scanning a database
Copy the file.	x	
Move the file.	x **Note:** Box and SharePoint scans support moving files only to SMB/CIFS shares.	
Apply RM policy to the file.	x	
Classify file as	x	
Remove automatic classification	x	
Modify anonymous share to login required.	Box scans only **Note:** McAfee DLP Discover cannot prevent Box users from reenabling external sharing on their files.	
Take no action.	x	x

Note

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.

Automatic classification with remediation scans

Remediation scans can classify files by embedding a classification in the file's properties.

You can classify files as part of a remediation action. The classification is embedded into the file's properties. As a result, the classification is not lost when the files are changed, moved between repositories, uploaded to the web, or sent by email.

To classify files with remediation scans, configure the scan using a network discovery rule with a **Classify File As** action. When the repository is scanned, files that meet the conditions configured in the rule are classified according to the selected classification. Also, the classification's **Tag ID** is embedded into the file's properties.

To be classified, files must meet one of the following classification conditions specified in the rule.

- Content classification — keyword, dictionary, advanced pattern, proximity, or document properties
- Classification with registered documents
- File sharing type (Box only)

The classification applied by the rule is selected on the **Reaction** tab, allowing the user to set the **Classify File As** classification to be:

- The same as the classification on the **Condition** tab.
- A different classification from the **Condition** tab classification with criteria.
- A different classification from the **Condition** tab classification without any criteria (for labeling).

Limitations

The following limitations apply to applying classifications with remediation scans:

- A rule can have only one classification configured in the **Classify File As** reaction.
- A file is limited to five embedded classifications. (That is, up to five rules can apply to one file.)
- The user credentials configured in the remediation scan must have read, write, and modify permissions.
- Protected or secured files (when **Modify** isn't allowed) can't be classified.
- Only the following file extensions are supported:

aif	mpeg	tiff
aiff	mpg	vsd
avi	msg	vsdx
dng	pdf	vss
doc	png	vst

docm	pot	wav
docx	potm	wma
dot	potx	wmv
dotm	pps	wps
dotx	ppsm	xdcam
eps	ppsx	xls
jpeg	ppt	xlsb
jpg	pptm	xlsm
mov	pptx	xlsx
mp2	ps	xlt
mp3	psd	xltm
mp4	swf	xltx
mpa	tif	xps

Note

For unsupported file types, the operational event `File type is not supported for auto classification.` is sent.

- The content of the file must match its extension or it can't be classified. For example, a txt file with extension changed to .doc is not classified.
- PostScript files (*.ps and *.eps) must be at least version 3.0. The standard library doesn't support versions earlier than 3.0, so they are not classified.
- MP3 files contain metadata inside a special ID3 tag. This tag usually contains information like track title, artist, and album. For the files to be classified, this tag must exist. MP3 files without such tag are not classified.
- *.mpeg and *.mpg files must be of ISO media file format to be classified. To verify this, open the file with Notepad. After the first 4 bits is some text starting with `ftyp`, for example `ftypmp42`, if the file format is ISO.
- Files with size=0 are not downloaded, so can't be tagged. The operational event `File is not supported.` is sent.

Removing automatic classifications

Note

> Discovery rules with the **Remove Automatic Classification** action are not backward compatible. Rules passed to earlier versions of McAfee DLP Discover use the fallback action **No Action**.

Remediation scans in File Server, SharePoint, or Box repositories can remove automatic classifications and apply them. Creating a rule with a **Remove Automatic Classification** action removes the specified classification tag from a file without affecting other tags that might be applied to the file. The rule can specify only one classification, and can't remove tags applied manually.

How registration scans work

Document registration scans extract signatures from files for use in defining classification criteria.

Registered documents are an extension of location-based content fingerprinting.

Note

> The registered documents created by a registration scan are referred to as automatic registration. They can be viewed on the **Classification** → **Register Documents** page by selecting **Type: Automatic Registration**. They can be used to define McAfee DLP Prevent and McAfee DLP Monitor policies, and for defining McAfee DLP Discover scans. They can't be used in McAfee DLP Endpoint policies.

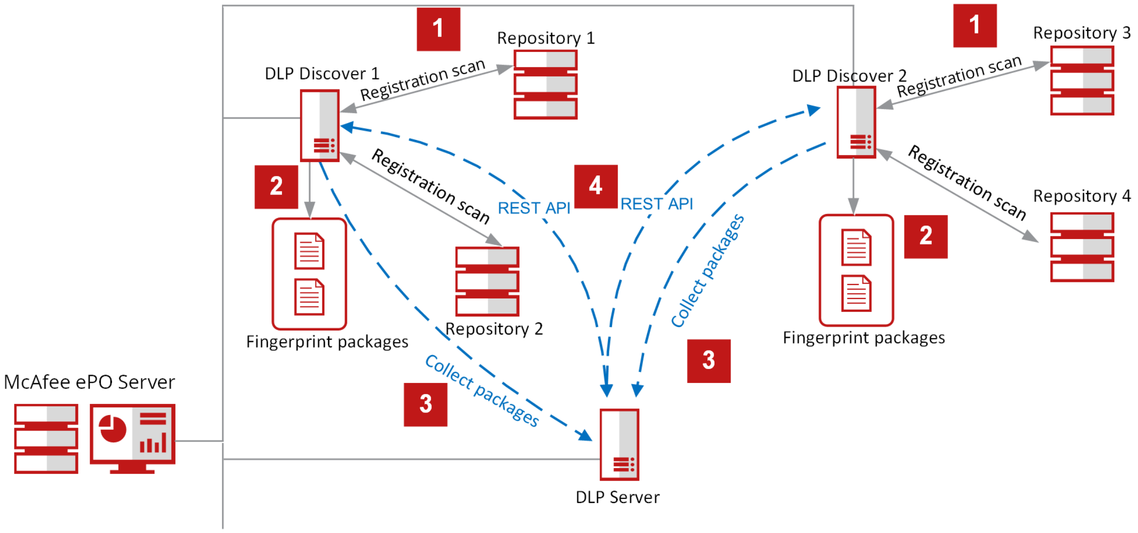
The DLP Server that performs the matching service is specified in the Policy Catalog on the **Registered Documents** page of the Server Configuration.

1. McAfee DLP Discover runs registration scans on repositories.
2. Each scan creates fingerprint signatures that are stored as a package on the network (by default, in the network evidence storage share).
3. At least one DLP Server per LAN (servers running the DLP Server software) collect the fingerprint packages.

   Note

   > All DLP Servers collect all packages. There is no longer a requirement for synchronizing servers, thus reducing network bandwidth.

4. McAfee DLP Discover servers running classification or remediation scans match fingerprints with REST API calls to the DLP Server.



Redistribution follows these rules:

- Fingerprint signature packages are stored on the network (default UNC: network evidence storage share).
- All signatures are added to the DLP Server database.
- Signatures are overwritten when the scan that recorded them runs again.

Limitations

Signatures can have a large RAM impact on the DLP Server. 100 million signatures, the maximum per run, takes about 7 GB of RAM.

- The maximum size of the database is set on the **Classification** page in DLP Settings, and can range from 10 million to 500 million signatures.
- The maximum number of registration scans, enabled and disabled, that can be listed in **Scan Operations** is 100.
- The DLP Server server host listed on the Policy Catalog**Server Configuration** → **Registered Documents** page must be in the same LAN as the McAfee ePO server. McAfee DLP Discover servers can be in another LAN or over WAN.
- User credentials provided for registration scans must have, as a minimum, READ permissions and WRITE attributes, and access to the scanned folders.

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:

- Antivirus software, including McAfee® VirusScan® Enterprise
- McAfee® Host Intrusion Prevention and other McAfee software
- Firewalls

- Access protection software
- On-access scanning

McAfee DLP Discover Items to exclude

Type	Exclude
Processes	• dscrawler.exe • dseng.exe • dssvc.exe • dstex.exe
Directories	• c:\programdata\mcafee\discoverserver • c:\program files\mcafee\discoverserver
Registry keys	• HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\McAfee\DiscoverServer • HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\DiscoverServer • HKEY_LOCAL_MACHINE\SOFTWARE\ODBC.INI\McAfeeDSPostgres

Repository definitions

Configuring repository locations in McAfee ePO has these limitations.

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

Note

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

- IPv6 is not supported.

SharePoint scans

SharePoint scans don't 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 the supported SharePoint versions can be crawled, such as:

- Announcements
- Contacts
- Discussion boards
- Events

- Generic list
- Issue trackers
- Links
- Meetings
- Tasks

Individual items in a list are combined and grouped 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 McAfee DLP Discover servers is not supported.

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

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

Database scans

The following database column types are ignored during all McAfee DLP Discover scans. Text is not extracted, and classifications are not matched.

- All binary types (blob, clob, image, and so forth)
- TimeStamp ×

Note

> In Microsoft SQL, TimeStamp is a row version counter, not a field with a time.

For Oracle databases, all multimedia types are ignored. This includes the following:

ADHEADER_TYP	ORDVIDEO	SI_STILLIMAGE
ORDAUDIO	SI_COLOR	SI_TEXTURE
ORDDOC	SI_COLORHISTOGRAM	TEXTDOC_TAB
ORDIMAGE	SI_FEATURELIST	
ORDIMAGESIGNATURE	SI_POSITIONALCOLOR	

McAfee DLP Discover database scans support special and foreign language characters in DB schemas, tables, and columns. But, if the scan encounters certain sequences of special characters in the names of databases, schemas, or tables, it might fail to read them. The unreadable sequences of special characters vary with database vendor. In this case, McAfee DLP Discover sends the vendor-defined error message and skips to the next object.

Database remediation scans now support reporting incidents per record. The **Report Incident per Record** field is only available when the scan type is set to **Remediation**. Inventory and Classification scans still report by table. The default is **Do not report incidents**. The drop-down list sets the number of incidents to report per DB table from 100–10,000.

If a database server is stopped (shut down) or disconnected during a scan, McAfee DLP Discover reports the run status as **Stopped** on the **Scan Operations** tab. The scan only restarts when the policy is reapplied.

Note

> MySQL doesn't send a notification when the server stops running, so McAfee DLP Discover keeps running, trying to complete the scan.

Restarting Discover service in classification or remediation scans

Restarting the Discover service in the middle of a classification or remediation scan can skip some files. The persistency mechanism that restarts the scan remembers which container was being scanned when the service was stopped, and restarts from the beginning of that container. Sometimes a fetch task might still be running on files from the previous container when the service is stopped. When this occurs, the files are skipped. There is no way for the scan to recover these files.

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. If scan bandwidth is excessive, you can enable bandwidth throttling on the **Scan Operations** → **Scan Details** page.

When bandwidth throttling is enabled, McAfee DLP Discover applies it to individual files being fetched rather than as an average across the entire scan. McAfee DLP Discover fetches files in blocks. The scan software checks the speed after reading each block. If it is above the set speed, the software sleeps to lower the average speed. The throughput can be above or below the configured throttle limit while fetching a block, but files are now fetched in blocks of 16 kilobits to minimize spiking. A scan might burst above or below the configured throttle limit, but the average throughput measured across the entire scan remains very close to the configured limit. When enabled, the default throttling value is 2000 Kbps.

Repositories and credentials for scans

McAfee DLP Discover supports Box, File Server, SharePoint, and Database repositories.

File Server and SharePoint repositories

File Server repositories can be either SMB/CIFS or NFS. When defining a File Server repository, the UNC path can be the fully qualified domain name (FQDN) (\\myserver1.mydomain.com) or the local computer name (\\myserver1). You can add both conventions to a single definition.

In the Linux environment, NFS path descriptions are case sensitive. You are allowed, for example, to have path \\server\share\folder and path \\server\share\FOLDER. DLP File Server repository definitions validate the paths you enter to prevent path repetition, so the example given is not valid for a single File Server repository definition. If you want to scan both paths, one solution is to enter the parent path (\\server\share) and scan all subfolders. Another solution is to define each path in a separate definition and add both repository definitions to the discovery rule.

File Server repositories support read-only permissions. If you scan a File Server repository when the user has read-only permissions, the last access time is changed. To preserve the file's last access time, select the option to skip files for which the user doesn't have write permissions. This can be done when you create the File Server repository definition. By default, classification and remediation scans fail to read the file if the user has only read-only permissions. To support classification and remediation scans with read-only permissions, change the default setting in **DLP Discover** → **Definitions** → **Repositories** → **File Server** → **Credentials** to **Always inspect file content**.

When defining a SharePoint repository, the host name is the server URL unless Alternate Access Mapping (AAM) is configured on the server. For information about AAM, see the SharePoint documentation from Microsoft.

A credential definition is specific to a File Server or SharePoint repository definition. In the credentials definition, if the user is a domain user, use the FQDN for the **Domain name** field. If the user is a workgroup user, use the local computer name. If the repository definition contains only one UNC version, for example FQDN, you must use that version in the credential definition.

For AD domain repositories, use the **Test Credential** option to verify the user name and password. Using incorrect credentials creates an event indicating the reason for the scan failure. View the event in the **Operational Event List** page for details.

Box repositories

When defining a Box repository, obtain the client ID and client secret from the Box website. Use the Box website to configure the McAfee DLP Discover application, the manage enterprise and as-user functionality. If you are not using an administrator account, contact Box support for more information about configuring this functionality.

Databases

When defining a database, you can identify the database server by host name or IP address. You also specify the port and database name. You can specify a particular SSL certificate, any SSL certificate, or no certificate. SSL certificates specified in database definitions are defined in **DLP Policy Manager** → **Definitions**.

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.

Definitions available by feature

Definition	Used for
Advanced Pattern*	Classifications
Dictionary*	
Document Properties	
True File Type*	
File Extension*	Classifications and scans
File Information	
Credentials	Scans
Scheduler	
SSL Certificate	
Box	
File Server	
Database	
SharePoint	

Note

* Indicates that predefined (built-in) definitions are available.

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.

Note

Classification and remediation scans can detect manually classified files, but McAfee DLP Discover cannot apply manual classifications to files.

McAfee DLP Discover can detect and identify manual or automatic classifications on files set by McAfee DLP Endpoint. You can view automatic classifications in the incident details or the **Data Inventory** tab.

McAfee DLP Discover does not use manually registered documents. It uses registered documents created by McAfee DLP Discover registration scans (automatically registered documents) stored on DLP Server database servers.

Using rules with scans

Remediation scans use rules to detect and act 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 applies the **Action** specified in the rule.

Actions available for remediation scans

Action	File System	SharePoint	Box	Database
Take no action	X	X	X	X
Create an incident	X	X	X	X
Store the original file as evidence	X	X	X	X
Copy the file	X [1]	X [1]	X [1]	
Move the file	X [1]	X[1] [2]	X [1]	
Apply an RM policy to the file	X	X [2]	X	
Classify File As	X	X	X	
Remove automatic classification	X	X	X	
Remove anonymous sharing for the file			X	

[1] Copying and moving files supported only to SMB/CIFS shares.

[2] Not supported for SharePoint lists; supported only for files attached to SharePoint lists or stored in document libraries, and to SMB/CIFS only. Some file types used for building SharePoint pages, such as .aspx or .js, cannot be moved or deleted.

Configure policy for scans

Create definitions for scans

Create scan definitions

All scans require definitions to specify the repository, credentials, and schedule. Scan definitions can be created on the **DLP Discover** page or in the DLP Policy Manager.

Before you begin

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

Task

1. In McAfee ePO select one of the following:
    - **Menu** → **Data Protection** → **DLP Discover**
    - **Menu** → **Data Protection** → **DLP Policy Manager**
2. Click the **Definitions** tab.
3. Create a credentials definition.

    Note

    > For remediation scans, the credentials must have read and write permissions. For remediation scans that apply RM policy or move files, full control permissions are needed.

    a. In the left pane, select **Other** → **Credentials**.
    b. Select **Actions** → **New Item** and replace the default name with a unique name for the definition.
    c. Fill in the credentials parameters. Click **Save**.
4. Create a repository definition.
    a. In the left pane, under **Repositories**, select the type of new repository you want to create.
    b. Select **Actions** → **New Item**, type a unique repository name in the **Name** field, and fill in the rest of the **Type** and **Definitions** information.

    Note

    > **Exclude** parameters are optional. At least one **Include** definition is needed.

5. Create a scheduler definition.
   a. In the left pane, select **Other** → **Scheduler**.
   b. Select **Actions** → **New Item** and fill in the scheduler parameters. Click **Save**.

   Note

   Parameter options depend on which **Schedule type** you select.

6. Create a file information definition.

   Note

   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.

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

Create a credentials definition

Credentials are needed 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

1. In McAfee ePO, select one of the following:
   - **Menu** → **Data Protection** → **DLP Discover**
   - **Menu** → **Data Protection** → **DLP Policy Manager**
2. Click the **Definitions** tab.
3. In the left pane, select **Other** → **Credentials**.
4. Select **Actions** → **New Item**.
5. 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.

   Note

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

6. 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.

   Note

   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 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**

Task

1. In McAfee ePO, select one of the following:
   - **Menu** → **Data Protection** → **DLP Discover**
   - **Menu** → **Data Protection** → **DLP Policy Manager**
2. Click the **Definitions** tab.
3. In the left pane, click **Scheduler**.
4. Select **Actions** → **New Item**.
5. Enter a unique name and select the schedule type.

   Note

   The display changes when you select the schedule type to provide the necessary fields for that type.

6. Fill in the required options and click **Save**.

User permissions needed for scans

SharePoint and databases such as Oracle and SQL require specific permissions to run Discover scans.

User type	Permissions needed	Commands	Description
SQL user	`dbo` permission set		
Oracle user (sysdb)	CREATE VIEW	`GRANT CREATE VIEW TO "username";`	Permissions to define a view.
	SELECT ANY TABLE	`GRANT SELECT ANY TABLE TO "username";`	Permissions to query tables or views
	CONNECT	`GRANT CONNECT TO "username";`	Permissions to open a database session.
	SELECT_CATALOG_ROLE	`GRANT SELECT_CATALOG_ROLE TO "username";`	Privileges on all data dictionary views.
	READ	`GRANT READ ON DIRECTORY EXT_TAB_DATA TO "username";`	Read-only permissions to external tables.
	WRITE	`GRANT WRITE ON DIRECTORY EXT_TAB_DATA TO "username";`	Write permissions to work with external tables.
	EXECUTE ANY TYPE	`GRANT EXECUTE ANY TYPE TO "username";`	Permissions to execute any type of object used. This is mandatory for nested tables.
SharePoint user	• For inventory and classification scans: Read-only permissions • For remediation scans: Full permissions		

Create a File Server or SharePoint repository definition

Configure a File Server 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 is skipped entirely from the scan.

Task

1. In McAfee ePO, select one of the following:
   - **Menu → Data Protection → DLP Discover**
   - **Menu → Data Protection → DLP Policy Manager**
2. Click the **Definitions** tab.
3. In the left pane, under **Repositories**, select the type of repository.
4. Select **Actions → New Item**.
5. Enter a name, select the credentials to use, and configure at least one **Include** definition.
6. (File Server 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.

   Note

   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.

   Note

   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).

Note

> You can look up the default view URL in the list or library settings page. If you do not have permission 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

1. In McAfee ePO, select one of the following:
   - **Menu** → **Data Protection** → **DLP Discover**
   - **Menu** → **Data Protection** → **DLP Policy Manager**
2. Click the **Definitions** tab.
3. In the left pane, under **Repositories**, select **Box**.
4. Select **Actions** → **New Item**.
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 exact address of the McAfee ePO server.

   Note

   > In other words, if you access McAfee ePO using the host name, you must use the host name for the redirect URI; you can't use an IP address. Any mismatch in addresses leads to a Box redirect URI error.

   - 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**.

Create a database repository definition

Configure a database repository for scanning.

Before you begin

Prepare the database IP server/host name to type or copy and paste in the definition. This field is required.

Task

1. In McAfee ePO, select one of the following:
   - **Menu** → **Data Protection** → **DLP Discover**
   - **Menu** → **Data Protection** → **DLP Policy Manager**
2. Click the **Definitions** tab.
3. In the left pane, select **Repositories** → **Database**, then select **Actions** → **New Item**.
4. Enter an optional description, and select the type of database from the drop-down list.
5. Enter the connection details.
6. Select or create a credentials definition and test the connection.
7. Specify the SSL connection type and click **Save**.
8. For Oracle databases, create an Oracle user.

Create an Oracle user

For McAfee DLP Discover to scan Oracle databases, create a user with the required permissions.

Task

1. Run SQL*Plus.
2. Logon as a database administrator.

   Example: username/password@SID as sysdba
3. Create a user using the following commands:

```
CREATE USER "username"  PROFILE "DEFAULT"
IDENTIFIED BY password DEFAULT TABLESPACE "USERS"
TEMPORARY TABLESPACE "TEMP"
QUOTA UNLIMITED
ON "USERS"
ACCOUNT UNLOCK;
```

4. Run each of the following commands in SQL*Plus to grant the required permissions:

```
GRANT CREATE VIEW TO "username";
```

```
GRANT SELECT ANY TABLE TO "username";
```

```
GRANT CONNECT TO "username";
GRANT SELECT_CATALOG_ROLE TO "username";
```

```
GRANT READ ON DIRECTORY EXT_TAB_DATA TO "username";
(mandatory to work with external tables)
```

```
GRANT WRITE ON DIRECTORY EXT_TAB_DATA TO "username";
(mandatory for logging enabled case on external tables)
```

```
GRANT EXECUTE ANY TYPE TO "username";
```

(mandatory to cover nested tables case)

⚠ **Caution**

EXT_TAB_DATA is the most commonly used tag for external tables storage, but can depend on the client database structure. Each client DBA must carefully consider granting READ/WRITE permission on DIRECTORY with external tables.

Results

The user created has the required permissions to allow McAfee DLP Discover to scan the Oracle database schemas.

Create a SQL user

To scan Databases, we recommend using the DBO permission set.

Before you begin

You must have SQL administrator permissions to create a SQL user.

Task

1. Open SQL Server Management Studio (SSMS) and connect to SQL Server.
2. Expand **Security** → **Logins** in the left panel.
3. Right-click **Logins** and select **New Login** from the drop-down list.
4. Add the user, specifying **SQL Server authentication**.

Export or import repository definitions

If you have many 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 using the **ID** value in the XML file.

Task

1. In McAfee ePO, select one of the following:
   - **Menu** → **Data Protection** → **DLP Discover**
   - **Menu** → **Data Protection** → **DLP Policy Manager**
2. Click the **Definitions** tab.
3. Select **File Server** or **SharePoint**.
4. Perform one of these tasks.
   - To export repositories:
      • Select **Actions** → **Export**.
      •

        Select whether to open or save the file and click **OK**.
   - To import repositories:
      • Select **Actions** → **Import**.
      • Browse to the file and click **OK**.

Create rules for remediation scans

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

Task

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. Enter the name and optional note, then click **OK**.
4. 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

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

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Discover**.
2. On the **Discover Servers** tab, select **Actions** → **Detect Servers** to refresh the list.

   Note

   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.

   Note

   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.

      Tip

      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

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Discover**.
2. On the **Discover Servers** tab, select **Actions** → **Detect Servers** to refresh the list.

   Note

   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.

   Note

   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.

      Note

      You can create repository and credentials definitions if needed 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**.

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

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Discover**.
2. On the **Discover Servers** tab, select **Actions** → **Detect Servers** to refresh the 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.

    Note

    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.

    Note

    You can create repository and credentials definitions from the selection window, if needed.

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 rules for the scan.
    a. On the **Rules** tab, click **Actions** → **Select Rule Sets**.

    b. Select one or more rule sets from the list.

9. Click **Save**.
10. Click **Apply policy**.

Configure a registration scan

Registration scans extract signatures from files.

Before you begin

- Discover servers must be predefined. Deploy the McAfee DLP Discover software to network servers, and verify the installation.
- Create one or more classifications with fingerprint criteria based on the repository to be scanned.

Task

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, define a filter to display a shorter list.
3. On the **Scan Operations** tab, select **Actions** → **New Scan** and select the repository type.
   You can run registration scans on Box, File Server, or SharePoint repositories only.
4. Type a unique name and select **Scan Type: Documents Registration**. Select a server platform and a schedule.

   Note

   > You can select a defined schedule or create one.

5. (Optional) Set values for **Throttling**, **Files List**, **Signatures**, 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.

   Note

   > You can create repository and credentials definitions if needed 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 criteria for the scan.
   a. On the **Fingerprint Criteria** tab, click **Actions** → **Select Classifications**.
   b. Select classifications from the list, then click **OK**.

9. Click **Save**.
10. Click **Apply policy**.

DLP Discover

Discover Servers page

Use this page to detect Discover servers and to view information on servers in the network.

The **Discover Servers** page displays information on Discover servers in the network. You can filter the display by selecting limiting values for one or more parameters with the filter **Edit** control. You can reuse unsaved filters throughout the work session, or **Save** the filter for future use as either a public or private filter.

Filter definitions

Option	Definition
Filter	Drop-down list of saved filters. If no filter has been defined, it displays **no custom filter**. If a filter has been defined but not saved, it displays **unsaved**.
Edit	Opens the McAfee ePO **Edit Filter Criteria** page. Select from the available properties list, and click **Update Filter**.
Delete	Deletes the currently displayed filter.
Save	Saves an **unsaved** filter. If you have changed a filter definition, you can select **Override existing filter** to save the changes.

Actions definitions

Option	Definition
Detect Servers	Updates the server list. You can also perform this task with **Detect Discovery Servers** from McAfee ePO: **Menu** → **Automation** → **Server Tasks**.
Remove	Deletes the selected server from the list.
Set system name	Sets the optional **System Name** of the selected computer.

Discovery definitions

Definitions page (McAfee DLP Discover)

Use this page to create definitions for McAfee DLP Discover scan operations.

Option definitions

Option	Definition
Show built-in definitions	When selected, displays the predefined definitions.
Actions	**New** Creates a definition of the type selected in the left pane. For File Server and SharePoint only: • **Export** Exports repositories and credentials to an XML file. • **Import** Imports repositories and credentials from an XML file.
Edit	Opens the definition for editing. This option applies to user-defined definitions only.
Delete	Deletes the definition. This option applies to user-defined definitions only. Definitions currently in use cannot be deleted. To delete a definition, first remove it from all rules.
Duplicate	Duplicates the definition.
Usage	Displays all places where the definition is used.
View	Opens the definition for viewing. This option applies to built-in definitions only.

Credentials definition page

Use this page to define user credentials.

Option definitions

Option	Definition
Name	Replace the default name with a unique name for this definition. This field is required.
Description	Use this field for information to describe the definition or indicate when it is used. This field is optional.
Domain name	This field is required for all repository types except Database. Leave this field blank when creating a database credential definition.
User name	All of these fields are required.
Password	
Confirm password	
Test Credential	Tests the definition by attempting to reach the AD server. This option becomes available when you have filled in all required fields. You must have DNS resolution for the target domain. **Note:** This action is not available for database credential definitions. Database credentials are tested in database repository definition.

Scheduler page

The **Scheduler** stores schedules for running McAfee DLP Discover and endpoint discovery scans.

The options available depend on the **Schedule type** selected. Table 1 shows the options that apply to all schedule types.

Table 1

Option	Description
Name	Replace the default name **Scheduler** with a unique name. This field is required.

Option	Description
Suspend time	Scans can be suspended to prevent them from interfering with work schedules. You can set a different suspension time for each day of the week.

Table 2 describes the additional options for all schedule types other than **Run immediately**.

Table 2

Option	Description
Time Zone	Start and stop times can be according to the local time on the server platform or UTC, that is, simultaneously across the entire enterprise.
Start Time	Sets the start of the scan.
Effective period	Sets the start date for scans run once; sets start and end dates for all other schedule types.

Table 3 describes the **Schedule type** options for different types

Table 3

Schedule type	Description
Run immediately and **Once**	No options, other than setting the schedule type.
Options	Runs a task that has been missed. Not available for **Run immediately**.
Daily	You can set a frequency for scans of 1–30 days. The scan repeats every *x* days within the specified period.
Weekly	You can set a frequency for scans of 1–52 weeks. You can also select the day of the week the scan runs.
Monthly	You can set either the numerical day of the month for the scan or a specific day of the month (first Sunday, third Tuesday). You can also skip specific months by selecting the monthly checkboxes.

SSL Certificate definition page

Use this page to define an SSL certificate definition.

Option definitions

Option	Definition
Name	Replace the default name with a unique name for this definition. This field is required.
Description	Use this field for information to describe the definition or indicate when it is used. This field is optional.
Certificate File	Click **Load File** to browse for certificate files.

Scan Operations page

Use this page to configure a scan, or to view existing configured scans.

This page displays information on configured scans, such as the scan names, the number of files scanned, and the time that scans were run. The display is user-configurable as to which parameters are displayed, and the order in which they are displayed by selecting **Actions** → **Choose Columns**. You can filter the display by selecting limiting values for one or more parameters with the filter **Edit** control. You can reuse unsaved filters throughout the work session, or **Save** the filter for future use as either a public or private filter.

Click **Apply Policy** to apply the settings to the McAfee DLP Discover servers.

Filter definitions

Option	Definition
View	Drop-down list of saved views. If no view has been defined, it displays **Default**. If a view has been defined but not saved, it displays **unsaved**. Duplicates the **Actions** → **Choose Columns** command, but allows you to save multiple views.
Filter	Drop-down list of saved filters. If no filter has been defined, it displays **no custom filter**. If a filter has been defined but not saved, it displays **unsaved**.
Edit (filter)	Opens the McAfee ePO **Edit Filter Criteria** page. Select from the available properties list, and click **Update Filter**.

Option	Definition
Edit (view)	See **Actions** → **Choose Columns**.
Delete	Deletes the currently displayed filter.
Save	Saves an **unsaved** filter. If you have changed a filter definition, you can select **Override existing filter** to save the changes.

Action definitions

Option	Definition
Choose Columns	This standard McAfee ePO option allows you to customize the **Scan Operations** page display.
Clone Scan	Opens the **Edit Scan** page with the information of the selected scan. Edit as required. Change the name to save the cloned scan.
Delete Scan	Removes the selected scan from the list.
Edit Scan	Opens the selected scan configuration for editing.
Synchronize Data	Updates the table with the current McAfee Agent properties.
New Scan	Creates a scan configuration.
Change State	Use this option to enable or disable configured scans.

Scan operations - New scan page

Use this page to configure a scan.

All discovery scans are configured in a similar manner. The scan options are selected in the upper **Scan Details** pane. The lower pane has multiple tabs for new scans.

We recommend creating schedule, repository, filter, and rule set definitions before configuring scans. If repositories require credentials for access, create the necessary credentials definitions as well.

Option definitions

Option	Definition
Name	Enter a unique name for the scan. This field is required.
Scan Type	Select an option from the drop-down list.
Discovery Server	Select an entry from the selection window. This field is required. **Note:** Only one server can be selected per scan.
Scheduler	Select an entry from the selection window. This field is required.
Throttling	Limits the bandwidth of the scan. When the checkbox is selected, you can change the default value.
Files List (All scan types except Database)	Select this option if you want to display **Data Inventory** information. If you deselect this option, you can view the counters on the **Data Analytics** page, but cannot expand them to display the detailed information. For large repositories, we recommend using this option with filters to limit the impact on the McAfee ePO database.
Tables Information (Database scans only)	Checkbox to store the database table information in Data Inventory.
Incident Handling (Remediation scans only)	Use the drop-down list to set the maximum number of incidents to report per scan. Select the checkbox to close the scan if a threshold is exceeded. **Range:** 100-100,000 **Note:** For Inventory and Classification scans, the field is displayed but can't be edited.
Report Incident per Record (Database scans only)	Drop-down list to report the maximum number of incidents per DB table. The default is **Do not report incidents**. You can only edit the drop-down list for remediation scans - inventory and classification scans report by table.

Option	Definition
Signatures (Registration scans only)	Use the drop-down list to set the maximum number of signatures to report per scan. **Range:** 100.000-100,000,000 **Note:** The approximate RAM required is displayed for the selected value.
Error Handling	Use the drop-down list to set the maximum errors to report per scan. Select the checkbox to close the scan if a threshold is exceeded. **Range:** 100-100,000

Tab options

Tabs

Tab	Scan type	Definition
Repositories	All scan types	Displays the selected Repository definitions.
Filters	Database scans `(classification and remediation scans only)`	Limits the number of records to scan per table.
	All other scan types	Displays the selected File Information definitions (dates, file extension, name, owner, and size) that are used to define the files included or excluded.
History	All scans that have run. Does not appear when creating a **New Scan** definition.	Displays the scan history information.
Classifications	Classification scans only	Displays the selected Classification definitions applied to the scan.
Rules	Remediation scans only	Displays the selected Rule Sets applied to the scan.

Tab	Scan type	Definition
Fingerprint Criteria	Registration scans only	Displays the fingerprint criteria and the network share and type (dictionary, keyword, and so forth) for each.

Actions definitions

Option	Definition
Select Classifications	Appears only for Scan Type: Classification. Opens the **Choose from existing values** window for selecting **Classification** definitions.
Select Filters	Opens the **Choose from existing values** window for selecting **File Information** definitions. **Note:** This option affects the crawler scan, not just the display. Use this option to improve scan efficiency when you don't want to scan the entire repository.
Select Repositories	Opens the **Choose from existing values** window for selecting **Repository** definitions. **Note:** Only repository definitions matching the scan type are displayed.
Select Rule Sets	Appears only for **Scan Type: Remediation**. Opens the **Choose from existing values** window for selecting **Rule Set** definitions.

Select Server page

Use this page to select the Discover server for a scan.

Option definitions

Option	Definition
Server list	Select the Discover server for the scan.
OK	Retains your changes and closes the window.
Cancel	Discards your changes and closes the window.

Box repository page

Use this page to define a Box repository.

Option definitions

Option	Definition
Name	Replace the default category name with a unique name for this category. This field is required.
Description	Optional text box for additional information.
Type	This field is filled in automatically. Verify that you have selected the correct type of repository for your requirements.
Host Name	Displays the host name of the repository. This field is blank if the token has not been retrieved.
Credentials	• *Box website link* — You can use this link to define the Discover server application and to get the client ID and secret. • **Client ID** — Specifies the client ID. • **Client Secret** — Specifies the client secret. • **Get Token** — Opens a page to Box to retrieve the token. **Note:** The Discover server automatically refreshes the token during the next scan. If the token expires, you must use **Get Token** to retrieve a new one.

Option	Definition
Accounts	Specifies whether to scan all user accounts or specific user accounts.
Save	Saves your changes.
Cancel	Discards your changes.

File Server repository page

Use this page to create a SMB/CIFS or NFS repository definition.

Repository definitions can contain both included and excluded repositories.

Option definitions

Option		Definition
Name		Replace the default category name with a unique name for this category. This field is required.
Type		Drop-down list to select CIFS or NFS repository. Default: **SMB/CIFS**
Credentials		Select an entry from the drop-down list, or click **New** to create a definition.
	File Access Permissions	Select **Inspect file content only if user has write attributes permission** if you need to restore last access time. If restoring last access time is not important, select **Always inspect file content**.
Advanced Options	**Administrative shares**	When selected, administrative shares on the file server are scanned.
	Reparse Points	When selected, NTFS reparse points are scanned.
Include	**Prefix Type**	The acceptable types are UNC or IP address range.
	Prefix	Text box for entering the path.

Option		Definition
	Regular expression	Text box for defining a path that fits a pattern.
	Add	Click to add the definition to the **Include** list.
Exclude	**Type**	Choose from **Path starts with** or **Path regular expression**.
	Definitions	Text box for entering the path type description (partial path or regular expression).
	Add	Click to add the definition to the **Exclude** list.

Database repository definition page

Use this page to define a database repository

Option definitions

Option	Definition
Name	Replace the default name with a unique name for this repository. This field is required.
Description	Optional text box for additional information.
Type	The type **Database** is filled in automatically. Select the type of database from the drop-down list.
Connection Details	The **Port** definition is added automatically, but can be edited. All three fields are required.
Credentials	Select a credential definition from the drop-down list.
SSL certificate	Select or create a certificate, or specify any certificate or none.
Filter	Use **Actions** → **Add Filter** to create a new filter. Filters can define included or excluded databases, schemas, or tables.

SharePoint repository page

Use this page to define a SharePoint repository.

Repository definitions can contain both included and excluded repositories. You can use the **Exclude** section to exclude specific directories of the SharePoint defined in the **Include** section, as well as excluding other shares.

Option definitions

Option	Definition
Name	Replace the default category name with a unique name for this category. This field is required.
Type	This field is filled in automatically. Verify that you have selected the correct type of repository for your requirements.
Credentials	Select an entry from the drop-down list, or click **New** to create a new definition.
Include	Do one of the following: • Select **SharePoint server** and type the URL in the text box • Select **Sites list** and enter the URLs one at a time using the text box. The section allows for specifying multiple URLs.
Exclude	Enter a site or sub-site URL in the text box.
Add	Add the definition to the list.

Choose from existing values page (Scan scheduler)

Use this page to select a scheduler definition for a scan.

Option definitions

Option	Definition
Filter items	Specifies a string filter. For example, entering `Discovery` displays only the items containing Discovery in the title.

Option	Definition
GO	Activates the definition in the **Filter items** field.
Name list	Displays schedulers based on the current filter.
Edit	Edits the selected scheduler definition.
New Item	Creates a scheduler definition.
OK	Retains your changes and closes the window.
Cancel	Discards your changes and closes the window.

Choose from existing values page (Scan repositories)

Use this page to select repositories for a scan.

Option definitions

Option	Definition
Filter items	Specifies a string filter. For example, entering `Discovery` displays only the items containing Discovery in the title.
GO	Activates the definition in the **Filter items** field.
Show selected items only	When selected, limits the display to selected items.
Repositories list	Displays repositories based on the current filter.
Credentials	Specifies the credentials for the repository.
Edit	Edits the selected repository definition.
New Credentials	Creates a credentials definition.

Option	Definition
New Repository	Creates a repository definition.
OK	Retains your changes and closes the window.
Cancel	Discards your changes and closes the window.

Choose from existing values page (Scan filters)

Use this page to select filters for a scan.

Filters apply **File Information** definitions to limit the scan by properties such as file size, date, or extension.

Option definitions

Option	Definition
Filter items	Specifies a string filter. For example, entering `Discovery` displays only the items containing Discovery in the title.
GO	Activates the definition in the **Filter items** field.
Show selected items only	When selected, limits the display to selected items.
Filters list	Displays classifications based on the current filter.
Include/Exclude	Specifies if the selected definition is used to include or exclude files for a scan.
Edit	Edits the selected definition.
New Item	Opens the **File Information** definition page to create a filter.
OK	Retains your changes and closes the window.
Cancel	Discards your changes and closes the window.

Choose classifications page

Use this page to select the classifications to use in a classification scan.

Option definitions

Option	Definition
Filter items	Specifies a string filter. For example, entering `Discovery` displays only the items containing Discovery in the title.
GO	Activates the definition in the **Filter items** field.
Show selected items only	When selected, limits the display to selected items.
Name list	Displays classifications based on the current filter.
New Classification	Enter a name for a new classification.
Add	Adds a classification using the specified name.
OK	Retains your changes and closes the window.
Cancel	Discards your changes and closes the window.

Choose from existing values page (Scan rule sets)

Use this page to select the rule sets to use in a remediation scan.

Option definitions

Option	Definition
Filter items	Specifies a string filter. For example, entering `Discovery` displays only the items containing Discovery in the title.
GO	Activates the definition in the **Filter items** field.

Option	Definition
Show selected items only	When selected, limits the display to selected items.
Rule Set list	Displays rule sets based on the current filter.
Rules list	Displays the number of McAfee DLP Discover rules in the rule set.
OK	Retains your changes and closes the window.
Cancel	Discards your changes and closes the window.

Perform scan operations

Manage and view information about configured scans.

Note

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

Task

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.

   Note

   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**.

    Note

    > 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**.

Analyzing scanned data

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 Inventory** tab in the **DLP Discover** module displays scan results from inventory, classification, and remediation scans.

Note

> Results are displayed for the last time the scan was run.

Results from registration scans can be viewed in the **Classification** module on the **Register Documents** tab when you select **Type: Automatic Registration**.

The tab has three analytic views: dashboard, grid, and raw data.

Dashboard view

The **Dashboard** analytic view displays results as pre-set graphs. Data is displayed for the scan selected in the **Scan Name** drop-down list. The display depends on the **Analytic Type** selected: files or classifications.

For files, the graphs are:

- Top repositories
- Top containers
- Top hosts
- File sizes
- Last modified time
- Top file extensions
- Top file extension groups
- Last access time

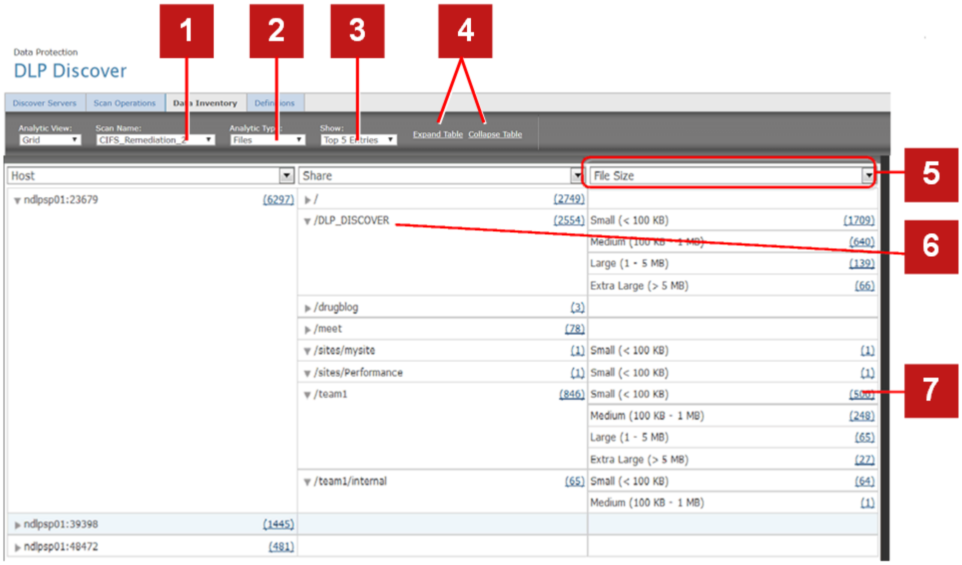
For classifications, the graphs are:

- Top repositories
- Top containers
- Top hosts
- Top classifications
- Top true file types
- Last access time

Grid view

The **Grid** analytic view 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.

Configuring data analytics



Analytic View: Grid
Scan Name: CIFS_Remediation_2
Analytic Type: Files
Show: Top 5 Entries

Host		Share		File Size	
ndlpsp01:23679	(6297)	/	(2749)		
		/DLP_DISCOVER	(2554)	Small (< 100 KB)	(1709)
				Medium (100 KB - 1 MB)	(640)
				Large (1 - 5 MB)	(139)
				Extra Large (> 5 MB)	(66)
		/drugblog	(3)		
		/meet	(78)		
		/sites/mysite	(1)	Small (< 100 KB)	(1)
		/sites/Performance	(1)	Small (< 100 KB)	(1)
		/team1	(846)	Small (< 100 KB)	(506)
				Medium (100 KB - 1 MB)	(248)
				Large (1 - 5 MB)	(65)
				Extra Large (> 5 MB)	(27)
		/team1/internal	(65)	Small (< 100 KB)	(64)
				Medium (100 KB - 1 MB)	(1)
ndlpsp01:39398	(1445)				
ndlpsp01:48472	(481)				

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 screen 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.

   Note

   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.

Raw Data view

The **Raw Data** analytic view displays the inventory of files from scans with the **File List** option enabled. You can define and use filters to adjust the information displayed, which might reveal patterns or potential policy violations.

Note

Classification, **File type**, and **Encryption 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

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Discover**.
2. Click the **Data Inventory** 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 Raw Data** 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.

   Note

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

View inventory results

View the inventory of files from all scan types.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Discover**.
2. Click the **Data Inventory** tab.
3. Select the **Raw Data** analytic view.
4. Perform any of these actions.
    - 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.

    Note

    Click **Edit** to modify and create filters.

    - To group files based on a certain property:
        - From the **Group By** drop-down list, select a category.

          The available properties appear in the left pane.
        - Select the property to group files.
    - To configure the displayed columns:
        - Select **Actions** → **Choose Columns**.
        - From the **Available Columns** list, click an option to move it to the **Selected Columns** area.
        - 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.
        - Click **Update View**.

The DLP Capture Search feature

Searching captured data

When enabled, the DLP Capture feature allows you to store email, web, and network data analyzed by your McAfee DLP Prevent or McAfee DLP Monitor appliances. The captured data can be searched later to identify a data loss event that was missed during real-time data analysis, or used to tune rules and classification settings to reduce false positives without affecting the analysis of live data.

You can create *datasets* that focus the search on specified properties to reduce the amount of data that will be searched on each appliance, so you get fewer and more targeted results.

You can create a McAfee DLP incident from a search result, then add the incident to a new or existing case. Any evidence associated with the search result can also be added to the incident.

Data and evidence storage

The captured data is stored on a disk on a physical or virtual appliance, or on an external storage device. The *data* is stored on a disk that is encrypted using a randomly generated encryption key. To recover the encrypted data, you can unlock it using the admin password. If you change the admin password, the unlock key is also updated. If you are upgrading from a previous version, the unlock key is a default value. You will see an alert in the **Appliance Management** dashboard until you change the password. To secure the encrypted data, change the admin password using the appliance console.

A captured event is stored on the appliance with its evidence. When a result is created, the associated evidence is copied to the evidence storage share.

Data retention

By default, captured data is removed automatically from storage after 28 days to avoid filling up the disk space but you can change that limit if you want to. If the captured data storage nears capacity before the specified limit is reached, some of the older captured items are automatically removed to provide enough space for new content to be captured.

When the DLP Capture feature starts a search task, it collates the items that will be analyzed in the search. If some of those items are older items that must be removed while a search is in progress to free up storage space, the removed items are not analyzed but the search continues.

Users and permissions

The ability to tune rules or search captured data is not automatically available to all McAfee DLP users. Specify who can use the feature in the **Data Loss Prevention** permission set. Unlike previous versions of McAfee DLP that could capture content, this version allows several people to set up and run searches at the same time.

Working with the DLP Capture feature

Follow these high-level steps to set up and work with the DLP Capture feature.

Task

1. Specify who can use the feature.
2. Build data sets to focus your searches.
3. Create and run the searches or tune rules and classifications.
4. Review search results.
5. Create incidents and add to cases.

Enabling the DLP Capture feature

Use the options in **McAfee DLP Capture Settings** to capture data from the McAfee DLP appliances and specify how long you want to retain that data for.

Before you begin

For the DLP Capture feature to appear in the McAfee ePO menu, you must add a license for one of the McAfee DLP appliances.

Task

1. In McAfee ePO, open the **Policy Catalog**.
2. Select the **DLP Appliance Management** product, select the **McAfee DLP Capture Settings** category, and open the policy that you want to edit.
3. In **Capture Settings**, select **Enable Capture**.
4. (Optional) Specify how long you want to keep captured items for.
   By default, captured items are removed after 28 days.
5. Click **Save**.
6. (Optional) Check whether the DLP Capture feature is enabled on a specific appliance.
   a. Open the **System Tree** and select the **Systems** panel.
   b. Click **Products** and select **DLP Capture**.
   c. Scroll down to **General**, and check the value for captureFeatureStatus:
      - 1: feature is enabled
      - 2: feature is disabled
      - 3: feature is not supported on this particular platform

      3 is normally shown when the McAfee DLP Capture Storage Array needs to be attached and the appliance re-imaged.

Datasets

Datasets focus your rule tuning and forensic investigation searches on a subset of captured data to reduce the amount of data searched. When you search a data set, the time it takes to run the search is reduced, and the results are more useful and easier to analyze. There are some pre-defined datasets, or you can create your own based on properties such as the appliance, email criteria, or user criteria.

If an appliance can support the DLP Capture feature (that is, it has disks available for storing captured data and it contains some captured data), it can be added to a dataset and the captured data searched.

Note

If you create a dataset and do not specify a specific appliance, any search that uses that dataset will evaluate all your appliances.

The user interface shows how many appliances will be searched as part of a dataset and an approximate number of captured events. The number of events is taken from the appliance in the dataset that contains the biggest number of captured events in the dataset.

For example, if the dataset contains four appliances, and three of them contain 1,000 items and the fourth contains 3,000, the number you see will be 3,000. Appliances are analyzed in parallel so you can use this number to help you decide whether the dataset needs further refining. When you save changes to the dataset, it shows you the revised number of captured events that will be searched with these properties.

Important

Changing definitions in a dataset used by either forensic investigation or rule tuning searches also changes that definition in any active rule sets that use it. McAfee recommends that you duplicate the definition and use the duplicate in your DLP Capture searches.

Datasets can be built using the following criteria:

Criteria	Definition
DLP Capture-enabled appliances	The list of McAfee DLP appliances that have the DLP Capture feature enabled. To search a specific DLP Capture-enabled appliance as part of a dataset, you need to select it in the dataset (or for the dataset to be "all" appliances). To select an appliance for a dataset, it needs to have sufficient storage available, and the DLP Capture feature needs to be enabled in the **DLP Capture Settings** policy. If the appliance has captured data but you subsequently disabled the DLP Capture feature in the policy, the appliance still appears in the list of datasets and the captured data will be included in the search.

Criteria	Definition
Incident Triggered	Adds events to the dataset that triggered an incident.
Protocol	Select one or more protocols: FTP, HTTP, IMAP, IRC, LDAP, POP3, SMB, SMTP, Telnet.
Subject	The subject line of an email message.
Time Range	The period of time that the events were captured for, such as the last seven days.
URL	The URL that the data was uploaded to if the original event was a web post.
VLAN ID	(*McAfee DLP Monitor only*) Shows the VLAN that the traffic was sent on.
Email Criteria	The email recipient and/or the email sender.
IP Criteria	The destination IP and/or the source IP address.
Port Criteria	The destination port and/or the source port.
User Criteria	The destination user and/or the source user.

Build a dataset

Create datasets to reduce the number of items that get analyzed in forensic investigation searches or rule tuning searches.

Task

1. From the McAfee ePO menu, select **DLP Capture**, and click **Datasets**.
2. Select **Actions** → **New Dataset**.
3. Add a name and an optional description, then add the items that the dataset will analyze from the list of available properties.
4. Click **Save**.
   The dataset appears in the list showing the number of captured events that will be analyzed.
5. (Optional) If the number of captured items is too large, select the dataset link and further refine the dataset properties, then click **Refresh** to see an updated number of events.

DLP Capture searches

You can perform two types of search on captured content: *Forensic Investigation* or *Rule Tuning*.

Forensic Investigation search

Use the Forensic Investigation search to find captured content that contains certain keywords or file names, or came from certain users. For example, you could look for a keyword in a document that has been leaked from your organization by a specific member of staff.

Forensic Investigation searches look for keywords in the body of an email message, any message attachments, and some email headers (From, To, Cc, Subject, Reply-To) using either exact matches on single words or phrases, or partial matches (inexact matches).

Your search terms can include numerals and special characters such as mathematical symbols and currencies, and you can include logical operators (and/or) to build searches that look for multiple words or phrases. You can also search for specific files by name as they move around your network, including items in archive files.

Note

A Forensic Investigation search does not look for keywords in web request headers.

To search for the activity of a particular user, the DLP Capture feature evaluates the LDAP membership and groups. It looks at the information that exists at the time you create the search, rather than the time the content was captured. If the entries in the LDAP server have been changed, the search might not be able to analyze all the email messages or web posts performed by the user you are interested in. For example, you might need to investigate the activity of a user who has already left the company, in which case, the user might have been removed from the LDAP server and the search will be unable to find them.

Note

It is possible to run a forensic investigation without specifying any criteria, but the search will match against all the results in the dataset up to the configured limit.

Stop words

To reduce the number of results returned, the Forensic Investigation search ignores certain words in all languages. These are known as *stop words*, and include words such as "if", "the", "and", "or".

Language support and word stemming

The DLP Capture feature can analyze content in any, or all, of the following languages: English, French, German, Spanish, Japanese, and Traditional Chinese.

When searching for an exact text match, the search ignores any language selections and just looks for an exact match of the text you entered. However, if you want to look for an inexact match, the search stems the word to broaden the results. For example, searching for *run* will also return *running*, or searching for *information* stems the word to *inform* and also matches *informal*.

If you select a language and look for a word from another supported language, the text in the other supported languages is ignored by the search. If you choose to search all languages, all text is searched and stemmed accordingly. Any unidentified sections of text, such as groups of numbers or text in an unsupported language, is searched using the original search term and is not stemmed.

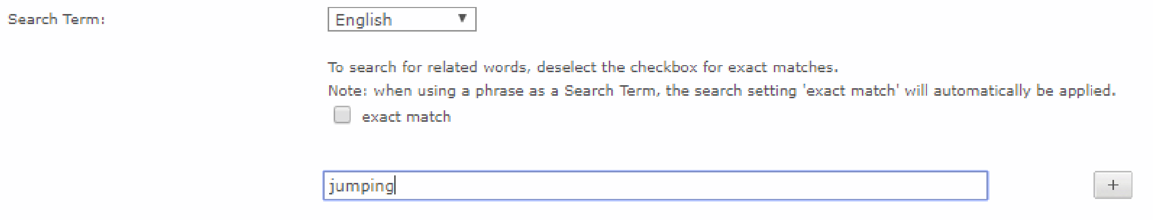
Note

If a plural or gerund of a complete word used in a search is found, the result returns all strings that contain that stem word.

Language and stemming example: Single keyword, single language

The keyword triggers if the language matches the input and they stem to the same word. If the input language is unrecognized or unsupported, the keyword will only trigger if it's an exact match.

Search selections



Search Term: English ▼

To search for related words, deselect the checkbox for exact matches.
Note: when using a phrase as a Search Term, the search setting 'exact match' will automatically be applied.
□ exact match

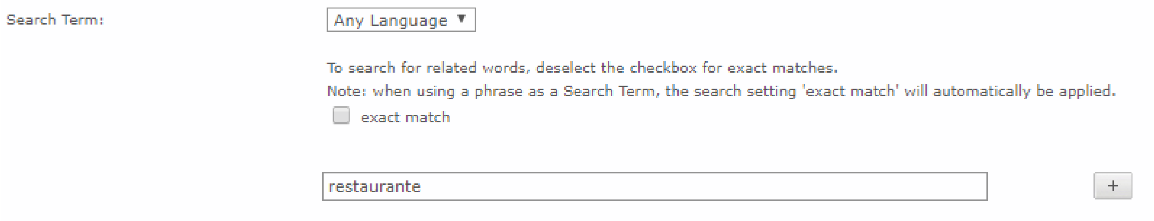
jumping

Stems to search for	Input text language	Input text	Triggers (in bold)
English: jump	English	The dog jumps very high	The dog **jumps** very high
	French	Le chien jumps très haut	Le chien jumps très haut

Language and stemming example: Single keyword, multiple (any) language

The keyword is stemmed in every supported language. The keyword triggers if any of the languages match the input and they stem to the same word. If the input language is unrecognized or unsupported, the keyword will only trigger if it's an exact match.

Search selections



Search Term: Any Language ▼

To search for related words, deselect the checkbox for exact matches.
Note: when using a phrase as a Search Term, the search setting 'exact match' will automatically be applied.
□ exact match

restaurante

Stems to search for	Input text language	Input text	Triggers (in bold)
English: restaurant French: restaur Spanish: restaur Unidentified: restaurante	English	Tequila Restaurante is closing and a new restaurant will occupy its space on the downtown square.	Tequila **Restaurante** is closing and a new restaurant will occupy its space on the downtown square.
	French	Découvrez l'actualité, les événements et les menus spéciaux des meilleurs restaurants de Paris.	Découvrez l'actualité, les événements et les menus spéciaux des meilleurs **restaurants** de Paris.
	Spanish	El sector de la restauración ha visto incrementada su rentabilidad en un 70% en menos de 5 años.	El sector de la **restauración** ha visto incrementada su rentabilidad en un 70% en menos de 5 años.
	Russian (unidentified)	Но и голы - это тоже еще не все, restaurant что нужно зрителю. Зрителю необходимы жертвы - и restaurante чем крупнее, тем лучше.	Но и голы - это тоже еще не все, restaurant что нужно зрителю. Зрителю необходимы жертвы - и **restaurante** чем крупнее, тем лучше.

Language and stemming example: Special cases

There are cases where a single keyword might stem into multiple stems. This can happen if the word contains a separator, like a hyphen.

Keyword	Language	Stems to search for	
non-humans	English	non	human
lighthouse-15	English	lighthouse	15

When this happens, the additional stems are added as extra stems in a multi-keyword rule and the logical operator selected is applied.

Create a Forensic Investigation search

Use a Forensic Investigation search to look for content that was not previously identified as a potential data loss event.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**.
2. Select **Actions** → **New Forensic Investigation**.
3. Add a name and optional description for the new search.
4. Select an existing dataset or create a new one, and click **OK**.
   The dataset shows an approximate number of captured items that will be evaluated with this dataset. If you are searching multiple appliances, the number shown is taken from the appliance that has the most events to evaluate.
5. If the number of events is too big to search in a reasonable amount of time, or too small to give a useful result, you can edit the dataset now.
   The data refreshes the evaluation automatically.
6. In **Max Results to Report**, specify the number of results that you want to be available from the **Search Results** list.
7. (Optional) Select **stop search when max results reached** to prevent the search from analyzing more events than the number specified in **Max Results to Report**.
8. (Optional) Deselect **Results: Store original files as evidence** to improve performance and reduce the amount of data stored.
9. Add the conditions that you want the search to look for.
10. Click **Save** or **Save & Run**.

Use case: Identify sensitive information sent to an external email address

Details of a secret project called "Project Lighthouse" have appeared in the press. You need to investigate how the leak occurred.

Before you begin

Identify a dataset that covers a broad range of captured items, such as the pre-defined **Last Month [built-in]** dataset.

Task

1. In McAfee ePO, open the DLP Capture feature, and create a new forensic investigation search called `Project Lighthouse`.
2. Select the required dataset, then type `Project Lighthouse` as the search term and run the search immediately.
   The search returns the number of results specified in **Max Results to Report**, and it is unclear whether any of the results are the source of the leak. You need to refine the dataset to get better results.
3. Create a new dataset called `Emails sent externally` and exclude email recipients whose email addresses do not end with "mydomain.dom".
4. Create a duplicate copy of the Project Lighthouse search, and name the new version `Project Lighthouse sent externally`.

5. Select the `Emails sent externally` dataset and save and run the search immediately.

   The new search produces a smaller list of results to analyze, so it is easier to identify potential sources of the data leak.

Tuning your rules

You can use the DLP Capture feature to tune your classifications and the email protection, web protection, and network communication protection rules enforced on McAfee DLP appliances to prevent false positives or negatives. The rule tuning feature analyzes captured data rather than active data so you can edit the rule or classification settings until it returns the type of results you want, without affecting your live data analysis.

You can either save an existing rule as a rule turning search, tune it, then use it to override an existing rule, or create a rule tuning search before creating a new rule, tune the settings until you are satisfied with the results, and save it as a new rule.

If you choose to override an existing rule, the **Enforced on** and **Reactions** options stay the same.

Rules that can be tuned

Rule	McAfee DLP Prevent	McAfee DLP Monitor
Email Protection	Yes	Yes
Web Protection	Yes	Yes
Network Communication Protection	No Tuning a network communication protection rule on a McAfee DLP Prevent appliance fails with the reason **Rule Type Not Applicable**.	Yes

Important

If you change classification settings or definitions in a rule tuning search, those changes are applied to the settings in the equivalent active items. For example, if you add a term to a classification in a rule tuning search, it might start triggering in the active rule. McAfee recommends that you duplicate the classification or definition and use the duplicate while you are tuning the rule. You can then use it to replace the original item in the active rules when you have the results you want.

Create a rule tuning search

Test a new rule before adding it to an active rule set by creating a rule tuning search.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**.
2. Select **Actions** → **New Rule Tuning**, then select the type of rule tuning search you want to create: **Email Protection**, **Network Communication Protection**, or **Web Protection**.
3. Add a name and optional description for the new search.
4. Select an existing dataset or create a new one, and click **OK**.
   The dataset shows an approximate number of captured items that will be evaluated with this dataset. If you are searching multiple appliances, the number shown is taken from the appliance that has the most events to evaluate.
5. If the number of events is too big to search in a reasonable amount of time, or too small to give a useful result, you can edit the dataset now.
   The data refreshes automatically.
6. In **Max Results to Report**, specify the number of results that you want to be available from the **Search Results** list.
7. (Optional) Select **stop search when max results reached** to prevent the search from analyzing more events than the number specified in **Max Results to Report**.
8. (Optional) Deselect **Results: Store original files as evidence** to improve performance and reduce the amount of data stored.
9. Add the conditions that you want to apply to the rule tuning search and click **Save**.
10. To add any exceptions, click **Exceptions**, then select **Actions** → **Add Rule Exception** and click **Save** or **Save & Run**.

Save a rule tuning search as a rule

Create a rule tuning search that you can save as a new email, web, or network communication protection rule, or override an existing rule.

Before you begin

Check that the user has permissions to use DLP Policy Manager.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**, and create a new rule tuning search or identify an existing rule tuning search that you want to save.
2. In the **Search List**, select the rule tuning search that you want to save, then select **Actions** → **Save as Rule**.
3. Select one of the following options, then click **OK**.
   - **Create new Rule** — (Default) Either select an existing rule set to save the rule to, or create a new one.
   - **Override existing Rule** — (Optional) This option becomes available if this search was originally created by saving a rule, or the search was saved as a new rule and you want to update it. Select it to save the new version of the rule over the existing rule. You can choose to keep the existing name and description or create new ones.
4. On the rule page, specify the reaction, severity, and state settings, then click **Save**.

The rule appears in the rule set in the **DLP Policy Manager**.

Results

(Optional) If you want to make further changes to the rule without affecting your live data analysis, you can select it in the rule set and click **Save as Capture Search**. You can repeat this process of saving the rule as a capture search and making changes until you are satisfied with the new rule settings.

Save an existing rule as a DLP Capture search

Save an email, web, or network communication protection rule as a rule tuning search to experiment with its settings without affecting your live data analysis. You can save the new version of the rule back to your active rules as a new rule, or replace the existing rule.

Note

Saving an email, web, or network communication protection rule as a rule tuning search is only supported for rules that are enforced on McAfee DLP appliances.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Policy Manager**.
2. Click the **Rule Sets** tab.
3. Select the rule set that contains the rule you want to save, then select the rule from the data protection rules.
   The rule must be enforced on a McAfee DLP appliance.
4. Select **Actions** → **Save as Capture Search**.
5. On the **Capture Search** → **Rule Tuning** page, edit the settings to tune the rule.
6. Click **Save** or **Save and Run**.
7. When the search event shows **Finished**, check the results to see if you need to make further changes.
8. When you are satisfied that the rule is getting the results you want, click **Actions** → **Save as Rule**, and either create a new rule from it, or override the original rule in the rule set.

Use case: Tuning a rule to eliminate false positives

A rule called `Block PCI information` in the `Protect financial data` ruleset is identifying a large number of false positives.

Before you begin

Select the pre-defined **Last 24 hours** dataset for this example and specify the appliances that you want to run the search on.

Task

1. From the **DLP Policy Manager**, open the `Protect financial data` rule set and convert the `Block PCI information` rule into a capture search.
2. Select the `Last 24 hours` dataset and save and run the search.
3. Check the search results.
   Most of the results are for emails sent from the Finance department to either internal recipients, or trusted-partner.dom. These are legitimate emails that are triggering the false positives.
4. Create an exception to `Block PCI information` rule that excludes messages sent from members of a Finance" LDAP group to recipients in the "Trusted recipients" email address list.

   Note

   Remember to enable the exception.
5. Run the search again and review the results.
   The number of false positives is reduced.
6. Save the search back to a rule, choosing to replace the original rule.

The Search List and Search Results

The DLP Capture feature displays information about each configured search in the **Search List**. From this page, you can create new searches and edit existing search settings. You can also select a search to see its results and export them. From the search results, you can select an individual result and see details about it.

The Search List

You can run up to five searches at the same time. If you try to run more than five searches concurrently, the later searches are queued until the required number of earlier searches finish.

Each search has a status, such as **In progress**, **Canceled**, **Starting**, or **Finished**. The **Starting** status displays until the **Run** action is received by one of the appliances in the dataset, when the status changes to **In progress**. You can also see when the search started, how long it took (elapsed time), and the number of positive matches that triggered.

Each search entry in the list shows the number of appliances that will be searched with this dataset and any search results. There are also some search-related actions: **Delete**, **Duplicate**, **Run**, or **Cancel**.

If you cancel a search while it is in progress, the number of results continues to increment for a short time until the appliance itself stops the search. You cannot edit a search that is in progress until all the appliances in the dataset have received the cancel command. A search cannot run if it references a single unavailable appliance.

ⓘ **Important**

Deleting a search from the list removes the search results and all its related evidence items from the evidence folder. Similarly, if you run a search again, all the results and evidence items from the previous time it ran will be deleted. If you try to re-run a search that is in progress, the original results are removed and a new run of the same search begins.

You can export search results into two files. One contains a summary of the results and the other gives detailed information about each positive match.

If you export the results from the Search List, the two files contain results from each appliance that was searched as part of the dataset. If you want to export the results from the Appliance List, you can select one or more appliances to download results from.

There are some additional options available for each search within the list.

- To view or edit a search settings, simply select the search name. If you make changes to the settings, you can save them to run later or run the search with the updated settings immediately.
- To view information about results from appliances that are part of the specified dataset and see their health status, select the appliances link. From the **Search Appliances List**, you can see an appliance's current health status (not its health status at the time the search ran), and link to the **Appliance Management** feature to get more detailed status information. You can also export a summary of the results from one or more appliances.
- For any search that produced results, you can select the number of results to get more information about those results.

Search Results

By default, the first 100 results from each appliance in a dataset are displayed in **Search Results**. For example, if the dataset includes five appliances, you can expect to see up to 500 results listed. However, you can specify a different number of results to display when you create the search.

Your selection of the **Max Results to Report** and **stop search when max results reached** options when you create a forensic investigation search or rule tuning search affect the results you see in the Search Results list.

For example, if you have one appliance in a dataset and the search criteria match against 150 items, the **Max Results to Report** option is set to 100, and the **stop search when max results reached** option is selected, the number of results in the **Results** tab, the **Results** column in the **Search** list, the Search Appliances list, and the results files are all 100. However, if **stop search when max results reached** is *not* selected, you see 100 results in the **Results** tab, but 150 results are reported in the results file, the **Results** column in the **Search** list, and the **Search Appliances** list.

Select a result to get more information about it, as well as any associated evidence and classifications that triggered. Each result has an individual identification number, and shows the reporting product and other information, such as the type of rule that triggered and any classifications.

If a captured item matches against any forensic investigation or rule tuning search, you can create an incident for that result that appears in the **DLP Incident Manager**. Details of the captured item are included in the incident in exactly the same way as if it had triggered a rule. You can also select one or more results to add to a new or existing case.

Search results details

Click a Result ID in **Search Results** to get detailed information about that individual result, including any classifications that triggered and associated evidence. You can deselect the option to collect evidence in the search settings to avoid storage and performance implications.

Note

> A rule tuning result's details will tell you about any classifications that triggered, but will not include details of the rule that triggered.

The result can be added to an incident, exported into a report file, or added to a new or existing case. If you choose to create an incident from the result, a link to the incident is added to the result details.

Export the results of a selected search

From the **Search List** view, you can select a search and export its results into two files.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**.
2. In the **Search List**, select the search that contains the results you want to export and click **Actions** → **Export Results Summary**.

Export the search results from specific appliances

You can export the search results of one or more appliances into two results files.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**.
2. In the **Search List**, click the appliances link for the search whose results you want to export.
3. In the **Search Appliances List**, select the appliances that contain the results you want to export and click **Actions** → **Export Results Summary**.

Results

A zip file that contains summary results and detailed results from each selected appliance is created.

Export selected results

Export one or more search results and evidence items.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**.
2. In the **Search List**, find the search whose results you want to export and click the number of results link.
3. From **Search Results**, select the results that you want to include and click **Actions** → **Export selected results**.
4. Specify the type of details that you want to export, where you want to store it, and whether you want to receive a notification when the export is complete, then click **Export**.

Create an incident from a result

You can create a incident from the **Search Results Details** view or from a selected result in the list of searches.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**.
2. In the **Search List**, find the search whose results you want to create an incident from and click the number of results link.
3. In **Search Results**, either select the result and click **Actions** → **Create Incident**, or click a specific **Result ID** and click **Actions** → **Create Incident**.

Results

An incident is added to the **DLP Incident Manager** and a link to it is added in the selected result's details.

Add search results to a case

From either the **Search Results** view or the **Search Results Details** view, you can add one or more search results to a new or existing case.

Task

1. In McAfee ePO, select **Menu** → **DLP Capture**.
2. In the **Search List**, find the search whose results you want to add to a case and click the number of results link.

3. In **Search Results**, either select one or more results and click **Actions** → **Case Management** or click a specific **Result ID** and click **Actions** → **Case Management**.
4. Select one of the following options:
   - **Add to existing case** — Select the case you want to add the results to and click **OK**.
   - **Add to new case** — Give the case a title and specify the owner, the status, the resolution, and the priority, then click **OK**.

Results

An incident is created automatically and added to the case.

Incidents, events, and cases

Incidents and operational events

There are different tools available to view incidents and operational events.

- **Incidents** — The DLP Incident Manager module displays incidents generated from rules. McAfee DLP Endpoint, Device Control, McAfee DLP Prevent, McAfee DLP Monitor, Cloud DLP, and MVISION Cloud enforce rules and send incidents to DLP Incident Manager.
- **Operational events** — The DLP Operations module displays errors and administrative information. McAfee DLP Discover, McAfee DLP Endpoint, and McAfee DLP Prevent send events to DLP Operations.
- **Cases** — The DLP Case Management module contains cases that have been created to group and manage related incidents.

When multiple McAfee DLP products are installed, the consoles display incidents and events from all products.

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

You can define custom status and resolution definitions. The definition consists of a custom name and color code, and can have the status of enabled or disabled. Custom definitions must be added and enabled in DLP Settings on the **Incident Manager**, **Operations Center**, or **Case Management** page before they can be used.

Logging events with Syslog

- You can send certain events using the Syslog protocol to a Syslog server. Configure the Syslog server in the Windows Client configuration on the **Debugging and Logging** page. The events are sent whether rules are configured to trigger the events or not. The following actions are sent automatically when **Send DLP Syslog events to Syslog server** is enabled:
    - Printing
    - Copy to removable storage
    - Uploading a file to the web
    - Uploading a file to the cloud
    - Sending email
    - Connect or disconnect a plug and play device
    - Connect or disconnect a removable storage device

Stakeholders

A stakeholder is anyone with an interest in a particular incident, event, or case. Typical stakeholders are DLP administrators, case reviewers, managers, or users with incidents. McAfee DLP sends automatic emails to stakeholders when an incident, event, or case is created or changed. It can also automatically add stakeholders to the list, for example, when a reviewer is assigned to a case. The administrator also can manually add stakeholders to specific incidents, events, or cases.

Automatic email details are set in **DLP Settings**. Options on the **Incident Manager**, **Operations Center**, and **Case Management** pages determine whether automatic emails are sent, and who is automatically added to the stakeholders list. The administrator can add stakeholders manually from the DLP Incident Manager, DLP Operations, or DLP Case Management modules.

Monitoring and reporting events

McAfee DLP products divide 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 a McAfee DLP product 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 products take a major role in an enterprise's effort to comply with all regulation and privacy laws, the **DLP Incident Manager** presents information about the transmission of sensitive data in an accurate and flexible way. Auditors, signing officers, privacy officials and other key workers can use the **DLP Incident Manager** to observe suspicious or unauthorized activities and act in accordance with enterprise privacy policy, relevant regulations or other laws.

The system administrator or the security officer can follow administrative events regarding agents and policy distribution status.

Based on which McAfee DLP products you use, the **DLP Operations** console can display errors, policy changes, agent overrides, and other administrative events.

You can configure an email notification to be sent to specified addresses whenever updates are made to incidents, cases, and operational events.

DLP Incident Manager/DLP Operations

Use the **DLP Incident Manager** module in McAfee ePO to view the security events from policy violations. Use DLP Operations to view administrative information, such as information about client deployment.

DLP Incident Manager has three tabbed pages. On each page the **Present** drop-down list determines the data set displayed: **Data-in-use/motion**, **Data-at-rest (Endpoint)**, or **Data-at-rest (Network)**.

- **Analytics** — A display of six charts that summarize the incident list. Each chart has a filter to adjust the display. The charts display:
  - **Top 10 RuleSets**
  - **Incidents per Type**
  - **Top 10 Users with Violations**
  - **Number of Incidents Per Day**
  - **Top 10 Destinations**
  - **Top 10 Classifications**
- **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 with all historic incidents. Purging the incident list does not affect the history.

DLP Operations has four tabbed pages:

- **Operational Event List** — The current list of administrative events.
- **Operational Event Tasks** — A list of actions you can take on the list or selected parts of it, similar to the incident tasks.
- **Operational Event History** — A list with all historic events.
- **User Information** — Displays data from the user information table.

Detailed information can be viewed by drilling down (selecting) a specific incident or event.

User Information

The **User Information** page displays data from the user information table. The table is populated automatically from user information in incidents and operational events. You can add more detailed information by importing from a CSV file.

Information displayed typically includes user principal name (username@xyz), user log on name, user operational unit, first name, last name, user primary email, user manager, department, and business unit. The complete list of available fields can be viewed from the **Edit** command for the **View** option.

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.

Note

To display the **User Principal Name** and **User Logon Name** in McAfee DLP appliance incidents, add an LDAP server to the **DLP Appliance Management** policy (**Users and Groups** category). You must do this even if your email protection rules do not use LDAP.

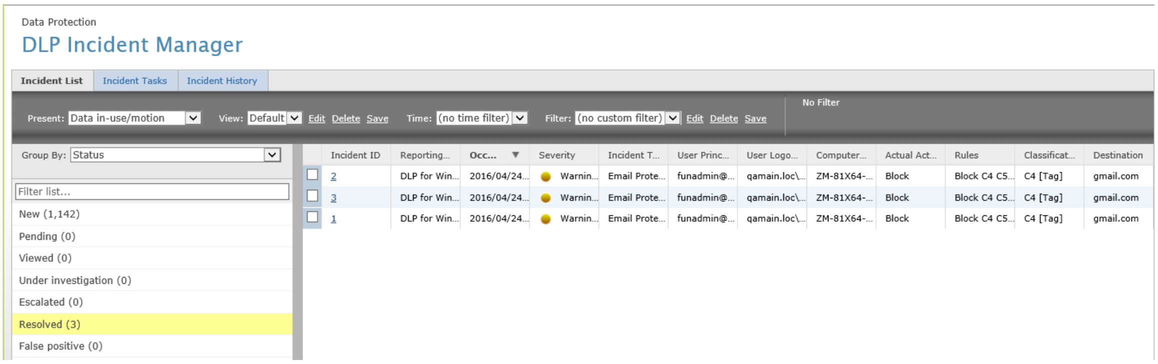
The **Incident List** tab works with McAfee ePO **Queries & Reports** to create McAfee DLP Endpoint and McAfee DLP appliance reports, and display data on McAfee ePO dashboards.

Operations you can perform on events include:

- **Case management** — Create cases and add selected incidents to a case
- **Comments** — Add comments to selected incidents
- **Email events** — Send selected events
- **Export device parameters** — Export device parameters to a CSV file (Data in-use/motion list only)
- **Labels** — Set a label for filtering by label
- **Release redaction** — Remove redaction to view protected fields (requires correct permission)

- **Set properties** — Edit the severity, status, or resolution; assign a user or group for incident review

DLP Incident Manager



Data Protection

DLP Incident Manager

Present: Data in-use/motion View: Default Edit Delete Save Time: (no time filter) Filter: (no custom filter) Edit Delete Save

No Filter

Group By: Status

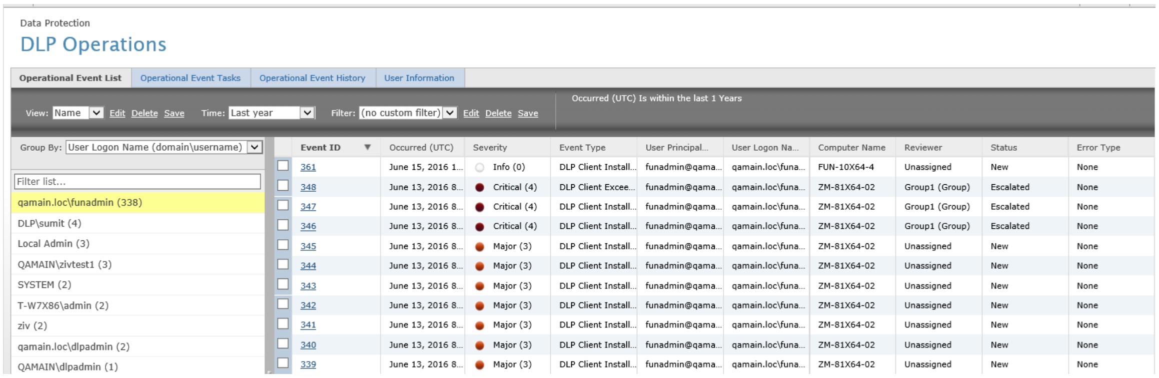
Filter list...

- New (1,142)
- Pending (0)
- Viewed (0)
- Under investigation (0)
- Escalated (0)
- Resolved (3)
- False positive (0)

	Incident ID	Reporting...	Occ... ▼	Severity	Incident T...	User Princ...	User Logo...	Computer...	Actual Act...	Rules	Classificat...	Destination
□	2	DLP for Win...	2016/04/24...	● Warnin...	Email Prote...	funadmin@...	qamain.loc\...	ZM-81X64-...	Block	Block C4 C5...	C4 [Tag]	gmail.com
□	3	DLP for Win...	2016/04/24...	● Warnin...	Email Prote...	funadmin@...	qamain.loc\...	ZM-81X64-...	Block	Block C4 C5...	C4 [Tag]	gmail.com
□	1	DLP for Win...	2016/04/24...	● Warnin...	Email Prote...	funadmin@...	qamain.loc\...	ZM-81X64-...	Block	Block C4 C5...	C4 [Tag]	gmail.com

The DLP Operations page works in an identical manner with administrative events. The events contain information such as why the event was generated and which McAfee DLP product reported the event. It can also include user information connected with the event, such as user logon name, user principal name (username@xyz), or user manager, department, or business unit. Operational events can be filtered by any of these, or by other parameters such as severity, status, client version, policy name, and more.

DLP Operations



Data Protection

DLP Operations

View: Name Edit Delete Save Time: Last year Filter: (no custom filter) Edit Delete Save

Occurred (UTC) Is within the last 1 Years

Group By: User Logon Name (domain\username)

Filter list...

- qamain.loc\funadmin (338)
- DLP\sumit (4)
- Local Admin (3)
- QAMAIN\zivtest1 (3)
- SYSTEM (2)
- T-W7X86\admin (2)
- ziv (2)
- qamain.loc\dlpadmin (2)
- QAMAIN\dlpadmin (1)

	Event ID ▼	Occurred (UTC)	Severity	Event Type	User Principal...	User Logon Na...	Computer Name	Reviewer	Status	Error Type
□	361	June 15, 2016 1...	○ Info (0)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	FUN-10X64-4	Unassigned	New	None
□	348	June 13, 2016 8...	● Critical (4)	DLP Client Excee...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Group1 (Group)	Escalated	None
□	347	June 13, 2016 8...	● Critical (4)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Group1 (Group)	Escalated	None
□	346	June 13, 2016 8...	● Critical (4)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Group1 (Group)	Escalated	None
□	345	June 13, 2016 8...	● Major (3)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Unassigned	New	None
□	344	June 13, 2016 8...	● Major (3)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Unassigned	New	None
□	343	June 13, 2016 8...	● Major (3)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Unassigned	New	None
□	342	June 13, 2016 8...	● Major (3)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Unassigned	New	None
□	341	June 13, 2016 8...	● Major (3)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Unassigned	New	None
□	340	June 13, 2016 8...	● Major (3)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Unassigned	New	None
□	339	June 13, 2016 8...	● Major (3)	DLP Client Install...	funadmin@qama...	qamain.loc\funa...	ZM-81X64-02	Unassigned	New	None

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.

	Data in-use/ motion	Data at-rest (Endpoint)	Data at-rest (Network)	Data in-use/ motion (History)
Set Reviewer	X	X	X	
Automatic mail notification	X	X	X	
Purge events	X	X	X	X
Purge evidence files	X	X	X	X

Use case: Setting properties

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

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

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

Use case: Changing the view

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

Creating a filter involves the following tasks:

1. To open the view edit window, click **Actions** → **View** → **Choose Columns**.
2. To move columns to the left or right, use the **x** icon to delete columns, and the arrow icons.
3. To apply the customized view, click **Update View**.
4. To save for future use, click **Actions** → **View** → **Save View**.

Note

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

Working with incidents

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

Using the **DLP 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.

Device plug incidents

Two options on the Incident List **Actions** menu allow you to work with device plug incidents. **Create Device Template** creates a device definition from a device plug incident. The option is available only when a single device plug incident is selected. If you select more than one incident, or a non-device plug incident, a popup informs you of your error. **Export Device Information to CSV** saves information from one or more device plug incidents. You can import saved device information from the **DLP Policy Manager** → **Definitions** → **Device Templates** page.

View incidents

DLP Incident Manager Displays all incidents reported by McAfee DLP applications. You can alter the way incidents appear to help you locate important violations more efficiently.

The **Present** field in the DLP Incident Manager displays incidents according to the application that produced them:

- **Data in-use/motion**
  - McAfee DLP Endpoint
  - Device Control
  - McAfee DLP Prevent
  - McAfee DLP Monitor
- **Data at rest (Endpoint)** — McAfee DLP Endpoint discovery
- **Data at rest (Network)** — McAfee DLP Discover

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

Sort and filter incidents

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

Task

1. In McAfee ePO, select **DLP Incident Manager**.
2. From the **Present** drop-down list, select the option for your product.

3. Perform any of these tasks from the **Incident List** or the **Incident History** tabs.
    - 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, or click **Edit** to create a filter.

    Note

    > Available properties for filters are selected from a list of McAfee ePO and McAfee DLP properties.

    - To group by attribute:
        - • 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.
        - • Select an option from the list. Incidents that match the selection are displayed.

Example

When working with McAfee DLP Endpoint incidents, select **User ID** to display the names of users that have triggered violations. Select a user name to display all incidents for that user.

Configure column views

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

Task

1. In McAfee ePO, select **DLP Incident Manager**.
2. From the **Present** drop-down list, select the option for your product.
3. From the **View** drop-down list, select **Default** and click **Edit**.
4. Configure the columns.
    a. From the **Available Columns** list, click an option to move it to the **Selected Columns** area.
    b. In the **Selected Columns** area, arrange and delete columns as needed.
        - To remove a column, click **x**.
        - To move a column, click the arrow buttons, or drag and drop the column.

    c. Click **Update View**.
5. Configure the view settings.
    a. Next to the **View** drop-down list, click **Save**.
    b. Select one of these options.
        - **Save as new view** — Specify a name for the view.

- **Override existing view** — Select the view to save.

c. Select who can use the view.

- **Public** — Any user can use the view.
- **Private** — Only the user that created the view can use the view.

d. Specify if you want the current filters or groupings applied to the view.

e. Click **OK**.

Results

Note

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

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

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. Do one of the following:
   - For McAfee DLP Endpoint: Select an incident type from the drop-down list (**Incident Tasks** only), select **Set Reviewer** in the **Task Type** pane, then click **Actions** → **New Rule**.
   - For McAfee DLP Discover: Select **Data at rest (Network)** from the drop-down list.
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**.

   Tip

   If there are multiple **Set Reviewer** rules, reorder the rules in the list.

Results

The task runs hourly.

Note

You cannot override the reviewer through the **Set Reviewer** task after the reviewer is set.

Configure incident filters

Use filters to display incidents that match specified criteria.

McAfee DLP Endpoint Example: You suspect a particular user has been sending connections containing sensitive data to a range of IP addresses outside the company. You can create a filter to display incidents that match the user name and the range of IP addresses.

Task

1. In McAfee ePO, select **DLP Incident Manager**.
2. From the **Present** drop-down list, select the option for your product.
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.

      Note

      To add additional values for the same property, click **+**.

   c. Select additional properties as needed.

      Note

      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**.

Results

Note

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

View incident details

View the information related to an incident.

Task

1. In McAfee ePO, select **DLP Incident Manager**.
2. From the **Present** drop-down list, select the option for your product.
3. Click an **Incident ID**.
   The page displays general details and source information. Depending on the incident type you select, destination or device details are displayed.
   The page displays general details about the incident.
4. To view additional information, perform any of these actions.
   - To view user information for incidents, click the user name in the **Source** area.
   - To view evidence files, click the **Evidence** tab and select a file name. 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.

   Note

   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

Managing incidents

Use the DLP Incident Manager to update and manage incidents.

Email selected events

Note

To optimize system performance, McAfee DLP purges incidents from the live incidents list table and moves them to the history list view when a million incidents are reached, starting with the oldest incidents.

Use the **Incident List** for viewing real-time information related to an incident. Purged incidents continue to be displayed on the **Incident History** page. Use the McAfee ePO **DLP Purge History of Operational Events and Incidents** and **DLP purge evidences** Server Tasks to mark evidence files for deletion and delete events and incidents from the history database tables.

If you have email notifications configured, an email is sent when an incident is updated.

The following tables give some details about the email and export selected events options.

Email selected events

Parameter	Value
Maximum number of events to mail	100
Maximum size of each event	unlimited
Maximum size of the compressed (ZIP) file	20 MB
From	limited to 100 characters
To, CC	limited to 500 characters
Subject	limited to 150 characters
Body	limited to 1000 characters

Export selected events

Parameter	Value
Maximum number of events to export	1000
Maximum size of each event	unlimited
Maximum size of the export compressed (ZIP) file	unlimited

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

1. In McAfee ePO, select **DLP Incident Manager**.
2. From the **Present** drop-down list, select the option for your product.
3. Select the checkboxes of one or more incidents.

   Note

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

4. Perform any of these tasks.
   - To add labels:
      - • Select **Actions** → **Labels** → **Attach**.
      - • To add a new label, enter a name and click **Add**.
      - • Select one or more labels.
      - • Click **OK**.
   - To remove labels from an incident:
      - • Select **Actions** → **Labels** → **Detach**.
      - • Select the labels to remove from the incident.
      - • Click **OK**.
   - To delete labels:

- • Select **Actions** → **Labels** → **Delete Labels**.
- • Select the labels to delete.
- • Click **OK**.

Update a single incident

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

Note

- MVISION Cloud incidents can only be updated in MVISION Cloud.
- The **Audit Logs** tab reports all updates and modifications performed on an incident.

Task

1. In McAfee ePO, select **DLP Incident Manager**.
2. From the **Present** drop-down list, select the option for your product.
3. Click an incident to open its details window.
4. In the **General Details** pane, perform any of these actions.

   - To update the severity, status, or resolution, select an option from the **Severity**, **Status**, or **Resolution** drop-down list, then click **Save**.
   - To update the reviewer, click next to the **Reviewer** field, select the group or user and click **OK** then **Save**.
   - To add a comment, select **Actions** → **Add Comment**, enter a comment, then click **OK**.

Update multiple incidents

Update multiple incidents with the same information simultaneously. Up to 10,000 incidents can be updated simultaneously.

Note

MVISION Cloud incidents can only be updated in MVISION Cloud.

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

Task

1. In McAfee ePO, select **DLP Incident Manager**.
2. From the **Present** drop-down list, select the option for your product.
3. Select the check boxes of the incidents to update.

Note

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

4. Perform any of these actions.
   - 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**.

     Note

     You can select a template, or create a template by entering the information and clicking **Save**.
   - To export the incidents, select **Actions** → **Export Selected Events**, enter the information, then click **OK**.
   - To release redaction on the incidents, select **Actions** → **Release Redaction**, enter a user name and password, then click **OK**.

     Note

     You must have data redaction permission to remove redaction.
   - To change the properties, select **Actions** → **Set Properties**, change the options, then click **OK**.

Create email notifications

Set up email notifications for incidents and operational events.

The process to add email notifications is similar for **DLP Incident Manager** and **DLP Operations**.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Incident Manager** or **Menu** → **Data Protection** → **DLP Operations**.
2. Select **Incident Tasks** or **Operational Event Tasks**, then select **Automatic mail Notification**.
   If you chose **Incident Tasks**, you must also select the type of incident, such as **Data-in-use/motion**.
3. Click **Actions** → **New Rule** and enter a name and optional description.
   Rules are enabled by default. You can change this setting to delay running the rule.
4. Select which events you want to process, then specify **Recipients**, **Subject**, and **Body**.
   Except for **Body**, these fields are required. You can insert variables from the drop-down list as needed.
5. Add the email body text.
6. (Optional for **DLP Incident Manager**) Select the checkbox to attach evidence information to the email.
7. Click **Next** to add the rule criteria and their **Comparison** and **Value** parameters, then click **Save**.

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.

McAfee DLP Endpoint Scenario: You notice that a particular user often generates several incidents after business hours. This could indicate that the user is engaging in suspicious activity or that the user's system has been compromised. Assign these incidents to a case to keep track of when and how many of these violations occur.

McAfee DLP Discover 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 cases

Create a case to group and review related incidents.

Task

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

Assign a reviewer

Assign reviewers to incidents and operational events. Assignments can be by reviewer group or individual reviewer.

Use the **Permission Sets** feature under **User Management** to create reviewers.

The process to set reviewers is similar for **DLP Incident Manager** and **DLP Operations**.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Incident Manager** or **Menu** → **Data Protection** → **DLP Operations**.
2. Select either **Incident Tasks** or **Operational Event Tasks**, then select **Set Reviewer**.
3. Click **Actions** → **New Rule** and enter a name and optional description.
   Rules are enabled by default. You can change this setting to delay running the rule.
4. Select a reviewer or group, then click **Next**.
5. Click **Next** to add the rule criteria and their **Comparison** and **Value** parameters, then click **Save**.

View case information

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

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Case Management**.
2. Click on a case ID.
3. Perform any of these actions.
   - To view incidents assigned to the case, click the **Incidents** tab.
   - To view user comments, click the **Comments** tab.
   - To view attached files related to the case, click the **Attachments** tab.
   - To view details about all stakeholders, click the **Stakeholders** 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

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.

Tip

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

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:
        - ▯ • Click the **Incidents** tab and select the incidents.
        - ▯ • Select **Actions** → **Move**, then select whether to move to an existing or new case.
        - ▯ • Select the existing case or configure options for a new case, then click **OK**.
    - To remove incidents from the case:
        - ▯ • Click the **Incidents** tab and select the incidents.
        - ▯ • Select **Actions** → **Remove**, then click **Yes**.
4. Click **OK**.

Results

Tip

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.
- An attachment is added.

Tip

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

Task

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, click **...** next to the **Owner** field, select the group or user, then click **OK** and **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, click **...** next to the **Send notifications to** field, select the users to send notifications to, then click **Save**.

     Note

     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**.

   - To add a comment to the case, click the **Comments** tab, enter the comment in the text field, then click **Add Comment**.
4. Click **OK**.

Add or remove labels to a case

Use labels to distinguish cases by a custom attribute.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Case Management**.
2. Select the checkboxes of one or more cases.

   Tip

   > To update all incidents displayed by the current filter, click **Select all in this page**.

3. Perform any of these tasks.
   - To add labels to the selected cases:
     - ▯ • Select **Actions** → **Manage Labels** → **Attach**.
     - ▯ • To add a new label, enter a name and click **Add**.
     - ▯ • Select one or more labels.
     - ▯ • Click **OK**.
   - To remove labels from the selected cases:
     - ▯ • Select **Actions** → **Manage Labels** → **Detach**.
     - ▯ • Select the labels to remove.
     - ▯ • Click **OK**.

Assign incident viewing permissions to users in an Active Directory

Select users from the Active Directory who can view incidents in the **DLP Incident Manager**.

Before you begin

Register an Active Directory server in McAfee ePO.

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**.
2. Select the role you want to edit, then click the **Edit** link under **Name and users**.
3. Click **Add**, select the Active Directory users you want to add, then click **OK**.
4. Click **Save**.
5. In **Data Loss Prevention**, click the **Edit** link.
6. Select **Incident Management**, then click **User can view all incidents**.
7. Click **Save**.

Assign case management viewing permissions to a user

Allow a specific user to view their cases in **DLP Case Management**.

Before you begin

Create a user in McAfee ePO and assign a permission set to the user.

Task

1. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets** and select the permission set that the user belongs to.
2. Click the **Edit** link under **Name and users**.
3. Select the recently created user, and click **Save**.
4. In **Data Loss Prevention**, click the **Edit** link.
5. Select **Case Management**, and click **Users can view cases assigned to them**.
6. Click **Save**.

Delete cases

Delete cases that are no longer needed.

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Case Management**.
2. Select the checkboxes of one or more cases.

   Tip

   To delete all cases displayed by the current filter, click **Select all in this page**.

3. Select **Actions** → **Delete**, then click **Yes**.

Monitoring appliances

Monitoring McAfee DLP appliances from McAfee ePO

You can monitor McAfee DLP Prevent and McAfee DLP Monitor appliances in McAfee ePO using the **Appliance Management** feature.

The **Tree View**, **System Health**, **Alerts**, and **Details** panes collectively provide the status of your appliances in the **Appliance Management** page. You can look for alerts and status of all your appliances and clusters managed by the Appliance Management feature in McAfee ePO. The type of information displayed varies depending on the type of appliance, and the way that you have configured your appliances.

System Health cards

Status is displayed in green, amber, or red. The status color depends on whether warning and critical threshold values are exceeded, or if there is an error. More information is provided in the **Alerts** and **Details** panes.

Areas of the System Health card

The information bar appears across the top of each **System Health** card. This information bar includes the appliance name, the number of currently reported alerts, and other information specific to the reported appliance.

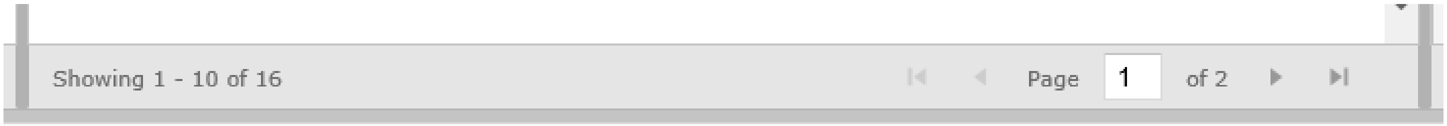
The primary statistics are displayed beneath the appliance name. These statistics are the two items of information that are considered of highest importance for the appliance type.

To the right of the primary statistics are the other health statistics for the appliance. These statistics vary, depending on the type of appliance to which they relate.

System Health card pagination ribbon

The system health information for your appliances and clusters is displayed in the **System Health** pane. You can view this **System Health** information a page at a time using the pagination ribbon at the bottom of the **System Health** pane. This ribbon includes summaries of the number of appliances or clusters displayed in the **System Health** pane, and the controls to move through the available pages.

System Health card pagination ribbon


Showing 1 - 10 of 16

Page 1 of 2

Note

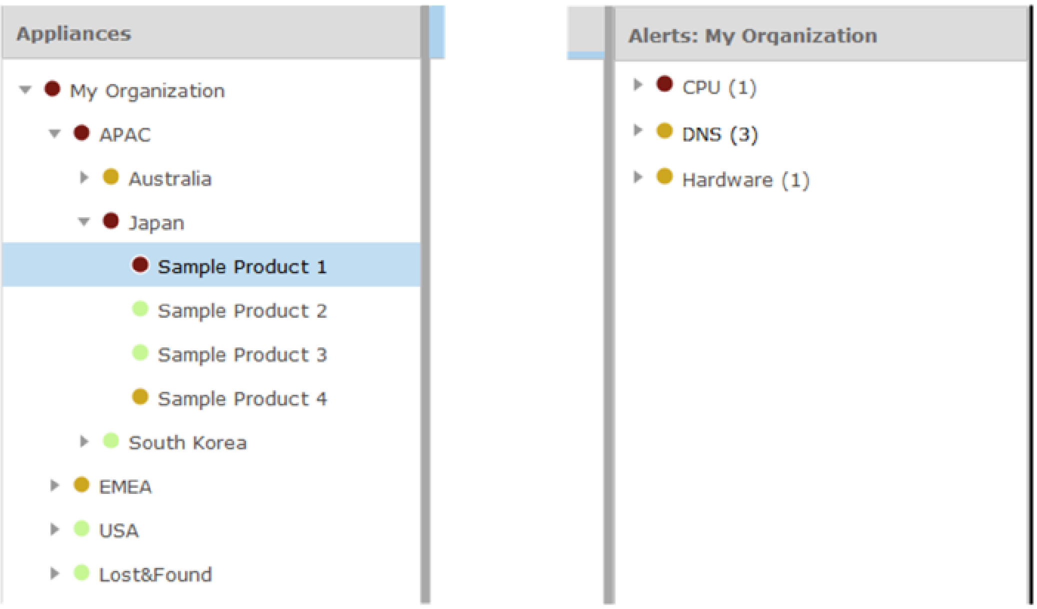
To view information about a group of appliances or clusters, use the **Appliances** tree view to filter the systems displayed. Then, use the pagination controls to view the **System Health** information for the system of interest.

Alerts pane

The **Alerts** pane shows information about any errors or warnings that relate to your managed appliances. If there are no current errors or warnings, this pane is empty.

The information shown in the **Alerts** pane reflects the appliance or group of appliances that are currently selected in the tree view. As you navigate to a different appliance or group of appliances, the alerts that are displayed change to show only the ones relevant to your selection.

Appliances tree view and Alerts pane



Alerts are grouped by category. By default, alerts are shown rolled up except for updates and DNS alerts. Examples of the types of category include:

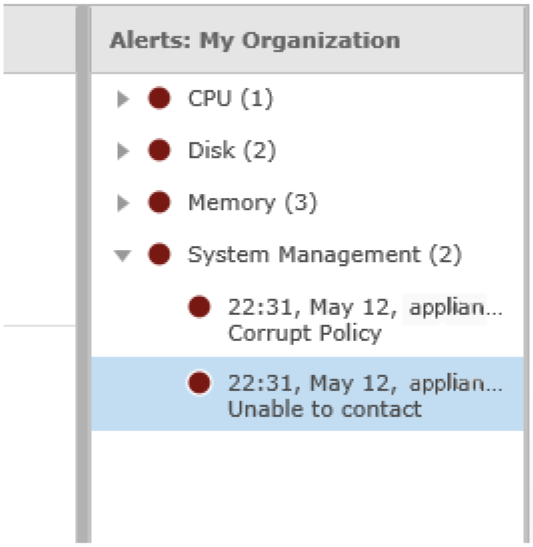
- CPU
- Memory
- Disk
- Network
- Updates
- DNS

Note

The categories that you see depend on the McAfee products you are managing from McAfee ePO, and the types of alert being issued.

To view the individual alert messages, click the ▶ to the left of the category.

Alerts pane with expanded alert category



Alerts: My Organization

- ● CPU (1)
- ● Disk (2)
- ● Memory (3)
- ● System Management (2)
  - ● 22:31, May 12, applian… Corrupt Policy
  - ● 22:31, May 12, applian… Unable to contact

All alerts in the chosen category are shown nested beneath the category label. Also included in each alert is a time stamp, the appliance name, and a brief description of the alert. To roll up the alerts, click the ▼.

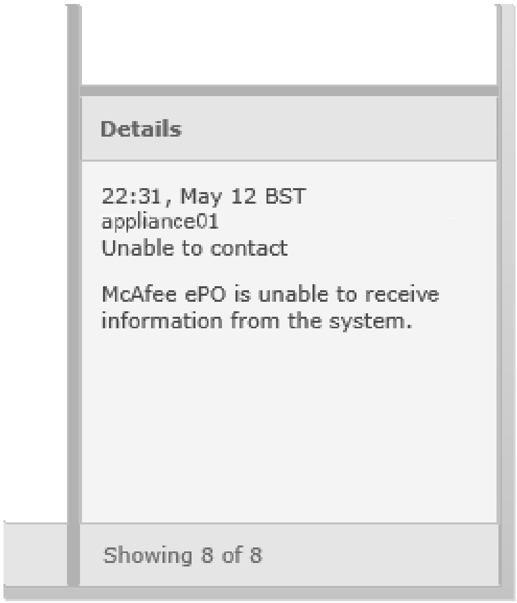
Details pane

The **Details** pane shows detailed information about the alert selected in the **Alerts** pane.

Note

> The type of information displayed in the **Details** pane varies depending on the type of warning or error being reported.

Details pane



Details

22:31, May 12 BST
appliance01
Unable to contact

McAfee ePO is unable to receive information from the system.

Showing 8 of 8

The alerts counters are displayed at the bottom of the **Details** pane. These counters show the number of alerts relating to the currently selected appliance or group of appliances. Also shown is the total number of currently listed alerts for all managed appliances.

View the status of an appliance

You can find out whether an appliance is operating correctly or needs attention by viewing information in **Appliance Management**.

Task

1. Log on to McAfee ePO.
2. From the menu, select **Systems** → **Appliance Management**.
3. From the **Appliances** tree view, expand the list of appliances until you locate the appliance that you want to view.

Remove appliances from the Appliances tree

You can remove appliances from the **Appliances** tree when they are no longer needed.

The **Appliances** tree view in **Appliance Management** is a filtered view of the **System Tree**. Use the **System Tree** to remove a decommissioned appliance that is listed in the **Appliances** tree.

Note

You can't unregister McAfee Agent from an appliance, or from McAfee ePO.

Task

1. In McAfee ePO, click **System Tree** from the top icon bar.
2. Browse to and select the appliance to be removed.
3. Click **Actions** and select **Directory Management** → **Delete**.
4. Click **OK**.

What to do next

Note

If the selected appliance is still running and connected to the network, McAfee ePO adds the appliance back into the **System Tree** after the next agent-server communication.

The appliance management dashboard

The **Appliance Management** dashboard shows information about each McAfee DLP Prevent and McAfee DLP Monitor appliance in your network.

- In a McAfee DLP Prevent cluster environment, the system health card shows the tree view display of the cluster master and cluster scanners.
- In a McAfee DLP Monitor cluster environment, the system health card shows the tree view display of the single packet acquisition device, the cluster master, and two or more dedicated scanners.
- Indicators to show whether an appliance needs attention.
- Detailed information about any detected issues.

The information bar includes the appliance name, the number of currently reported alerts, and other information specific to the reported appliance.

Viewing McAfee DLP Prevent appliance health information in McAfee ePO

The McAfee DLP Prevent system health cards display information about appliance type, system health, email and web statistics, and the evidence queue.

System health cards display McAfee DLP Prevent appliances as **Prevent Server**, and each functioning appliance is shown as **Active**. An appliance can be one of the following types, depending on whether it is standalone or part of a cluster:

- **Prevent Server Standalone**
- **Prevent Server Cluster Master**
- **Prevent Server Cluster Scanner**

Status is displayed in green, amber, or red. The status color depends on whether warning and critical threshold values are exceeded, or there is an error. More information is provided in the **Alerts** and **Details** panes.

McAfee DLP Prevent statistics

In addition to standard system health information about each appliance or cluster of appliances, you can see the following information:

- **Evidence Queue** — Shows the number of evidence files waiting to be copied to evidence storage. If the total combined size of the items in the queue exceeds a threshold, an alert is issued. If the evidence server is unavailable because, for example, it can't be contacted, the evidence is queued until the server becomes available again.

  The evidence queue has between 20–200 GB storage available, Depending on the platform. If it becomes full, no further incidents are created, any further traffic is refused, and a failure response is issued. For SMTP traffic, this is a temporary failure response. For ICAP traffic, the response is a server failure error.

- **Emails (per minute)** — Shows the number of messages that were delivered, were permanently or temporarily rejected, or could not be analyzed.
  - A message might be temporarily rejected if, for example, the Smart Host is unavailable.
  - A message might be permanently rejected if, for example, the recipient address is incorrect or the Smart Host blocks the message.
- **Web Requests (per minute)** — Shows the number of web requests that the McAfee DLP Prevent appliance received, and the number it could not analyze.
- **Capture** — (Optional) The Capture statistics are visible when the DLP Capture feature is enabled on the appliance. Capture statistics includes:
  - The number of days remaining before the capture storage reaches its capacity
  - The age of the oldest captured item held in the storage
  - The number of searches currently in progress.
- **CPU** — Displays information about CPU usage: % busy, % system, % user, % idle.
- **Memory** — Displays information about memory used, swap use, and swap rate.
- **Disk** — Disk state is added for each filesystem. A non-zero value is a faulty state and will show different alerts based on different state values.
- **OCR Scan** — When OCR scanning is enabled, images to be scanned are held in a queue. When the queue size exceeds the threshold limit, McAfee DLP Prevent appliance ignores extra images until the number of pending OCR scans fall below the maximum queue size. This is done to avoid disruption to email and web traffic. When this situation arises, an alert and its details are displayed in the **Appliance Management** dashboard.

See the information about error messages to find out what happens if a message or web request is blocked. Apart from the evidence queue counter, the counters are not cumulative.

McAfee DLP Prevent alerts

If a system health status appears in amber or red, more information is provided in the **Alerts** and **Details** panes. McAfee DLP Prevent also provides alert information in the following circumstances.

- The evidence queue exceeded the default threshold.
- McAfee DLP Prevent could not enforce a policy.
- The virtual IP address that you assigned is not on the same subnet or network as the McAfee DLP Prevent appliance.
- McAfee ePO could not contact the McAfee DLP Prevent appliance (for example, if the power supply was interrupted).

An alert is not generated if the appliance was shut down manually.

- If the DLP Capture feature is enabled, alerts are issued when:
  - The Capture partition is corrupt.
  - The password to secure encrypted data needs to be changed.

Viewing McAfee DLP Monitor appliance health information in McAfee ePO

The McAfee DLP Monitor system health cards display information about appliance type, system health, and analysis statistics.

System health cards display McAfee DLP Monitor appliances as **Monitor Server**. Each functioning appliance is shown as **Active**. An appliance can be one of the following types, depending on whether it is configured as a standalone appliance or as a member of a cluster:

- **Monitor Server Standalone**
- **Monitor Cluster Packet Acquisition Device**
- **Monitor Cluster Master**
- **Monitor Cluster Scanner**

Status is displayed in green, amber, or red. The status color depends on whether warning and critical threshold values are exceeded, or there is an error. More information is provided in the **Alerts** and **Details** panes.

McAfee DLP Monitor statistics

In addition to the standard system health information about each appliance or cluster of appliances, you can see the following information:

- **Evidence Queue** — Shows the number of evidence files waiting to be copied to evidence storage.

  If the total combined size of the items in the queue exceeds a threshold, an alert is issued. If the evidence server is unavailable because, for example, it can't be contacted, the evidence is queued until the server becomes available again.

  The queue has between 20–200 GB storage available, depending on the platform. If it becomes full, no further incidents are created.

  This statistic does not apply to a packet acquisition device.

- **CPU** — Displays information about CPU usage: % busy, % system, % user, % idle.
- **Memory** — Displays information about memory used, swap use, and swap rate.

- **Disk** — Disk state is added for each filesystem. A non-zero value is a faulty state and will show different alerts based on different state values.
- **Network** — Displays the information about received and transmitted data. For **capture1**, the following details are displayed:
  - **Packets per second** — The number of packets processed by McAfee DLP Monitor standalone appliance or a cluster packet acquisition device every second.
  - **Packet drops** — The number of packets dropped at the network interface.
- **Monitor** — Monitors the following information (these statistics apply to a standalone appliance and a cluster packet acquisition device):
  - **Active flows** — The current number of conversations on your network tracked by the McAfee DLP Monitor appliance.
  - **Flows filtered** — The current number of conversations that are not scanned according to filter rules.
  - **Payloads scanned** — Displays the number of payloads analyzed by McAfee DLP Monitor for each protocol.
  - **Payload scan failure** — Displays the number of payloads that can't be analyzed if, for example, an email message is corrupt or the time to analyze the payload exceeds the timeout limit.
  - **Payloads oversize** — Displays the number of payloads that exceed the configured limit.

  McAfee DLP Monitor can't analyze partially extracted .zip files.
- **Capture** — (Optional) The Capture statistics are visible when the DLP Capture feature is enabled on the appliance. Capture statistics includes:
  - The number of days remaining before the capture storage reaches its capacity
  - The age of the oldest captured item held in the storage
  - The number of searches currently in progress.
- **OCR Scan** — When OCR scanning is enabled, images to be scanned are held in a queue. When the queue size exceeds the queue size limit, McAfee DLP Monitor appliance ignores extra images until the number of pending OCR scans fall below the maximum queue size. This is done to avoid disruption to email and web traffic. When this situation arises, an alert and its details are displayed in the **Appliance Management** dashboard.

Counters are updated on the appliance every 60 seconds. Apart from the evidence queue counter, the counters are not cumulative.

McAfee DLP Monitor alerts

- The evidence queue exceeded the default threshold.
- The payload could not be analyzed.
- McAfee DLP Monitor could not enforce a policy.
- The virtual IP address that you assigned is not on the same subnet or network as the McAfee DLP Monitor appliance.
- McAfee ePO could not contact the McAfee DLP Monitor appliance (for example, if the power supply was interrupted).

  An alert is not generated if the appliance was shut down manually.
- If the DLP Capture feature is enabled, alerts are issued when:
  - The Capture partition is corrupt.

- The password to secure encrypted data needs to be changed.

Appliance event reporting

McAfee DLP appliance event reporting

A number of McAfee DLP appliance events are available in the **Client Events** page and the **DLP Operations** page in McAfee ePO. You can get additional information from the on-box syslog and a remote logging server if you have one enabled. The **Client Events** page also displays Appliance Management events.

Client Events

Go to the **System Tree**, and select the appliance for which you want to see the events. Select **Actions**, then go to **Agent** → **Show Client Events**. Some events include reason codes that you can use to search log files.

Tip

Regularly purge the **Client Events** page to stop it becoming full.

Event ID	UI event text	Description
15001	**LDAP query failure**	The query failed. Reasons are provided in the event descriptions.
15007	**LDAP directory synchronization**	Directory synchronization status.
185001	**DLP scanning policy**	Policy scanning events with reason codes: • 197 - Unable to load policy. • 258 - Unable to load rules. • 982 - Failed to load configuration.
210003	**Resource usage reached critical level**	McAfee DLP Prevent can't analyze a message because the directory is critically full.
210900	**Appliance ISO upgrade success** **Appliance ISO upgrade failed** **Appliance downgrading to lower version**	Appliance upgrade events with reason codes: • 983 — Appliance ISO upgrade failed. Detailed logs can be found under /rescue/logs/. • 984 — Appliance ISO upgrade success. The appliance was successfully upgraded to a higher version.

Event ID	UI event text	Description
	Internal install image updated successfully **Failed to update internal install image**	• 985 — Appliance downgrading to lower version. This event is sent when the downgrade attempt is initiated. Upgrade success or failure events are sent after the upgrade is complete. If a clean upgrade or downgrade is requested, the success or failure event is sent after the McAfee ePO connection is established. Internal installation image updates using SCP events: • 986 — Internal installation image was updated successfully. • 987 — Failed to update the internal installation image.
220000	**User logon**	User log on events with reason codes: • 354 — GUI logon successful. • 355 — GUI logon failed. • 424 — SSH logon successful • 425 — SSH logon failed. • 426 — Appliance console logon successful. • 427 — Appliance console logon failed. • 430 — User switch successful. • 431 — User switch failed.
220001	**User logoff**	User log off events with reason codes: • 356 — GUI user logged off. • 357 — The session has expired. • 428 — The SSH user logged off. • 429 — The appliance console user logged off. • 432 — The user logged off.
220900	**Certificate Install**	• Certificate installation success • Certificate installation failed: <*reason*> A certificate might not get installed due to one of the following reasons: • Bad passphrase • No private key • Chain error • Bad certificate • Expired certificate • Not yet valid • Bad signature • Bad CA certificate

Event ID	UI event text	Description
		• Chain too long • Wrong purpose • Revoked • Bad or missing CRL The reason is also reported in the syslog. If the reason does not match any of the available reasons, it gives the default Certificate installation failed event.
240155	**Capture PII Deletion**	Personal data deletion succeeded.
244005	**Misconfigured McAfee Logon Collector**	McAfee Logon Collector client has invalid configuration.
244006	**Certificate rejected by MLC Server**	Certificate rejected by McAfee Logon Collector.
244007	**MLC client has started**	McAfee Logon Collector client has started.
244008	**MLC client has stopped**	McAfee Logon Collector client has stopped.
244009	**MLC client has been restarted**	McAfee Logon Collector client has restarted.
244010	**Invalid MLC certificate BER/DER data**	The certificate is not base64 encoded.
244011	**Illegal MLC Certificate footer**	The certificate footer is not valid.
244012	**Illegal MLC Certificate header**	The certificate header is not valid.
244013	**Extra data given to DerValue constructor**	SSL error using certificate file.
244014	**MLC**	McAfee Logon Collector synchronization complete.

Event ID	UI event text	Description
300000	**Channel Event**	Send a heartbeat signal to all channels.

DLP Operations events

Event ID	UI event text	Description
19100	**Policy Change**	Appliance Management successfully pushed a policy to the appliance.
19105	**Evidence Replication Failed**	• An evidence file could not be encrypted. • An evidence file could not be copied to the evidence server.
19400	**Policy Push Failed**	Appliance Management failed to push a policy to the appliance.
19401	**Analysis Failed**	• Possible denial-of-service attack. • The content could not be decomposed for analysis.
19402	**DLP Prevent Registered**	The appliance successfully registered with McAfee ePO.
19403	**DLP Monitor Registered**	The appliance successfully registered with McAfee ePO.

Using syslog entries to track and analyze messages

McAfee DLP appliances send protocol and hardware logging information to the local syslog, and one or more remote logging servers if you have them enabled. Examples of information sent to the syslog are certificate installation status and ICAP events.

Note

Use settings in the **General** category of the **Common Appliance** policy to set up remote logging servers. Use the TCP protocol to send McAfee DLP appliances events data to a remote logging server. UDP has a limit of 1024 bytes per packet so events that exceed that amount are truncated.

McAfee DLP appliances send information to the syslog in the Common Event Format (CEF). CEF is an open log management standard that improves the interoperability of security-related information from different security and network devices and applications. To simplify integration, syslog is used as a transport mechanism. This applies a common prefix to each message that contains the date and host name.

Syslog entries contain information about the device itself (the vendor, product name, and version), the severity of the event, and the date the event occurred.

Note

SMTP message events can include the sender and recipient, the subject, the source, and destination IP addresses. Every attempt to send a message results in at least one entry in the log. If the message contains content that violates a data loss prevention policy, another entry is added to the log. When two entries are added to the log, both entries contain the corresponding McAfeeDLPOriginalMessageID number.

For information about the description of fields that appear in syslog entries and event IDs, see KB93612.

Managing data

Collecting and managing data

Monitoring the system consists of gathering and reviewing evidence and events, and producing reports.

Incident and event data from the DLP tables in the McAfee ePO database is viewed in the **DLP Incident Manager** and **DLP Operations** pages or is collated into reports and dashboards. User information is collated on the **User Information** tab of the **DLP Operations** module, and can be exported to a .csv file.

Administrators review recorded events and evidence to determine when rules are too restrictive and cause unnecessary work delays, or when they are too lax and allow data leaks.

Edit server tasks

McAfee DLP uses the McAfee ePO **Server Tasks** to run tasks for McAfee DLP Discover and McAfee DLP appliances, DLP Incident Manager, DLP Operations, and DLP Case Management.

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 for incidents and events are:

- **DLP delete systems that were removed from ePO system tree**
- **DLP events conversion 9.4 and above**
- **DLP Import MVision Cloud Events**
- **DLP incident migration from 9.3.x to 9.4.1 and above**
- **DLP operational events migration from 9.3.x to 9.4.1 and above**
- **DLP Policy Conversion from 9.3.x to 9.4.100 and above**
- **DLP purge evidences**
- **DLP Purge History of Operational Events and Incidents**
- **DLP Send Email for Operational Events and Incidents**
- **DLP Set Reviewer for Operational Events and Incidents**

McAfee DLP server tasks for McAfee DLP Discover and McAfee DLP appliances are:

- **Detect Discovery Servers**
- **LDAPSync: Sync across users from LDAP**

In addition, the **Roll Up Data (Local ePO Server)** task can be used to roll up McAfee DLP incidents, operational events, or endpoint discovery data from selected McAfee ePO servers to produce a single report.

Consult the product guide for information about these tasks.

Task

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

   Tip

   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**.

Create a Purge events task

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

You can create purge tasks for the **Incident List**, data in-use incidents on the **History** list, or the **Operational Event List**.

Note

To optimize system performance, McAfee DLP automatically purges incidents from the live incidents list table when a million incidents are reached, starting with the oldest incidents.

Task

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

Results

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

Create an automatic mail notification task

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

Task

1. In McAfee ePO, under **Menu** → **Data Protection**, select **DLP Incident Manager** or **DLP Operations**.
2. Click the **Incident Tasks** or **Operational Events Tasks** tab.
3. Select an incident type from the drop-down list (**Incident Tasks** only), select **Automatic mail Notification** in the **Task Type** pane, then click **Actions** → **New Rule**.
4. Enter a name and optional description.
   Rules are enabled by default. You can change this setting to delay running the rule.
5. Select the events to process.
   - Process all incidents/events (of the selected incident type).
   - Process incidents/events since the last mail notification run.
6. (Optional) Do one of the following:
   - If you have saved a template, select it from the drop-down list.
   - If you do not have any saved templates, enter a name for the template in the **Save As** text box. When you have filled out all relevant fields (that is, all fields that you want to save as a template) click **Save**.
7. Select **Recipients**.

   Note

   This field is required. At least one recipient must be selected.
8. (Optional) Select **CC** recipients.
9. Enter a subject for the email.

   Note

   This field is required.

   You can insert variables from the drop-down list as required.
10. Enter the body text of the email.
    You can insert variables from the drop-down list as required.
11. (Optional) Select evidence information attached to the email.
    You can select any, all, or none of the options.
    - Attach CSV file with evidence list information
    - Attach decrypted evidence files, match-string HTML files, and incident details page
      - incident details page (HTML page)
      - decrypted evidence files
      - decrypted match-string HTML files
12. Select an email size limitation, or accept the default (5MB). Click **Next**.
13. Click **>** to add criteria, **<** to remove them. Set the **Comparison** and **Value** parameters. When you have finished defining criteria, click **Save**.

Results

The task runs hourly.

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

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. Do one of the following:
    - For McAfee DLP Endpoint: Select an incident type from the drop-down list (**Incident Tasks** only), select **Set Reviewer** in the **Task Type** pane, then click **Actions** → **New Rule**.
    - For McAfee DLP Discover: Select **Data at rest (Network)** from the drop-down list.
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**.

   Tip

   > If there are multiple **Set Reviewer** rules, reorder the rules in the list.

Results

The task runs hourly.

Note

> You cannot override the reviewer through the **Set Reviewer** task after the reviewer is set.

Monitor task results

Monitor the results of incident and operational event tasks.

Task

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

   Tip

   Enter `DLP` in the **Quick find** field or set a custom filter.
3. Click the name of the task.
   The details of the task appear, including any errors if the task failed.

Creating reports

Report types

Use the McAfee ePO reporting features to monitor performance.

Four types of reports are supported in McAfee ePO dashboards:

- DLP Incident summary
- DLP Endpoint discovery summary
- DLP Policy summary
- DLP Operations summary

The dashboards provide a total of 22 reports, based on the 28 queries found in the McAfee ePO console under **Menu** → **Reporting** → **Queries & Reports** → **McAfee Groups** → **Data Loss Prevention**.

Report options

McAfee DLP products use McAfee ePO Reports to review events. In addition, you can view information about product properties on the McAfee ePO Dashboard.

McAfee ePO Reports

McAfee DLP Endpoint software integrates reporting with the McAfee ePO reporting service.

McAfee ePO rollup queries and rolled up reports, which summarize data from multiple McAfee ePO databases, are supported.

McAfee ePO Notifications are supported.

ePO Dashboards

You can view information about McAfee DLP product properties in the McAfee ePO **Menu** → **Dashboards** page. These are the four predefined dashboards:

- DLP Incident summary
- DLP Endpoint discovery summary
- DLP Policy summary
- DLP Operations summary

You can edit and customize Dashboards and create monitors.

The predefined queries summarized in the Dashboards are available by selecting **Menu** → **Queries & Reports**. They are listed under **McAfee Groups**.

Create a data rollup server task

McAfee ePO rollup tasks draw data from multiple servers to produce a single report. You can create rollup reports for McAfee DLP operational events and incidents.

Task

1. In McAfee ePO, select **Menu** → **Automation** → **Server Tasks**.
2. Click **New Task**.
3. In the **Server Task Builder**, enter a name and optional note, then click **Next**.
4. From the **Actions** drop-down list, select **Roll Up Data**.
   The rollup data form appears.
5. (Optional) Select servers in the **Roll up data from** field.
6. From the **Data Type** drop-down list, select **DLP Incidents**, **DLP Operational Event**, or **McAfee DLP Endpoint Discovery**, as required.
7. (Optional) Configure the **Purge**, **Filter**, or **Rollup method** options. Click **Next**.
8. Enter the schedule type, start date, end date, and schedule time. Click **Next**.
9. Review the **Summary** information, then click **Save**.

DLP Help Desk

What is DLP Help Desk?

DLP Help Desk generates overrides that allow users to perform functions that are normally prohibited.

Quarantine release

McAfee DLP Endpoint discovery can quarantine local file system (Windows and Mac) or email storage files (Windows only) with sensitive content. To release the files from quarantine, the user must request a quarantine release code from the administrator.

Policy bypass

When there is a legitimate business case, a user can request permission to access or transfer sensitive information. The administrator can then grant permission for a limited time. When this is done, all sensitive information is monitored, rather than blocked, according to existing rules. Both the user and the system administrator receive messages about the bypass status when it is enabled and disabled. The user sees a pop-up message. The administrator sees an event entry in the **Operational Event List**.

Client uninstall

The McAfee DLP Endpoint client is protected from unauthorized removal. While it is typically uninstalled by an administrator using McAfee ePO, there are situations where you need to uninstall it in the field. When an administrator issues a release code (also known as a *challenge-response* key) you can remove the client using the standard Microsoft Windows or macOS functions or third-party uninstallers.

How override keys work

DLP Help Desk allows administrators to create release keys for situations outside the normal workflow.

McAfee DLP Endpoint uses a challenge-response mechanism to bypass security in special cases. When a situation affects multiple users, a different mechanism is applied.

Individual release keys

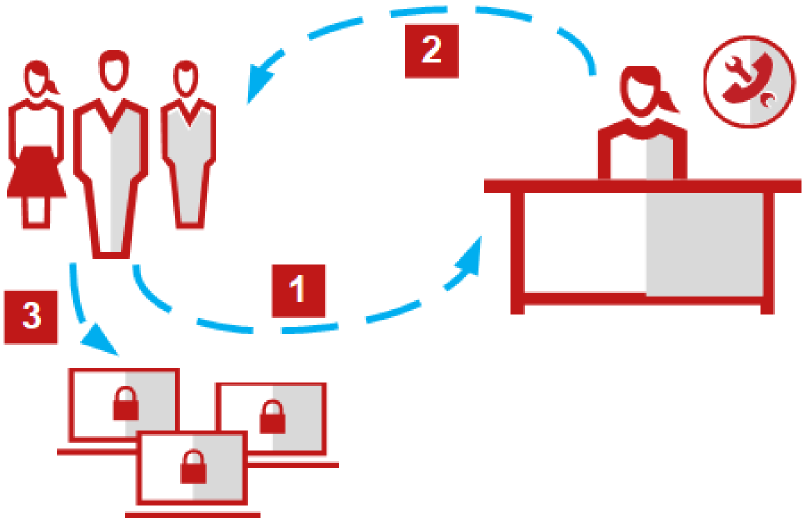
Examples of situations requiring an individual release key are:

- A user needs to release emails from quarantine to delete sensitive information.
- McAfee DLP Endpoint client needs to be uninstalled, but McAfee ePO can't be used because the computer is outside the corporate network.
- A user has a valid business reason to perform a one-time operation that a security policy is blocking.

Challenge-response protocol

The endpoint user opens the **Tasks** tab in the McAfee DLP Endpoint console where an Identification Code (*the challenge*) and Policy Revision information are displayed. This information is specific to the McAfee DLP Endpoint client computer requesting the override.

1. The user sends the ID code and policy revision number to an administrator, typically by text message, phone, or email.
2. The administrator enters the information provided in the DLP Help Desk console, and generates a Release Code (*the response*), and sends it to the user.
3. The user enters the release code in the appropriate text box and continues with the release, bypass, or uninstall task.



Multiple user release keys

Release keys generated with a master release code are not keyed to the entry of a challenge code generated by a specific McAfee DLP Endpoint client. Rather, they can be used by any computer in the network. To prevent misuse, they are time-limited and must be applied within 60 minutes of being generated. Master release keys can be generated with standard or strengthened security. The administrator selects the security level on the **DLP Settings** → **Advanced** page. Only more recent versions of McAfee DLP Endpoint support the secured master release code. It must not be used with unsupported versions. See KB90417 for information about supported versions.

Understanding revision numbers

Revision numbers are automatically assigned to policies, and are used for troubleshooting and DLP Help Desk override key creation.

All DLP Help Desk functions create release codes using revision numbers, referred to in the UI as **Revision ID**. For bypass release codes, using the revision number is optional, but it is the default setting.

When an administrator creates a policy in McAfee DLP the policy is assigned the revision number 1. This number is incremented each time the policy is changed. In addition to being used for requesting a bypass or uninstall key, the revision number is important for supporting troubleshooting processes, to ensure that policy changes are actually applied to the endpoints.

Locating the revision number

	Location of revision number information
McAfee ePO	DLP Policy Manager, on the **Policy Assignment** tab
on the endpoint	• McAfee DLP Endpoint for Windows — endpoint console, **Tasks** tab • McAfee DLP Endpoint for Mac — endpoint console **Data Loss Prevention** page

Create override keys

An administrator generates an override key for each challenge key request. Alternately, you can generate a master release code when multiple computers are involved.

All override keys require similar entries. The following differences should be noted:

Task

1. In McAfee ePO, select **Menu** → **Data Protection** → **DLP Help Desk**.
2. Select a key type.
3. Fill in the required (and optional) fields.
   Filling in all required fields activates the **Generate Key** button.
4. Generate the release code and send it to the user.

DLP Help Desk page

Use this page to set up an override key request.

Option definitions

Option	Definition
Key Type	Selects the type of key from a drop-down list. **Options:** • Client bypass key • Release from quarantine key • Uninstall key
End user name *	Text field for user name.
End user email address *	Text field for user email address.
End user computer name	Text field for user computer name
Request details (Business reason)	Text field for business reason for the key.
Client bypass password	Provides two options for bypass password: • Policy name and revision number • Manual entry
Identification code *	Provides two options for identification code: • Challenge code generated by the McAfee DLP Endpoint client and supplied by the user when requesting an override key • Master release code
Release code	Click **Generate Key** to generate a release code. The button is not available until all required fields are filled in.
Bypass duration	Selects the override duration from a drop-down list. Option varies from 5 minutes to 30 days.

* indicates required fields

Diagnostics

Diagnostic tool

Diagnostic Tool

The Diagnostic Tool is designed to aid troubleshooting McAfee DLP Endpoint problems on Microsoft Windows endpoint computers. It is not supported on OS X computers.

The Diagnostic Tool gathers information on the performance of client software. The IT team uses this information to troubleshoot problems and tune policies. When severe problems exist, it can be used to collect data for analysis by the McAfee DLP development team.

The tool is installed with the McAfee DLP Endpoint client software package. It consists of seven tabbed pages, each devoted to a different aspect of McAfee DLP Endpoint software operation.

Note

On all pages displaying information in tables (all pages except **General information** and **Tools**), you can sort the tables on any column by clicking the column header.

General information	Collects data such as whether the agent processes and drivers are running and general policy, agent, and logging information. Where an error is detected, information about the error is presented.
DLPE Modules	Displays the agent configuration (as shown in the McAfee DLP Endpoint policy console as the **Agent Configuration** → **Miscellaneous** page). It shows the configuration setting and status of each module, add-in, and handler. Selecting a module displays details that can help you determine problems.
Data Flow	Displays the number of events and the memory used by the McAfee DLP Endpoint client, and displays event details when a specific event is selected.
Tools	Allows you to perform several tests and displays the results. When necessary, a data dump is performed for further analysis.
Process list	Displays all processes currently running on the computer. Selecting a process displays details and related window titles and application definitions.

Devices	Displays all Plug and Play and removable devices currently connected to the computer. Selecting a device displays details of the device and related device definitions. Displays all active device control rules and relevant definitions from the device definitions.
Active policy	Displays all rules contained in the active policy, and the relevant policy definitions. Selecting a rule or definition displays the details.

Checking the agent status

Use the General information tab to get an overview of the agent status.

The information on the General information tab is designed to confirm expectations and answer basic questions. Are the agent processes and drivers running? What product versions are installed? What is the current operation mode and policy?

Agent processes and drivers

One of the most important questions in troubleshooting is, "Is everything running as expected?" The **Agent processes** and **Drivers** sections show this at a glance. The checkboxes show if the process is enabled; the colored dot shows if it is running. If the process or driver is down, the text box gives information on what is wrong.

The default maximum memory is 150 MB. A high value for this parameter can indicate problems.

Agent processes

Term	Process	Expected status
Fcag	McAfee DLP Endpoint agent (client)	enabled; running
Fcags	McAfee DLP Endpoint agent service	enabled; running
Fcagte	McAfee DLP Endpoint text extractor	enabled; running
Fcagwd	McAfee DLP Endpoint watch dog	enabled; running
Fcagd	McAfee DLP Endpoint agent with automatic dump	enabled only for troubleshooting.

Drivers

Term	Process	Expected status
Hdlpflt	McAfee DLP Endpoint minifilter driver (enforces removable storage device rules)	enabled; running
Hdlpevnt	McAfee DLP Endpoint event	enabled; running
Hdlpdbk	McAfee DLP Endpoint device filter driver (enforces device Plug and Play rules)	can be disabled in configuration
Hdlpctrl	McAfee DLP Endpoint control	enabled; running
Hdlhook	McAfee DLP Endpoint Hook driver	enabled; running

Agent info section

Operation mode and **Agent status** are expected to match. The **Agent Connectivity** indication, together with **EPO** address, can be useful in troubleshooting.

Note

> **Agent Connectivity** has three options: online, offline, or connected by VPN.

Run the Diagnostic Tool

The Diagnostic Tool utility provides IT teams with detailed information on the agent status.

Before you begin

Diagnostic Tool requires authentication with McAfee® Help Desk.

Task

1. Double-click the hdlpDiag.exe file.
   An authentication window opens.
2. Copy the Identification Code to the Help Desk **Identification Code** text box on the **Generate DLP Client Bypass Key** page. Fill in the rest of the information and generate a Release Code.
3. Copy the Release Code to the authentication window **Validation Code** text box and click **OK**.
   The diagnostic tool utility opens.

What to do next

Note

The **General Information**, **DLPE Modules**, and **Process List** tabs have a **Refresh** button in the lower right corner. Changes that occur when a tab is open do not update information automatically on these tabs. Click the **Refresh** button frequently to verify that you are viewing current data.

Tuning policies

The Diagnostic Tool can be used to troubleshoot or tune policies.

Use case: High CPU usage

Users are sometimes plagued by slow performance when a new policy is enforced. One cause might be high CPU usage. To determine this, go to the **Process List** tab. If you see an unusually large number of events for a process, this could be the problem. For example, a recent check found that *taskmgr.exe* was classified as an **Editor**, and had the second highest number of total events. It is quite unlikely that this application is leaking data, and the McAfee DLP Endpoint client does not need to monitor it that closely.

To test the theory, create an application template. In the Policy Catalog, go to **DLP Policy** → **Settings** and set an override to **Trusted**. Apply the policy, and test to see if performance has improved.

Use case: Creating effective content classification and content fingerprinting criteria

Tagging sensitive data lies at the heart of a data protection policy. Diagnostic Tool displays information that helps you design effective content classification and content fingerprinting criteria. Tags can be too tight, missing data that should be tagged, or too loose, creating false positives.

The **Active Policy** page lists classifications and their content classification and content fingerprinting criteria. The **Data Flow** page lists all tags applied by the policy, and the count for each. When counts are higher than expected, false positives are suspected. In one case, an extremely high count led to the discovery that the classification was triggered by Disclaimer text. Adding the Disclaimer to the whitelist removed the false positives. By the same token, lower than expected counts suggest a classification that is too strict.

If a new file is tagged while the Diagnostic Tool is running, the file path is displayed. in the details pane. Use this information to locate files for testing.

Troubleshoot high CPU usage

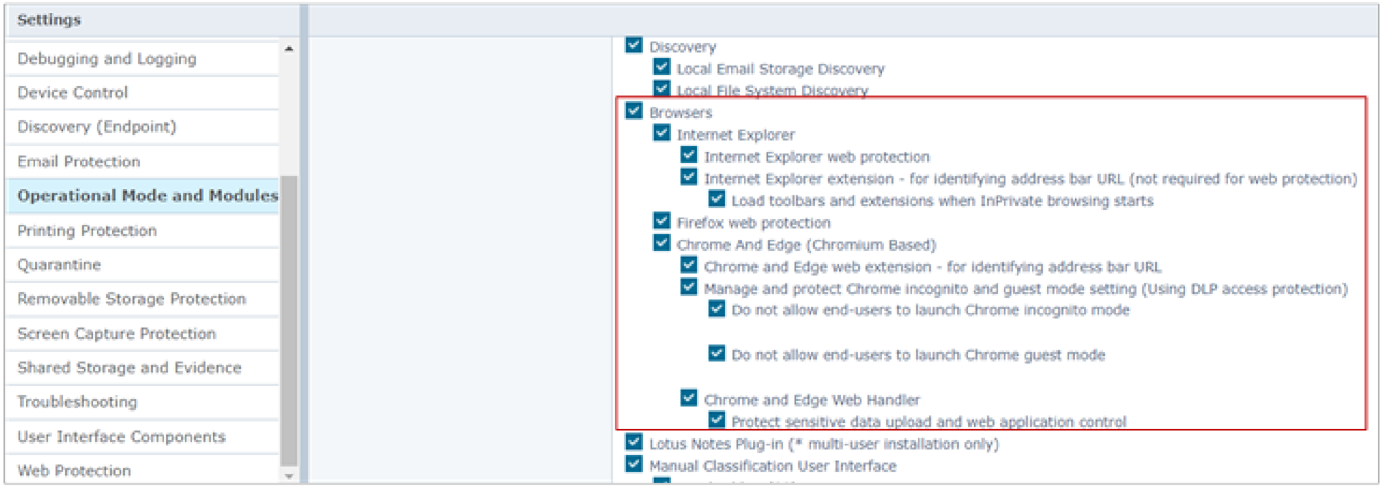
Determine the source of high CPU usage.

An analysis of customer reports of high CPU usage by the McAfee DLP Endpoint client (fcag.exe) has shown that many cases are due to one of two root causes:

- Detection of the browser address bar URL.
- Specific applications that are opening a large number of files for read purposes.

Task

1. In **Policy Catalog**, create a new Windows client configuration.
   Duplicate a policy that has a problem with CPU usage.
2. In the **Browsers** section of the **Operational Modes and Modules** page, deselect web protection for the browser you want to test.



☑ Discovery
  ☑ Local Email Storage Discovery
  ☑ Local File System Discovery
☑ Browsers
  ☑ Internet Explorer
    ☑ Internet Explorer web protection
    ☑ Internet Explorer extension - for identifying address bar URL (not required for web protection)
      ☑ Load toolbars and extensions when InPrivate browsing starts
  ☑ Firefox web protection
  ☑ Chrome And Edge (Chromium Based)
    ☑ Chrome and Edge web extension - for identifying address bar URL
    ☑ Manage and protect Chrome incognito and guest mode setting (Using DLP access protection)
      ☑ Do not allow end-users to launch Chrome incognito mode
      ☑ Do not allow end-users to launch Chrome guest mode
    ☑ Chrome and Edge Web Handler
      ☑ Protect sensitive data upload and web application control
☑ Lotus Notes Plug-in (* multi-user installation only)
☑ Manual Classification User Interface

3. Apply the policy to a small set of computers.
   If the issue is resolved, apply the client configuration to other systems.

Results

Disabling browser address bar URL detection doesn't affect web protection, and doesn't affect web application awareness in web post protection rules, but it does affect web application awareness in the following rules:

- **Clipboard protection** — You can't create rules that block copy/pasting text from a specific web application page.
- **Network share protection** — You can't create rules that block saving a file or web page from a specific web application page to a network share.
- **Printing protection** — You can't block printing from specific web applications.
- **Removable storage protection** — You can't block saving files from a specific web application page.
- **Screen capture protection** — You can't block screen shots when a specific web application page is visible on screen.
- **Web application content fingerprinting** — You can't configure fingerprinting criteria to fingerprint files downloaded from a specific web application page.

In all of these cases, the browser address bar URL is required to identify the specific web-application.

Appliance maintenance and troubleshooting

Monitoring dropped packets on a virtual appliance

Dropped packets are not reported in the **System Health** card in the **Appliance Management** dashboard. You can get information about them from the virtual application instead.

Task

1. Log on to the VMware ESXi or VMware ESX host, or the vCenter Server using the vSphere Client.
2. Select the VMware ESXi or ESX host in the inventory list.
3. Select the virtual appliance and click the **Performance** tab.
4. Click **Advanced** → **Chart Options**.
5. Select **Network** → **Real-time**.
6. Enable the **Transmit packets dropped** and **Receive packets dropped** counters and click **Apply**.

McAfee DLP Prevent appliance does not accept email

If a Smart Host is not configured, McAfee DLP Prevent appliance can't accept email messages because it has nowhere to send them to.

McAfee DLP Prevent issues a *451 System problem: retry later. (No SmartHost has been configured)* error, and closes the connection.

Tip

You can check whether McAfee DLP Prevent can accept email using telnet. If the appliance is correctly configured, you get a 220 welcome message:
220 host.domain.example PVA/SMTP Ready

To resolve a connection issue, you must:

Task

1. Install the required extensions in McAfee ePO.
2. Register the appliance with a McAfee ePO.
   Follow the steps in the Setup Wizard help.
3. Configure at least one DNS server in the **Common Appliance Management** policy.
4. Configure a Smart Host in the **McAfee DLP Prevent Email Settings** policy category.
5. Apply a McAfee Data Loss Prevention policy.
   See the policy assignment section in the *McAfee ePolicy Orchestrator Product Guide*.

Purge appliance data from the McAfee ePO

To enable the smooth running of your McAfee appliances, you should periodically perform some maintenance tasks.

Appliances managed by the Appliance Management extension send usage and system information that is stored in the McAfee ePO database.

Tip

Allow the scheduled **Purge Appliance Management Historical Data** task to run as defined, to prevent the database becoming too large.

Replace the default certificate

You can replace the default McAfee DLP appliance self-signed certificate with the certificate issued by a certificate authority (CA) or an intermediate CA so that other hosts on the network can validate the appliance's SSL certificate.

Before you begin

SSH must be enabled.

To replace the certificate, you can either:

- Upload a new certificate and private key.
- Download a certificate signing request (CSR) from the appliance, have it signed by a CA, and upload the certificate that the CA gives you.

Tip

Downloading a CSR from the appliance ensures that the appliance's private key can't be inadvertently exposed.

Only ECDSA and RSA certificates and keys are allowed in the uploaded file. The certificate must be suitable for use as both a TLS server and a TLS client and the upload must include the whole certificate chain. Uploads can be in the following formats:

- PEM (Base64) — Certificate chain and private key or certificate chain only
- PKCS#12 — Certificate chain and private key
- PKCS#7 — Certificate chain only

If the upload format is PKCS#12 or PKCS#7, the correct file endings must be used:

- PKCS#12 must have the file ending .p12 or .pfx.
- PKCS#7 must have the file ending .p7b.

The certificate might fail to get installed if:

- The certificate is not usable for its intended role.

- The certificate has expired.
- The uploaded file does not contain the CA certificates that it needs to verify it.
- The certificate uses an unsupported public key algorithm, such as DSA.

If installation fails, detailed information is available in the appliance syslog. To view it, log on to the appliance console, select the **Shell** option, and type `$ grep import_ssl_cert /var/log/messages`.

Task

1. In a browser, go to https://APPLIANCE:10443/certificates/ and select one of the CSR links for download.
   Two files are available: one contains an RSA public key (the file ending in .rsa.csr) and the other contains an ECDSA public key (the file ending in .ec.csr).
2. Follow your CA's instructions to get the request signed.
3. Use an SCP client, such as winscp, to copy the root CA and any intermediate CA certificates used to sign the appliance certificate to the `/home/admin/upload/cacert` directory on the appliance.
   You can see whether the installation succeeded or failed in the **Client Events** page.

   Note

   CA certificate and intermediate CA certificates must be imported before importing the appliance certificate.

4. Use an SCP client, such as winscp, to copy the signed appliance certificate to the `/home/admin/upload/cert` directory on the appliance.
   You can see whether the installation succeeded or failed in the **Client Events** page.

Results

The file gets installed automatically.

Regenerate the appliance's private key

You can regenerate the private key if it was compromised, or if you need to renew a certificate that was signed externally.

Task

1. Log on to the appliance console.
2. Select the **Shell** option.
3. Type `sudo /opt/NETAwss/mgmt/make_ssl_cert`.
   The appliance's private key, self-signed certificate, and certificate signing requests are renewed.

What to do next

If the appliance was using a certificate that was signed externally, you must upload a signed certificate again.

Configuration backups

In McAfee DLP, you can create backups of your configuration data that can be restored. Backup tasks are run as needed from the backend, and cannot be scheduled.

The following components are included in a McAfee DLP backup.

- The SQL database
- The installed extensions
- Keys for McAfee ePO agent-server communication and the repositories
- All products that have been checked in to the Master Repository
- The server configuration settings for Apache, the SSL certificates needed to authorize the server to handle agent requests, and console certificates

To create a backup of your McAfee ePO server and configuration, see KB66616.

McAfee DLP appliance configuration backups

You can create backups of your McAfee DLP appliance configuration settings if you need to refer to the configuration settings in future.

Task

1. In the McAfee ePO menu, select **Policy** → **Policy Catalog**.
2. On the **Policy Catalog** page, select **DLP Appliance Management <version>** from the **Products** drop-down list.
3. On McAfee ePO 5.9 and earlier, select **All** from the **Category** drop-down list.
    a. Click **Export** from **Product policies**, to back up the configuration settings. **OR**
4. On McAfee ePO 5.10, select **New Policy** → **Export**.
5. From the **Export** page, download and save each file.
6. On the **Policy Catalog** page, select **Common Appliance Management <version>** from the **Product** drop-down list.
7. Repeat steps 3 through 5 to back up the Common Appliance Management settings.

What to do next

When you reinstall the appliance, use the **Import** option to reuse the McAfee DLP appliance configuration settings.

- On McAfee ePO 5.10, select **New Policy** → **Import**.
- On McAfee ePO 5.9 and earlier, select **Product Policies** → **Import**.

Error messages

If the appliance is not configured correctly, it tries to identify the problem and sends a temporary or permanent failure message.

The text in parentheses in the error message provides additional information about the problem.

Some error messages relay the response from the Smart Host so the McAfee DLP Prevent response contains the IP address, which is indicated by x.x.x.x.

For example, 442 192.168.0.1 : Connection refused indicates that the Smart Host with the address 192.168.0.1 did not accept the SMTP connection.

Temporary failure messages

Text	Cause	Recommended action
451 (The system has not been registered with an ePO server)	The initial setup was not completed.	Register the appliance with a McAfee ePO server using the **Graphical Configuration Wizard** option in the appliance console.
451 (No DNS servers have been configured)	The configuration applied from McAfee ePO did not specify any DNS servers.	Configure at least one DNS server in the **General** category of the **Common Appliance** policy.
451 (No Smart Host has been configured)	The configuration applied from McAfee ePO did not specify a Smart Host.	Configure a Smart Host in the **McAfee DLP Prevent Email Settings** policy category.
451 (Policy OPG file not found in configured location)	The policy configuration applied from McAfee ePO was incomplete.	• Confirm that the **Data Loss Prevention** extension is installed. • Configure a **Data Loss Prevention** policy. • Contact technical support. The configuration OPG file must be applied with the policy OPG file.
451 (Configuration OPG file not found in configured location)	The configuration applied from McAfee ePO was incomplete.	• Ensure that the **Data Loss Prevention** extension is installed. • Configure a **Data Loss Prevention** policy.

Text	Cause	Recommended action
		• Contact Technical Support. The configuration OPG file must be applied with the policy OPG file.
451 (LDAP server configuration missing)	This error occurs when both these conditions are met: • McAfee DLP Prevent contains a rule that specifies a sender as a member of an LDAP user group. • McAfee DLP Prevent is not configured to receive group information from the LDAP server that contains that user group.	Check that the LDAP server is selected in the **Users and Groups** policy category.
451 (Error resolving sender based policy)	A policy contains LDAP sender conditions, but can't get the information from the LDAP server because: • McAfee DLP Prevent and the LDAP server have not synchronized. • The LDAP server is not responding.	Check that the LDAP server is available.
451 (FIPS test failed)	The cryptographic self-tests required for FIPS compliance failed	Contact technical support.
451 (Unable to verify data against the registered document server)	The registered documents server is unavailable.	Check your configuration to confirm that the server is available, and the details you entered are correct.
442 x.x.x.x: Connection refused	McAfee DLP Prevent could not connect to the Smart Host to send the message, or the connection to Smart Host was dropped during a conversation.	Check that the Smart Host can receive email.

Permanent failure messages

Error	Cause	Action
530 Authentication required	MTA doesn't send AUTH credentials.	Configure MTA to send AUTH LOGIN credentials.
530 Authentication required - AUTH conversation is required for onward delivery	The Smart Host doesn't present AUTH as part of its response to the McAfee DLP Prevent appliance's EHLO request.	Configure the Smart Host to send AUTH LOGIN credentials.
504 Error: Supported authentication mechanism unavailable for onward delivery	The Smart Host doesn't support the LOGIN mechanism for authentication.	The Smart Host must support the LOGIN mechanism for authentication.
550 Host / domain is not permitted	McAfee DLP Prevent refused the connection from the source MTA.	Check that the MTA is in the list of permitted hosts in the **McAfee DLP Prevent Email Settings** policy category.
550 x.x.x.x: Denied by policy. TLS conversation required	The Smart Host did not accept a STARTTLS command but McAfee DLP Prevent is configured to always send email over a TLS connection.	Check the TLS configuration on the host.

ICAP error messages

Error	Cause	Action
500 (Unable to verify data against the registered document server)	The registered documents server is unavailable.	Check your configuration to confirm that the server is available, and the details you entered are correct.
500 (LDAP server configuration missing)	This error occurs when both these conditions are met: • McAfee DLP Prevent contains a rule that specifies an end-user as a member of an LDAP user group.	Check that the LDAP server is selected in the **Users and Groups** policy category.

Error	Cause	Action
	• McAfee DLP Prevent is not configured to receive group information from the LDAP server that contains that user group.	
500 (Error resolving end-user based policy)	A policy contains LDAP sender conditions, but can't get the information from the LDAP server because: • McAfee DLP Prevent and the LDAP server have not synchronized. • The LDAP server is not responding.	Check that the LDAP server is available.

Troubleshooting evidence copy failures

Evidence copy can fail because of incorrect configurations, lack of storage space, or loss of network connectivity.

- Cause1 — Incorrectly specified evidence share: The evidence share is incorrectly specified in the **Default Evidence Storage** of McAfee DLP **General Settings**. If the share location (UNC) is misconfigured, the agent can't upload evidence files.
- Cause 2 — Evidence share has run out of disk space: The evidence share on the McAfee ePO server has run out of disk space.
- Cause 3 — Loss of network connectivity: Due to loss of network connectivity between the appliance and the share or between ePO and the share.

Cause 1: Incorrectly specified evidence share

Solution: Verify the evidence share configuration

To verify the evidence share configuration in **Policy Catalog**:

1. Log on to McAfee ePO
2. Select **Policy Catalog** → **Data Loss Prevention <version>** → **Server Configuration** → **My Default Server Configuration**.
3. Click **Evidence Copy Service** and verify the configuration.

To verify the evidence share configuration in **DLP Settings**:

1. Log on to McAfee ePO.
2. Select **Data Protection** → **DLP Settings**.
3. On the General Settings page, in the **Default Evidence Storage** section, verify the **Storage Share (UNC)** path provided.

To verify the evidence path against the share on the McAfee ePO server, view the properties of the directory and click the **Sharing** tab. The UNC path for the evidence share is the correct display for **Network Path**.

Cause 2: Evidence share has run out of disk space

Solution: Free up the disk space on the drive where the evidence share was created.

Cause 3: Loss of network connectivity

Solution: Make sure that the share is reachable from McAfee ePO and the appliance.

To verify if the share is reachable from McAfee ePO:

1. Select **Data Protection** → **DLP Settings** → **General**.
2. In the **Default Evidence Storage** section, add the correct Storage Share (UNC) path.
3. Click **Test Credential**.

To test the connectivity from the appliance:

1. Log on to the appliance `ssh <appliance>`.
2. Run `scm mash`
3. Go to **MER and Diagnostic tests**.
4. Click **Evidence share tests**.
5. Select the required test to see if connection is successful.

Troubleshooting and maintenance

Use the appliance console for general maintenance tasks such as changing network settings and performing software updates.

Troubleshooting options, sanity checks, and error messages are available to help you identify and resolve problems with appliances.

Troubleshooting tips

Use this information to identify and troubleshoot issues with installing, registering, using, and maintaining McAfee DLP.

The appliance failed to register with McAfee ePO

Verify that the network connection is working, and any static routes that you created are correct. Ping the default gateway and McAfee ePO from the appliance console to test your network connection.

ⓘ **Important**

> If the registration continues to fail, call Technical Support. Do not try to register again.

You can verify the connection status for all your physical and virtual appliances using the **Appliance Management** feature in McAfee ePO.

To restore a failed connection, open the **System Tree** and select the appliance that has lost the connection. Then select **Action** → **Agent** → **Wake Up Agents** and click **OK**.

Registration failures

Registration events are available from the **DLP Operations** log in McAfee ePO.

Event ID	UI event text	Description
19402	**DLP Prevent Registered**	The appliance successfully registered with McAfee ePO.

Event ID	UI event text	Description
19403	**DLP Monitor Registered**	The appliance successfully registered with McAfee ePO.

No events are sent if the appliance is not registered. You can get more information from /var/log/messages.

Email delivery issues

If an email is not delivered, verify whether it is blocked by a McAfee DLP Prevent. Go to the **DLP Incident Manager** in McAfee ePO to verify if there is any corresponding incident for the message.

If email notification is configured in McAfee ePO as a **Reaction**, the sender is notified.

Verify if the Smart Host can receive email, if:

- McAfee DLP Prevent appliance could not connect to the Smart Host to send the message.
- The connection to Smart Host was dropped during a conversation.

Email rejection issues

If a Smart Host is not configured, the McAfee DLP Prevent appliance can't accept email messages because it has nowhere to send them to.

Web Gateway and McAfee DLP Prevent ICAP issues

Verify the **McAfee DLP Web Settings** category settings in **DLP Appliance Management** in **Policy Catalog**. McAfee DLP Prevent processes ICAP and ICAPs traffic based on selected services from secure ICAP, unencrypted.

If neither is selected, the ICAP server on the McAfee DLP Prevent appliance does not accept any connection.

If only secure ICAP is enabled, make sure that the ICAP client is ICAPs capable.

You can select the modes where McAfee DLP Prevent appliance can operate for the ICAP traffic from REQMOD and RESPMOD. If any mode is deselected, that traffic is ignored by the McAfee DLP Prevent appliance and is not processed. REQMOD and RESPMOD can't be disabled at the same time.

LDAP and Logon Collector issues

If there are communication issues between the appliance and the Active Directory while querying user information:

- Verify the Active Directory credentials configured on McAfee ePO.
- If SSL is selected, verify that Active Directory accepts secure connections.

If you configured Active Directory to use **Global Catalog** ports, check that at least one of these attributes is replicated to the **Global Catalog** server from the domains in the forest:

- Proxy addresses
- Mail

If an appliance needs to use NTLM authentication for ICAP traffic, these LDAP attributes must also be replicated:

- configurationNamingContext
- netbiosname
- msDS-PrincipalName

For Logon Collector, verify the Logon Collector certificate in the appliance.

Extension installation failures

- Dependency issues — There might be a dependency issue if the following extensions are missing:
  - Common UI package
  - Appliance Management Extension
  - Data Loss Prevention Management Extension
- Upgrade issues — the following error occurs if you install the same version or earlier version of the extension: *Can't upgrade the extension dlp-prevent-server-app to <version x.x.x.x > because <version x.x.x.x> is already installed.*

Policy push failures

Policy push events are also available from the **DLP Operations** log in McAfee ePO.

If policy push fails, details can be obtained from the appliance at /wk/mca/ ame_policy_DLPPS___1000_error.log

System health

The **Appliance Management** dashboard in McAfee ePO provides information to manage your appliances, view system health status, and get detailed information about alerts.

System health show status of:

- Evidence Queue
- Email and web requests (McAfee DLP Prevent)
- Packet analysis (McAfee DLP Monitor)
- CPU usage
- Memory
- Disk

- Network

Displays errors or warnings that relate to:

- System health
- Evidence queue size
- Policy enforcement
- Communication between McAfee ePO and appliances.

Viewing client events

Issues with user, LDAP, or certificate installation are listed in the **Client Events** page.

1. In McAfee ePO, go to the **System Tree**.
2. Select the checkbox next to the appliance.
3. Select **Actions**, then go to **Agent** → **Show Client Events**.

Incidents are not showing in the DLP Incident Manager

1. Use the Remote Desktop Protocol (RDP) to access McAfee ePO.
2. Go to **Services**.
3. Confirm that the McAfee ePO **Event Parser** is running. If it has stopped or paused, restart it to resolve the issue.

Setting up remote log servers

Logging information is sent to the local syslog, and one or more remote logging servers if you have them enabled. Syslog entries contain information about the device itself (the vendor, product name, and version), the severity of the event, and the date the event occurred. Use **Logging** settings in the **General** category of the **Policy Catalog** → **Common Appliance Management** policy to set up remote logging servers.

Create a Minimum Escalation Report (MER)

Create a Minimum Escalation Report to provide the Technical Support the information they need to diagnose a problem with McAfee DLP.

You can download the Minimum Escalation Report. Up to five reports can be available at any one time, and each is deleted after 24 hours. If another report is generated, the oldest report is deleted. It can take several minutes to generate a Minimum Escalation Report, and the file is several megabytes in size.

The report contains information such as hardware logs, software versions, disk and memory usage, network and system information, open files, active processes, process I/O, IPC, log files, status counters, reporting, internal install image details, and the results of various system tests. It also provides information about DLP Capture and metadata related to its search tasks.

Note

> The report does not contain details of evidence or hit highlight information.

Task

1. Log on to the appliance with administrator credentials.
   The general console menu opens.
2. Use the down arrow key to select **Generate MER**.
3. Type a password that McAfee Support can use to open the MER, and use the arrow key to move to the password confirmation field.
4. Press **ENTER** to start generating the report.
   When the report is ready, you receive notification of the URL (https://<*APPLIANCE*>:10443/mer) that you can download the report from.
5. Browse to the URL, and select the Minimum Escalation Report that you want to download.
6. Follow instructions from McAfee support to send the report.

   ⓘ **Important**

   When you create a Minimum Escalation Report, specify a password to secure the report. Remember to include the password when you send the report to McAfee support if you set one.

Appendix

Glossary

McAfee DLP terminology

Term	Definition
Action	What a rule does when content matches the definition in the rule. Common examples of actions are block, encrypt, or quarantine.
Crawling	Retrieving files and information from repositories, file systems, and email. Applicable to McAfee DLP Endpoint (Discovery)
Classification	Used to identify and track sensitive content and files. Can include content classifications, content fingerprints, registered documents, and whitelisted text.
Content classification	A mechanism for identifying sensitive content using data conditions such as text patterns and dictionaries, and file conditions such as document properties or file extensions.
Content fingerprinting	A mechanism for classifying and tracking sensitive content. Content fingerprinting criteria specify applications or locations, and can include data and file conditions. The fingerprint signatures remain with sensitive content when it is copied or moved.
Data vector	A definition of content status or usage. McAfee DLP protects sensitive data when it is stored (data at rest), as it is used (data in use), and when it is transferred (data in motion).
Definition	A configuration component that makes up a classification.
Discover server	The Windows Server where the McAfee DLP Discover software is installed. You can install multiple Discover servers in your network.
DLP Server	A McAfee DLP Discover server that has the server role set to DLP Server. DLP Servers are used to store the registered document database. You can also configure DLP Server as a proxy server to copy evidence files to the evidence file share in scenarios where the McAfee DLP appliance doesn't have direct access to the evidence file share.

Term	Definition
Device class	A collection of devices that have similar characteristics and can be managed in a similar manner. Device classes apply to Windows computers only, and can have the status Managed, Unmanaged, or Whitelisted.
File information	A definition that can include the file name, owner, size, extension, and date created, changed, or accessed. Use file information definitions in filters to include or exclude files to scan.
Fingerprinting	A text extraction procedure that uses an algorithm to map a document to signatures. Used to create registered documents and for content fingerprinting.
FIPS compliancy	Cryptographic software is configured and used in a way that is compliant with Federal Information Processing Standard 140-2.
Managed devices	A device class status indicating that Device Control manages the devices in that class.
Match string	The found content that matches a rule.
MTA	Message Transfer Agent or Mail Transfer Agent Software that transfers electronic mail messages from one computer to another using a client–server application architecture.
Path	A UNC name, IP address, or web address. McAfee DLP Endpoint (Discovery)
Policy	A set of definitions, classifications, and rules that define how the McAfee DLP software protects data.
Redaction reviewer	Allows confidential information in the DLP Incident Manager and DLP Operations consoles to be redacted to prevent unauthorized viewing.
RegDoc package	A package of fingerprint data produced by a McAfee DLP Discover registration scan. RegDoc packages are stored in a registration server (DLP Server) database and can be called by McAfee DLP Discover scans or McAfee DLP Monitor and McAfee DLP Prevent policies using REST API calls.
Registered documents	Pre-scanned files from specified repositories. See *Fingerprinting*. **Manual registration** — Signatures of the files are uploaded to McAfee ePO from McAfee DLP when you manually upload files and create a package. These signatures are made available to and

Term	Definition
	downloaded by the endpoints and appliances from the shared location, which are used to track and classify content.
Repository	A folder, server, or account containing shared files. The repository definition includes the paths and credentials for scanning the data. McAfee DLP Endpoint discovery.
Rule	Defines the action taken when an attempt is made to transfer or transmit sensitive data.
Rule set	A combination of rules.
Scheduler	A definition that specifies scan details and the schedule type, such as daily, weekly, monthly, once, or immediately. Applicable to McAfee DLP Endpoint (Discovery)
Strategy	McAfee DLP Endpoint divides applications into four categories called strategies that affect how the software works with different applications. In order of decreasing security, the strategies are Editor, Explorer, Trusted, and Archiver.
Unmanaged devices	A device class status indicating that the devices in that class are not managed by Device Control. Some endpoint computers use devices that have compatibility issues with the McAfee DLP Endpoint device drivers. To prevent operational problems, these devices are set to Unmanaged.
Whitelisted devices	A device class status indicating that Device Control does not try to control the devices in that class. Examples are battery devices and processors.

General

Default ports

McAfee DLP uses several ports for network communication. Configure any intermediary firewalls or policy-enforcing devices to allow these ports where needed.

All listed protocols use TCP only, unless noted otherwise.

For information about ports that communicate with McAfee ePO, see KB66797.

McAfee DLP Discover default ports

Port, protocol	Use
• 137, 138, 139 — NetBIOS • 445 — SMB	SMB/CIFS scans
Any standard NFS port.	NFS scans
• 80 — HTTP • 443 — SSL	• Box and SharePoint scans • Evidence storage service • DLP Server REST API for registered documents fingerprint matching SharePoint servers and evidence storage service might be configured to use non-standard HTTP or SSL ports. If needed, configure firewalls to allow the non-standard ports.
53 — DNS (UDP)	DNS queries
• 1801 — TCP • 135, 2101*, 2103*, 2105 — RPC • 1801, 3527 — UDP * Indicates that the port numbers might be incremented by 11 depending on the available ports at initialization. For more information, see Microsoft KB article 178517.	Microsoft Message Queuing (MSMQ)
1433	Microsoft SQL
1521	Oracle
3306	MySQL
50000	DB2

McAfee DLP Endpoint default port

Port	Use	Direction
514	Syslog	Outbound

McAfee DLP Prevent and McAfee DLP Monitor default ports

Port	Use	Direction from the appliance
22 — SSH	SSH (when enabled)	Inbound
161 (UDP)	SNMP (when enabled)	Inbound
162 (UDP)	SNMP traps (when enabled)	Outbound
445 — SMB, 137, 138, 139 — NetBIOS	Evidence copy	Outbound
8081 — McAfee ePO	McAfee ePO agent service	Inbound
10443 — HTTPS	HTTPS traffic to download, for example, the Minimum Escalation Report (MER) and MIB files	Inbound
53 — DNS (UDP)	DNS queries	Outbound
123 — NTP (UDP)	NTP requests	Inbound and outbound
389 — LDAP 636 — LDAP over SSL 3268 — (LDAP) Active Directory Global Catalog 3269 — (LDAP) Active Directory Global Catalog over SSL	Obtaining groups for rule evaluation	Outbound

Port	Use	Direction from the appliance
80, 443 — HTTP and HTTPS	McAfee ePO server communication, evidence copy operations via DLP Server, and queries to registered documents services	Outbound
61613	McAfee Logon Collector	Outbound
514	Syslog	Outbound

McAfee DLP Prevent default ports

Port	Use	Direction
25 — SMTP	SMTP traffic with the MTA	Inbound and outbound
587 — SMTP AUTH	SMTP AUTH traffic with the MTA	Inbound and outbound
1344, 11344 — ICAP and ICAP over SSL	ICAP traffic with the web proxy	Inbound

McAfee DLP Monitor default port

Port	Use	Direction
941 — over SSL	Receives scanning requests from the packet acquisition device	Inbound

Shared policy components

McAfee DLP products share many policy configuration components.

Component	Device Control	McAfee DLP Endpoint for Windows	McAfee DLP Endpoint for Mac	McAfee DLP Discover	McAfee DLP Prevent and McAfee DLP Monitor
Definitions	X	X	X	X	X
Classifications	X*	X	X	X	X
Content classification criteria	X*	X	X	X	X
Content fingerprinting criteria		X			
Manual classifications		X	X	X**	X**
Registered documents		Manual registration only		Automatic registration only	Manual and automaticregistration
Whitelisted text		X			X
Rules and rule sets	X	X	X	X	X
Client configuration	X	X	X		
Server configuration				X	X
Evidence	X*	X	X	X	X
Rights management	X***	X		X	

*Device Control uses classifications, content classification criteria, and evidence only in removable storage protection rules.

** McAfee DLP Discover,McAfee DLP Monitor, and McAfee DLP Prevent can analyze files for manual classifications, but these products can't assign manual classifications.

*** Rights management is supported with the Removable Storage protection rule only.

DLP predefined dashboards

The following table describes the predefined McAfee DLP dashboards.

Predefined DLP dashboards

Category	Option	Description
DLP: Incident Summary	**Number of Incidents per day**	These charts show total incidents, and give different breakdowns to help analyze specific problems.
	Number of Incidents per severity	
	Number of Incidents per type	
	Number of Incidents per rule set	
DLP: Operations Summary (All products)	**Number of Operational events per day**	Displays all administrative events.
DLP: Operations Summary (These options are applicable to McAfee DLP Endpoint)	**Agent Version**	Displays the distribution of endpoints in the enterprise. Used to monitor agent deployment progress.
	Distribution of DLP products on endpoint computers	Displays a pie chart showing the number of Windows and Mac endpoints, as well as the number of endpoints where no client is installed.

Category	Option	Description
	DLP Discovery (Endpoint): Local File System Scan Status	Displays a pie chart showing the number of local file system discovery scan properties and their states (completed, running, undefined).
	DLP Discovery (Endpoint): Local Email Scan Status	Displays a pie chart showing the number of local email discovery scan properties and their states (completed, running, undefined).
	Agent Status	Displays all agents and their status.
	Agent Operation Mode	Displays a pie chart of agents by DLP operation modes. Operation modes are: • Device control only mode • Device control and full content protection mode • Device control and content aware removable storage protection mode • Unknown
	DLP Discovery (Endpoint): Local Email Storage Scan Status	Displays a pie chart showing the number of local email storage scan discovery properties and their states (completed, running, undefined).
DLP: Policy Summary (All products)	**Policy distribution**	Displays the DLP policy distribution by version throughout the enterprise. Used to monitor progress when deploying a new policy.
	Privileged Users	Displays the system name/user name and the number of user session properties.
	Policy revision distribution	Similar to Policy distribution, but displays revisions – that is, updates to an existing version.
DLP: Policy Summary (These options are applicable to McAfee DLP Endpoint)	**Enforced Rule Sets per endpoint computers**	Displays a bar chart showing the rule set name and the number of policies enforced.

Category	Option	Description
	Bypassed Users	Displays the system name/user name and the number of user session properties.
	Undefined Device Classes (for Windows devices)	Displays the undefined device classes for Windows devices.
DLP: Endpoint Discovery Summary (These options are applicable to McAfee DLP Endpoint)	**DLP Discovery (Endpoint): Local File System Scan Latest Status**	Displays a pie chart showing the run status of all local file system scans.
	DLP Discovery (Endpoint): Local File System Scan Latest Sensitive Files	Displays a bar chart showing the range of sensitive files found on systems files.
	DLP Discovery (Endpoint): Local File System Scan Latest Errors	Displays a bar chart showing the range of errors found in systems files.
	DLP Discovery (Endpoint): Local File System Scan Latest Classifications	Displays a bar chart showing the classifications applied to systems files.
	DLP Discovery (Endpoint): Local Email Scan Latest Status	Displays a pie chart showing the run status of all local email folders.
	DLP Discovery (Endpoint): Local Email Scan Latest Sensitive Emails	Displays a bar chart showing the range of sensitive emails found in local email folders.
	DLP Discovery (Endpoint): Local Email Scan Latest Errors	Displays a bar chart showing the range of errors found in local email folders.
	DLP Discovery (Endpoint): Local Email Scan Latest Classifications	Displays a bar chart showing the classifications applied to local emails.

Rules

Client configuration support for data protection rules

Data protection rules work with settings in the client configuration. Applicable for McAfee DLP Endpoint.

Tip

To optimize data protection rules, create client configurations to match the requirements of different rule sets.

The following table lists data protection rules, and the specific settings in the client configuration that affect them. In most cases, you can accept the default setting

Data protection rules and client configuration settings

Data protection rule	Client configuration page and settings
Application File Access Protection	**Content Tracking** — Add or edit whitelisted processes
Clipboard Protection	• **Operational Mode and Modules** — Activate the clipboard service. • **Clipboard Protection** — Add or edit whitelisted processes. Enable or disable the Microsoft Office Clipboard. **Note:** Microsoft Office Clipboard is enabled by default. When enabled, you can't prevent copying from one Office application to another.
Cloud Protection	**Operational Mode and Modules**: Select cloud protection handlers.
Email Protection	• **Operational Mode and Modules** — Activate available email software (Lotus Notes, Microsoft Outlook). For Microsoft Outlook, select the required add-ins. **Note:** In systems where both Microsoft Exchange and Lotus Notes are available, email rules do not work if the outgoing mail server (SMTP) name is not configured for both. • **Email Protection** — Select Microsoft Outlook third-party add-in (Titus or Boldon James). Set the timeout strategy, caching, API, and user notification

Data protection rule	Client configuration page and settings
	Note: When the third-party add-in is installed and active, the McAfee DLP Endpoint Outlook add-in sets itself to bypass mode.
Network Communication Protection	• **Corporate connectivity** — Add or edit corporate VPN servers • **Operational Mode and Modules** — Activate or deactivate the network communication driver (activated by default).
Network Share Protection	No settings
Printer Protection	• **Corporate connectivity** — Add or edit corporate VPN servers • **Operational Mode and Modules** — Select printer application add-ins • **Printing Protection** — Add or edit whitelisted processes. **Note:** Printer application add-ins can improve printer performance when using certain common applications. The add-ins are only installed when a printer protection rule is enabled on the managed computer.
Removable Storage Protection	• **Operational Mode and Modules** — Activate advanced options. • **Removable Storage Protection** — Set the deletion mode. Normal mode deletes the file; aggressive mode makes the deleted file unrecoverable.
Screen Capture Protection	• **Operational Mode and Modules** — Activate the screen capture service. The service consist of the application handler and the Print Screen key handler, which can be activated separately. • **Screen Capture Protection** — Add, edit, or delete screen capture applications protected by screen capture protection rules. **Note:** Disabling the application handler, or the screen capture service, disables all the applications listed on the Screen Capture Protection page.
Web Protection	• **Operational Mode and Modules** — Enable supported browsers for web protection.

Data protection rule	Client configuration page and settings
	• **Web Protection** — Add or edit whitelisted URLs, enable HTTP GET request processing (disabled by default because they are resource-intensive), and set the web timeout strategy.

Removable storage protection advanced options details

The following sections describe the **Windows Client Configuration** → **Operational Mode and Modules** → **Removable Storage Protection Advanced Options**.

Protect TrueCrypt Local Disks Mounts

TrueCrypt encrypted virtual devices can be protected with TrueCrypt device rules, or with removable storage protection rules. TrueCrypt protection is not supported on McAfee DLP Endpoint for Mac .

- Use a device rule if you want to block or monitor a TrueCrypt volume, or make it read-only.
- Use a protection rule if you want content-aware protection of TrueCrypt volumes.

Note

Signatures are lost when content fingerprinted content is copied to TrueCrypt volumes because TrueCrypt volumes do not support extended file attributes. Use document properties, file encryption, or file type groups definitions in the classification definition to identify the content.

Portable Devices Handler (MTP)

Media Transfer Protocol (MTP) is used for transferring files and associated metadata from computers to mobile devices such as smartphones. MTP devices are not traditional removable devices because the device implements the file system, not the computer it is connected to. When the client is configured for MTP devices, the removable storage protection rule allows it to intercept MTP transfers and apply security policies. Only USB connections are currently supported.

The handler works with all data transfers made by Windows Explorer. It does not work with iOS devices, which use iTunes to manage the data transfers. One alternative strategy with iOS devices is to use a removable storage device rule to set the devices to read-only.

Advanced file copy protection intercepts Windows Explorer copy operations and allows the McAfee DLP Endpoint client to inspect the file at source before copying it to the removable device. It is enabled by default, and should only be disabled for troubleshooting.

Note

There are use cases where advanced copy protection does not apply. For example, a file opened by an application and saved to a removable device with **Save As** reverts to normal copy protection. The file is copied to the device, then inspected. If sensitive content is found, the file is immediately deleted.

Reactions available for rule types

The available reactions for a rule vary depending on the rule type.

- All data protection rules are available for McAfee DLP Endpoint. Some data protection rules are available for McAfee DLP Prevent and McAfee DLP Monitor.
- Device Control rules are available for McAfee DLP Endpoint and Device Control.
- Some discovery rules are available for McAfee DLP Endpoint, some are available for McAfee DLP Discover.

Rule reactions

Reaction	Applies to rules:	Result
No Action	All	Allows the action.
Block and return email to sender	**Email Protection** (McAfee DLP Prevent only)	Blocks the email message when there is a policy violation. The email is sent back to the sender as an attachment with a notification. You can customize the notification and specify as to why the email was sent back.
Add header X-RCIS-Action	**Email Protection** (McAfee DLP Prevent only)	Adds an action value to the X-RCIS-Action header
Apply RM Policy	• **Data Protection** • **Removable Storage Protection** • **Network Discovery** Not supported on McAfee DLP Endpoint for Mac	Applies a rights management (RM) policy to the file. The RM policy can be applied to Microsoft RMS on-premise, Azure RMS and Seclore.
Block	• **Data Protection** • **Device Control**	Blocks the action.
Classify file	• **Endpoint Discovery** • **Network Discovery**	Applies automatic classifications and embeds the classification Tag ID into the file format.
Copy	**Network Discovery**	Copies the file to the specified UNC location.

Reaction	Applies to rules:	Result
Create Content Fingerprint	**Endpoint Discovery**	Applies content fingerprinting to the file.
Encrypt	• **Data Protection** • **Endpoint Discovery** Not supported on McAfee DLP Endpoint for Mac .	Encrypts the file. Encryption options are FRP or StormShield Data Security encryption software.
Modify anonymous share to login required	**Network Discovery Box Protection**	Removes anonymous sharing for the file.
Move	**Network Discovery**	Moves the file to the specified UNC location. Allows creation of a placeholder file (optional) to notify the user that the file has been moved. The placeholder file is specified by selecting a user notification definition.
Quarantine	**Endpoint Discovery**	Quarantines the file.
Read-only	**Device Control**	Forces read-only access.
Remove Automatic Classification	**Network Discovery**	Removes embedded classification ID from the file property.
Report Incident	All	Generates an incident entry of the violation in **DLP Incident Manager**.
Request justification	**Data Protection**	Produces a pop-up on the end-user computer. The user selects a justification (with optional user input) or selects an optional action.
Show file in DLP Endpoint console	**Endpoint Discovery**	Displays **Filename** and **Path** in the endpoint console. **Filename** is a link to open the file, except when the file is quarantined. **Path** opens the folder where the file is located.

Reaction	Applies to rules:	Result
Store original email as evidence	- **Data Protection** Not supported on McAfee DLP Endpoint for Mac .	Stores the original message on the evidence share. Applies to McAfee DLP Endpoint and McAfee DLP Prevent email protection rules only. **Note:** Requires a specified evidence folder and activation of the evidence copy service.
Store original file as evidence	- **Data Protection** - **Endpoint Discovery** - **Network Discovery**	Saves the file for viewing through the **DLP Incident Manager**. **Note:** Requires a specified evidence folder and activation of the evidence copy service.
User notification	- **Data Protection** - **Device Control** - **Endpoint Discovery** - **Web Protection for Prevent**	Sends a message to the endpoint to notify the user of the policy violation. **Note:** When **User Notification** is selected, and multiple events are triggered, the pop-up message states: *There are new DLP events in your DLP console*, rather than displaying multiple messages.

Reconfigure action rules for web content.

You must reconfigure McAfee DLP Prevent action rules for use on proxy servers.

Note

> Proxy servers can only ALLOW or BLOCK web content.

McAfee DLP Prevent data protection rule reactions

Rules	Reactions							
	No action	Apply RM Policy	Block	Encrypt	Report Incident	Request justification	Store original file (email) as evidence	User notification
Email protection	X		X		X	X	X	X
Web protection	X		X		X	X	X	X

McAfee DLP Endpoint data protection rule reactions

Rules	Reactions							
	No action	Apply RM Policy	Block	Encrypt	Report Incident	Request justification	Store original file (email) as evidence	User notification
Application File Access Protection	X		X		X		X	X
Clipboard protection	X		X		X	X	X	X
Cloud protection	X	X	X	X	X	X	X	X
Email protection	X		X		X	X	X	X

Rules	Reactions							
	No action	Apply RM Policy	Block	Encrypt	Report Incident	Request justification	Store original file (email) as evidence	User notification
Network communication protection	X		X		X		X	X
Network share protection	X	X		X	X		X	X
Printer protection	X		X		X	X	X	X
Removable storage protection	X	X	X	X	X	X	X	X
Screen capture protection	X		X		X		X	X
Web protection	X		X		X	X	X	X

Device Control rule reactions

Rules	Reactions		
	No action	Block	Read-only
Citrix XenApp device		X	
Fixed hard drive	X	X	X
Plug-and-play device	X	X	

Rules	Reactions		
	No action	Block	Read-only
Removable storage device	X	X	X
Removable storage file access	X	X	
TrueCrypt device	X	X	X

McAfee DLP Endpoint discovery rule reactions

Rules	Reactions					
	No action	Encrypt	Apply RM policy	Quarantine	Create content fingerprint	Classify file
Endpoint file system	X	X	X	X	X	X
Endpoint mail storage protection	X			X	X	

McAfee DLP Discover discovery rule reactions

Rules	Reactions							
	No action	Copy	Move	Apply RM policy	Store original file as evidence	Classify file as	Remove Automatic Classification	Modify anonymous share to login required
Box protection	X	X [1]	X [1]	X	X	X	X	X [2]

Rules	Reactions							
	No action	Copy	Move	Apply RM policy	Store original file as evidence	Classify file as	Remove Automatic Classification	Modify anonymous share to login required
File server protection	X	X [1]	X [1]	X	X	X	X	
SharePoint protection	X	X [1]	X [1] [3]	X [3]	X	X	X	
Database protection	X				X			

[1] Box, File Server, and SharePoint scans support copying and moving files only to SMB/CIFS shares.

[2] McAfee DLP Discover can't prevent Box users from reenabling external sharing on their files.

[3] Supported for files attached to SharePoint lists or stored in document libraries. Not supported for SharePoint lists.

Data protection rule actions

The action performed by a data protection rules is entered on the **Reaction** tab.

By default, the action for all data protection rules is **No Action**. When combined with the **Report Incident** option, this creates a monitoring action that can be used to fine-tune rules before applying them as blocking rules. Along with reporting, most rules allow you to store the original file that triggered the rule as evidence. Storing evidence is optional when reporting an incident.

Tip

Set the default for all rules to report incidents in **DLP Settings**. This prevents accidental errors by failing to enter any reaction. You can change the default setting when required.

The user notification option activates the user notification pop-up on the endpoint. Select a user notification definition to activate the option.

Different actions can be applied when the computer is disconnected from the corporate network. Some rules also allow different actions when connected to the network by VPN.

The table lists the available actions other than **No Action**, **Report Incident**, **User Notification**, and **Store original file as evidence**.

Available actions for data protection rules

Data protection rule	Reactions	Additional information
Application File Access Protection	Block	When the classification field is set to **is any data (ALL)**, the block action is not allowed. Attempting to save the rule with these conditions generates an error.
Clipboard Protection	Block	
Cloud Protection	• Block • Request Justification • Apply RM Policy • Encrypt	Encryption is supported on Box, Dropbox, GoogleDrive, iCloud, OneDrive personal, OneDrive for Business, and Syncplicity. Attempting to upload encrypted files to other cloud applications fails to save the file.
Email Protection	McAfee DLP Endpoint actions: • Block • Request Justification For McAfee DLP Prevent, the reactions are: • Block and return email to sender • Add header X-RCIS-Action • No Action For McAfee DLP Monitor, the only reaction is No Action.	McAfee DLP Endpoint for Mac currently supports only monitoring emails (**Report incident**). Supports different actions for McAfee DLP Endpoint when the computer is disconnected from the corporate network.
Network Communication Protection	Block (For McAfee DLP Endpoint) For McAfee DLP Monitor, the only reaction is No Action.	Storing evidence is not available as an option for McAfee DLP Endpoint. McAfee DLP Endpoint supports different actions when the computer is connected to the corporate network using VPN.

Data protection rule	Reactions	Additional information
Network Share Protection	• Request Justification • Encrypt	Encryption options are McAfee® File and Removable Media Protection (FRP) and StormShield Data Security encryption software. Encrypt action is not supported onMcAfee DLP Endpoint for Mac .
Printer Protection	• Block • Request Justification	Supports different actions when the computer is connected to the corporate network using VPN.
Removable Storage Protection	• Block • Request Justification • Encrypt	Encrypt action is not supported on McAfee DLP Endpoint for Mac .
Screen Capture Protection	Block	
Web Protection	McAfee DLP Endpoint reactions: • Block • Request Justification McAfee DLP Prevent reactions • No Action • Block For McAfee DLP Monitor, the only reaction is No Action.	Request Justification action is not available on McAfee DLP Prevent.

Device properties

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

The table provides device property definitions, which definition types use the property, and which operating system they apply to.

Types of device properties

Property name	Device definition	Applies to operating systems	Description
Bus Type	All	- Windows — Bluetooth, Firewire (IEEE1394), IDE/ SATA, PCI, PCMIA, SCSI, USB - macOS — Firewire (IEEE1394), IDE/ SATA, SD, Thunderbolt, USB	Selects the device BUS type from the available list. **Note:** For plug-and-play device rules, McAfee DLP Endpoint for Mac only supports USB bus type.
CD/DVD Drives	Removable storage	- Windows - macOS	Select to indicate any CD or DVD drive.
Content encrypted by Endpoint Encryption	Removable storage	Windows	Devices protected with Endpoint Encryption.
Device Class	Plug and Play	Windows	Selects the device class from the available managed list.
Device Compatible IDs	All	Windows	A list of physical device descriptions. Effective especially with device types other than USB and PCI, which are more easily identified using PCI VendorID/DeviceID or USB PID/VID.
Device Instance ID (Microsoft Windows XP)	All	Windows	A Windows-generated string that uniquely identifies the device in the system. *Example:* `USB\VID_0930&PID_6533\5&26450FC&0&6.`

Property name	Device definition	Applies to operating systems	Description
Device Instance Path (Windows Vista and later Microsoft Windows operating systems, including servers)			
Device Friendly Name	All	• Windows • macOS	The name attached to a hardware device, representing its physical address.
File System Type	• Fixed hard disk • Removable storage	• Windows — CDFS, exFAT, FAT16, FAT32, NTFS, UDFS • macOS — CDFS, exFAT, FAT16, FAT32, HFS/HFS+, NTFS, UDFS macOS supports FAT only on disks other than the boot disk. Mac OS X supports NTFS as read-only.	The type of file system. • For hard disks, select one of exFAT, FAT16, FAT32, or NTFS. • For removable storage devices, any of the above plus CDFS or UDFS.
File System Access	Removable storage	• Windows • macOS	The access to the file system: read only or read-write.
File System Volume Label	• Fixed hard disk	• Windows • macOS	The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.

Property name	Device definition	Applies to operating systems	Description
	• Removable storage		
File System Volume Serial Number	• Fixed hard disk • Removable storage	Windows	A 32-bit number generated automatically when a file system is created on the device. It can be viewed by running the command-line command `dir x:`, where x: is the drive letter.
PCI VendorID / DeviceID	All	Windows	The PCI VendorID and DeviceID are embedded in the PCI device. These parameters can be obtained from the Hardware ID string of physical devices. *Example:* `PCI\VEN_8086&DEV_2580&SUBSYS_00000000 &REV_04`
TrueCrypt devices	Removable storage	Windows	Select to specify a TrueCrypt device.
USB Class Code	Plug and Play	Windows	Identifies a physical USB device by its general function. Select the class code from the available list.
USB Device Serial Number	• Plug and Play • Removable storage	• Windows • macOS	A unique alphanumeric string assigned by the USB device manufacturer, typically for removable storage devices. The serial number is the last part of the instance ID. *Example:* `USB\VID_3538&PID_0042\00000000002CD8` A valid serial number must have a minimum of 5 alphanumeric characters and must not contain ampersands (&). If the last part of the instance ID does not follow these requirements, it is not a serial number. You can enter a partial serial number by using the comparison **Contains** rather than **Equals**.

Property name	Device definition	Applies to operating systems	Description
USB Vendor ID / Product ID	• Plug and Play • Removable storage	• Windows • macOS	The USB VendorID and ProductID are embedded in the USB device. These parameters can be obtained from the Hardware ID string of physical devices. *Example:* `USB\Vid_3538&Pid_0042`

Classifications

Classification definitions and criteria

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

Available conditions

Property	Applies to:	Definition	Supported products
Advanced Pattern	Definitions, criteria	Regular expressions or phrases used to match data such as dates or credit card numbers.	All products
Dictionary	Definitions, criteria	Collections of related keywords and phrases such as profanity or medical terminology.	
Keyword	Criteria	A string value. You can add multiple keywords separated by semicolon (;) to content classification or content fingerprinting criteria. The default Boolean for multiple keywords is OR, but can be changed to AND.	
Proximity	Criteria	Defines a conjunction between two properties based on their location to each other. Advanced patterns, dictionaries, or keywords can be used for either property. You can add multiple keywords separated by comma (,).	

Property	Applies to:	Definition	Supported products
		The **Closeness** parameter is defined as "less than x characters," where the default is 1. You can also specify a **Match count** parameter to determine the minimum number of matches to trigger a hit.	
Document Properties	Definitions, criteria	Contains these options: • **Any Property** • **Author** • **Category** • **Comments** • **Company** • **Keywords** • **Last saved by** • **Manager Name** • **Security** • **Subject** • **Template** • **Title** **Any Property** is a user-defined property.	
File Encryption	Criteria	Contains these options: • Not encrypted* • McAfee Encrypted Self-Extractor • McAfee Endpoint Encryption • Microsoft Rights Management encryption* • Azure Rights Management encryption* • Seclore Rights Management encryption • Unsupported encryption types or password protected file*	• McAfee DLP Endpoint for Windows (All options are supported) **Note:** File encryption isn't supported with McAfee DLP Endpoint for Mac. • McAfee DLP Discover, McAfee DLP Prevent, and McAfee DLP Monitor support only the options marked with *

Property	**Applies to:**	**Definition**	**Supported products**
File Extension	Definitions, criteria	Groups of supported file types such as MP3 and PDF.	All products
File Information	Definitions, criteria	Contains these options: • **Date Accessed** • **Date Created** • **Date Modified** • **File Extension*** • **File Name*** • **File Owner** • **File Size***	• All products • McAfee DLP Prevent and McAfee DLP Monitor support only the options marked with *
Location in file	Criteria	The section of the file the data is located in; Header, Footer, Body or within the first characters. Specifying the number of characters for the **within first (characters)** option in a classification looks for the sensitive content in the Header, that is, in the first part of the first page in a document. • Microsoft Word documents — the classification engine can identify **Header**, **Body**, and **Footer**. • PowerPoint documents — WordArt is considered **Header**; everything else is identified as **Body**. • Other documents — **Header** and **Footer** are not applicable. The classification criteria does not match the document if they are selected.	
Third Party tags	Criteria	Used to specify Titus field names and values.	• McAfee DLP Endpoint for Windows • McAfee DLP Prevent • McAfee DLP Monitor
True File Type	Definitions, criteria	Groups of file types. For example, the built-in **Microsoft Excel** group includes Excel XLS, XLSX, and XML files, as well as	All products

Property	Applies to:	Definition	Supported products
		Lotus WK1 and FM3 files, CSV and DIF files, Apple iWork files, and more.	
Application Template	Definitions	The application or executable accessing the file.	• McAfee DLP Endpoint for Windows • McAfee DLP Endpoint for Mac
End-User Group	Definitions	Used to define manual classification permissions.	
Network Share	Definitions	The network share the file is stored in.	McAfee DLP Endpoint for Windows
URL List	Definitions	The URL the file is accessed from.	

Regular expressions for advanced patterns

McAfee DLP advanced patterns use regular expressions (regex) to allow complex pattern matching.

Advanced pattern definitions use the Google RE2 regex syntax. By default they are case sensitive. While a full description of RE2 syntax is beyond the scope of this document, some of the more commonly used terms are listed in the table.

[abc]	Matches a single character a, b, or c
[^abc]	Matches a single character not a, b, or c
[0-9]	Matches a single character in the range 0-9
[^0-9]	Matches a single character not in the range 0-9
(ab|cd)	Matches ab or cd
\d	Matches any ASCII digit
\D	Matches any non-digit character

\s	Matches any whitespace character
\S	Matches any non-whitespace character
\w	Matches any alphanumeric character
\W	Matches any non-alphanumeric character
\b	ASCII word boundary
\ (when used with punctuation, for example \]	Matches] (Escapes the next character, that is, removes its special meaning.)
.	Any single character
*	Modifies the previous token to match 0 or more times
+	Modifies the previous token to match 1 or more times
{3,4}	Modifies the previous token to match 3 or 4 times
?	Modifies the previous token to match 0 or 1 times (makes it optional)
(?i)	Sets matching to be case insensitive up to next closing) (Accounts for nested () for example ((?i)insensitive)sensitive
(?-i)	Sets matching to be case sensitive up to next closing)

Convert policies and migrate data

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

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

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

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

Task

1. In McAfee ePO, select **Menu** → **Automation** → **Server Tasks**.
2. Select **DLP Policy Conversion**, then click **Actions** → **Run**.
   The **Server Task Log** page opens, where you verify that the task is running. The converted policy is compatible with version 9.4.100 and later policies.

   Note

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

3. Return to the **Server Tasks** page, select **DLP incident migration from 9.3.x to 9.4.1 and above**, then click **Actions** → **Edit**.
   DLP operational events Migration from 9.3.x to 9.4.1 and above is performed in the same way.
4. Select **Schedule status** → **Enabled**, then click **Next** twice.

   Note

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

5. Select a schedule type and occurrence.

   Tip

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

   a. Set the start date and end date to define a time period, and schedule the task for every hour.
   b. Schedule repeating the task according to the size of incident database you are migrating.
      Incidents are migrated in chunks of 200,000.
6. Click **Next** to review the settings, then click **Save**.

Scan behavior

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

Effect of changing properties during a scan

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

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

Screen reader support

McAfee DLP Endpoint for Windows supports Job Access With Sound (JAWS).

The widely-used screen reader software for the visually impaired, JAWS, is supported on endpoints. The following McAfee DLP Endpoint features are supported:

- **End-user notification pop-up** — If the pop-up dialog box is set to close manually (in **DLP Policy Manager**), dialog text is read allowing a visually impaired person to navigate the buttons and links.
- **End-user justification dialog** — The combo box is accessible with the tab key, and justification can be selected with arrow keys.
- **End-user console Notification History tab** — When the tab is selected, JAWS reads, "Notification history tab selected." There is no actionable content. All information in the right pane is read.
- **End-user console Discovery tab** — When the tab is selected, JAWS reads, "Discovery tab selected." There is no actionable content. All information in the right pane is read.
- **End-user console Tasks tab** — When the tab is selected, JAWS reads, "Tasks tab selected." All steps are accessible with the tab key, and appropriate instructions are read.
- **End-user console About tab** — When the tab is selected, JAWS reads, "About tab selected." There is no actionable content. All information in the right pane is read.

Identifying remote users with McAfee Logon Collector

McAfee DLP Prevent and McAfee DLP Monitor uses McAfee Logon Collector (MLC) servers to identify remote users when they make web requests. With McAfee Logon Collector, McAfee DLP appliances can map an IP address to a Windows user name if no other authentication information is available.

With McAfee Logon Collector, remote users are identified through Security Identifiers (SIDs) instead of IP addresses, host names, or other user parameters that are subject to change.

For more information about McAfee Logon Collector, see the McAfee Logon Collector Administration Guide.

The certificate used between McAfee Logon Collector and McAfee DLP appliances must be valid, or you cannot add a Logon Collector server.

Follow these topics to learn more about setting up McAfee Logon Collector with McAfee DLP appliances:

- Downloading and accessing the McAfee Logon Collector software
- Add Domain Controller and Logon Monitor to McAfee Logon Collector
- Add a McAfee Logon Collector server and certificate to a McAfee DLP appliance
- How McAfee Logon Collector works with McAfee DLP appliance

Downloading and accessing the McAfee Logon Collector software

For McAfee DLP to retrieve user information and logon data from McAfee Logon Collector, you must first install and configure McAfee Logon Collector.

You can download the McAfee Logon Collector from the McAfee product downloads portal (https://www.mcafee.com/enterprise/en-in/downloads/my-products.html).

McAfee Logon Collector needs a Windows 2008 R2 or later version of Windows Server. For more information about installing McAfee Logon Collector, see the McAfee Logon Collector Administration Guide.

Accessing McAfee Logon Collector interface

McAfee Logon Collector has a web-based user interface for configuration and management. After you install McAfee Logon Collector, you can access its user interface using this URL:

https://mlc.host.name:8443

What is Logon Monitor?

Logon Monitor is the component of McAfee Logon Collector that monitors and receives security events. McAfee Logon Collector has a built-in Logon Monitor.

You can install Logon Monitors separately and so when adding domains to **Managed Domains**, you can select Logon Monitors as needed for monitoring security events.

For more information about installing Logon Monitors, see the McAfee Logon Collector Administration Guide.

Add Domain Controller and Logon Monitor to McAfee Logon Collector

McAfee Logon Collector can work with multiple domains and multiple forests. Each domain from which the McAfee Logon Collector receives security events must be added to the monitored domains of the McAfee Logon Collector.

Before you begin

You must have installed McAfee Logon Collector.

Task

1. Select **Menu** → **Configuration** → **Monitored Domains**.
2. Click **New Domain**.
3. In the **Domain Name** tab, provide the credentials of the administrator user for the domain.
   The domain name must be the complete domain name and not the NetBIOS name.

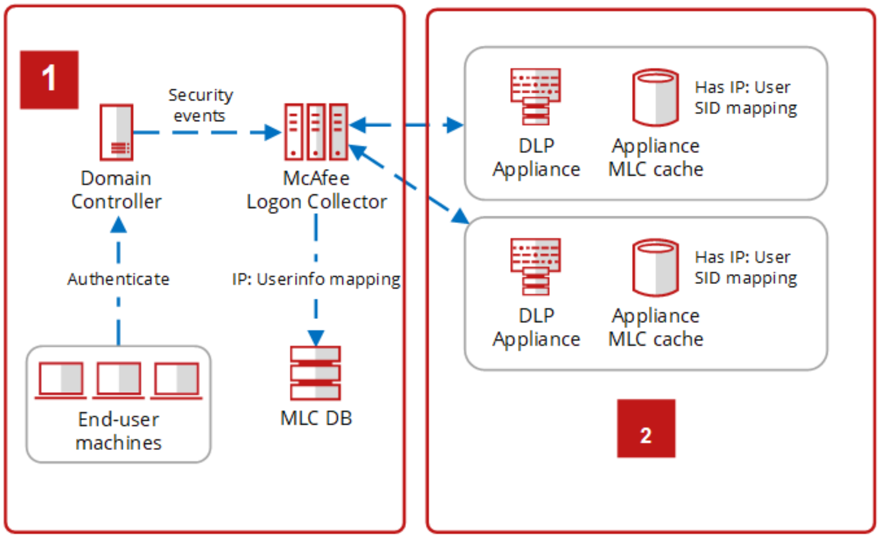
4. In the **Domain Controller** tab, select from the list of domain controllers from which McAfee Logon Collector fetches data for that domain.
5. Select the Logon Monitor to be used. This can be the localhost. For example, McAfee Logon Collector itself can be the Logon Monitor.

Results

These steps must be repeated for each domain with which the McAfee Logon Collector is integrated.

How McAfee Logon Collector works with McAfee DLP appliance

McAfee Logon Collector (MLC) communicates Windows user logon events to McAfee DLP appliances. McAfee DLP appliances can map an IP address to a Windows user name if no other authentication information is available.



1. When a user logs on to the network, the domain controller creates an event in the security event log.

   This is a special, protected log file that can be accessed using the Windows Management Interface (WMI). McAfee Logon Collector uses this interface to receive log-on events and stores a mapping of the user's device IP to the user data.

2. When McAfee Logon Collector integrates with McAfee DLP appliances, the appliances synchronize the client IP and the user's SID from McAfee Logon Collector on to a local cache available on each appliance.

COPYRIGHT