Product Guide

Revision A

McAfee Total Protection for Data Loss Prevention 9.2 Software

COPYRIGHT

TRADEMARK ATTRIBUTIONS

LICENSE INFORMATION

License Agreement

Contents

Preface

This guide provides the information you need to configure, use, and maintain McAfee Total Protection for Data Loss Prevention software.

McAfee Total Protection for DLP software runs on Microsoft Windows and Linux platforms - in McAfee® ePolicy Orchestrator® and McAfee Data Loss Prevention Manager, both of which serve as management consoles.

McAfee Total Protection for DLP is a configurable product suite. You choose one or more of the products that are implemented through the management console: McAfee DLP Monitor, McAfee DLP Discover, McAfee DLP Prevent, or McAfee DLP Endpoint.

Contents

About this guide

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

Audience

McAfee documentation is carefully researched and written for the target audience.

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Security officers** — People who determine sensitive and confidential data, and define the corporate policy that protects the company's intellectual property.

Conventions

This guide uses the following typographical conventions and icons.

Book title or *Emphasis*	Title of a book, chapter, or topic; introduction of a new term; emphasis.
Bold	Text that is strongly emphasized.
`User input` or `Path`	Commands and other text that the user types; the path of a folder or program.
`Code`	A code sample.
User interface	Words in the user interface including options, menus, buttons, and dialog boxes.
Hypertext blue	A live link to a topic or to a website.

ℹ	**Note**: Additional information, like an alternate method of accessing an option.
💡	**Tip**: Suggestions and recommendations.
❗	**Important/Caution**: Valuable advice to protect your computer system, software installation, network, business, or data.
⚠	**Warning**: Critical advice to prevent bodily harm when using a hardware product.

About this guide

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

Chapters 1 and 2 provide concepts and an overview of McAfee Total Protection for Data Loss Prevention.

Chapters 3–8 provide information on using the McAfee Total Protection for Data Loss Prevention products and features.

Chapters 9–16 provide information on setting up, configuring and administering the McAfee Total Protection for Data Loss Prevention systems.

Chapter 17 provides typical scenarios and use case for deploying and learning the McAfee Total Protection for Data Loss Prevention system.

Finding product documentation

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

Task

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

To access...	Do this...
User documentation	1 Click **Product Documentation**. 2 Select a product, then select a version. 3 Select a product document.
KnowledgeBase	• Click **Search the KnowledgeBase** for answers to your product questions. • Click **Browse the KnowledgeBase** for articles listed by product and version.

1

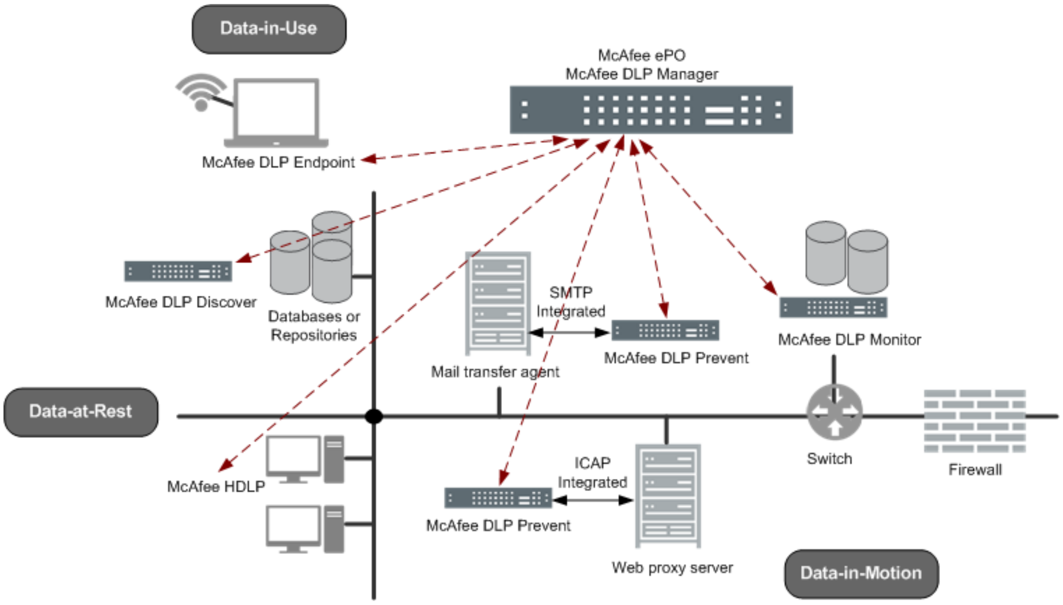
Introducing McAfee Total Protection for Data Loss Prevention

This section contains information about McAfee Total Protection for Data Loss Prevention features and gives a brief description of how the system works.

Contents

How McAfee DLP works

McAfee Data Loss Prevention Manager manages all of the McAfee DLP products from a centralized console, then displays incidents and events found by them on its dashboards.



- The McAfee DLP Monitor capture engine analyzes all content on a network, classifies it into types, and stores the resulting objects on capture partitions. Some traffic can be filtered out to improve performance.
- McAfee DLP Prevent monitors all email and webmail and applies actions to resolve any problems.
- McAfee DLP Discover monitors file systems and repositories, locates significant data, and reports data that is in violation of policy.
- McAfee DLP Endpoint finds significant events occurring at endpoints and reports any policy violations.

McAfee DLP products

McAfee Total Protection for Data Loss Prevention is a suite of products that work together to find problems in network traffic, file systems and repositories, and on network endpoints.

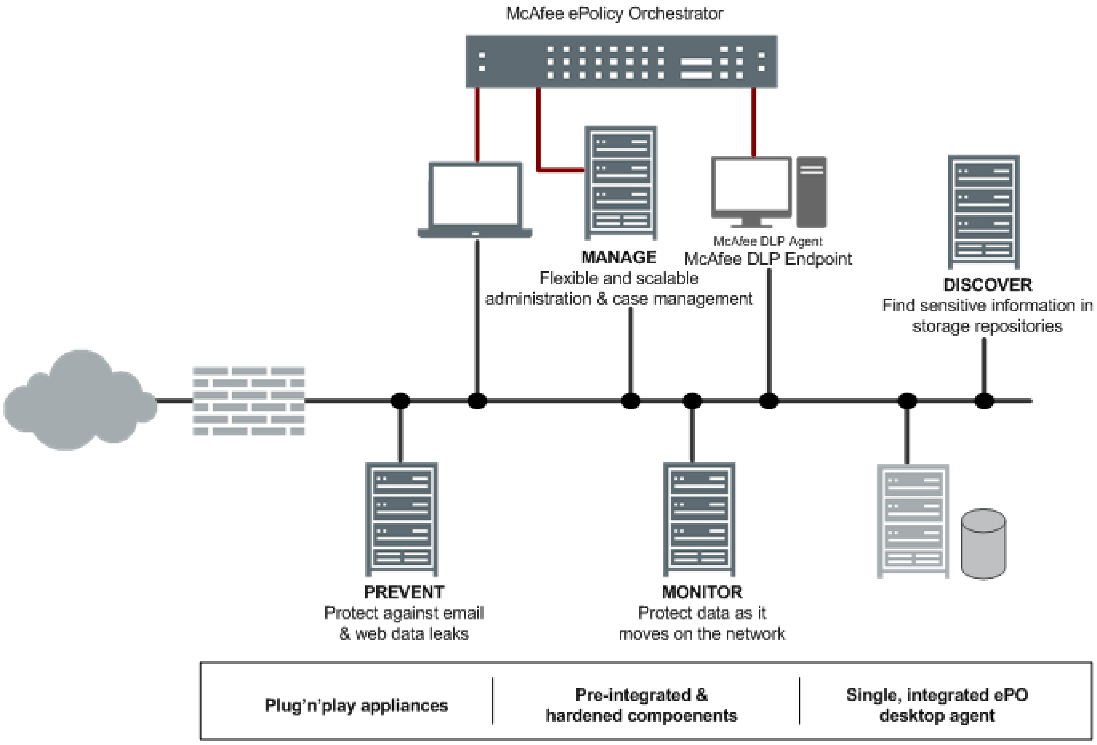


Figure 1-1 McAfee Total Protection for Data Loss Prevention Products

McAfee DLP Endpoint integration

McAfee DLP Endpoint and device control and application tagging features are available from McAfee DLP Manager.

You can configure device control and application tagging through McAfee DLP Manager. You can also manage endpoint rules and events through the same workflow as the other products in the DLP solution.

Digital rights management support is not yet supported through McAfee DLP Manager.

Hardware and operating system improvements

A more powerful, Intel-based platform is available, the Linux operating system has been updated, and virtual image support has been added.

Hardware improvements and operating system updates encompass a number of new features.

- The new hardware platform replaces the current SuperMicro 1650s and 3650s, which have been EOL'd. It is a 2U platform with Intel-based quad core CPU, 24 GB of memory and 12 TB of storage. The new appliance delivers greater horsepower, memory and storage, and uses less rack space than the 3650.
- The Fedora Core 3-based operating system has been updated to McAfee Linux Operating System. It is based on the more current Centos 5.2, patching many known holes in Fedora. It also offers the ability to provide virtual support and more network controls (e.g., SNMP). Finally, MLOS is handled by a central technology team for all patches and updates.
- MLOS also provides the ability to create virtual images of McAfee DLP Monitor, McAfee DLP Discover, and McAfee Data Loss Prevention Prevent. Virtual images support replacement of the 1650, technical educational tools, and channel enablement.
- Support for advanced hardware features such as IPMI, SNMP, and daisy-chaining of additional storage appliances has been added, leveraging the new operating system (prototype for this release, productized in a subsequent release). There is also better integration into existing network ecosystems and greater management capabilities and ability to increase storage beyond 12 TB.
- Virtual images of the products are available.

Discover features

McAfee DLP Discover now uses data classification for optimized scanning, and OLAP tools have been added to allow for exploration and manipulation of classified data. Other features include improved credentialing for database scan operations, Microsoft SharePoint crawling, expanded scan scheduling, usability improvements, and higher scan speeds.

McAfee DLP Discover operations are now accessed through the **Classify** tab in the user interface.

The new Classification scan type does an inventory scan, fetches and classifies content into file types and uses existing policies to screen it for potential violations.

Credentialing for database crawling has been enhanced by support for use of SSL certificates.

- The process now aligns more closely with the way credentials are exchanged for database access in large enterprise environments;
- The need for coordination between McAfee DLP Administrators and DBAs for password updates has been reduced.

Usability has been improved.

- Managability of Inventory and Discover scans has been enhanced;
- Scan speeds have been increased;
- The Scheduler has been enhanced;
- The dashboard has been updated;
- Repositories can be identified by machine name instead of IP address;
- Basic access control lists can be identified.

Microsoft SharePoint servers are supported, leveraging existing McAfee GroupShield presence on Exchange servers to crawl for sensitive data and add remediation capabilities (prototype in this release, productized in a subsequent release).

Internationalization features

International policies have been expanded to include new rules developed for China, Russia, Japan, Korea, and the Czech Republic. In addition, the capture engine now supports Japanese, Greek, Korean, Hungarian, Czech and Italian.

New international policies and rules and additional language support will provide better coverage for customers in the Asia Pacific, European and Middle Eastern regions.

Usability improvements

Usability improvements include additional features on the **Home** dashboard, enhancements to the **Incident Details** page, improvement of the workflow, full match string displays, and addition of a **Network Statistics** page.

Usability improvements streamline usage for users and administrators.

- The **Home** page includes more customization options;
- The **Incident Details** page has been improved to include more information;
- The improved workflow on the **Incident Details** page gives users more options for viewing their incidents:
- Full match strings and the content immediately preceding or following the incident are displayed, providing more content for better understanding of the significance of incidents;
- The **Network Statistics** page gives administrators information about the McAfee DLP system at a glance.

System improvements

OpenLDAP is supported, the system is FIPS-compliant, and the products are entered into Common Criteria evaluation.

Directory server integration is extended to OpenLDAP servers, allowing for LDAP integration in non-Active Directory environments. This delivers the ability to configure rules, generate reports, review incidents, paginate directory entries, identify users, create roles, and support multiple domain controllers using OpenLDAP parameters.

The products have been entered into lab evaluation for Common Criteria (Q4, 2010), potentially allowing entry into the U.S. Federal government vertical.

FIPS readiness updates all cryptographic modules (OpenSSL, OpenSSH, Java libraries, MD5 to SHA-2 conversion) to be FIPS-compliant, potentially allowing entry into the U.S. Federal government vertical.

Capture engine enhancements

The capture engine now extracts headers and footers from Microsoft Office documents, archiving support has been expanded, and the capture database allows time-based wiping.

Because sensitive data that might exist in the headers, footers, and properties of Microsoft Office documents can be extracted, there is better data loss coverage for common applications. Enhancements to classification engine also allows those areas to be analyzed against defined policies.

Content can now be extracted from the 7Zip archiving application.

Erasing of capture data, which can be configured by the user, can be done via time-based parameters. This allows for a better fit into specific data retention policies in large enterprise environments.

Browser support

McAfee Total Protection for DLP products support Internet Explorer versions 6 and 7, and Mozilla Firefox 3.0.x.

Internet Explorer 8 and 9 and subsequent versions of Firefox are not supported.

McAfee DLP data types

The three product dashboards display the incidents and events found by the McAfee DLP products.

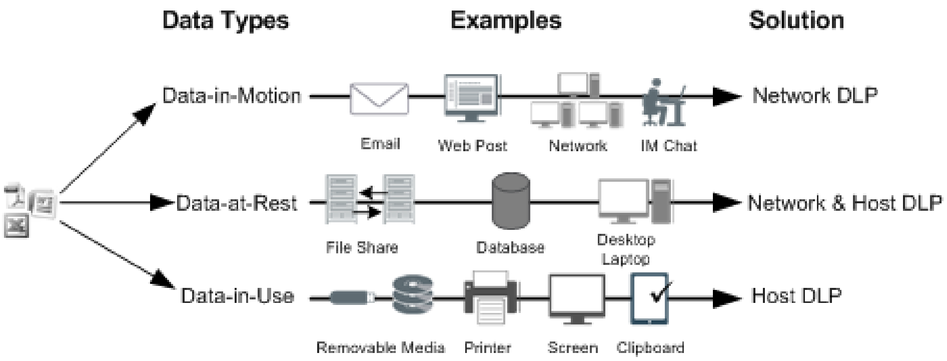


Figure 1-2 Data types

Table 1-1 Data type descriptions

Product	Function
Data-in-Motion	Data-in-Motion on the network is captured and parsed into hundreds of different categories by McAfee DLP Monitor. All real-time and historical data on the network is searchable, allowing for the creation of rules that adapt to changing content.
Data-at-Rest	Data-at-Rest in network repositories is inventoried by McAfee DLP Discover and sensitive data is registered automatically when it is matched to existing rules and policies. Not only is the contents of documents recognized and protected, but individual documents are explicitly protected individually or in groups. McAfee DLP Endpoint defines Data-at-Rest on endpoints by location, document properties, user-defined metadata, file types, text patterns and attributes, encryption types, and user groups.
Data-in-Use	Data-in-Use on endpoints is matched to the same rules and policies as all other network data, but addition of one or more endpoint parameters can add the ability to keep data from being compromised in a variety of ways. Rule parameters can also be extended to specific shares, network paths, file or encryption types.

2 Home

The **Home** page configuration is determined by the settings in the user's account.

Contents

How the Home page is configured

The **Home** page displays a brief summary of the problems found by McAfee DLP appliances. Its configuration depends on what data the user considers most significant.

The **Home** page provides an overview of systems monitored by McAfee DLP. Users can configure up to four dashboards to provide the most relevant information at a glance.

> The **Home** page contains only report summaries. The **Incidents** dashboard must be used to sort, filter, or manage the incidents.

How the Home page is used

The **Home** page is used to display a brief summary of the problems found by McAfee DLP appliances. Its format depends on the role and permissions of the user.

The **Data-in-Motion**, **Data-at-Rest**, and **Data-in-Use** windows display incidents and events that have been generated by McAfee DLP Monitor, McAfee DLP Discover, and McAfee DLP Endpoint. These categories correspond to data found in network traffic, repositories, and at network endpoints.

> The **Home** page contains only report summaries. The **Incidents** dashboard must be used to sort, filter, or manage the incidents.

Customize the Home page

Customize the **Home** page to display reports of the most significant incidents and events found by the McAfee DLP appliances.

Up to four reports can be customized at one time.

Task

1 Select **Home**.

2 Click **Options** and select **Customize.**

3 On the **Dashboard Type** page, check the boxes of one or more dashboards.

- Select **Pre-defined** and select one of the pre-configured dashboards from the drop-down list.
- Select **Chart**, name the dashboard, then select from the options available.

4 Click **Apply**.

Check Home page permissions

Check the **Home** page permissions to verify that the type of data displayed matches the user's role in the organization.

Task

1 Select **System** | **User Administration** | **Groups** .

2 Double-click the icon in the **Details** column next to the group you want to review.

The detailed information table appears.

3 Select **Task Permissions** | **Incident Permissions**.

4 Verify that the **View Home page** box has been selected. If it is not, the **Home** tab will not appear.

3 Using the Incidents dashboard

The **Incidents** dashboard displays a detailed and comprehensive picture of the incidents and events detected by McAfee DLP systems. The objects reported are stored in three different databases, which correspond to the appliances that produced them.

Table 3-1 Database vectors

Database vector	Definition
Data-in-Motion	Incidents are produced by McAfee DLP Monitor when its rules match data in the network stream.
Data-at-Rest	Incidents are produced by McAfee DLP Discover when a scan finds sensitive data in network repositories or databases.
Data-in-Use	Events are produced by McAfee DLP Endpoint when data violations are found at network endpoints.

Contents

How incidents are sorted

The capture engine sorts all network data and stores it in the McAfee DLP databases. Each object in the database is defined by its attributes, which can be sorted to reveal significant patterns.

Columns on the dashboard display the attributes of all incidents. They can be sorted by clicking in the table header.

Attachments to incidents can be displayed if they are under 50 MB. The number of incidents that can be reported is limited to 150,000. After that number is reached, chunks of supporting data are wiped, starting with the oldest incidents first.

Sorting allows you to set aside results that are not immediately relevant, but might be significant at a later date. Save a view or report to revisit the data.

Find policy violations

Find policy violations by selecting the incidents in the display pane and viewing the policies and rules displayed in the navigation pane.

Task

1. Select **Incidents**.
2. Select one of the policies listed in the **Group by** frame. The incident listing displays only incidents found by that policy.
3. Click the **Group Detail** icon. Violations are grouped by policy by default.

Find violations by attribute

Find violations by attributes of incidents saved in the McAfee DLP databases. Sorting by attribute displays incidents that have the selected attributes in common.

Task

1. Select **Incidents**.
2. Click a column header to sort by attribute.

   The dashboard displays all incidents that have that attribute in common.

Delete incidents

Delete incidents that are not useful to clear the display pane for significant results.

Task

1. Select **Incidents**.
2. Select the checkboxes of incidents to be deleted.
3. From the **Actions** menu, select **Delete**.

Delete similar incidents

Delete similar Incidents if they are no longer useful, or if they share attributes that trigger false positives.

Task

1. Select **Incidents**.
2. Click on a column that identifies the attribute shared by the false positive incidents.
3. Select the checkboxes of incidents that share the attribute.
4. From the **Actions** menu, select **Delete**.

How incidents are filtered

The capture engine sorts captured data into objects and their attributes. Each incident displayed on the McAfee DLP dashboard is supported by a wide range of supporting data.

So many incidents are reported that filtering is necessary to display only those that are significant. Incidents can be grouped or filtered using the sorting tools in the frame that supports the incident dashboard.

With this release, filters can be added to the incident dashboard whether or not there are values in an attribute field.

> Click on any data cell, even if it is empty, to use the attributes of an incident can be used as sorting keys.

Filter incidents

Filter incidents that have been reported to the dashboard into configurations that reveal significant data patterns.

Task

1. Select **Incidents**.
2. Click the **List** icon, if necessary.

   List is the default dashboard view.
3. In the **Filter by** pane, pull down the second timestamp menu to select a time frame. If you select **Custom Dates**, click the **?** to launch input fields.

   The time frame must not exceed the limits of the data captured.

   For example, if you select **Yesterday** but your McAfee DLP appliances were set up **Today**, you will filter out everything on your dashboard.
4. Click the plus icon to add another sorting key.
5. Click **Apply**.
6. Repeat as needed until a significant data pattern is revealed.

Group incidents

Group incidents that have been reported to the dashboard into configurations that reveal significant data patterns.

Task

1. Select
2. Click the **Group Detail** icon.
3. In the **Group by** pane, pull down the first menu and select a primary sorting key for the incidents on the dashboard.
4. In the **Group by** pane, pull down the second menu and select a secondary sorting key for the incidents on the dashboard.
5. Change the groups as needed until a significant data pattern is revealed.

Set a time filter for incidents

Set a time filter to limit the incidents displayed to a relative time frame. Customized dates can also be set to define a specific time frame.

Task

1. Select **Incidents**.
2. Click the **List** icon, if necessary.

   List is the default dashboard view.

3. In the **Filter by** pane, pull down the second timestamp menu to select a time frame. If you select **Custom Dates**, click the **?** to launch input fields.

   The time frame must not exceed the limits of the data captured.

   For example, if you select **Yesterday** but your McAfee DLP appliances were set up **Today**, you will filter out everything on your dashboard.

4. Click **Apply**.

Clear filters

Clear filters to release configurations that display a specific set of attributes. When incidents are filtered, the configuration will block all other results until the filter is cleared.

Task

1. Select **Incidents**.
2. Click on the **List** icon, if necessary.

   List is the default dashboard view.

3. In the **Filter by** pane, click **Clear All**.
4. Click **Apply**.

How to work with incident details

The **Incident Details** page provides in-depth information about incidents and events detected by McAfee DLP systems.

Tasks

- *Get incident details* on page 29
  Get incident details by clicking the **Details** icon of incidents reported to the dashboard. The **Incident Details** page displays incident attributes in an easily accessible layout.
- *Find concept matches* on page 30
  Find the concepts that match the content identified by a rule by clicking on the **Details** icon. The **Incident Details** page displays match strings for incidents that were generated by concepts.
- *Find match strings* on page 30
  Find match strings that display the content found by a rule by clicking on the **Details** icon. The **Incident Details** page displays match strings for incidents that contain alphanumeric strings.
- *Get history of incidents* on page 30
  Get the history of an incident by clicking on its **Details** icon. The **Incident Details** page displays the history by reporting what actions have been taken on it.
- *Find case status of incidents* on page 30
  Find the case status of incidents by clicking on the **Details** icon. The **Incident Details** page displays case status for incidents that were generated by concepts.
- *Assign incidents to cases* on page 31
  Add incidents to cases to add additional relevant information that will facilitate resolution.
- *Add attributes to incidents* on page 31
  Incidents might already share some of the same attributes, but if not, they can also be assigned directly from the dashboard. The value of each attribute can be modified at the same time.
- *Tune rules* on page 32
  Tune rules using historical data to modify parameters until the needed results are retrieved. In this release, rules can be tuned from the **Incidents** dashboard.
- *Get related incidents* on page 33
  When an incident is viewed on the **Incident Details** page, **Related Incidents** might also be displayed.

Get incident details

Get incident details by clicking the **Details** icon of incidents reported to the dashboard. The **Incident Details** page displays incident attributes in an easily accessible layout.

> Incidents that are captured in real time, like chat and FTP sessions, cannot display details (like file names and user information) because they cannot be synchronized with the existing flow.

> If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1. Select **Incidents**.

2. Select an incident and click the **Details** icon.

3. Select from the tabs and links on the page.

   Clicking an attachment (**Info | Content**) will launch the file if the corresponding software is installed.

Find concept matches

Find the concepts that match the content identified by a rule by clicking on the **Details** icon. The **Incident Details** page displays match strings for incidents that were generated by concepts.

> If you cannot see incident details, you need **View Incident Object** permission. See your administrator.

Task

1. Select **Incidents**.
2. Select an incident and click the **Details** icon.
3. View the **Concepts** box under the **Related Incidents** tab.

Find match strings

Find match strings that display the content found by a rule by clicking on the **Details** icon. The **Incident Details** page displays match strings for incidents that contain alphanumeric strings.

> If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1. Select **Incidents**.
2. Select an incident and click the **Details** icon.
3. Click the **Match String** or **Match String in File** tab.

Get history of incidents

Get the history of an incident by clicking on its **Details** icon. The **Incident Details** page displays the history by reporting what actions have been taken on it.

> If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1. Select **Incidents**.
2. Select an incident and click the **Details** icon.
3. Click the **History** tab.

Find case status of incidents

Find the case status of incidents by clicking on the **Details** icon. The **Incident Details** page displays case status for incidents that were generated by concepts.

> If you cannot see incident details, you will need **View Incident Object** permission. See your administrator.

Task

1. Select **Incidents**.
2. Select an incident and click the **Details** icon.
3. Click the **Cases** tab.

Assign incidents to cases

Add incidents to cases to add additional relevant information that will facilitate resolution.

No more than 100 incidents can be added to a case at one time.

Task

1. On your Linux-based appliance, select **Incidents** | **Incidents**.
2. Select one or more incidents.
3. Click **Assign to Case**, then select **Assign to Case** | **New Case** or **Assign to Case** | **Existing Case**. For a new case, do the following:
   a. Fill in the **New Case** form. Required fields are **Headline**, **Keywords**, and **Owner**.
   b. Click **Apply**.

   The new case is created and the incidents are assigned to it.
4. For an existing case, do the following:
   a. Review the case details and modify menus as necessary.
   b. Make **Notes** to indicate how the case has changed by the addition of this incident.
   c. Click **Apply**.

   The incidents are assigned to the case.

Tasks

- *Change the ownership of cases* on page 92
  Change the ownership of cases to give primary responsibility for resolution to a specific user group.
- *Change the resolution status of cases* on page 92
  Change the stage of resolution of cases if their conditions have changed.
- *Change the status of cases* on page 92
  Change the status of cases to indicate their states of resolution.
- *Reprioritize cases* on page 93
  Reprioritize cases according to their changing states as they move through states of resolution.
- *Collect credit card violations in cases* on page 93
  Collect credit card violations in a single case to resolve privacy violations in one operation.
- *Notify users of a case* on page 93
  Notify users of changes in a case.
- *Add comments to cases* on page 94
  Add comments to cases to add information about one or more incidents contained in them.

Add attributes to incidents

Incidents might already share some of the same attributes, but if not, they can also be assigned directly from the dashboard. The value of each attribute can be modified at the same time.

Before you begin

Attributes can be set in two locations: from the incident listing, or on the **Incident Details** page after selecting the incident.

The attributes available for modification are **Status**, **Status**, **Reviewer**, **Resolution**, **Severity**, and **Comments**.

> If you do not have permission to view an attribute, it will not be displayed for modification.

Task

1. Select **Incidents**.
2. Select one or more incidents whose attributes you want to modify.
3. Do one of the following:
   - If you want to modify attributes from the incident listing, click **Attributes** in the dashboard header. Select the checkboxes of the attributes to be modified, then select a new value from the drop-down menu and click **Apply**.
   - If you want to modify attributes from the **Incident Details** page, click the **Details** icon. Select new values from the drop-down menus, and add optional comments.

Tune rules

Tune rules using historical data to modify parameters until the needed results are retrieved. In this release, rules can be tuned from the **Incidents** dashboard.

> Tune a rule from an incident by modifying the parameters of the rule that triggered it. Use the **Chart** and **Compare** charts to determine the results fits into the trend and the activity of the other rules.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.
2. Construct a query that might retrieve significant results.
3. Click **Search**.
4. If some significant incidents are reported, click **Save as Rule**.

   The **Edit Rule** page launches.
5. Enter a rule name and add an optional description.
6. Assign the rule to a policy by selecting one from the **Policy** menu.

   > Store the new rule in a policy containing rules like it.
7. Select a **Severity** to rate the importance of the rule.
8. Since the rule is to be tuned, leave the **Inherit Policy State** set to **Disabled** so it can be run independent of its policy until it reports the needed results reliably.
9. Click **Test Rule** and examine the results.

   > Take note of the incidents that are not useful, and try to match them up with the parameters that produced them.
10. Modify the rule to eliminate the parameters that produced the incorrect results.

    For example, if the text pattern of your rule matched all Microsoft Office documents, but you needed only spreadsheet data, deselect **Select All** in the Office Applications category to retrieve only Microsoft Excel documents.
11. Click **Test Rule**.

12 Repeat the process until your rule retrieves the correct results.

13 Set the **Inherit Policy State** to **Enabled** to bind the rule to its policy.

It will run whenever the policy runs.

14 Click **Save**.

Get related incidents

When an incident is viewed on the **Incident Details** page, **Related Incidents** might also be displayed.

> **Before you begin**
>
> Related incidents are based on values in six fields: Signature, File name, Source IP, Destination IP, Sender, and user ID.

Task

1 Select **Incidents**.

2 Select an incident and click the **Details** icon.

3 View the statistics in the **Related Incidents** tab in the right pane.

How views are set up

Pre-configured dashboard views reflect the content of the incident and event databases. They can be selected from the **Incident Listing** menu, and custom views are automatically added to the list.

When incidents are grouped and filtered, significant data patterns emerge. When this happens, the configuration can be saved so that it can be re-used as new incidents are added over time.

Attachments to incidents can be displayed if they are under 50 MB, and the number of incidents that can be reported is limited to 150,000. After that number is reached, chunks of supporting data are wiped, starting with the oldest incidents first.

Select different views from the **Incident Listing** menu to get ideas about how to filter your results.

Save views

Save views to record incident configurations that result from grouping and filtering incidents. Saving effective configurations allows re-use when new incidents are found.

To save the content of a dashboard view instead of the settings, create a report.

Task

1 Select **Incidents** | **My Views**.

2 Select **Data-at-Rest**, **Data-in-Motion**, or **Data-in-Use** from the view vector menu.

3 Click the **Disk** (**Save View**) icon.

4 Name the view.

5 Select an owner.

Ownership is determined by the groups to which a user belongs. If a user's group is not listed, add a new one and assign the user to it.

6 Select the **Set as Home View** checkbox.

7 Click **Save**.

Select pre-configured views

Pre-installed views display incidents in a wide variety of configurations.

💡 This is a good way to figure out how to filter your incidents into the most significant data patterns.

Task

1 Select **Incidents**.

2 Select any view from the **Incident Listing** menu and review the results.

Select view vectors

Select view vectors to display incidents from three different databases.

Table 3-2 View vectors

Vector	Database
Data-at-Rest	Static data found in network file systems or databases
Data-in-Motion	Dynamic data found in network traffic
Data-in-Use	Static data found at network endpoints (desktops, laptops, removable media, printers, etc.)

Task

1 Select **Incidents**.

2 Select **Data-at-Rest**, **Data-in-Motion**, or **Data-in-Use** from the view vector menu.

Select graphical views

Select from the default graphical views to display incidents in configurations that can be understood at a glance.

💡 Use these views to get ideas on how to display your incidents graphically.

Task

1 Select **Incidents**.

2 Click the **Group Detail** or **Summary** icons and review the results.

Copy views to users

Copy views that display useful configurations to groups of users who will find them useful.

Task

1 Select **Incidents** | **My Views**.

2 Check one or more boxes.

3 From the **Actions** menu, select **Copy View to Users** and select one or more user groups.

4 Click **Apply**.

The warning appears: **This operation will overwrite views with the same name for the selected users if it exists.** If you want to continue, click **OK**.

Delete views

Delete views if their settings do not display incidents in useful configurations.

Task

1 Select **Incidents** | **My Views**.

2 Check one or more boxes.

3 From the **Actions** menu, select **Delete**.

How reports are generated

Reports contain the content of the incidents and events displayed on the dashboard. They are available in PDF, HTML, or CSV format.

Reports can be generated from dashboard incidents in PDF, HTML or CSV output. If you want to save only the dashboard settings, save a **View** instead.

> There are limitations on size and number of incidents supported in reports. The maximum size of reports is 5 MB; an incident that is exported cannot be saved if it is larger than that.

CSV reports must not exceed 150,000 incidents.

Create PDF reports

Create PDF reports by selecting the format from the **Options** menu on the **Incidents** dashboard. Reports from the **Incident Details** page include one incident unless the **List** button is selected.

Task

1 Select **Incidents**.

- From the **Incidents** dashboard, click **Options** and select the PDF report format.
- From the **Incident Details** page, click the PDF icon.

2 Allow some time for the report to generate.

3 **Open** or **Save** the report.

4 Click **OK**.

Create HTML reports

Create HTML reports by selecting the format from the **Options** menu on the **Incidents** dashboard. Reports from the **Incident Details** page include one incident unless the **List** button is selected.

Task

1 Select **Incidents**.

- From the **Incidents** dashboard, click **Options** and select the HTML report format.
- From the **Incident Details** page, click the HTML icon.

2 Allow some time for the report to generate.

3 **Open** or **Save** the report.

4 Click **OK**.

Create CSV reports

Create CSV (comma-separated values) reports by selecting one or more incident checkboxes, then selecting **Export CSV** from the **Options** button.

If you are on the **Incident Details** page when you decide to create a report, click the **List** button to return to the previous view.

> ℹ For the CSV report type, there is no maximum number of incidents or maximum report size. The report will launch in spreadsheet format if you have Microsoft Excel installed.

Task

1 Select **Incidents**.

- From the **Incidents** dashboard, click **Options** and select the CSV report format.
- From the **Incident Details** page, click **List** and check the box of a single incident, then click **Options** to select the CSV report format.

2 Allow some time for the report to generate.

3 **Open** or **Save** the report.

4 Click **OK**.

Schedule reports

Schedule reports of incidents to run on a regular schedule by defining options on the **Disk** page. You can also set up notification on this page for users who have a need to know.

> ℹ Reports and Views share the same interface. From the **View Properties** page, you can set the current dashboard configuration as a **Home View** or schedule one or more reports.

Task

1 Select **Incidents**.

2 Click the **Disk** (Save View) icon.

3 Type a report name (**View Name**) and select an owner.

4 Select the **Schedule Reports** checkbox.

5 Select a checkbox to choose a report type.

6 Select start and end dates, time of day, and frequency of the report.

7 (Optional) Set up notification.

By default, the email address of the user who is logged on is automatically entered in the **From** field.

a Type a different or additional email address in the **From** field.

b Type one or more email recipients in the **To** field.

c Type an email subject in the **Subject** field.

8 Enter a message in the **Message** field.

9 Click **Save**.

Add report titles

Add a company name or other identifying information to a report.

Task

1 Select **System**.

2 Click the **Configure** link for the McAfee DLP Manager being used to create the report.

3 Scroll down to **Company Information (for reports)**.

4 Type in a company or organization name.

5 Click **Update**.

How dashboards are customized

Dashboards can be customized to expand the display area, list of more incidents, or display additional attributes that are hidden by the default configuration.

Expand dashboard display

Expand dashboard displays by collapsing or expanding the navigation pane. The size of the display and navigation panes can be reconfigured by dragging the separator between them.

Task

1 Select **Incidents**.

2 Double-click the vertical separator between the incidents and the navigation pane.

3 Repeat to restore.

Drag the separator to change the size of the panes.

Add rows to the dashboard

Add rows to the standard number displayed on dashboards (25 per page) by selecting a number on the **Columns** page.

> Viewing a large number of incident rows at one time (1,000 or more) could cause an HTTP REQUEST timeout.

Task

1. Select **Incidents**.
2. Click the **Columns** icon.
3. Select a number from the **Incidents per page** drop-down menu.
4. Click **Apply**.

Configure dashboard columns

Configure dashboard columns to modify the display of attributes of an object by selecting different columns from the **Columns** page.

Task

1. Select **Incidents**.
2. Click the **Columns** icon.
3. On the **Table Columns** page, under **Selected**, select a column.

   Reposition the order of the columns by using the **Move** buttons. Expand your dashboard if you cannot see them.
4. Click **Apply**.

Add a match string column

Add match string columns that reflect the content detected by a search or rule. Because match strings do not relate to all incidents, the column that contains them is not displayed by default.

Task

1. Select **Incidents**.
2. Click the **Columns** icon.
3. On the **Table Columns** page, under **Available**, select **MatchString** and click **Add**.

   MatchString can only be applied to **Data-in-Motion** and **Data-at-Rest** incidents.
4. Click **Apply**.

How dashboard settings work

McAfee DLP systems capture everything on the network (except traffic which is deliberately filtered out using capture filters). Changing the settings can control how many incidents are reported at once, and how they are delivered to the dashboard.

Expanding the number of incidents reported to the dashboard could overburden the system, but configuring throttling can remediate that problem.

Similarly, you can comply with PII (personally identifiable information) requirements by encrypting certain elements, but you can configure throttling to manage the system resources that are being consumed while doing so.

Encrypt incidents

When incidents that contain sensitive information are found, they can be encrypted to prevent exposure of their contents.

When the encryption feature is enabled, two significant files (subject and matchstring) that might contain PII information are encrypted before storing to the database. They are decrypted before displaying on the dashboard.

Task

1. Select **Policies** | **Settings**.
2. Select the **Encrypt Sensitive Incident Data** checkbox to encrypt all incidents found.
3. Select the **Encrypt Capture Data** checkbox to encrypt the entire capture database.

   Selecting this option might impede performance.

4. Click **Save**.

Configure throttling to limit incidents reported

Configure throttling to limit the number of incidents reported to the dashboard.

You can set throttling to report between 1 and 9,999 incidents in from 10 to 3600 seconds. Throttling is enabled by default; to report all incidents, deselect the **Enable Throttling** checkbox.

The throttling parameters "Time Duration" and "Number of Incidents" are global and applicable for all rules in the system. When throttling is enabled, if any rule triggers more incidents than specified in throttling parameters in the specified time duration, all extra incidents from that time duration will be suppressed.

Task

1. Select **Policies** | **Settings**.
2. Under **Configure Throttling Parameters**, leave the **Enable Throttling** checkbox selected.
3. Enter the maximum **Number of Incidents** to be reported.
4. Enter the maximum **Time duration** in seconds.
5. Click **Save**.

4 Search

The McAfee DLP interface allows basic and advanced searches. You can use logical operators on command lines in the interface, but only when using concept and keyword expressions that define data patterns.

Open random rules under policies in the **Policies** tab to learn how to use search parameters to build queries.

Searching captured data is role-based and dependent upon permissions. If you need additional permissions, consult your administrator.

Contents

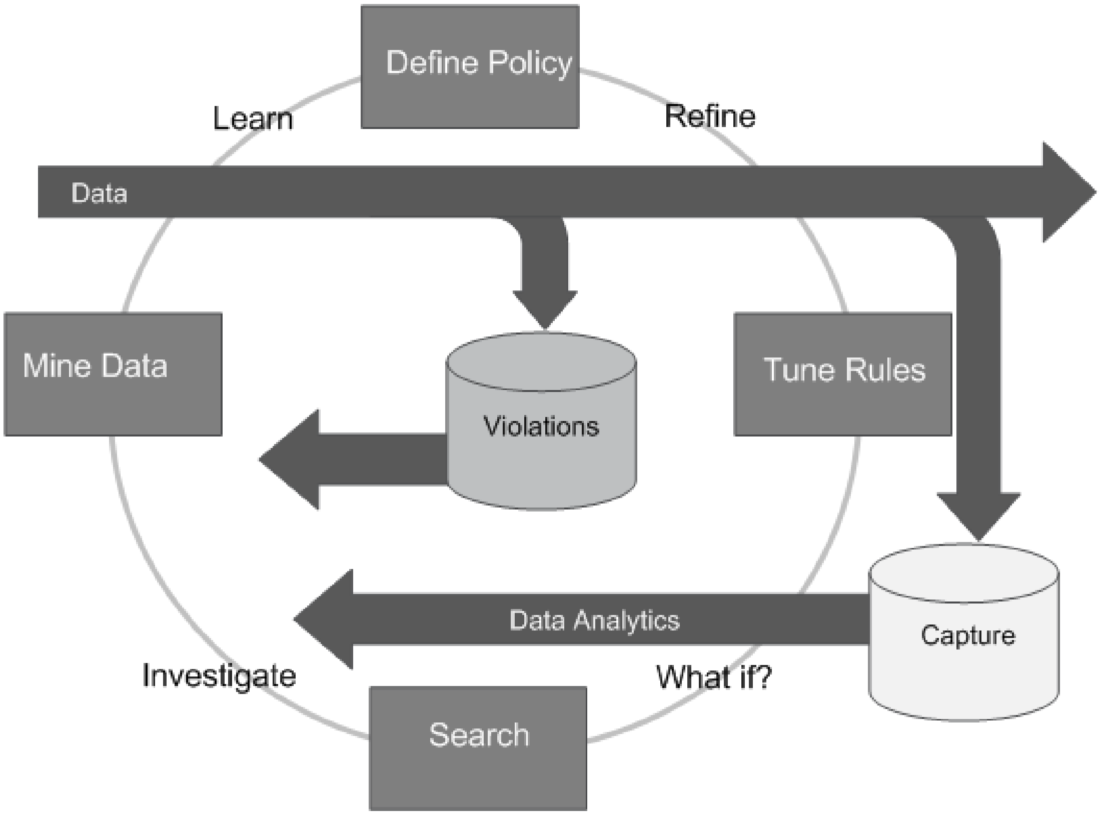
How data is captured and processed

The capture engine classifies and parses all data by object and attribute type.

Capture data is not indexed for **Data-in-Use**.

The core component of McAfee DLP is a capture engine that allows reassembly of packets that have been extracted from network traffic or repositories by McAfee DLP Monitor or McAfee DLP Discover.

The reassembled objects are classified into object types that are saved in the McAfee DLP Monitor database. Each object has many attributes, all of which can be retrieved by queries.



Captured data is indexed and analyzed in three different databases that hold **Data in Motion**, **Data at Rest**, and **Data in Use**. You can query the databases directly using the options available in the user interface, or save queries that are to be run regularly as rules.

When an object matches a query or rule, the result is reported to the McAfee DLP dashboards as an incident. Incidents can be sorted and filtered according to their attributes so that the most significant information can be identified and displayed.

ℹ You need not search or save rules to get results. Standard policies that contain collections of rules automatically search live data in real time to produce incidents.

How the capture engine works

The capture engine captures, analyzes, and stores all network data. When the capacity of McAfee DLP Monitor reaches 70% capacity, the earliest captured data is wiped.

The core component of McAfee DLP is a capture engine that extracts packets from network traffic or repositories. They are indexed and analyzed, classified into object types, and saved in databases on capture partitions on the McAfee DLP Monitor and McAfee DLP Discover appliances.

You can query the McAfee DLP Monitor and McAfee DLP Discover databases directly using the options available in the user interface, and save queries that are to be run regularly as rules.

When an object matches a query or rule, the result is reported to the dashboard as an incident.

> You need not search or save rules to get results. Standard policies that contain sets of rules automatically search captured data to produce incidents, and concepts that match related parameters to network data can be used as a shortcut to find text-based data quickly.

How capture works

McAfee DLP Monitor captures all network traffic, and performance and results can be improved by deploying capture filters that limit the amount of data that will be recognized and indexed. After capture and classification, incidents can be extracted from the database automatically or manually.

Both Microsoft Active Directory and OpenLDAP servers can be used with McAfee DLP Manager. With this release, the following OpenLDAP features are supported.

- Automatic extraction - Standard policies are pre-configured to apply rules to classified network data. When a rule hits on a match, an incident is created in the database and reported on the Data-in-Motion dashboards. For example, if you have the HIPAA (Health Insurance Portability and Accountability Act) policy deployed, the system will identify and report any medical privacy violation.
- Through McAfee DLP Manager, you can query all databases directly using the search options available. When a query hits on significant data, the search can be repeated on a regular basis by saving it as a rule under a new or existing policy.
- When a query or rule matches any stored attribute, the entire object to which it belongs is reported to the dashboard as an incident.

Get search details

Search history and parameters are recorded on every McAfee DLP appliance and displayed on the McAfee DLP Manager dashboard as **Search Details**. This display is different from search **results**, which are displayed on the McAfee DLP Manager dashboard.

Task

1. On your Linux-based appliance, select **Capture** | **Search List**.
2. Click the **Details** link.

   Search results are displayed.

Stop searches

You can stop searches that are running, but no useful results are retrieved.

Task

1. On your Linux-based appliance, select **Capture** | **Search List**.

   All searches are listed in chronological order by database searched.
2. Click **Abort** for the search you want to stop.

Set search parameters

Add or subtract McAfee DLP parameters by clicking red or green icons in the user interface.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.

   This page is used as an example. Any search, rule, filter or case page offers the same icons and responds to the same actions.

2. Open any category.
3. Click the green **plus** icon to define a new parameter.
4. Click the red **minus** icon to delete any existing parameter.

Set up search notification

Set up search notification for searches that take over 60 seconds. Time-consuming queries run in background mode, and when results are available, email notification is sent.

The user who is to receive the notification must log out and log on to register the change.

> Set up the email client to prompt the user when new email comes in.

Task

1. On your Linux-based appliance, select **System** | **User Administration**.
2. Click the **Details** icon of the user's group.
3. Enter an email address in the **Email** field.
4. Click **Apply**.
5. Construct a search.

   If the search takes over 60 seconds, check your email periodically for notification of its completion. If a search is aborted, no notification is sent.

Search by attribute

Search by document and user attributes to narrow your searches.

Tasks

- *Find chat sessions* on page 55
  Find chat sessions by searching for chat content types. Sessions lasting up to four hours can be retrieved.
- *Find geographic users and incidents* on page 55
  Find incidents generated by users in other countries by defining geographic locations in your query. The classification engine sorts all network data into geographic locations.
- *Find IP addresses* on page 56
  Find IP addresses, a range of addresses, or a subnet containing IP addresses in captured data by typing them into value fields.
- *Find a range of IP addresses* on page 56
  Find IP addresses by entering them into value fields. Define multiple addresses or address ranges by separating them with commas or dashes.
- *Find IP addresses on subnets* on page 56
  Find IP addresses on subnets by using subnet masks. Subnet searching is supported whether or not network and host portions of an IP address are standard classful IP (address fields separated into four 8-bit groups).
- *Exclude IP addresses* on page 56
  Exclude single IP addresses or IP address ranges from a query to rule out incidents that contain them.
- *Find source code* on page 57
  Find source code that might be leaving the network by searching with the **Source Code** content type.
- *Find websites* on page 57
  Find websites that violate rules by searching traffic to or from a user or host, or query the source or destination of a known transmission.

Finding email

Email objects are stored in capture databases as separate tokens. Search for one or more components of an email address (for example, user, host or domain names) to produce related results.

Because email attributes are captured, email can also be found by port, protocol, attachment, sender, recipient, cc, or bcc.

Email addresses or domain names that contain numbers are searchable only if they are in the addressing, subject, cc, or bcc fields. Only alphabetic characters are supported in the body of email messages.

> In rare cases, email addresses that are not present in SMTP mail may be displayed in strikeout mode in the highlighting on the dashboard.

Find email by address

Find email by searching for addresses.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

You can do a simple **to** or **from** address query from the **Basic Search** page.

2 Open the **Source/Destination** category.

3 Select **Email Address | sender is any of**.

Use **sender is none of** to exclude specific addresses.

Select the **sender** condition to indicate that the email address found was the source of the email. Use the green plus icon to add another parameter if you also want to define the recipient of the email.

4 Enter one or more email addresses into the value field.

5 Click **Search** or **Save as Rule**.

Find email attachments

Find email attachments by searching for the protocols used to send them. For example, HTTP_Webmail_Attach is used to find webmail attachments, and SMTP_Attach and POP3_Attach find email attachments.

Attachments larger than 50 MB cannot be reported.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Protocol** category and click **?**.

3 Open the **Mail Protocols** category.

4 Select one or more attachment types.

5 Click **Apply**.

6 Click **Search** or **Save as Rule**.

Find email by BCC

Find email by searching for entries on the **bcc:** line.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **Email BCC | is any of** and type the BCC addressee into the value field.

4 Click **Search** or **Save as Rule**.

Find email by CC

Find email by searching for entries on the **cc:** line.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **Email CC | is any of** and enter the CC addressee in the value field.

4 Click **Search** or **Save as Rule**.

Find email by domain

Find email in discovered data by searching for domain names.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.
2. Open the **Discover** category.
3. Select **Domain Name** | **contains any of** and enter one or more domain names in the value field.
4. Click **Search** or **Save as Rule**.

Find email by port

Find email by using common email types that are transported through well-known ports. For example, SMTP mail usually uses port 25, while HTTP webmail uses port 80.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.
2. Open the **Protocol** category.
3. Select **Port** | **is any of**.

   Use **is none of** or use **source** or **destination** options to exclude or focus results.
4. Enter a port number in the value field.
5. Click **Search** or **Save as Rule**.

Find email by protocol

Find email by searching for the protocols used to send it. For example, use the SMTP protocol to find email, or the HTTP_Webmail protocol to find webmail.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.
2. Open the **Protocol** category.
3. Click **?**.
4. Open the **Mail Protocols** category.
5. Select one or more email types.
6. Click **Apply**.
7. Click **Search** or **Save as Rule**.

Find email by recipient

Find email by using the **recipient** condition.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.
2. Open the **Source/Destination** category.

3. Select **Email Address | recipient is any of**.

   Use **recipient is all of** or **recipient is none of** to include or exclude specific recipients.

   Add more parameters to narrow the focus of your search.

4. Enter one or more email recipients in the value field.

5. Click **Search** or **Save as Rule**.

Find email by sender

Find email by using the **sender** condition.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.

2. Open the **Source/Destination** category.

3. Select **Email Address | is any of**.

   Use **is none of** to exclude specific senders.

   Add more parameters to narrow the focus of your search.

4. Enter one or more email senders in the value field.

5. Click **Search** or **Save as Rule**.

Find email by subject

Find email by searching for the text contained in subject fields.

Task

1. On your Linux-based appliance, select **Capture**.

2. Click either **Basic Search** or **Advanced Search**.

3. Open the **Source/Destination** category.

4. Select **Email Subject | contains any of**.

   Use **contains none of** to exclude specific subjects.

   Select the **sender** condition to indicate that the email subject found was the source of the email. Use the green plus icon to add another parameter if you also want to define the **recipient**.

5. Enter one or more email subjects in the value field.

6. Click **Search** or **Save as Rule**.

Find webmail by port

Find webmail by port by searching for communications using port 80. Web traffic commonly uses port 80, and a port search is especially useful when the direction of traffic is known.

> ℹ By default, a port search returns results in both directions, but in separate flows. For complete results, define both source and destination values.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.

2. Open the **Protocol** category.

3 Select **Port** | **source is any of** and enter `80` in the value field.

4 Select **Port** | **destination is any of** and enter `80` in the value field.

5 Click **Search** or **Save as Rule**.

Find webmail by protocol

Find webmail by searching for communications that use port 80. Web traffic commonly uses port 80.

ℹ You can use **Basic Search** to find all traffic on a single port quickly, but such a search is likely to return too many results. Use **Advanced Search** to add parameters that will focus your query.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Protocol** | **is any of** and click **?**.

The Protocols palette opens.

4 Open the **Mail Protocols** category.

5 Select one or more webmail types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Finding files

When the DLP search engine captures files, each file attribute is stored as a separate token in the capture database. You can find files by using any of the attributes of a file, such as type, owner, size or signature.

Search Examples

From the **Basic Search** menu, select **Host Name**, **Host IP**, **File Name Pattern**, or **File Owner** to find files in **Data at Rest**.

From the **Advanced Search** menu, select **File Information**, **Content Types**, or **Discover** to find files in **Data in Motion** and **Data at Rest**.

Find files by signature

Find files by searching for signatures created by the `SHA-2` algorithm (the `SHA-256` cryptographic hash function). The `SHA-256` sum utility creates compact digital signatures that can be used to find all copies of a uniquely-identified file.

The utility is available only on the McAfee DLP 9.2 appliance (Intel Server System SR3612UR), but you can also use open source file checksum tools to generate a unique signature.

ℹ File signatures cannot be used in a direct query, but they can be attached to a rule.

Task

1 Log on to the back end of the McAfee DLP Manager or McAfee DLP Monitor appliance.

2 Go to the `/usr/bin` directory on the Intel appliance and locate the `sha2sum` utility.

3. Use the utility to generate a signature.

   ```
   # sha256sum <filename>
   ```

4. Select and copy the resulting hexadecimal number.

5. Open a browser and launch the McAfee DLP user interface.

6. On your Linux-based appliance, select **Policies**.

7. Click a policy to open it for editing, then click a rule.

8. On the **Edit Rule** page, open the **File Information** category.

9. Select **Signature** | **is any of** and paste the hexadecimal number in the value field.

10. Click **Save**.

    When the rule runs, the file will be detected and displayed on the McAfee DLP dashboards.

    "Rule modification completed successfully" is displayed on the **Edit Policy** page.

Find files by size

Find files by defining their upper or lower size limits in a query.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.

2. Open the **File Information** category.

3. Select **File Size** | **range** and enter a value.

   Use **greater than** or **less than** to define upper or lower limits. For example, 0-10 (less than 10 bytes), 100-1k (between 100 bytes and 1 kilobyte), 10M-1G (between 10 megabytes and 1 gigabyte).

4. Click **Search** or **Save as Rule**.

Find files by type

Find files by searching for specific file types.

Narrow your selection to one or two file types and add parameters to keep from getting too many results.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.

2. Open the **Content** category.

3. Select **Content type** | **is any of** and click **?**.

   The Content Type palette opens.

4. Open a content type category.

5. Select checkboxes of file types.

6. Click **Apply**.

7. Click **Search** or **Save as Rule**.

Find document types

Find documents by searching for document file types.

> 💡 Narrow your selection to one or two document types and add parameters to keep from getting too many results.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.
3. Select **Content type | is any of** and click **?**.

   The **Content Type** palette launches.
4. Open the **Advanced Documents** category.
5. Select checkboxes of file types.
6. Click **Apply**.
7. Click **Search** or **Save as Rule**.

Find Microsoft or Apple documents

Find Microsoft or Apple documents by searching with office documentation content types. The classification engine sorts all network data into content types, allowing searches for engineering drawings, different types of source code, office documents, images, and countless other file types.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.
3. Select **Content Type | is any of** and click **?**.

   The Content Type palette opens.
4. Open the **Microsoft** or **Apple Application** categories.

   Microsoft Office documents are found in the **Office Documents** category.
5. Select checkboxes of file types.
6. Click **Apply**.
7. Click **Search** or **Save as Rule**.

Find office documents

Find common office documents that might be compromised by searching with office documentation content types.

> 💡 Narrow your selection to one or two file document types to keep from getting too many results.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

The Content Types palette opens.

4 Open the **Office Applications** category.

5 Select checkboxes to define one or more office document types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find proprietary documents

Find proprietary documents that might be compromised by searching with documentation content types.

> Narrow your selection to one or two file document types to keep from getting too many results.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

The Content Types palette opens.

4 Open the **Engineering Drawings and Designs** category.

5 Select checkboxes to define one or more design document types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find images of people

Find human imagery by searching with the **Fleshtone** concept. This is a good way to find images of people, which define advertising or x-rated sites.

> Add a **Thumbnail Match** column to your dashboard to scan results quickly. Avoid timeouts caused by retrieving large image files by adding additional search terms.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Concept** | **is any of** and enter `Fleshtone` in the value field.

4 Click **Search** or **Save as Rule**.

Find images using file types

Find images by searching for file types used by graphics.

> Add a **Thumbnail Match** column to your dashboard to scan results quickly. Avoid timeouts caused by retrieving large image files by adding additional search terms.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.
3. Select **Content type | is any of** and click **?**.

   The Content Type palette opens.
4. Open the **Image** category.
5. Select checkboxes of image file types.
6. Click **Apply**.
7. Click **Search** or **Save as Rule**.

Finding keywords

The properties of the language that is being used to query the capture database determine the techniques that are used to find keywords. Use logical operators with keyword expressions and exact phrases to get the most relevant results. Non-English keywords are considered exact phrases.

Search Examples

When keywords are used with the **contains all of** condition, spaces between words imply AND. For example, **Keywords | contains all of | Intel AMD NVidia**

When keywords are used with the **contains any of** condition, spaces between words imply OR. For example, **Keywords | contains any of | Intel AMD NVidia**

When keywords are used with the **exact phrase** condition, spaces between words are literal. For example, **Keywords | exact phrase | NVidia supports AMD and Intel platforms.**

When keywords are used with the **contains none of** condition, results that contain the keyword are excluded; but negative searches are not supported, so some positive condition must first be specified. For example, **Keywords | contains any of | Intel AMD.** Another parameter can then be added to exclude a related keyword from the results. For example, **Keywords | contains none of | NVidia.**

Custom queries can be typed directly into value fields. For example, the following expression finds one of the expressions in the first set of parentheses, but neither of the expression in the second set of parentheses. For example, `(Intel || AMD) !(Nvidia && ATI)`.

Paste in UTF-8 characters as exact phrases. For example, **Keywordsexact phrase** `<characters>`.

Find exact keyword matches

Find exact keywords by entering them into value fields and using the **Exact Phrase** feature.

Because search is case-insensitive, you need not capitalize the keywords. Do not add quotation marks and parentheses; they are added by the search engine.

Logical operators can be used only for queries containing keyword expressions and exact phrases.

Task

1. On your Linux-based appliance, go to **Capture | Advanced Search**.
2. Open the **Content** category.

3 Select **Keywords** | **exact phrase** and type the keywords to be matched into the value field.

4 Click **Search** or **Save as Rule**.

Find non-English keywords

Find non-English keywords by using the **Exact Phrase** feature. The search engine supports the UTF-8 standard, making it possible to find words using many different character sets.

Logical operators can be used only for queries containing keyword expressions and exact phrases. Non-English searches contain exact characters.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keywords** | **exact phrase** and paste the keywords and logical operators into the value field.

4 Click **Search** or **Save as Rule**.

Exclude keywords

Exclude keywords from a query to rule out incidents that contain them.

Narrow your selection to one or two file types and add parameters to keep from getting too many results.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keywords** | **contains none of** and enter one or more keywords in the value field.

4 Click **Search** or **Save as Rule**.

Use keyword expressions

Use keyword expressions (keywords and logical operators) to find violations in network data.

Use keyword expressions with regular expressions to extend pattern-matching queries.

Logical operators can be used only for queries containing keyword expressions and exact phrases.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Keywords** | **expression** and enter keywords and logical operators in the value field.

4 Click **Search**.

Use keywords

Use keywords to find significant incidents and violations in network data.

Narrow your selection to one or two file types and add parameters to keep from getting too many results.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.
3. Select **Keywords | contains all of** and enter one or more keywords in the value field.

   Alternatively, use the **contains any of** condition.
4. Click **Search**.

Find chat sessions

Find chat sessions by searching for chat content types. Sessions lasting up to four hours can be retrieved.

If you don't have to exclude incidents containing specific chat sessions, use **Basic Search** instead.

Encrypted chat sessions (for example, Skype and AOL Instant Messenger 6) cannot be captured.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.
3. Select **Content Type is any of** and click **?**.

   The Content Type palette launches.
4. Select the **Chat** category.
5. Select the chat protocol.
6. Click **Apply**.
7. Click **Search** or **Save as Rule**.

   Chat sessions are reported in chronological order.

Find geographic users and incidents

Find incidents generated by users in other countries by defining geographic locations in your query. The classification engine sorts all network data into geographic locations.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Source/Destination** category.
3. Select **GeoIP location | is any of** and click **?**. Use **is none of** to exclude a geographic location.

   The Geographic Locations palette launches.
4. Select continents and/or countries from the lists.
5. Add **Sender** and **Recipient** values to find users in the defined geographic locations.
6. Click **Apply**.
7. Click **Search** or **Save as Rule**.

Find IP addresses

Find IP addresses, a range of addresses, or a subnet containing IP addresses in captured data by typing them into value fields.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Source/Destination** category.
3. Select **IP Address | is any of** and enter IP addresses separated by a comma into the value field.

   `192.168.1.244,172.25.3.100-172.25.3.199`
4. Click **Search** or **Save as Rule**.

Find a range of IP addresses

Find IP addresses by entering them into value fields. Define multiple addresses or address ranges by separating them with commas or dashes.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Source/Destination** category.
3. Select **IP Address | is any of** and enter the IP addresses, separated by a comma, in the value field. Identify IP address ranges by separating IP addresses with a dash.

   192.168.1.244,172.25.3.100-172.25.3.199
4. Click **Search** or **Save as Rule**.

Find IP addresses on subnets

Find IP addresses on subnets by using subnet masks. Subnet searching is supported whether or not network and host portions of an IP address are standard classful IP (address fields separated into four 8-bit groups).

> CIDR (Classless Inter-domain Routing) notation is supported.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Source/Destination** category.
3. Select **IP Address | is any of** and enter the subnetted IP addresses in the value field.

   For example, for subnet mask 255.255.255.128, you can type in `192.168.2.1/25`.
4. Click **Search** or **Save as Rule**.

Exclude IP addresses

Exclude single IP addresses or IP address ranges from a query to rule out incidents that contain them.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Source/Destination** category.

3 Select **IP Address | is none of** and enter an IP address or range in the value field.

Add another parameter to narrow the focus of the query.

4 Click **Search** or **Save as Rule**.

Find source code

Find source code that might be leaving the network by searching with the **Source Code** content type.

Narrow your selection to one or two code types to keep from getting too many results.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type | is any of** and click **?**.

The Content Types palette opens.

4 Open the **Source Code** category.

5 Select checkboxes to define one or more code types.

6 Click **Apply**.

7 Click **Search** or **Save as Rule**.

Find websites

Find websites that violate rules by searching traffic to or from a user or host, or query the source or destination of a known transmission.

When defining a URL in a Discover scan, the URL must be preceded by the protocol used and terminated by a slash. If the URL is not terminated, the scan will run not only within the targeted directory and subdirectories, but will be extended to directories above the parent URL.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Source/Destination** category.

3 Select **URL | is any of** and enter one or more website names in the value field.

4 Click **Search** or **Save as Rule**.

Rules used by the capture engine

McAfee DLP captures all data on the network. The indexer uses a set of rules to classify and store data so that it can be handled efficiently

The following search topics explain rules used by the indexer.

- Distributed searching
- Large-scale searches
- Negative searches
- Proper name treatment

- Number of results supported
- Time-stamping files
- Archive handling
- Case insensitivity
- Microsoft Office 2007 anomalies
- Parts of speech excluded from capture
- Short word handling
- Special character exceptions
- Word stemming

Distributed searching

Searches that are distributed to more than one McAfee DLP appliance are handled through McAfee DLP Manager.

Although distributed searches default to **All Devices**, the **Devices** button on the **Advanced Search** page supports searches on specific McAfee DLP devices.

Large-scale searches

Searches that take over 60 seconds to process are run in background mode. When the search is complete, the user who is logged on is notified by email.

Although distributed searches default to **All Devices**, the **Devices** button on the **Advanced Search** page supports searches on specific McAfee DLP devices.

Number of results supported

The search engine imposes limitations on the number of search results supported by McAfee DLP.

The search engine is designed to retrieve no more than 10,000 results at a time. If this limit is exceeded, match strings will not be retrieved, and hits on substrings may return overly broad results.

> The dashboard incident list is limited to 5,000 results, but up to 150,000 incidents can be exported via CSV. Export from dashboard is limited to 5K. If your search results exceed this number, narrow your query and repeat the search.

Time-stamping files

Every file is time-stamped when it is added to one of the McAfee DLP databases.

Objects are time-stamped in UTC Universal Coordinated Time at the moment they are captured in network traffic, found in file systems or databases, or generated as endpoint events. McAfee DLP systems do conversion between local and global time automatically.

For this reason, it is essential to set time frames for searches or rules, and to remember the date of installation of a McAfee DLP appliance. (The system cannot retrieve results that have not yet been found.)

> If a time frame is set as a filter, any results reported as the result of a search or rule will be constrained to that time frame. The filter must be cleared before the results outside of that time frame can be viewed.

Archive handling

When archived files are captured, they are opened and their contents are analyzed by the indexer.

The search engine finds, extracts, and evaluates content in .zip, .gzip, and .tar archives, but only if the compressed file type is identified in the query.

Eight other compressed file types are also supported.

Case insensitivity

The indexer does not distinguish between cases.

Case sensitivity is ignored by the search engine. For example, if a query is defined in ALL CAPS, the system will retrieve and report the matching content, whether it is in upper or lower case.

Microsoft Office 2007 anomalies

The indexer ignores certain Microsoft Office attributes because of the way those applications handle fonts, colors, macros, and page definition.

- If two dictionary words are merged together, the merged word will not be found. For example, `American` and `Recovery` are two dictionary words. If they are merged into the word `AmericanRecovery`, they will not be found.
- If a word in a Microsoft Office document has different fonts and colors, the word will not be read as a whole and will not be found. For example, if all the letters in the word `Recovery` are of different fonts and colors, it will not be found.
- If a word continues across two different pages, it will not be found. For example, if the word `Recovery` is spread across two pages (one page contains `Rec` and the second page contains `overy`), it will not be found.
- Words in documents that use special Microsoft Office font features like WordArt, SmartArt, and watermarks will not be found.
- Words present in macros in Microsoft Office documents, and headers and footers in PowerPoint and Excel, will not be found.

Negative searches

The database does not recognize queries that consist entirely of negative terms.

A query containing only words that are not to be found is essentially instructing the search engine not to search. Therefore, some scope of data within which the term will not be found must be defined.

Proper name treatment

The indexer treats proper names like keywords.

For this reason, it is not necessary to capitalize proper names.

Parts of speech excluded from capture

The capture engine excludes common parts of speech to prevent insignificant results from being stored and retrieved.

Common parts of speech are ignored by the indexer.

For example, parts of speech like `a`, `and`, `this`, `therefore`, `else`, `while`, and `with` are excluded from capture.

Special character exceptions

Certain special characters are not supported in queries. Words that include non-alphabetic characters, such as numbers or spaces, are supported only if they are identified in an Exact Search.

Table 4-1 Characters that cannot be used in queries

Character	Description
.	period
;	semicolon
|	pipe
`	back tick
<>	less than/greater than
( )	parentheses
\ \\	backslashes
/>]]>	markup
*	control characters
/	escape characters

Word stemming

The capture engine supports word stemming to return words that are related to a query, but imposes restrictions to retrieve the most significant results.

The search engine does not recognize incomplete or partial words.

If an exact search is defined, stemming is disabled.

Example:

- Searching for "basket" to retrieve "basketball" will not return a result.
- Searching for "run" in "running" will return a result.

If the plural of a complete word used in a search is found, the result is reported as if it were a word stem.

Languages supported by search engine

McAfee DLP supports the following languages.

- English
- French
- German
- Spanish
- Portuguese
- Italian
- Japanese
- Russian
- Dutch
- Korean
- Chinese (simplified)
- Chinese (traditional)
- Polish
- Greek
- Hungarian
- Czech
- Turkish

Use logical operators in queries

McAfee DLP supports specific logical operators in queries.

All operators, including **Exact Match**, are case-insensitive. For example, if you search for a term in ALL CAPS, the system will return that term not only in capital letters, but initial caps or lowercase as well.

Use logical operators (`||` or `OR`) instead of a comma to construct an OR query. You cannot use AND operators between URLs and email fields.

Logical operators supported in queries

Logical operator	Notation	Examples
AND	`+ &&`	`Confidential Restricted Secret`
		`Confidential AND Restricted AND Secret`
		`Confidential and Restricted and Secret`
		`Confidential + Restricted + Secret`
		`Confidential && Restricted && Secret`
OR	`or ||`	`Confidential OR Restricted OR Secret`
		`Confidential or Restricted or Secret`
		`(Confidential || Restricted) && Secret`
NOT	`- !`	`Confidential -Restricted -Secret`
		`Confidential !Restricted !Secret`
Word Stemming	`~`	`Confident~ Restrict~ Secret~`
Parenthese	`( )`	`Confidential AND (Restricted OR Secret)`
Exact Match	`" "`	`"Confidential and Secret"`

Examples of queries using logical operators

Enter customized queries by using logical operators in McAfee DLP search fields.

Use the following examples to learn to construct keyword queries using the expressions and exact phrases fields.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Content** category.

3 Select **Keyword | exact phrase** or **Keyword | expression**.

4 Enter a query using logical operators in the value field.

5 Click **Search**.

Compound queries that will produce the same results

confidential + "Eyes Only" OR "Do Not Distribute" -secret -security

Confidential "Eyes Only" || "Do Not Distribute" !secret !security

Complex query that adds grouping of search terms and use of word stemming

Confidential + (("Eyes Only" || "Do Not Distribute") || (secret~ or secure~)) This query finds documents containing the word "Confidential" that are also marked EITHER "Eyes Only" or "Do Not Distribute" OR contain variations of the words "secret" or "secure".

Tips for searching

Search queries consist of one or more conditions, each of which is made up of an element, an operator, and value.

Logical operators are supported, but when helper pop-ups are available to ensure that correct values are being entered. You can use the simple examples provided here, or use them in combination to extract specific information from the McAfee DLP Manager databases.

Tasks

- *Search by excluding content concepts* on page 63
  Exclude content concepts from queries to prevent collections of data relevant to a single issue from appearing in search results.
- *Search by excluding ports* on page 64
  Exclude ports from a query to prevent incidents using them from appearing in search results.
- *Search by excluding protocols* on page 64
  Exclude protocols from a query to prevent incidents using them from appearing in search results.
- *Search by file creation time* on page 64
  Search for files that were created at a particular time.
- *Search by file last modification time* on page 65
  Search for files by the last time they were modified.
- *Search by global time* on page 65
  When you define a time in a search or rule, your local time is automatically converted to Greenwich Mean Time (GMT). If you are managing several McAfee DLP Monitor locations, you can find captured data at the same global moment in each of those locations.
- *Search by local time globally* on page 66
  When you define a time in a search or rule, your local time is automatically converted to Greenwich Mean Time (GMT). But if you are managing several McAfee DLP Monitor locations, you will want to use the local time (same clock time) in each of those locations.
- *Search by port* on page 66
  Search by port to identify incidents by source, destination, or in both directions.
- *Search by port range* on page 67
  Search by port range to identify incidents in a type of traffic by source, destination, or both.
- *Search by protocol* on page 67
  You can identify a specific type of traffic by using protocols as search qualifiers.
- *Search in a relative time frame* on page 68
  The search engine is able to locate files that are time-stamped within a relative time frame.
- *Search using content concepts* on page 68
  Because content concepts are collections of data relevant to a single issue, they can be used efficiently to find related incidents.
- *Use concept expressions* on page 68
  Because content concepts are collections of data relevant to a single issue, they can be used efficiently to find related incidents. The efficacy of a concept query is enhanced by use of concept expressions.

Search by excluding content concepts

Exclude content concepts from queries to prevent collections of data relevant to a single issue from appearing in search results.

Task

1 On your Linux-based appliance, select **Policies**.

2 Click a policy to open it and select a rule that retrieves too many results.

  Because a rule is a search that has been saved, this procedure also relates to an over-broad search.

3 Open the **Content** category.

4 Click on the green plus icon to add a parameter to the rule.

5 Select **Concept** | **is none of** and click **?**.

The content concepts palette opens.

6 Open one or more concept categories.

7 Select one or more concepts.

8 Click **Apply**.

9 Click **Save**.

For example, if you wanted to find credit cards using any possible numbering pattern except American Express, you could select the AMEX concept to exclude those results from a general payment card query.

Search by excluding ports

Exclude ports from a query to prevent incidents using them from appearing in search results.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Port** | **source is none of** and enter a port number in the values field.

4 Click the green plus icon to add a destination parameter (optional).

5 Select **Port** | **destination is none of** and enter a port number in the values field.

6 Click **Search**.

Search by excluding protocols

Exclude protocols from a query to prevent incidents using them from appearing in search results.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Protocol** | **is none of** and click **?**.

The Protocols palette opens.

4 Open categories and select protocol checkboxes.

5 Click **Apply**.

6 Click **Search**.

Search by file creation time

Search for files that were created at a particular time.

The time zone of the McAfee DLP appliance determines the file creation time displayed.

Task

1. On your Linux-based appliance, search **Capture | Advanced Search**.
2. Open the **Date/Time** category.
3. Select **File Creation Time | between** and click on the calendar icon to enter dates in the values field.

   Select **before** or **after** to get closer to a specific time.
4. Select a time from the hour, minute and second menus.
5. Click **Search**.

Search by file last modification time

Search for files by the last time they were modified.

The time zone of the McAfee DLP appliance determines the last modification time displayed.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Date/Time** category.
3. Select **Last Modification Time | between** and click the calendar icon to enter dates in the values field.

   Select **before** or **after** to get closer to a specific time.
4. Select a time from the hour, minute and second menus.
5. Click **Search**.

Search by global time

When you define a time in a search or rule, your local time is automatically converted to Greenwich Mean Time (GMT). If you are managing several McAfee DLP Monitor locations, you can find captured data at the same global moment in each of those locations.

The time zone displayed in the **Date/Time** category on your rules and search pages is determined by the time zone in which your device was installed.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Date/Time** category.
3. Select **Exact Time | between** and click the calendar icon to enter dates in the value field.

   Select **before** or **after** to get closer to a specific time.
4. Select a time from the hour, minute and second menus.
5. Click **Search**.

Search by local time globally

When you define a time in a search or rule, your local time is automatically converted to Greenwich Mean Time (GMT). But if you are managing several McAfee DLP Monitor locations, you will want to use the local time (same clock time) in each of those locations.

For example, if you are managing a global network, you may expect confidential data to be entering or leaving the network data stream during business hours. But after 5 PM local time, movement of sensitive data may indicate a leak.

By creating a rule that tracks sensitive data between the hours of 5 and 6 PM in your Los Angeles, New York, London, and Tokyo offices, you can monitor data at the time most employees are leaving each of those facilities.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Date/Time** category.

3 Select **Exact Time** | **between (local time)** and click the calendar icon to enter dates in the values field.

  Select **before (local time)** or **after (local time)** to get closer to a specific time.

4 Select a time from the hour, minute and second menus.

5 Click **Search**.

Search by port

Search by port to identify incidents by source, destination, or in both directions.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Protocol** category.

3 Select **Port** | **source is any of** and enter a port number in the values field.

4 Click the green plus icon to add a destination parameter (optional).

5 Select **Port** | **destination is any of** and enter a port number in the values field.

6 Click **Search**.

Common port assignments

Well-known ports are commonly associated with specific types of traffic, and can be used to search network data.

The list in this table contains only a few of the well-known ports. IANA (Internet Assigned Numbers Authority) updates are online at http://www.iana.org/assignments/port-numbers.

Table 4-2 Common port assignments

Port Number	Service
20/21	FTP
22	SSH
23	Telnet
25	SMTP

Table 4-2 Common port assignments *(continued)*

Port Number	Service
80	HTTP
110	POP3
123	NTP
143	IMAP
144	NNTP
443	HHTPS
465, 587	SMTP-SSL
993	IMAP-SSL
995	POP3-SSL

Search by port range

Search by port range to identify incidents in a type of traffic by source, destination, or both.

> This is especially useful when a specific type of traffic can be identified by a range. For example, the Solaris operating system often uses the 1000-1023 range.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.
2. Open the **Protocol** category.
3. Select **Port** | **source is any of** and enter a port number range in the values field.
4. Click the green plus icon to add a destination parameter (optional).
5. Select **Port** | **destination is any of** and enter a port number range in the values field.
6. Click **Search**.

Search by protocol

You can identify a specific type of traffic by using protocols as search qualifiers.

> For example, HTTP protocols might be identified to find incidents in web traffic, or FTP might be used to detect large quantities of data being transmitted.

Task

1. On your Linux-based appliance, enter **Capture** | **Advanced Search**.
2. Open the **Protocol** category.
3. Select **Protocol** | **is any of** and click **?**.

   The Protocols palette opens.
4. Open categories and select protocol checkboxes.
5. Click **Apply**.
6. Click **Search**.

Search in a relative time frame

The search engine is able to locate files that are time-stamped within a relative time frame.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Date/Time** category.
3. Select **File Creation Time**, **File Last Accessed**, or **Last Modification Time** and **between** then click the calendar icon to enter dates in the values field.

   Select **before** or **after** to get closer to a specific time.
4. Select a time from the hour, minute and second menus.
5. Click **Search**.

Search using content concepts

Because content concepts are collections of data relevant to a single issue, they can be used efficiently to find related incidents.

> The number of concepts usable in a compound search or a rule is limited only by the number of concepts defined in the system.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.
3. Select **Concept | is any of** and click **?**.

   The Concept palette opens.
4. Open categories and select concept checkboxes.
5. Click **Apply**.
6. Click **Search**.

Use concept expressions

Because content concepts are collections of data relevant to a single issue, they can be used efficiently to find related incidents. The efficacy of a concept query is enhanced by use of concept expressions.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Content** category.
3. Select **Concept | expression** and enter a complex command line query in the value field.

   Click **?** to determine the syntax supported by McAfee DLP.
4. Click **Search**.

For example, the expression `concept:CCN -concept:AMEX(concept:SSNORconcept:EIN)` finds credit card numbers that are neither American Express nor social security or employee identification numbers.

5 Policies

Policies are containers for groups of related rules that target specific issues. When the rules that make up the policies display incidents found on a dashboard, the navigation pane displays the names of the policies and rules used to generate them.

Standard policies are installed on McAfee DLP Monitor, McAfee DLP Discover, or McAfee DLP Prevent appliances before shipment. Geographic location, industry sector, and business type determine which ones are active. There are three basic types.

Table 5-1 Policy types

Policy type	Examples
Compliance	SOX, HIPAA, PCI, PII, GLBA, FISMA, ITAR, SB 1386
Intellectual property	Customer lists, Price/Cost lists, Target Customer lists, new designs, company logos, source code, formulas, process advantages, pending patents
High Business Impact information	Board minutes, financial reports, merger/acquisition documents, product plans, hiring/firing/RIF plans, salary information, acceptable use standards

Customized policies can be created at any time to address issues specific to business operations.

Policies are grouped by type of the rules they contain. Compliance policies contain regulatory rules; Intellectual Property policies contain privacy rules, and High Business Impact policies contain rules that manage business operations.

When an incident is produced by the rules of a policy, the **Group by** window displays the name of the policy that produced it.

Contents

International policies

International policies contain rules that monitor local network traffic and repositories for significant regional incidents and events. They monitor privacy data from more than two dozen countries in EMEA, APAC, Latin and North America.

International rules monitor numbering patterns for passports, driver's licenses, governmental and banking entities, and health and social services documents. They include new rules developed for China, Japan, Russia, Korea, and the Czech Republic.

Customized regional policies and rules can also be created at any time to address local issues specific to business operations.

How policy inheritance works

Inheritance establishes the relationship of rules to their policies. If a rule inherits **Active** status from its policy, it runs only when all the other rules of the policy run. If it is **Inactive**, it can be run independently.

Policy-based inheritance is enabled by default because policies produce the best results when their rules work as a cohesive unit. For this reason, inheritance is disabled by default.

Rules are most often deactivated when they are created or tuned. A multi-step process is required to assure their efficacy. The rule must be run, its hits evaluated, and its parameters modified until it produces significant incidents and events.

This can be done only if the **Inherit Policy State** of a rule is disabled so it can be run apart from its policy.

How policy activation works

Policies must be activated before their rules can be matched to network data. By default, rules are enabled when the policies are activated, but they can be configured to run independently.

Policies must not only be activated, but published to at least one DLP appliance before the system can report incidents and events. They are inactive by default, which allows users to focus only on the rule sets that meet their needs.

For example, United Kingdom users may add the EMEA regional policy package, but activate only the UK policy. Similarly, North American users may want to use only the U.S. government regulatory policies, like HIPAA, SOX and ITAR.

There are three ways to activate a policy.

- During installation, check the boxes of the policies to be activated.
- On the **Policies** page, policies can be checked and activated from the **Actions** menu.
- On the **Edit Policy** page, the **State** menu can be changed.

Activate policies

Not all policies are activated during installation. Activate these policies to find incidents and events in network traffic and repositories.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Review the **State** column to find policies that are inactive.
3. For each inactive policy, select the checkbox in the left column and select **Actions** | **Activate**.
4. Verify that the **State** column shows that the policy is **Active**.

Deactivate policies

Deactivate policies to keep them from finding incidents and events in network traffic and repositories.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. On the **Policies** page, select one or more policies by checking the box in the left column.
3. Select **Actions** | **Deactivate**.
4. Verify that the **State** column shows that the policy is **Inactive**.

Work with policies

You can modify most policy parameters on the **Edit Policy** page. Click the name of the policy to open it.

Tasks

- *Add policies* on page 74
  Add policies to the standard ones that are pre-installed on McAfee DLP appliances. Custom policies can be added at any time.
- *Rename policies* on page 75
  Rename policies to create policies that have the same attributes as the original. None of the incidents and events found by that policy will be maintained.
- *Clone policies* on page 75
  Clone policies to create a new one with the same attributes.
- *Change ownership of policies* on page 75
  Policy ownership determines user groups whose members can modify policy parameters.
- *Change states of policies* on page 76
  Policy states determine whether or not rules can run. They can be activated during installation, in the interface, or from within each policy definition.
- *Modify policies* on page 76
  Modify policies to makes changes to owners, devices, and other parameters of policies.
- *Execute policies* on page 76
  Execute permission is required to deploy policies.
- *Delete policies* on page 77
  Delete policies individually or in groups.
- *Publish policies* on page 77
  Publish policies to deploy them on one or more McAfee DLP appliances.

Add policies

Add policies to the standard ones that are pre-installed on McAfee DLP appliances. Custom policies can be added at any time.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Select **Actions** | **Add Policy**.
3. (Optional) Enter a name and description.
4. Select an **Owner**.

   Standard policies are owned by the admin user. If another policy owner is needed but not listed, add the user to an existing group, or create a new one before adding the policy.
5. Set **State** to **Active** if you are going to use the rule immediately. An inactive policy cannot produce incidents.
6. Select **Data-at-Rest** or **Data-in-Motion** if you want to limit the rule to either static or dynamic data.
7. Select one or more device checkboxes to publish the policy to specific appliances. Select **None** if you want to publish the policy at a later time.
8. Click **Save**.
9. Assign access rights to the policy.
10. Add rules to the policy.

See also

Add rules on page 78
Check user permissions on page 238

Policy fields

Policy fields define the properties of policies.

Option	Definition
Name	Policy names must use only alphanumeric characters. Non-alphanumeric characters might generate an error message.
Description	Optional.
Owner	A group whose members can access the policy. If you are logged in as a member of one of the default groups, only that group is displayed, and other options are not available.
State	Policies can only have one of two states: active or inactive. New policies are active by default to allow deployment to a device.
Region	Policies usually belong to a group that is defined by a region. The default region is North America.
Suppression of incidents	Eliminating reporting of irrelevant hits will exclude results that are not useful and improve performance. Selecting **Data-in-Motion** suppresses all incidents found in moving network traffic. Selecting **Data-at-Rest** suppresses all incidents found in static file or database repositories. **Data-in-Use** events must be displayed if McAfee DLP Endpoint or McAfee Host DLP is installed — so there is no suppression option available.
Devices	McAfee DLP devices that are attached to McAfee DLP Manager are listed so that you can publish policies to one or more of them. The None category is used for policies that are not yet deployed. A Host device will not be available unless it has been registered to McAfee DLP Manager.

Rename policies

Rename policies to create policies that have the same attributes as the original. None of the incidents and events found by that policy will be maintained.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Click a **Policy Name** to open the **Edit Policy** page.
3. On the **Edit Policies** page, enter a new name and add a description (optional).
4. Click **Save**.
5. On the **Policies** page, verify that the policy has been renamed.

Clone policies

Clone policies to create a new one with the same attributes.

Policies are cloned by changing the policy name.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Click a **Policy Name** to open the **Edit Policy** page.
3. Enter a new policy name and add a description (optional).
4. Edit other parameters as needed.
5. Click **Save As**.

   > The **Save As** button appears when you edit the policy name.

6. On the **Policies** page, verify that the cloned policy has been added.

Change ownership of policies

Policy ownership determines user groups whose members can modify policy parameters.

> There are several ways to change ownership of a policy. With this method, you make the change within the policy definition.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Click a **Policy Name** to open the **Edit Policy** page.
3. From the **Owner** menu, make another selection.

   Owners are determined by the group to which they belong. If an owner is not listed, create a user group.

4. Click **Save**.

Change states of policies

Policy states determine whether or not rules can run. They can be activated during installation, in the interface, or from within each policy definition.

> There are several ways of activating or deactivating policies. With this method, you make the change within the policy definition.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Click a **Policy Name** to open the **Edit Policy** page.
3. From the **State** menu, select **Active** or **Inactive**.
4. Click **Save**.

Modify policies

Modify policies to makes changes to owners, devices, and other parameters of policies.

> Some policy modifications can be performed from the **Actions** menu.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Click a **Policy Name** to open the **Edit Policy** page.
3. Revise the **Policy Name** or **Description**.

   > Changing the policy name allows you to **Save** (rename) or **Save As** (clone) the policy.

4. From the **Owner**, **State**, and **Region** menus, make another selection.
5. In the **Suppress incidents** field, select a checkbox to constrain incident results to one of the available datasets.
6. In the **Devices** box, select checkboxes to publish the policy to one or more devices.
7. Click **Save**.

Execute policies

Execute permission is required to deploy policies.

Task

1. On your Linux-based appliance, select **System** | **User Administration** | **Groups**.
2. Click the **Details** icon of a user group.
3. Click the **Policy Permissions** tab.
4. Open the **Policies** category.
5. Check the **Execute** box of the policy.
6. Click **Apply**.

Delete policies

Delete policies individually or in groups.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Select one or more policy checkboxes.

3 Select **Actions** | **Delete**.

> Delete a single policy quickly by clicking its trash can icon.

Publish policies

Publish policies to deploy them on one or more McAfee DLP appliances.

Task

1 On your Linux-based appliance, select **Policies**.

2 On the **Policies** page, click a policy.

3 On the **Edit Policy** page, select a **Devices** radio button.

4 Click **Save**.

Rules

Rules contain patterns that are matched against data in network traffic and repositories to produce incidents and events. When the rules of a policy produce incidents, they are saved in a database, then reported to the dashboard.

Standard policies that are pre-installed on McAfee DLP Monitor, McAfee DLP Discover, or McAfee DLP Prevent appliances contain groups of related rules. The rules filed under them are enabled by default so that they will run whenever the policy applies.

> New rules are disabled by default because their states must be defined before they are used with a policy. Usually they are tuned to assure efficacy before state is defined.

Custom rules can be created at any time to address issues specific to business operations. The system can manage 512 active rules, but they can be deactivated to allow addition of new rules.

> User permissions, including the ability to create or use rules, depend upon group membership.

See also

Assign task and policy permissions on page 238

View rule parameters

View rule parameters by opening the policy the rule is filed under, then opening the rule.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name to open the **Edit Rule** page.

4 Open the categories under the **Define**, **Actions**, and **Exceptions** tabs.

5 If no changes are warranted, click **Cancel**.

Add rules

Add rules by searching captured data, then saving the search when it returns reliable results.

Task

1 On your Linux-based appliance, click **Capture**.

2 Select either **Basic Search** or **Advanced Search**.

3 Enter a query that might retrieve significant results. If significant incidents are reported do one of the following;

- Click **Save as Rule**.
- Modify the parameters until the needed results are returned, then click **Save as Rule**.

The **Edit Rule** page launches.

4 Enter a rule name and add a description (optional).

5 Assign the rule to a policy by selecting one from the **Policy** menu.

Store the new rule in a policy containing rules like it.

6 Select a **Severity** to rate the importance of the rule.

7 Select the **Inherit Policy State** to **Enabled**.

If the rule is to be tuned, leave it in **Disabled** state so it can be run independent of its policy until it reports the needed results reliably.

8 Make any needed changes to the parameters of the rule.

9 Click **Save**.

Disable rule inheritance

Pre-installed policies contain rules that inherit the state of their policies by default; they act as a group and run whenever the policy runs. Because their policy states are not yet defined, new rules are disabled by default.

Clone a standard rule and use its parameters to build a new one. Disable inheritance immediately to disconnect it from the original policy and rule.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name to open the **Edit Rule** page.

4 Change the **Inherit Policy State** parameter to **Disabled**.

5 Click **Save**.

If the rule needs further definition, consider tuning it until it returns the results you need.

Copy rules to policies

Rules can be copied from one policy to another.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name to open a rule.

4 In the **Rule Name** field, enter a new name.

If a similar name is needed, add a single character or space to distinguish it from the original.

5 (Optional) Enter a new description.

6 Assign the rule to a different policy by selecting one from the **Policy** menu.

Store the new rule in a policy containing rules like it.

7 Select a **Severity** to rate the importance of the rule.

8 Set the **Inherit Policy State** to **Enabled**.

If the rule is to be tuned, leave it in **Disabled** state so it can be run independent of its policy until it reports the needed results reliably.

9 Make any needed changes to the parameters of the rule.

10 Click **Save**.

11 Open the policy containing the new rule to verify that it has been copied over.

Modify rules

Modify rules to assure their efficacy. Rules can be modified many times, or *tuned*, before they are finalized.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name to open the **Edit Rule** page.

4 Make changes to parameters under the **Define**, **Actions**, and **Exceptions** tabs.

5 Click **Save**.

Delete rules

Delete rules individually or in groups.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Select one or more rules using the checkbox in the left column.

4 Select **Actions** | **Delete**.

> Delete a single rule quickly by clicking its trash can icon.

5 Click **Save** to save the modified policy.

Reconfigure rules for web traffic

Reconfigure rules to monitor web traffic by redefining the protocol targeted.

> This state is used primarily for tuning rules.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** to open the **Edit Policy** page.

3 Click a **Rule** name that you want to adapt for web traffic.

4 Enter a new name and add a description (optional).

5 Click **Save As**.

> The **Save As** button appears when you edit the name field.

6 Open the **Protocol** category.

7 Select **Protocol** | **is any of**, then click **?**.

The **Protocols** menu launches.

8 If any checkboxes are selected, deselect them, then select all HTTP options.

9 Click **Apply** then click **Save**.

Exceptions to rules

Creating exceptions excludes attributes that tag irrelevant data and keeps the classification engine from reporting it again. When rules produce incidents that contain no useful information, they are referred to as false positives.

An incident may technically match a rule, but it might not contain any useful information. False positives get in the way of significant results, preventing accurate reporting of the problems detected in network traffic.

When false positives are reported and rules are redefined to prevent it from being reported again, the classification engine ignores any data that contains the attributes identified by the exceptions.

> Tune rules using historical data to prevent false positive matches.

Classify incidents as false positives

When the parameters of a rule literally match network data but produce no useful information, the resulting incident is referred to as a false positive. Incidents classified as false positives should be identified to keep the rules that triggered them from reporting them again.

With this release, rules can be tuned directly from the **Incidents** or **Incident Details** pages.

When the **Edit Rule** page is launched from the **Tune Rule** command, it is populated with the current values of the rule under the **Exceptions** tab.

Task

1. Select **Incidents | Incidents.**
2. Find one or more incidents from the same policy and rule that contain useless or insignificant information.
3. Select one or more checkboxes and click the **Tune Rule** button.

   The **Tune Rule** button is also available from the **Incident Details** page.

   The **Edit Rule** page opens on the **Exceptions** tab.
4. Enter a name and optional description in a note describing the exception.
5. Select an element that did not produce useful information. Edit the values to define the exceptions.
6. Click **Save.**

See also
Exceptions to rules on page 80

Add exceptions to rules

Add exceptions to rules by searching captured or historical data, then saving the search when it returns reliable results.

Eight exceptions are supported for each rule, so you can define precisely the conditions that are not to be matched. The capture engine will drop any incident matching the exceptions.

Exceptions apply to real-time searches only. **Test Rule** is available only when tuning rules because the test uses only historical data.

Task

1. On your Linux-based appliance, select **Policies | Policies.**
2. Click a **Policy Name**, then a **Rule** that needs an exception definition.
3. Click the **Exceptions** tab.
4. Open **Exception 1**, enter a note describing the exception, then use the components to define the exception to the rule.
5. If additional parameters are needed, create more exceptions.
6. Click **Save.**

See also
Exceptions to rules on page 80

Add new rules with exceptions

Add exceptions to rules to assure that it reports only relevant results. When rules contain attributes that are overly broad, false positives may be reported.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Click a **Policy Name** to which the rule will be added.
3. On the **Edit Policy** page, select **Actions** | **Add Rule**.
4. Enter a rule name and optional description.
5. Set the **Inherit Policy State** to **Enabled**.

   If the rule is to be tuned, leave it in **Disabled** state so it can be run independent of its policy until it reports the needed results reliably.
6. Select a **Severity** to rate the importance of the rule.
7. Click the **Exceptions** tab.
8. Open **Exception 1** and enter a note describing the exception, then use the components to define the exception to the rule.
9. If additional parameters are needed, open more **Exceptions** and define them.
10. Click **Save**.

See also

Exceptions to rules on page 80

Action rules

Action rules work by extending rules, and immediately applying when the rule finds an incident. Actions may be preventive, corrective, or protective, and the actions available depend on whether McAfee DLP Prevent or a proxy server is used to implement them.

When a rule produces an incident in network data or a scanned repository, use of an action rule can prevent damage, trigger a remedial action, or react to an action that has been taken at a network endpoint.

McAfee DLP Endpoint protection rules are pre-configured with reactions to events that occur at endpoints. Other McAfee DLP products add optional action rules to define disposition of a detected incident in network traffic or repositories. Because the design of endpoint and network McAfee DLP products differs, action and protection rules work in different ways.

- McAfee DLP network products allow action rules to have multiple actions that are attached to many different rules. Each of those rules can deploy the action once to network traffic, a repository, or endpoints.
- The McAfee DLP Endpoint product uses protection rules to apply reactions to many different endpoints that may be on- or offine (in contact with a domain controller) when a violation occurs.

Preventive, corrective, or protective actions are applied depending on whether they are used in **Data-in-Motion**, **Data-at-Rest**, or **Data-in-Use**.

- If preventive action is to be taken, action rules are applied to **Data-in-Motion**, which monitors email and webmail in network traffic. This feature requires configuration of an MTA (Mail Transport Server) or proxy server with McAfee DLP Prevent, which must be registered to McAfee DLP Manager.
- If corrective action is to be taken, action rules are applied to **Data-at-Rest**, which identifies data at risk in network repositories. This feature requires McAfee DLP Discover, which must be registered to McAfee DLP Manager.
- If protective action is to be taken, action rules are applied to **Data-in-Use**, which identifies problems at endpoints. This feature requires McAfee DLP Endpoint, which must be registered to McAfee DLP Manager.

If McAfee DLP Monitor and McAfee DLP Discover devices are both managed by McAfee DLP Manager, every rule can be configured to deploy one action of each of the three incident types.

How McAfee DLP Prevent uses action rules

Depending on whether McAfee DLP Prevent is configured with an MTA (Mail Transport Agent) or a proxy server, McAfee DLP Prevent can take up to eight different actions when a significant incident is detected.

McAfee DLP Prevent might use action rules to perform any of the following actions:

- Allow email that is determined to be legitimate.
- Block confidential data breaches.
- Bounce email that violates policies.
- Encrypt authorized transmissions.
- Monitor traffic and record incidents in a system log.
- Notify supervisory personnel of a violation.
- Quarantine suspicious traffic.
- Redirect messages that violate policy.

McAfee DLP Prevent can also capture network traffic for later forensic analysis, and block the transmission of sensitive data sent using specific protocols (for example, HTTP, SMTP, HTTP POST, etc.).

Add action rules

Add action rules to extend the usability of rules. When rules extended with action rules hit on matching data, the defined actions are applied immediately to resolve it.

Task

1. Select **Policies** | **Action Rules**.
2. Under one of the data categories, select **Actions** | **Add Action Rule**.

   The **Data-in-Motion**, **Data-at-Rest**, or **Data-in-Use** categories determine where the actions will be implemented: on the network, in a repository, or on an endpoint.
3. Enter a name and description (optional).

4 From the **Actions** components, select the parameters of the action rule.

5 Click **Save**.

Apply action rules

Apply action rules to rules monitoring data in motion, scanning data at rest, or identifying significant events on endpoints. When an incident is detected, the action defined in the action rule is immediately applied.

Task

1 Select **Policies** | **Action Rules**.

2 Select the appropriate action rule.

- For **Data-in-Motion**, open the **Data-in-Motion Prevent Action** category and select an action from the list.
- For **Data-at-Rest**, open the **Remediation Policy** category and select an action from the list.

  Selecting different actions displays other fields related to that action to be filled in.

- For **Data-in-Use**, open the **Data-in-Use Policy** category and select one or more actions. For each action, select whether the action applies *Online*, *Offline*, or both.

  These terms actually refer to where the computer is located in relation to the internal network. For example, a user who is *offline* is actually *off-site*. Online/offline status is actually determined by whether or not the ePolicy Orchestrator IP address can be resolved with a DNS query.

  Selecting certain actions displays other fields related to that action to be filled in.

  Some actions (for example block/encrypt) are incompatible with each other. If you select incompatible actions, an error message appears when you attempt to save your changes.

3 Click **Save**.

Assign responsibility for actions

Assign responsibility for actions by setting up action rules. For example, reviewers might be assigned to monitor results when incidents are found by a rule containing an action rule.

The **Incident Reviewer** parameter applies to **Data-in-Motion** and **Data-at-Rest** action rules. It does not apply to **Data-in-Use** rules.

Task

1 Select **Policies** | **Action Rules**.

2 Click a rule.

The **Edit Action Rule** page launches.

3 From the **Incident Reviewer** menu, select a group or user.

The existing groups and users are displayed.

4 Click **Save**.

Change incident status with action rules

Change the status of incidents on the fly by defining action rules that are applied when they are found.

Task

1 Select **Policies** | **Action Rules**.

2 Click a rule.

The **Edit Rule** page opens.

3 From the **Incident Status** menu, select a status.

4 Click **Save**.

Clone action rules

Clone action rules to apply the same action, or a modified one, to another rule.

Task

1 Select **Policies** | **Action Rules**.

2 Click an action rule.

The **Edit Rule** page opens.

3 In the **Action Rule Name** field, enter a new name.

4 Click **Save**.

Delete action rules

Delete action rules individually or in groups.

> Action rules that have been applied to rules are in use and cannot be removed.

Task

1 Select **Policies** | **Action Rules**.

2 Select one or more action rules.

3 Select **Actions** | **Delete**.

> Click the trash can icon to delete a single action rule.

4 Click **Confirm** or **Cancel**.

Log actions taken

Log actions taken and send a record to a syslog server, if one has been configured to receive log entries.

The **Syslog Notification** parameter applies to **Data-in-Motion** and **Data-at-Rest** action rules. It does not apply to **Data-in-Use** rules.

Task

1 Select **Policies** | **Action Rules**.

2 Click the action rule to be modified.

3 Open the **Syslog Notification** menu.

4 Select **Enable**.

5 Click **Save**.

Modify action rules

Modify action rules to serve new purposes.

Task

1 Select **Policies** | **Action Rules**.

2 Click the action rule to be modified.

3 Open the **Actions** components and edit the parameters.

4 Click **Save**.

Notify users of actions taken

Notify users of actions taken when incidents are found by setting up email notifications in action rules. For example, users who are tasked with monitoring results might be automatically informed.

The **Email Notification** parameter applies to **Data-in-Motion** and **Data-at-Rest** action rules. It does not apply to **Data-in-Use** rules.

Task

1 Select **Policies** | **Action Rules**.

2 Click an action rule, or create a new one.

3 On the **Edit Action Rule** page, open the **Email Notification** component.

4 Enter a valid email address in the **From** field.

Email addresses are invalid if they include special characters (for example, &, *, %), but if valid addresses are also included, notification will still be sent to those users.

5 Enter one or more addresses in the **To** and **Cc** fields.

6 (Optional) Select checkboxes to notify managers, reviewers, senders, or recipients.

The options available depend on the McAfee DLP appliance. Managers can be identified only if an Active Directory server has been added, but other categories are user-defined. Reviewer is the only option available on McAfee DLP Discover.

7 (Optional) Type in a **Subject** and **Message**.

These fields accept dynamic variables, enabling you to set up automatic responses to routine situations. They an be used to alert users to details of the violation automatically (for example, `##Filename found by the ##Rule violated the ##Policy`).

8 Click **Save**.

Reconfigure action rules for webmail

You must reconfigure McAfee DLP Prevent action rules for use on proxy servers.

McAfee DLP Prevent supports BOUNCE, ENCRYPT, MONITOR, NOTIFY, QUARANTINE or REDIRECT actions, but proxy servers can only ALLOW or BLOCK data in motion.

Task

1. Select **Policies** | **Action Rules**.
2. Click the action rule to be reconfigured.
3. Enter a new name and optional description.
4. Click **Save As** to create a copy of the action rule.

   > The **Save As** button appears only when you change the name.

   The new rule appears on the **Action Rules** page.
5. Open the new action rule.
6. On the **Edit Action Rule** page, open the **Prevent Action** component and select a new action from the menu.
7. Click **Save**.

Remove actions from rules

Remove actions from rules without affecting other parameters of the rule.

> This task removes only actions that have been applied to rules, not the rules themselves. Action rules that have been applied to rules in use cannot be removed.

Task

1. Select **Policies** | **Policies**.
2. Click the **Policy Name**, then the **Rule** that contains the action that is to be removed.
3. On the **Edit Rule** page, select the **Actions** tab.
4. On the list of actions, locate the action to be removed.
5. Click the **X** in the right column.

   > If you cannot see the column, expand your dashboard.
6. Click **Save**.

Using document properties

The Document Properties feature makes it possible to tag and retrieve metadata that consists of attributes of documents. Values in properties fields can be extracted in context, increasing the granularity of search results.

For example, using the name of an author as a keyword in a search or rule would successfully retrieve that name from any location in the capture database. But using that name with the Microsoft Word Author property retrieves only the keyword in the defined context.

Types of document property

Document properties types might be pre-defined metadata, metadata added by users, or property values only.

There are three types of document property.

Table 5-2 Types of document property

Property type	Definition
Pre-defined properties	Standard properties shared by most document types, such as *author*, *keywords*, *subject*, and *title*.
Custom properties	User-defined properties added to the document metadata, allowed by some applications such as Microsoft Word. A user-defined property can also reference a standard document property that is not on the predefined properties list, but cannot duplicate a property that is on the list.
Any property	Allows definition of a property by value alone. This 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.

Partial matching of document properties

Partial matching of document properties is supported only on endpoint devices.

Document properties definitions might be made up of one or more pre-defined or custom properties. When property values are defined, users can opt to allow partial matches.

If a partial match is indicated, when the definitions are used in rules, matches related to the property value will be reported.

Add document properties and groups

You can use document properties and groups of document properties to not only retrieve objects through their attributes, but narrow the search to the context in which they are used.

Task

1. Go to **Policies | Document Properties**.
2. From the appropriate **Actions** menu, select **Add**.
3. Enter a name and optional description.
4. Select the components of the property or property group.
   - In the **Create Document Properties** window, select pre-defined, custom, or any property values, then add instances of those property values as appropriate.
   - In the **Create Document Properties Group** window, select property checkboxes.
5. Click **Save**.

6 Cases

Case management allows users to collaborate in the resolution of related incidents.

Contents

How case management works

When significant incidents are found and reported by the McAfee DLP system , they generally have one or more attributes in common. Assigning incidents with common attributes to a single case allows users to collaborate to resolve them more quickly. Each staff member involved can focus on a single attribute to advance the resolution of the case.

For example, a case that contains emailed evidence might be assigned to members of a legal team, who might develop it so that it can be used in court. Each member of that team might add notes and citations, change status and priority, notify stakeholders, or redirect the case to another user who may be able to add information.

> Case dashboards display information based on organizational responsibilities. For example, Human Resources personnel might see Acceptable Use violations, but not SOX compliance issues.

Add new cases

Add new cases to set up a common resolution for related incidents.

> No more than 100 incidents can be added to a case at one time.

Task

1 On your Linux-based appliance, select **Case | Case Management**.

2 From the **Actions** menu, select **New Case**.

3 Enter a **Headline**.

4 Select an **Owner**.

5 (Optional) Select a **Resolution** state.

6 (Optional) Select a **Status**.

7 (Optional) Select a **Priority**.

8 Type in keywords.

9 (Optional) Select the **Notify Owner** checkbox.

10 (Optional) Select the **Notify Submitter** checkbox.

11 (Optional) Type in **Notes**.

12 Click **Apply**.

Tasks

- *Customize case configuration* on page 90
  Customize case configuration by adding customized columns, updating notifications, or creating periodic reminders.
- *Manage case permissions* on page 90
  Manage case permissions from within each case without launching a system page.

Customize case configuration

Customize case configuration by adding customized columns, updating notifications, or creating periodic reminders.

Task

1 On your Linux-based appliance, select **Case** | **Case Management**.

2 From the **Options** menu, select **Customize Case Configuration**.

3 Enter customized column names in the value field.

4 If notification is to be sent when the case is updated, select the **Submitter** or **Owner** checkboxes.

5 If periodic reminders of case statuses are to be sent, set the time and date of notification.

6 Click **Apply**.

Manage case permissions

Manage case permissions from within each case without launching a system page.

Cases must be reviewed and processed only by authorized users.

Task

1 On your Linux-based appliance, select **Case** | **Case Management**.

2 Click the **Details** icon of a case.

3 Select **Options** | **Permissions**.

4 Select the **Read**, **Write**, or **Delete** boxes corresponding to the assignment of the case to users and groups.

Users who create cases are automatically allocated all three permissions - but if a case owner is changed, permissions are lost.

5 Click **Apply**.

> Global permissions that are set under **System** | **User Administration** | **Groups** | **Details** | **Task Permissions** take precedence over cases configured individually. If there is a conflict between permissions assigned under an individual case and those that are assigned globally, global group permissions take precedence.

When **Write** permission is assigned, **Read** permission is implicit.

How user permissions might be assigned

John has been given read access, so case information will be displayed on his home page. But because his permission is restricted to **Read**, he will not see the **Apply**, **Save**, **Delete**, or **Assign** buttons.

Sheila has been given responsibility for developing court cases, so she has been given **Read** and **Write** but not **Delete** privileges. Because of the nature of legal actions, only her manager is can see the **Delete** button on his console.

Assign incidents to cases

Add incidents to cases to add additional relevant information that will facilitate resolution.

> No more than 100 incidents can be added to a case at one time.

Task

1 On your Linux-based appliance, select **Incidents** | **Incidents**.

2 Select one or more incidents.

3 Click **Assign to Case**, then select **Assign to Case** | **New Case** or **Assign to Case** | **Existing Case**. For a new case, do the following:

   a Fill in the **New Case** form. Required fields are **Headline**, **Keywords**, and **Owner**.

   b Click **Apply**.

   The new case is created and the incidents are assigned to it.

4 For an existing case, do the following:

   a Review the case details and modify menus as necessary.

   b Make **Notes** to indicate how the case has changed by the addition of this incident.

   c Click **Apply**.

   The incidents are assigned to the case.

Tasks

- *Change the ownership of cases* on page 92
  Change the ownership of cases to give primary responsibility for resolution to a specific user group.
- *Change the resolution status of cases* on page 92
  Change the stage of resolution of cases if their conditions have changed.
- *Change the status of cases* on page 92
  Change the status of cases to indicate their states of resolution.
- *Reprioritize cases* on page 93
  Reprioritize cases according to their changing states as they move through states of resolution.
- *Collect credit card violations in cases* on page 93
  Collect credit card violations in a single case to resolve privacy violations in one operation.
- *Notify users of a case* on page 93
  Notify users of changes in a case.
- *Add comments to cases* on page 94
  Add comments to cases to add information about one or more incidents contained in them.

Change the ownership of cases

Change the ownership of cases to give primary responsibility for resolution to a specific user group.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Select the **Details** icon of a case.
3. From the **Owner** menu, select a user group.

   Select the **Notify Submitter** checkbox to notify the originator by email.
4. Click **Apply**.

Change the resolution status of cases

Change the stage of resolution of cases if their conditions have changed.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Select the **Details** icon of a case.

   Select the **Notify Submitter** checkbox to notify the originator by email.
3. From the **Resolution** menu, select a new status.
4. Click **Apply**.

Change the status of cases

Change the status of cases to indicate their states of resolution.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Select the **Details** icon of the case.

3. From the **Status** menu, select a new status.
4. Select the **Notify Submitter** checkbox to notify the originator by email.
5. Click **Apply**.

Reprioritize cases

Reprioritize cases according to their changing states as they move through states of resolution.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Select the **Details** icon of a case.
3. From the **Priority** menu, select a new priority.
4. (Optional) Select the **Notify Submitter** or **Notify Owner** checkboxes.
5. Click **Apply**.

Collect credit card violations in cases

Collect credit card violations in a single case to resolve privacy violations in one operation.

> Privacy policies containing credit card rules must be installed to detect violations.

Task

1. On your Linux-based appliance, select **Incidents** | **Incidents**.
2. Select one or more incident checkboxes.
3. Click **Assign to Case** | **New Case** or **Assign to Case** | **Existing Case**. For a **New Case** do the following:
   a. Fill in the **New Case** form. Required fields are **Headline**, **Keywords**, and **Owner**.
   b. Click **Apply**.
4. For an existing case, do the following:
   a. Select a case and click **Assign**.

      > If you cannot see the **Assign** link, expand your dashboard.

   b. Review the case details and modify as necessary.
   c. Click **Apply**.

   The incidents are assigned to the case.

Notify users of a case

Notify users of changes in a case.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Click the **Details** icon for a case.

3. Check the **Notify Submitter** or **Notify Owner** boxes.
4. Click **Apply**.

Add comments to cases

Add comments to cases to add information about one or more incidents contained in them.

No more than 100 incidents can be added to a case at one time.

Task

1. On your Linux-based appliance, select **Case | Case Management**.
2. Select a case.
3. Click the **Details** icon.
4. Enter comments in the **Add Notes** text box.
5. Click **Apply**.

Customize the Case List page

Customize the **Case List** page to display the attributes that are most significant.

Task

1. On your Linux-based appliance, select **Case | Case Management**.
2. From the **Options** menu, select **Customize columns**.
   - Click the **Add** button to move **Available** columns to the **Selected** box.
   - Click the **Remove** button to move **Selected** columns to the **Available** box.
3. Click the **Move** button to move **Selected** column headers up or down.

   On the **Case List** page, selecting the up and down arrows moves columns from left to right.

   > If you cannot see the **Move** controls, expand your dashboard.

Tasks

- *Customize case columns* on page 95
  Customize case columns to display only the most significant information.
- *Customize case notifications* on page 95
  Customize case notifications to notify users of changes in a case.
- *Export cases* on page 95
  Export cases to save records of cases for future use.
- *Delete incidents from cases* on page 96
  Delete incidents from cases as they are resolved or lose their usefulness.
- *Delete cases* on page 96
  Delete cases from the **Case List** as they are resolved or are no longer useful.

Customize case columns

Customize case columns to display only the most significant information.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. From the **Options** menu, select **Customize Columns**.
3. Select a column header from the **Available** menu and click **Add** to move it to the **Selected** menu.
4. Use the **Move** buttons to arrange the order of the columns.
5. Click **Apply**.

Customize case notifications

Customize case notifications to notify users of changes in a case.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Select one or more case checkboxes.
3. From the **Options** menu, select **Customize Case Config**.
4. Select checkboxes to automatically send email to the **Submitter** or **Owner** when the case is updated.
5. Select radio buttons to set a standard interval, or add items from the weekly and monthly menus to add more specific parameters.
6. Click **Apply**.

> **How cases might be customized**
>
> Case responsibilities and actions change as cases are resolved. Set up a daily email reminder to distribute that knowledge to case developers.

Export cases

Export cases to save records of cases for future use.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Select one or more case checkboxes, or select the box in the column header to select all cases.
3. Select **Actions** | **Delete**.

   Delete individual cases by clicking the **Delete** icon.

   The case appears in the **Case** | **Exported Cases** file list.
4. Click the exported case link to open or save it.

Delete incidents from cases

Delete incidents from cases as they are resolved or lose their usefulness.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. Select the **Details** icon of the case.
3. On the **Case Details** page, select one or more incident checkboxes.
4. Click **Delete**.

> Use the **Delete** button to delete individual incidents. Use **Options** | **Delete** to delete multiple incidents.

Delete cases

Delete cases from the **Case List** as they are resolved or are no longer useful.

Task

1. On your Linux-based appliance, select **Case** | **Case Management**.
2. In the **Delete** column, click the trash can icon.

7 Concepts

Content, network, and session concepts are used to classify and process data flows on three OSI layers.

Contents

Expedite search with concepts

Expedite searches with concepts to find collections of related data.

Concepts provide ready-made parameters to find all data of a similar type. They can be used in queries, or added to rules that contain other parameters.

How concepts are used

Concepts contain related patterns of data that can be matched to packets in motion on the **Application**, **Transport**, and **Session** layers.

Content concepts, the most common type, find collections of significant data related to a single issue in application data.

Most of the concepts that are shipped with your McAfee DLP appliances are listed under the **User-Defined** tab. Only a few **Built-in** concepts are constructed with proprietary algorithms.

For example, a content concept can be used to collect credit card numbering patterns that can be matched to network data. You might use one of the factory default concepts (AMEX, CCN, DISCOVER, MASTERCARD) to find them quickly, or you can add one that focuses only on patterns used by retail cards.

If you are an advanced user, you can construct network or session concepts to identify data in the **Transport** and **Session** layers.

> Network policies contain collections of related rules, while McAfee DLP Endpoint rules are all part of a single global policy.

Types of concepts

Three concept types are used to find related patterns of data in network traffic or data repositories.

- *Content concepts* contain text patterns and regular expressions to match patterns to data on the **Application** layer (Layer 7).
- *Network concepts* monitor activity on the **Transport** layer (Layer 4). They can be used to find spiders, robots, crawlers, types of webmail, browser versions, and operating systems in use.
- *Session concepts* focus on exchanges of data between applications on the **Session** layer (Layer 5). They can be used to recognize content found in multiple objects contained in a single flow.

How to work with concepts

You can add the three concept types (content, network, and session), modify, restore, and delete concepts, set conditions to narrow pattern matches, and apply concepts to extend configured rules.

Tasks

- *Add content concepts* on page 98
  Add content concepts to match text patterns and regular expressions to data in traffic and repositories.
- *Add session concepts* on page 99
  Add session concepts to inspect all communications between two parties when a pattern is matched. Because the session layer is monitored, you will be able to find multiple objects contained in a single flow (for example, an email attachment as well as the mail body).
- *Set concept conditions* on page 100
  Set concept conditions to narrow matches to specific circumstances in which a pattern is found. Matches are reported only if certain conditions are met.
- *Apply concepts to rules* on page 100
  Apply concepts to extend rules that are configured to find specific types of data.
- *Modify concepts* on page 101
  Modify the parameters of a concept to capture data patterns that are similar to a previously-defined set.
- *Restore concepts* on page 101
  Restore the standard (user-defined) concepts to their original state if they have become corrupted or difficult to handle.
- *Delete concepts* on page 101
  Delete concepts if they are no longer useful.

Add content concepts

Add content concepts to match text patterns and regular expressions to data in traffic and repositories.

When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, _). You can add up to 512 content, session and network concepts to match patterns in network and repository data.

Task

1. On your Linux-based appliance, select **Policies** | **Concepts**.
2. Click **Add Concept**.
3. Enter a name (uppercase only) and description (optional).

4 Select an algorithm to ensure self-correction of incorrectly entered parameters.

For example, if you create a MasterCard expression that uses an incorrect numbering sequence, the algorithm will ignore the pattern and replace it with the correct sequence.

5 Click **?** and select a category from the list.

Packages of related concepts can be used to amplify searches and rule matching.

6 If you want to upload a list of existing expressions or patterns, click **Browse** and select the file.

If you want to edit the list of expressions, or just keep a copy, click **Export Expressions** to save them to your desktop. You can debug them in a text editor, then reimport.

7 If you don't have a document to upload, or want to use text and regular expressions to build a new concept, enter a value in the **Expression 0:** field. Click the green **+** to add an expression, and repeat until all expressions are added.

8 Click **Validate**, then enter a sample string. If it matches, go on to the next step. Review the **Matches String** field to get a true or false acknowledgement.

9 Use one of the concept conditions (**Count**, **Percentage Match**, and so forth.) to modify the action of the concept.

10 Click **Save**.

> ! When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, `hello\_world`). Other metacharacters and ASCII characters (such as `&#x0020`, `&#x0009`, `&#x000C`, and `&#x200B` for space, tab, form feed, and zero-width space) can also be used to define concept expressions.

Concept conditions

Concept conditions narrow the match to specific circumstances. For example, if you want the system to wait until the concept conditions are found three times before being reported to the dashboard, select **greater than** from the **Condition** menu, and enter `3` in the value field.

Add session concepts

Add session concepts to inspect all communications between two parties when a pattern is matched. Because the session layer is monitored, you will be able to find multiple objects contained in a single flow (for example, an email attachment as well as the mail body).

> i When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, `\_`).

Task

1 On your Linux-based appliance, select **Policies** | **Concepts**.

2 Click **Add Concept**.

3 Open **Advanced** at the bottom of the page and select the **Session Type** radio button.

4 Enter a name (uppercase only) and description (optional).

5 Click **?** and select a category from the list.

Packages of related concepts can be used to amplify searches and rule matching.

6 Click **Import Expressions** to load expressions from a file, or enter expressions in the **Expression** field. Escape all metacharacters to ensure literal interpretation (for example, `www\.deadspin\.com`).

7 Click **Validate**, then enter a sample string. If it matches, go on to the next step. Select **Matches String** to get a true or false acknowledgement.

8 Use one of the concept conditions to modify the action of the concept.

9 Click **Save**.

When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, `hello\_world`). Other metacharacters and ASCII characters (such as `&#x0020`, `&#x0009`, `&#x000C`, and `&#x200B` for space, tab, form feed, and zero-width space) can also be used to define concept expressions.

Set concept conditions

Set concept conditions to narrow matches to specific circumstances in which a pattern is found. Matches are reported only if certain conditions are met.

> Only **User-Defined** or custom concepts accept conditions.

Task

1 On your Linux-based appliance, select **Policies** | **Concepts**.

2 Open a category and click a **Concept Name**.

3 On the **Edit Concept** page, open a condition.

4 Define one or more concept conditions to modify the circumstances under which a match is reported.

5 Click **Save**.

Apply concepts to rules

Apply concepts to extend rules that are configured to find specific types of data.

Whenever a content concept is used with a rule, the pattern identified in the concept matches captured data whenever the rule runs.

> When creating concepts that have multiple words, you must escape spaces between words with a backslash (for example, `\_`).

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Open a policy by clicking a **Policy Name** and then clicking a **Rule Name**.

3 If you want the rule to run independently of its policy, set its **Inherit State** to **Disabled**.

This is useful for trying out rules before they are implemented with the other rules in the policy.

4 Open the **Content** category.

5 Select **Concept** | **is any of**.

6 Click **?**, open one or more concept categories, and select the concepts to be added.

7 Add one or more concept conditions to modify the action of the concept, if needed.

8 Click **Save** to save the modified rule.

9 Wait for the rule to run, then select **Incidents** to view the result.

Modify concepts

Modify the parameters of a concept to capture data patterns that are similar to a previously-defined set.

> You might want to remove one of the expressions used in a content concept if it generates false positive results.

Task

1 On your Linux-based appliance, select **Policies** | **Concepts**.

2 Open a category and click a **Concept Name** to open the concept.

3 Make any needed changes.

4 Click **Save**.

Restore concepts

Restore the standard (user-defined) concepts to their original state if they have become corrupted or difficult to handle.

> Only the original list of concepts under the **User-Defined** tab can be restored. Custom concepts cannot be recovered. Concepts listed under the **Built-in** tab cannot be edited, so they need not be restored.

Task

1 On your Linux-based appliance, select **Policies** | **Concepts**.

2 Open a category and select one or more concepts.

3 Select **Actions** | **Restore Default**.

Delete concepts

Delete concepts if they are no longer useful.

Task

1 On your Linux-based appliance, select **Policies** | **Concepts**.

2 Open a category and select concepts to be deleted.

3 Select **Actions** | **Delete**.

> To delete concepts one by one, click the trash can icon.

McAfee DLP regular expression syntax

Regular expressions are used to build McAfee DLP concepts. These expressions are customized for McAfee DLP; they do not use POSIX syntax.

Table 7-1 Regular expressions used in McAfee DLP operations

Expression	Definition
\n	line feed
\r	carriage return
\f	form feed
\b	backspace
\a	bell
\t	tab
\k	disables Perl/POSIX set range restrictions
\K	enables Perl/POSIX set range restrictions
\0xN	the hex ascii character equivalent to N
\nnn	the octal character of value nnn
\d	digit 0-9
\D	not digit 0-9
\c	any alpha A-Z or a-z
\C	not any alpha A-Z or a-z
\w	any alphanumeric \c or \d
\W	not alphanumeric ^\w
\s	any space [\ \f \n \r \t \[\]]
\S	not any space ^\s
\p	any space or field delimiter [\ -\\ :-@\[-`{-~ \[\]]
\P	not any space or field delimiter ^\p
\i	case sensitivity off
\I	case sensitivity on
[...]	character sets, for example, [3-6a-c] = 3,4,5,6,a,b,c
x-y	character ranges T-X = T,U,V,W,X
^	invert, for example, ^\0x0 are all characters except NULL
\	literal backslash (transforms metacharacters into ordinary characters). Examples: \\ \. \& \[\] \<space> * \+

8 Templates

Templates contain collections of content types. When used with rules or in a search, they save keystrokes.

Contents

How templates work

Templates are collections of elements that eliminate the need to perform routine operations repetitively.

Using templates saves time when searching, creating rules, or building capture filters. They make entering the same values multiple times unnecessary.

Pre-installed standard templates can be used as tools to help find groups of related elements in network data.

For example, the source code template contains patterns for most of the source code file types. It might be used to monitor network data for proprietary programs that insiders are attempting to send outside of the company.

Example of how a standard template works

Templates contain collections of data types that can be located on networks, in network repositories, and at network endpoints.

Using templates saves time when searching, creating rules, or building capture filters. They make entering the same values multiple times unnecessary.

Source code template

The source code template contains most of the source code file types. It might be used with a rule that is matched to static or dynamic data. By pairing a source code template with parameters including code samples, proprietary programs that insiders are attempting to send outside of the company can be located quickly and stored for legal follow-up.

Types of templates

Whether standard or customized, templates are organized by component type. Because they usually work on related elements, this limitation allows the greatest flexibility.

Pre-installed standard templates are configured to serve a variety of purposes, but custom templates can also be constructed.

Examining the list of standard templates and their construction can give you some ideas about how to build one that serves your own purposes.

How templates can be used to amplify queries

Templates can be used with any component to provide a wide-ranging qualifier for a search or rule.

On search and rule pages, each component menu includes a Template selection. When it is used as an additional parameter to extend any other component selection, the effect of a query or rule can be significantly amplified very quickly.

If a query uses the a keyword or concept component to find any file containing the confidential content, it can be extended to specific document types by using templates that group related types.

> For example, the CONFIDENTIAL concept is used to match data containing common words and phrases found in proprietary data. A template could be added to limit that search to office documents, source code, or email message bodies.

How to work with templates

You can add, modify, and delete templates, remove templates that have been applied to rules or filters, and use templates to create search queries.

Tasks

- *Add templates* on page 105
  Add templates to define collections of data that can be used as wide-ranging qualifiers. They can be used to save time on repetitive or complex searches.
- *Modify templates* on page 106
  Modify templates to tune their parameters for better performance.
- *Review template construction* on page 106
  Review standard or custom templates to learn to construct one. Examine their components and use them in sample searches to understand how they can be of use.
- *Use templates to search* on page 106
  Use templates to avoid repetitive searching. Using groups of related elements shorten queries and retrieve results quickly.
- *Find images using templates* on page 107
  Find images using templates to expedite searching of large graphics caches. The different image types included can retrieve image data in any format.
- *Remove templates from rules* on page 107
  Remove templates that have been applied to rules or filters if they are no longer useful.
- *Delete templates* on page 107
  Delete templates that are no longer useful. Templates can be deleted individually or as groups.
- *Archive handling* on page 58
  When archived files are captured, they are opened and their contents are analyzed by the indexer.

Add templates

Add templates to define collections of data that can be used as wide-ranging qualifiers. They can be used to save time on repetitive or complex searches.

> You can use a template to create a name for a range of IP addresses so you can refer to them as a group.

Task

1. On your Linux-based appliance, select **Policies | Templates**.
2. Select **Actions | Add Template**.
3. Enter a name and optional description.
4. Select a **Component Type**.

   This determines what type of object will be used in your template.
5. Click **Construction**.
6. Select a content type and modifier from the drop-down menus, then enter a value, or click **?** to select a value from the Content palette to complete the definition.
7. Click **Save**.

Modify templates

Modify templates to tune their parameters for better performance.

Task

1 On your Linux-based appliance, select **Policies** | **Templates**.

2 Click a **Template Name** to open a template for modification.

3 Open the **Construction** component.

4 Edit the parameters of the template.

5 Click **Save**.

Review template construction

Review standard or custom templates to learn to construct one. Examine their components and use them in sample searches to understand how they can be of use.

Task

1 On your Linux-based appliance, select **Policies** | **Templates**.

2 Click any **Template Name** on the page.

Use the same procedure for standard or custom templates.

3 Open **Construction**.

4 Review the parameters by examining the value field, or by clicking the **?** icon.

Use templates to search

Use templates to avoid repetitive searching. Using groups of related elements shorten queries and retrieve results quickly.

Each category on the **Advanced Search** and **Add/Edit Rule** pages includes a set of templates related to that category.

Learn to construct a custom template by looking at those listed under **Policies** | **Templates.**

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Template** | **equals**, then click **?**.

The Templates palette opens. If you added a custom template, it is included on the menu.

4 Select one or more templates from the menu.

5 Click **Search** or **Save as Rule**.

Templates are especially useful to tune rules because that process requires repetitive searching until the rule returns the correct results.

See also

Review template construction on page 106

Find images using templates

Find images using templates to expedite searching of large graphics caches. The different image types included can retrieve image data in any format.

> Add a Thumbnail Match column to your dashboard to scan results quickly. Avoid timeouts caused by retrieving large image files by adding additional search terms.

Task

1. On your Linux-based appliance, select **Capture** | **Advanced Search**.
2. Open the **Content** category.
3. Select **Template** and click **?**.

   The Template palette opens.
4. Select the **Common Image Files** template.
5. Click **Search** or **Save as Rule**.

Remove templates from rules

Remove templates that have been applied to rules or filters if they are no longer useful.

Task

1. On your Linux-based appliance, select **Policies** | **Policies**.
2. Click a **Policy Name** containing a rule to which a template has been applied.
3. On the **Edit Policy** page, click the rule to which the template has been applied.

   > Use the same procedure for a template that has been applied to a capture filter.
4. Click the red minus icon to remove the element containing the template.
5. Click **Save**.

Delete templates

Delete templates that are no longer useful. Templates can be deleted individually or as groups.

Task

1. On your Linux-based appliance, select **Policies** | **Templates**.
2. In the left column, select checkboxes for templates to be deleted.
3. Select **Actions** | **Delete**.

   > To delete templates one by one, click the trash can icon.

Archive handling

When archived files are captured, they are opened and their contents are analyzed by the indexer.

The search engine finds, extracts, and evaluates content in .zip, .gzip, and .tar archives, but only if the compressed file type is identified in the query.

Eight other compressed file types are also supported.

9 McAfee DLP Endpoint

McAfee DLP Endpoint is integrated into the McAfee Total Protection for DLP through the management console, McAfee DLP Manager. It adds protection for data in use to the product suite by monitoring and managing the activities of enterprise users.

What is McAfee DLP Endpoint?

McAfee DLP Endpoint is a content-based agent solution that monitors enterprise users' actions through the devices they use in the course of their work. It prevents compromise of sensitive data at a variety of network endpoints — not only on desktops and laptops, but on removable media, printers, clipboards, screens, windows, and defined shares and paths. Through McAfee DLP Manager, significant events that occur at those endpoints can be controlled, recorded, and responded to with an appropriate action.

The software is managed by ePolicy Orchestrator and deployed through McAfee DLP Agent, which distributes policies to endpoints and enforces them by generating and storing significant events in an evidence folder. When integrated into the product suite, the events are distributed to the McAfee DLP Manager **Data-in-Use** dashboard.

From that point, McAfee DLP Endpoint events follow the same workflow as the other products in the suite. Through McAfee DLP Manager, they share the ability to view, group and filter results in different configurations, get details on the attributes of the objects found, prepare reports, and manage related events by adding them to cases.

There are some differences between data generated through McAfee DLP Endpoint and the other products in the suite. Because data in motion and data at rest are detected through the McAfee DLP capture engine, processed, and stored on the McAfee DLP appliances, it can be queried. But data in use is stored in an evidence folder on ePolicy Orchestrator and is copied over to McAfee DLP Manager in a data stream. As a result, it is not searchable, but it can be used to construct rules.

What is McAfee Device Control?

McAfee Device Control software prevents unauthorized use of removable media devices, the most widespread and costly source of data loss in many companies today. It is automatically installed when McAfee DLP Endpoint is registered to McAfee DLP Manager and configured within the McAfee Total Protection for DLP product suite.

What does McAfee DLP Endpoint add to network DLP?

McAfee DLP Monitor, McAfee DLP Discover, and McAfee DLP Prevent can detect and trace the activity of users, but cannot manage their actions as they are occurring on or off the premises of the organization. They also cannot monitor and regulate communications between users within an organization.

McAfee DLP Endpoint provides that coverage, completing the McAfee Total Protection for DLP product suite.

Contents

How McAfee DLP Endpoint works

Integration of McAfee DLP Endpoint into the network product suite begins when a trust relationship is established between ePolicy Orchestrator and McAfee DLP Manager. After credentials are used to authenticate the connection, ePolicy Orchestrator extensions for the network product suite and McAfee DLP Endpoint cooperate to allow communication between McAfee DLP Agent (through a host plugin), the evidence server, ePolicy Orchestrator, and McAfee DLP Manager.

Policies are deployed through a secure channel created by McAfee DLP Agent, and events are sent back through that channel. When a significant event is detected, its path is stored in the database, and the file (which is encrypted before leaving the endpoint) is transferred to an evidence store on a remote share.

> Before McAfee DLP Endpoint can be integrated into the product suite, its host must be registered to McAfee DLP Manager, and a user account (epouser) must be created to access the evidence folder. Consult the *McAfee Total Protection for Data Loss Prevention 9.2 Installation Guide* for more information.

McAfee DLP Endpoint location in McAfee DLP Manager

In McAfee DLP Manager, McAfee DLP Endpoint functionality is located either under the **Endpoint Configuration** page, or under the **Endpoint** category on the **Add Rule** or **Edit Rules** page.

Endpoint Configuration in McAfee DLP Manager includes setting up the system, defining unmanageable printers, and defining an agent override password. Device control and application definitions are also managed from this page.

Parameters for device control, application tagging, and endpoint protection rules are located in on the **Endpoint Configuration** pages. Endpoint parameters can potentially be added to every rule in the network product suite through the **Endpoint** category. This is where administrators can configure new McAfee DLP Endpoint rules and deploy them through the connection with ePolicy Orchestrator.

Any network policy can contain endpoint parameters in its rules. After they are configured, the rules are deployed to the network extension, which integrates their global policy into the unified policy design.

How McAfee DLP Endpoint rules work with unified policy

Because unified policy rules can contain parameters that are deployed separately by McAfee DLP Monitor, McAfee DLP Discover, and McAfee DLP Endpoint, a single unified rule can be used to monitor traffic, scan repositories, and manage data at endpoints in the same operation. For example, a

Payment Card Industry policy that has been deployed through McAfee DLP Manager can be used to identify privacy violations in network traffic, in data repositories, and on endpoints.

💡 Multiple endpoints can be added to a rule as a group by creating a template, then selecting it from the menu before saving the rule. Adding frequently used collections of endpoints to a rule increases its efficiency and scope.

McAfee DLP Manager, Monitor, Prevent, and Endpoint all work to protect email and webmail through the unified rules.

With this unified design, a single rule can find and store related violations for each data type, and it can also apply actions to resolve each incident or event, then report it to the **Data-in-Motion**, **Data-at-Rest**, **Data-in-Use** dashboards.

Configuring McAfee DLP Endpoint

After McAfee DLP Endpoint and its components are installed on McAfee DLP Manager, you must set up essential functionality to establish communication through ePolicy Orchestrator.

Integrating McAfee DLP Endpoint into McAfee DLP Manager

The process of integrating McAfee DLP Endpoint with McAfee DLP Manager includes the following steps:

- Register ePolicy Orchestrator with McAfee DLP Manager
- Create an ePolicy Orchestrator user (epouser) in McAfee DLP Manager to allow ePolicy Orchestrator access to the MySQL database on McAfee DLP Manager
- Register McAfee DLP Manager as a registered server on ePolicy Orchestrator
- Register an evidence server on McAfee DLP Manager

Setting up McAfee DLP Endpoint

After McAfee DLP Endpoint is integrated into McAfee Total Protection for DLP, you must set up the software to work with the network product suite by completing the following tasks:

- Enable unified policy management by generating a policy, setting a posting period, and selecting a backward compatibility mode.
- Add an agent override password to encrypt and decrypt evidence and override default reactions.
- Add a list of printer models that cannot be controlled by McAfee DLP software.

When these operations are complete, you can define unified rules on the **Policies** page, then view the **Incidents** | **Data-in-Use** dashboard to verify that the endpoint events are being generated and reported.

Define unmanaged printers

Because some printers might not work with the proxy driver architecture required for McAfee DLP management, they should be whitelisted and excluded from management by the system.

Unmanaged printer definitions are created by selecting printer model information from the Active Directory server pop-up. There might not be any printers in your organization that cannot be managed, so this is an optional operation.

ℹ If you have not added an Active Directory server to the McAfee DLP Agent system, type printer paths and names to be whitelisted in the **Printer Model** field, then click **Add Printer**.

Task

1. On your Linux-based appliance, select **System** | **Endpoint Configuration** | **Miscellaneous** and click **Unmanaged Printer Models**.
2. Click **?**, then **Find**, and select from an existing **Directory Server** list.
3. Click **Apply**.
4. Click **Add Printer**.

Add an Agent Override password

An **Agent Override** password must be defined before doing any McAfee DLP Endpoint task to ensure encryption and decryption of evidence, and the possibility of reversing any default reactions.

A key must be used to unblock quarantined files, unlock and decrypt encrypted files, request justification for blocked actions, or work around any other events that have been generated by McAfee DLP Agent. The administrator provides this password when appropriate.

For example, a unified rule might protect a certain group of financial files on certain network shares and all endpoints. But because certain endpoint users will need read and write access to those files, it might include a selected **Request Justification** checkbox in the **Data-in-Use** action rule that is applied to that rule. As a result, when an authorized user opens the blocked file, he might be presented with a Request Justification pop-up that will allow the administrator to make an exception to the rule by providing the password. (The specific process and action is determined by the administrator.)

Task

1. On your Linux-based appliance, select **System** | **Endpoint Configuration** | **Miscellaneous** and click **Agent Override Password**.
2. Enter a password in the **Password** field and confirm it.
3. Click **Submit**.

Maintaining compatibility with installed agents

Because McAfee DLP Manager supports multiple versions of McAfee DLP Endpoint, the system must be configured to handle the correct McAfee DLP agent before the system is implemented.

Management of endpoints by McAfee DLP Manager is disabled by default to avoid interference with any existing McAfee Host DLP or McAfee DLP Endpoint operations that might already be running on ePolicy Orchestrator.

Because any existing software installations must continue to be supported, the default unified policy configuration is not activated until you generate a policy to provide the groundwork for connection with McAfee DLP Agent through ePolicy Orchestrator. Endpoints cannot be managed until a policy is assigned, and events cannot be monitored until McAfee DLP Agent has been updated.

The default configuration is **DLP Agent 9.0 and above**. If the McAfee Host DLP product installed on McAfee ePolicy Orchestrator was released before version 9.1, no change is needed on the **Manage Endpoints** page. The unified policy management process is initiated by selecting the **Generate Policy for Endpoint** checkbox on the system **Manage Endpoints** page.

The most significant reason for maintaining earlier versions of the endpoint product is the need for digital rights management, which controls use of digital content not authorized by the content provider. This feature of McAfee DLP Endpoint (also known as McAfee Host DLP) is not supported in McAfee DLP Manager, so network and endpoint applications must be run separately.

But if McAfee DLP Endpoint 9.1 is installed and digital rights management is not needed, **No compatibility** should be selected. This means that the new features in that release will be available in the network product suite. Features like **Document Scan Scope** and **Password Protected Files** will appear in the user interface only if the 9.1 version of McAfee DLP Agent is accessible through McAfee DLP Manager.

Manage endpoints

When you manage endpoints from McAfee DLP Manager, you must generate a policy, set a posting interval, and select a compatibility mode. These settings support the distribution of McAfee DLP Endpoint events to McAfee DLP Manager dashboards through ePolicy Orchestrator.

If McAfee Host DLP is already installed on ePolicy Orchestrator, using the McAfee DLP Endpoint networked version will overwrite the events on the evidence server. Because of this potential problem, you must deliberately generate a policy to support installation of the updated endpoint product.

You must also set an interval for posting policy modifications through ePolicy Orchestrator. By default, rule definitions are updated on the McAfee DLP Endpoint extension every 30 seconds, but you can define a more conservative transfer interval (up to two hours, or 7200 seconds) by editing the **Time Duration for Posting Policy Definition** setting.

Task

1. On your Linux-based appliance, select **System** | **Endpoint Configuration** | **Miscellaneous** and click **Manage Endpoints**.

2. Select the **Generate Policy for Endpoint** checkbox.

3. In the **Time Duration for Posting Policy Definition** field, enter a number between 30 and 7200 seconds.

   The policy is generated, posted from McAfee DLP Manager to ePolicy Orchestrator, saved in the database, forwarded to the connected agents, and updated at the defined interval.

4. Click **Submit**.

Viewing events

Problems identified by the McAfee DLP Agent might include critical system events, rule violations, or events associated with a particular user or computer.

The events displayed might also include registered and classified content that has been tagged for protection purposes, disallowed user actions, access violations, or detection of a controlled element.

The roles users play in an organization determine what types of events they are allowed to view.

Once displayed on the dashboard, events can be filtered by general, administrative, or outgoing conditions and evaluated. For example, an administrative event might indicate that an agent or policy state has changed, and an outgoing event might be generated when protected data is in motion.

View endpoint events

You can view events detected by McAfee DLP Endpoint on the McAfee DLP Manager **Data-in-Use** dashboard.

If you cannot see endpoint events, you might not have the right permissions set. Contact your administrator.

The order and placement of dashboard columns determines the display of event details. Click the column icon to modify the presentation of the attributes of the events.

Task

1. On McAfee DLP Manager, select **Incidents**.
2. From the thumbwheel menu, select the **Data-in-Use** vector.

   The default **Incident Listing** page appears.
3. Click a **Details** icon.

   The **Incident Details** page appears.
4. Click any tab on the page to get additional information about the event.

   > If a document link is available, it will open if the supporting software is installed. If there is another link inside the document, it is likely to be the database object that triggered the incident.

How events are transferred and displayed

McAfee DLP Endpoint events detected by McAfee DLP Agent are copied to a McAfee DLP Manager database and displayed on its **Data-in-Use** dashboard.

When a McAfee DLP Endpoint parameter that is included in a unified rule hits, an event is generated at the endpoint. It is encrypted, then delivered through McAfee DLP Agent on ePolicy Orchestrator to McAfee DLP Manager, which stores the object and its attributes in the **Data-in-Use** database.

You can view the event and its details on the **Data-in-Use** dashboard, whose columns can be configured to display the most significant information about the event. For example, users might want to display the columns that disclose the origin or destination of an event, its owner, and what activity generated it. By clicking the **Details** icon, the user might view more attributes of the event, create a report, or assign it to a case.

Finally, any attribute of the event might be used to create a new rule with actions that might resolve similar events in the future. When that rule is completed, it is deployed back through ePolicy Orchestrator and communicated through McAfee DLP Agent to provide enhanced protection at other endpoints.

Events displayed in McAfee DLP Manager

Specific events are distributed through ePolicy Orchestrator to McAfee DLP Manager dashboards.

Table 9-1 Events reported to McAfee DLP Manager

Event type	Event display name	Event localization key
112	Agent enters bypass mode	AGENT_ENTERS_BYPASS
113	Agent leaves bypass mode	AGENT_ENTERS_BYPASS
401	User returned from safe mode	SAFE_MODE_WAS_DETECTED
10000	Device plugged in	DEVICE_PLUG
10001	Device unplugged	DEVICE_UNPLUGGED
10002	New device class found	UNKNOWN_DEVICE_PLUGGED
40101	Network file system protection	OUTGOING_FS
40102	Removable storage protection	OUTGOING_FS_REMOVABLE
40200	Email protection	OUTGOING_EMAIL
40301	Printing protection	OUTGOING_PRINTER
40400	Network protection	OUTGOING_NETWORK
40401	Device access	OUTGOING_DEVICE

Table 9-1 Events reported to McAfee DLP Manager *(continued)*

Event type	Event display name	Event localization key
40500	Web post protection	OUTGOING_HTTP
40601	Application file access protection	OUTGOING_MEMORY_VIA_FS
40602	Clipboard protection	OUTGOING_MEMORY_VIA_CLIPBOARD
40603	Screen capture protection	OUTGOING_MEMORY_VIA_SCREEN_CAPTURE
50000	Discovery	DISCOVERY

Unified policies and McAfee DLP Endpoint

Rule definitions for McAfee DLP Endpoint were originally designed to share a single global policy definition — only one policy supported multiple rules. But McAfee Total Protection for DLP is designed around a collection of unified international policies, and the McAfee DLP Endpoint global policy is accommodated within that system.

Unified policy handles endpoint events by adding an **Endpoint** category to every rule of every policy. When that category is opened on the **Add** or **Edit Rule** page, a menu listing the McAfee DLP Endpoint parameters is displayed. One or more can be selected to add specific endpoints to the parameters of any rule.

Parameters outside of the **Endpoint** menu also apply to endpoints. The entire **Content** category and much of the **Source/Destination** category (for example, GeoIP location is not supported) contain parameters that can be used on endpoints as well as networks.

The same rule might also contain parameters that will match data found by the McAfee DLP Monitorcapture engine or McAfee DLP Discover scans. In other words, one unified rule can be configured to add incidents and events to all three dashboards (**Data-in-Motion**, **Data-at-Rest**, **Data-in-Use**).

For example, a *Payment Card Industry* policy that has been deployed on through McAfee DLP Manager can be used to identify privacy violations in network traffic, in data repositories, and on endpoints.

> Multiple endpoints can be added to a rule as a group by creating a template, then selecting it from the menu before saving the rule. Adding frequently used collections of endpoints to a rule increases its efficiency and scope.

How McAfee DLP Endpoint rules are mapped

When McAfee DLP Endpoint was integrated into McAfee Total Protection for DLP, its rule structure had to be adapted to the unified policy design.

Standard rules are organized under sets of policies that might have multiple owners. McAfee DLP Endpoint rules preserve this hierarchy by feeding into this structure as attributes, or rule types.

The merged structure is changed to `<policy owner> <policy> <rule> <rule type>`.

McAfee DLP Endpoint rule exceptions

If a unified rule contains attributes that are not supported by McAfee DLP Endpoint, the rule will not produce accurate results.

If the following parameters are used in a unified rule, they will not be applied to endpoints:

- Email address sender variants
- Email subject (except for the condition **contains none of**, which is supported)

- GeoIP locations
- User city
- User country
- File size
- Keyword expressions
- Concept expressions

McAfee DLP Endpoint search limitations

McAfee DLP Endpoint data cannot be searched because it is not indexed.

Although McAfee DLP Endpoint data cannot be searched, it can be identified if it is tagged or registered - and user activities can be monitored and controlled to prevent compromise of sensitive data.

Configuring endpoint rules in McAfee DLP Manager

When you configure an endpoint rule in McAfee DLP Manager, you are adding one or more endpoint parameters to a new or existing unified rule.

The rule types that make up the McAfee DLP Endpoint policy are designed for specific functions. The collection is made up of classification rules, tagging rules, protection rules, device rules, and user and group assignments. All of these rules can be configured through McAfee DLP Manager by selecting and defining their parameters on individual rule definition pages. When added to the existing rules in the product suite, endpoint parameters can be used to extend internationalized standard or customized rules to desktops, laptops, removable media, printers, clipboards, screens, windows, shares and paths.

When that category is opened on the **Add** or **Edit Rule** page, a menu listing the McAfee DLP Endpoint parameters is displayed. One or more can be selected to add specific endpoints to the parameters of any rule.

Protection rules

When activated, protection rules generate specific reactions that vary depending on a number of conditions, including whether the user is on- or offsite. For example, a user who attempts to upload a file to a social media site might be prevented from doing so by the *Web Post Protection Rule*, which might also have been configured to send notification of the event and store evidence relating to it.

Protection rules define the action taken when an attempt is made to transfer or transmit tagged data. Each protection rule can deploy different combinations of reactions, which can be viewed by clicking each protection rule on the **Action Rules** page under **Data-in-Use**.

Add endpoint parameters to rules

Adding endpoint parameters to rules that run under unified policy allows you to extend rules that have been applied to **Data-in-Motion** and **Data-at-Rest** to **Data-in-Use**.

For example, adding a **Protect Network Printers** parameter to an existing *Banking and Financial Sector* rule might block users on laptops from printing sensitive financial data.

> Open the **Endpoint** component on any **Edit Rule** page to see what parameters are available.

Task

1 On your Linux-based appliance, go to **Policies** and click on any rule under any policy.

2 Open the **Endpoint** component.

3 Select an endpoint parameter and define it. If it is a protection rule, click **?**, then select **Enable** and **Apply**.

Protection rules are disabled by default.

4 If a reaction is to be added, click the **Actions** tab, then **Add Action**.

5 Select a suitable action from the **Data in Use** section.

6 Click **Save**.

Assign endpoint events to cases

Assign endpoint events to McAfee Total Protection for DLP cases if further investigation is warranted. **Data-in-Use** events can be assigned to the same cases as **Data-at-Rest** and **Data-in-Motion** incidents.

> If an error is encountered while assigning incidents to a case (for example, the object cannot be fetched from the evidence share), you must reassign each of the failed incidents to the case.

Task

1 On your DLP appliance, go to **Incidents** and select one or more endpoint events.

2 Click **Assign to Case** and select **New Case** or **Existing Case** from the sub-menu.

3 Click **Apply**.

Using McAfee DLP Endpoint protection rules

All McAfee DLP products are capable of deploying rules to data in motion and data at rest, but McAfee DLP Endpoint also protects data in use.

Discovery, application, and web post protections are deployed to endpoints from the network product suite through the use of unified policies. Rules providing protection in specific circumstances can be used to provide reactions to significant events from the network applications, but they must be enabled.

McAfee DLP Endpoint protection rules are integrated into McAfee DLP Manager through unified policies, and action rules are applied to the events detected. But rules containing endpoint protection parameters are disabled by default, and reactions fire only if they have been enabled on the **Edit Rule** page under **Endpoint**.

For the other managed DLP products, protection actions are optional, and are applied to rules that are deployed from McAfee DLP Monitor or McAfee DLP Discover. The action rules that apply to those products are displayed under the **Data-in-Motion** and **Data-at-Rest** sections of the **Policies** | **Action Rules** page. The endpoint protection rules are now also classified as action rules, and they are listed under the **Data-in-Use** section.

> With unified policy, one rule can potentially support many different actions. The rule can match the same parameters in data in motion, at rest, or in use, and can apply different actions to each. Because McAfee DLP Manager is the central console for all of the DLP products, endpoint actions operate in the same way as the other managed products.

Protect data from being printed on local printers

If the **Protect Local Printers** rule is deployed, McAfee DLP printer drivers are installed in place of third party drivers. This prevents users from printing sensitive data.

Before you begin

If you want to trigger an action when the rule hits, configure the action rule you intend to use with the appropriate settings, or add a new one under the **Data-in-Use** section on the **Action Rules** page.

For example, if you suspect that local users are attempting to print and email corporate confidential documents, you might use the following procedure to detect that activity, extract the content of the document to the evidence server, and notify a manager that the attempt has been made.

Task

1. On your DLP appliance, select **Policies**.
2. Click a policy and a rule, or create new ones.

   Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.
3. On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

   The concepts palette appears.
4. From the **Corporate Confidential** menu, select document types or click **Select All**.
5. Click **Apply**.
6. From the **Source/Destination** menu, select **Email Address** and enter the user's email address in the value field, or select the **Any Email Address** checkbox.
7. From the **Endpoint** menu, select **Protect Local Printers**, click **?**, select the **Enable** checkbox, and click **Apply**.
8. Click the **Actions** tab and click **Add Action**, then select **Email Reaction** from the **Data-in-Use** menu.
9. Review the reaction settings in the **Actions** column.

   If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.
10. Click **Save**.

Protect data from being printed on network printers

If the *Network Printer* rule is deployed and a directory server is added to McAfee DLP Manager, you can prevent users from printing sensitive data on network printers.

Before you begin

If you want to trigger an action when the rule hits, configure the action rule you intend to use with the appropriate settings, or add a new one under the **Data-in-Use** section on the **Action Rules** page.

Some printers cannot be managed in this way, and must be defined during the **Endpoint Configuration** phase.

For example, if you suspect that network users on- and off-site are attempting to print confidential documents, you might use the following procedure to detect that activity, and notify the user that a company policy against printing confidential documents has been violated and blocked.

Task

1 On your DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

> Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Keyword** from the **Content** menu and enter an identifying word or phrase into the value field (for example, *Confidential* or *Top Secret*).

If you know the document type, you might want to add another element (for example, **Content Type is any of MS Word**) to identify the content type.

4 From the **Source/Destination** menu, select **User Groups**, and click **?**.

5 From the directory server pop-up, click **Find** and click the appropriate user name, group, or organization.

6 Click **Apply**.

7 From the **Endpoint** menu, select **Network Printer**, click **?**, select the **Enable** checkbox, and click **Apply**.

8 Click the **Actions** tab and click **Add Action**, then select **Printer Reaction** from the **Data-in-Use** menu.

9 Review the reaction settings in the **Actions** column.

If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one

> In this case, you must select the **Online** and **Offline** checkboxes for both **Block** and **Notify** when creating or modifying the action rule.

10 Click **Save**.

Protect data from being printed to file

McAfee DLP Endpoint can be configured to block print functionality that allows printing to the Adobe PDF or Microsoft Image Writer file types. If the *Protect PDF/Image Writers* rule is deployed, McAfee DLP printer drivers are installed in place of third party drivers. This prevents users from printing sensitive data to a file.

Before you begin

If you want to trigger an action when the rule hits, configure the action rule you intend to use with the appropriate settings, or add a new one under the **Data-in-Use** section on the **Action Rules** page.

For example, if you suspect that local users are attempting to print and email corporate confidential documents, you might use the following procedure to detect that activity, extract the content of the document to the evidence server, and notify a manager that the attempt has been made.

> McAfee DLP Endpoint uses Microsoft Word and Adobe Reader plug-ins to improve performance.

Task

1 On your DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

> Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Template** from the **Content** category menu and click **?**.

The templates palette appears.

4 From the **Content** menu, click **Common Content Types**.

5 From the **Source/Destination** menu, select **Email Address** and enter the user's email address in the value field, or select the **Any Email Address** checkbox.

6 From the **Endpoint** menu, select **Protect PDF/Image Writers**, click **?**, select the **Enable** checkbox, and click **Apply**.

7 Click the **Actions** tab and click **Add Action**, then select **Printer Reaction** from the **Data-in-Use** menu.

8 Review the reaction settings in the **Actions** column.

If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.

9 Click **Save**.

Protect data from being transferred via clipboards

McAfee DLP Endpoint can be configured to disable clipboard functionality, making it impossible for users to cut or paste data between existing and new documents.

Before you begin

If you want to trigger an action when the rule hits, configure the action rule you intend to use with the appropriate settings, or add a new one under the **Data-in-Use** section on the **Action Rules** page.

> Trusted processes are not part of the clipboard rule logic. Applications with a *Trusted* strategy are not exempt from screen capture rules, and will be blocked like any other application.

For example, if you want to ensure that the contents of financial documents cannot be cut and pasted into new documents, use the *Banking and Financial Sector* with the *Protect Clipboard* rule to protect those documents.

Task

1 On your DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

> Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

4 From the **Template** menu, select the *Banking and Financial Sector* document set.

5 Click **Apply**.

6 From the **Endpoint** menu, select **Protect Clipboard**, click **?**, select the **Enable** checkbox, and click **Apply**.

7 Click the **Actions** tab and click **Add Action**, then select **Clipboard Reaction** from the **Data-in-Use** menu.

If you want to add other reactions, such as notifying the owner of the documents or storing evidence of the attempt to copy content, go to the **Action Rules** page, open the **Clipboard Reaction** action rule, and modify it to include those actions.

8 Click **Save**.

Protect data from screen capture

McAfee DLP Endpoint can be configured to disable screen capture functionality, making it impossible for users to record sensitive data by capturing the image on a desktop or laptop monitor.

Before you begin

If you want to trigger an action when the rule hits, configure the action rule you intend to use with the appropriate settings, or add a new one under the **Data-in-Use** section on the **Action Rules** page.

> Trusted processes are not part of the screen capture rule logic. Applications with a *Trusted* strategy are not exempt from screen capture rules, and will be blocked like any other application.

For example, if you want to ensure that engineering drawings cannot be captured, use the *Engineering Drawing and Design Files* with the *Protect Screen Capture* rule to protect those documents.

Task

1. On your DLP appliance, select **Policies**.
2. Click a policy and a rule, or create new ones.

   > Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3. On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.
4. From the **Template** menu, select the *Engineering Drawing and Design Files* document set.
5. Click **Apply**.
6. From the **Endpoint** menu, select **Protect Screen Capture** , click **?**, select the **Enable** checkbox, and click **Apply**.
7. Click the **Actions** tab and click **Add Action**, then select the **Print Screen Reaction** from the **Data-in-Use** menu.

   If you want to add other reactions, such as notifying the owner of the documents or storing evidence of the attempt to capture content, go to the **Action Rules** page, open the **Print Screen Reaction** action rule, and modify it to include those actions.

8. Click **Save**.

Protect data with Document Scan Scope

The Document Scan Scope feature allows you to search for strings in the header, footer, and/or body of a Microsoft Office document. This feature improves performance because the agent need not extract and analyze content from complete documents.

Before you begin

If you want to trigger an action when the rule hits, make sure that the action rule you intend to use has the right action settings. If not, add a **Data-in-Use** action rule, or create a new one.

If you have to find and control documents in which a known word or phrase appears in a specific location in a document, you can use **Document Scan Scope** to find them quickly and keep them from being distributed.

> Both network and endpoint applications support document properties, but because **Date Creation** and **Date Modified** are Windows parameters, the network applications do not support them.

Task

1 On your DLP appliance, select **Policies**.

2 Add a new policy and rule, or open existing ones.

> Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 Open the **Content** category, and enter a word or phrase that can be found in the documents you want to protect into the value field, such as "Confidential".

4 Open the **Endpoint** category and select **Document Scan Scope**.

5 Open the **Source/Destination** category, select **URL** and **is none of**, and enter the name and domain of your company.

By selecting a negative condition, you ensure that documents exchanged legitimately within your company will not be affected, but all others being sent out of your intranet will be detected.

6 Click **?** and select the **Body**, **Footer**, and/or **Header** checkboxes from the **Select items** window.

7 Click **Apply**.

8 Click the **Action** tab, click **Add Action**, and select an action from the **Data-in-Use** actions.

In this case, you might want to use an **Email** or **WebPost** reaction to block, monitor, and store evidence of the activity, whether they are found online or offline (in computers that are on-site, or disconnected from the network). Those reactions also allow notification and requests for justification, so you might want to modify the rule if those actions are not needed.

9 Click **Save**.

Protect data using encryption types

Encryption types can be used in rules to act on files that are unencrypted, password-protected, or encrypted with a specific algorithm.

> **Before you begin**
>
> If you want to trigger an action when the rule hits, make sure that the action rule you intend to use has the right action settings. If not, add a **Data-in-Use** action rule, or create a new one.

For example, if you suspect that members of your Finance Department are emailing files encrypted with McAfee Endpoint Encryption for PC to their own email accounts so they can work on them at home, you can find them quickly and block that activity. If some users are permitted to do transmit encrypted files, you can create a **Source/Destination** user exception, or add a **Request Justification** option to the reaction.

Task

1 On your DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

> Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

The concepts palette appears.

4 From the **Corporate Confidential** menu, select document types or click **Select All**.

5 Click **Apply**.

6 From the **Source/Destination** menu, select **User Groups**, and click **?**.

7 From the directory server pop-up, click **Find** and select the finance user group.

8 Click **Apply**.

9 If you want to define a user exception, add another **Source/Destination** parameter.

You might select a **User Name** from the directory server and add a **sender is none of** condition. Alternatively, you might enter the email address of the authorized user into the value field and accept the default **sender is any of** condition.

10 From the **Endpoint** menu, select **Encryption Types** and click **?**.

11 Select the **McAfee Endpoint Encryption for PC** checkbox and click **Apply**.

12 Click the **Actions** tab, click **Add Action**, and select **Email Reaction**.

13 Review the settings in the **Actions** column.

If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.

14 Click **Save**.

Protect data from removable media

McAfee DLP Endpoint can be configured to block, monitor, notify, or allow read-only access to removable media. You can combine a *Protect Removable Media* rule with other rule parameters to keep defined data from being copied to one of these devices.

> **Before you begin**
>
> Create a **Removable Storage File Access Rule** to identify the device types to which the rule is applied.

Data that is available through top secret governmental networks relies on the scruples of its users. Using a removable media ensures that secret information cannot be copied and distributed to unauthorized users or organizations.

Task

1 On your DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

> Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

3 On the **Add Rule** or **Edit Rule** page, select **Keyword** from the **Content** menu and enter an identifying word or phrase into the value field (for example, *Confidential* or *Top Secret*).

If you know the document type, you might want to add another element (for example, **Content Type is any of MS Word**) to identify the content type.

4 From the **Endpoint** menu, select **Protect Removable Media** , click **?**, select the **Enable** checkbox, and click **Apply**.

5 Click the **Actions** tab and click **Add Action**, then select **Removable Media Reaction** from the **Data-in-Use** menu.

6 Review the reaction settings in the **Actions** column.

If they do not match your objectives, go to **Actions Rules** and edit the rule, or create a new one.

> In this case, you must select the **Online** and **Offline** checkboxes for both **Block** and **Notify** when creating or modifying the action rule.

7 Click **Save**.

Use endpoint templates in unified rules

Using a template with other unified rule parameters allows you to apply the same condition to many rules.

> **Before you begin**
>
> If you want to trigger an action when the rule hits, configure the action rule you intend to use with the appropriate settings, or add a new one under the **Data-in-Use** section on the **Action Rules** page.

For example, if you are protecting your source code from off-site employees who are not programmers or developers, you can use a template to create lists of users who are authorized to work on it from their laptops or desktops. The same list of of engineering employees might be used to provide access to functional specifications, design documents, and engineering drawings.

Task

1 On your DLP appliance, select **Policies**.

2 From the **Actions** menu on the **Templates** page, select **Add Template**.

The **Add Template** page appears.

3 Enter a name for the group of users, and add an optional description.

4 From the **Component Type** menu, select **Source/Destination**.

5 From the **Construction menu** menu, select **User Groups** and click **?**.

If you have added a directory server to McAfee DLP Manager, a pop-up appears.

6 Click **Find**, select the engineering user group, and click **Apply**.

7 Click a policy and a rule, or create new ones.

> Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

8 On the **Add Rule** or **Edit Rule** page, select **Template** from the **Content** category menu and click **?** and select **Source Code** from the templates palette.

9 Click **Apply**.

10 From the **Endpoint** category menu, click **?** and select the template you created for engineering users.

11 Click **Save**.

If you want to protect engineering documents as well as source code to all but authorized employees, you can create another rule with the same parameters, but select the **Engineering Drawing and Design Files** template from the **Content** menu instead. In addition, you might want to create a new policy and add both rules to it, then add others as similar situations arise.

Use Window Titles at endpoints to unified rules

If the *Protect Screen Capture* **Endpoint** rule is deployed with the **Windows Title** parameter, McAfee DLP printer drivers are installed in place of third-party drivers. This prevents users from taking screenshots of sensitive data. If an application opens windows containing sensitive data, remote users can be prevented from taking screenshots by identifying the title of the window.

Task

1 On your DLP appliance, select **Policies**.

2 Add a new rule, or open an existing one.

The **Edit Rule** page appears.

3 Open the **Endpoint** category and select **Windows Title**.

4 Select **is any of** or **is none of**. The latter will produce results that do not contain the string.

5 Enter the string in the value field and click **?**.

The **Select items** window appears.

6 Select one or more checkboxes and click **Apply**.

7 Click **Save**.

The new or edited rule will be listed under the appropriate policy.

Using endpoint action rules

McAfee DLP Endpoint action rules were originally called *reactions* and were associated only with protection rules. In McAfee DLP Manager, action rules can be appended to any unified rule containing endpoint parameters, and the actions can be applied when the rule hits.

In the network product suite, if a unified rule is deployed to the network as well as endpoints, **Data-in-Use** endpoint action rules can be applied to that rule. But **Data-in-Motion** and **Data-at-Rest** action rules can also be applied to the rule, so that when it hits, three different actions might be deployed to three different data types.

> In McAfee DLP Manager, McAfee DLP Endpoint protection rules are disabled by default, and action rules must be explicitly attached through the user interface.

Data-in-Use action rules are unique because they can be set to fire whether or not the user is on- or off-site — that is, connected directly to the network, or off the network. (The terminology used in the user interface is *Online* or *Offline*.)

Types of endpoint action rule

McAfee DLP Endpoint actions, originally called *reactions*, are taken when protection rules deployed through McAfee DLP Manager find matching data on endpoints. If the rule is enabled, an action is applied when the rules hit.

Each action rule might contain multiple actions. For example, a user's action might be blocked, his manager might be notified, and evidence of the user's action might be stored.

In addition, each of the endpoint actions might be applied to endpoints depending on whether the user is on-site or off-site.

- Block
- Delete
- Encrypt
- Monitor
- Notify User
- Quarantine
- Request Justification
- Store Evidence
- Tag

Add endpoint action rules

Action rules that are applied to rules with endpoint parameters can be set to react to significant events that are reported by McAfee DLP Agent. If multiple actions are selected, they will be applied simultaneously when an event is detected.

For example, a **Removable Media** reaction might block, monitor, and store evidence of a significant event, whether the device is on-site or off-site.

> Open the list of action rules on the **Policies** page, then scroll down to **Data-in-Use** to view the standard **Endpoint** parameters.

Task

1. On your Linux-based appliance, select **DLP Policies > Action Rules**.
2. From the **Actions** menu under **Data-in-Use**, select **Add Action Rule**.

   Endpoint actions can be taken if the detected device is on- or offsite. Select one or both.
3. Enter a name for the action rule.
4. Select one or more actions to be taken when a protected event is detected.
   - If the event detected is to be encrypted, provide an encryption key. Consult the updated *Endpoint Encryption for Files and Folders 4.0 Product Guide* for more information.
   - If the event detected is significant, select a **Severity** from the drop-down list.
   - If users are to be notified when the event is detected, enter a message. Entering link text or a URL is optional.
5. Click **Save**.

   After you have created the endpoint action rule, apply it to one or more rules.

Apply endpoint action rules

Apply endpoint action rules by selecting a rule, adding a **Data-in-Use** action, and saving the rule.

Unified policy allows application of actions to network traffic, data repositories, and endpoints. Each rule can support one action rule for each of the three types of data.

Task

1. On your DLP appliance, select **Policies** and click on a rule that has one or more endpoint parameters.
2. Click the **Actions** tab and select **Add Action**.
3. Select one or more **Data-in-Use** actions to be taken when a protected endpoint is detected.
4. Click **Save**.

Releasing quarantined files

When sensitive content is located during a scan of endpoints, a policy setting allows for potential resolution of the problem detected. For example, the event might trigger deletion of a file that is being accessed, but it might also be released if the user obtains a release key.

Release keys for quarantined files might be granted by generating a challenge key and sending it to an administrator. If the case is justified, the administrator issues an **Agent Quarantine Release Key**.

Endpoint discovery through McAfee DLP Manager

When a Discover scan operation is defined on McAfee DLP Discover through McAfee DLP Manager, the scan is extended to local drives as well. The connection is made through unified policies, which are defined in the Discover scan and deployed to both network locations and endpoint file systems.

It is not possible to tag all files at risk on laptops, desktops, and any mounted volumes, but Discover scans of CIFS (Windows-based) shares can be used to deploy rules to any file found on C$ (the local drives) through that share. Using this method, McAfee DLP Manager can identify and tag potential problems on large volumes of endpoint files.

But endpoint scans can only be constructed in McAfee DLP Discover; they cannot be run until the conditions defined on the Agent Configuration page in ePolicy Orchestrator are met. After the scan is run, the results are returned to McAfee DLP Manager through the secure channel maintained by McAfee DLP Agent.

Data classification and registration differences

Because the McAfee Total Protection for DLP product suite uses a classification engine that differs from that used by McAfee DLP Endpoint, a different content strategy is used to deploy unified rules to endpoint parameters.

McAfee DLP Endpoint uses built-in dictionaries with terms that are commonly used in health, banking finance, and other industries, and text patterns that identify known strings and complex patterns through the use of POSIX regular expressions. File properties and registered document repositories, which are identified by location-based tags, are also used to classify content, and whitelists define text that is ignored by the tracking mechanism.

By contrast, the McAfee Total Protection for DLP classification engine sorts all captured data into content types and stores it on the McAfee DLP appliances, and that data store can be searched in a variety of ways. Signatures that fingerprint significant data are generated by matching text patterns, regular expressions, content types, keyword expressions, and built-in or user-defined concepts to dynamic and static data, producing incidents and violations in network traffic and repositories. The results of those matches are registered in DocReg and DBReg concepts that function as *signature banks* that are automatically shared across all McAfee DLP appliances that are registered to McAfee DLP Manager.

Data is also classified by source and destination (including email/webmail and geographic location), file properties, protocols, and database components (including data sorted into tables, columns and rows). All of these parameters can be viewed on any rules page on the unified policies dashboard.

In the unified policy design, the same rule definitions can be used to find incidents and violations in network traffic, static repositories, and on endpoints, and actions can be programmed to apply to all three types of data. Because of these differing data designs, endpoint parameters are combined with all other parameters available in unified rules. There is no need for repetitive rule setting, since all protection rules can use the same defined parameters.

How McAfee DLP Endpoint registration scans work

Endpoint registration scans deploy registered index packages via McAfee DLP Agent, which distributes them to endpoints and blocks distribution of files containing registered content.

McAfee DLP Endpoint uses document registration and location-based tagging to define data at risk. Documents that existed before the location-based tag might not be detected by those tagging rules, but the original file might be opened or copied from the original endpoint. Registered document classification rules detect all files at risk in the defined folders.

If the same confidential content exists in several documents, McAfee DLP Endpoint might categorize it only once using a registered document repository. When location-based tagging is used, every network share where the confidential content is located must be tagged.

Scan data at rest on endpoints

Discovery scans on laptops, desktops and mounted devices (such as USB and extended drives) are configured using McAfee DLP Discover to create a CIFS Discover scan. But the scan is actually run through ePolicy Orchestrator by configuring the scan definition (schedule, credentials, etc.) on the **Agent Configuration | Discovery Settings** page.

Before you begin

Determine which policies you are going to use to scan endpoints, and deploy them by selecting the Host device checkbox. All rules of the policy must be enabled so that they can inherit the state of the policy.

Because ePolicy Orchestrator is a Microsoft Windows server, the Discover scan must be configured to use the CIFS protocol.

The network-based Discover scan is used as a framework for endpoint scans. Since scan definitions are defined by configuring the agent, those parameters should be skipped in the **Edit Scan Operation** pages.

Task

1. On your DLP appliance, select **Classify | Scan Operations**.
2. From the **Actions** tab, select **New**.
3. Enter a scan task name and optional description.
4. From the **Repository Type** menu, select CIFS.
5. Do not make a selection from the **Credential** and **Schedule** menus.
6. From the **Mode** menu, select the Discover scan type.
7. Under **Devices**, select the Discover appliance from which the scan will be run.
8. On the **Node Definition** tab, provide the IP address of the CIFS server that is the target of your scan.
9. If you want to test the connection, select your device before clicking **Test**.
10. Click **Include** to add the defined node to the **Included** list.

    If you want to exclude one or more addresses from an IP adress range or subnet, click **Exclude**.
11. Click the **Filters** tab to define the exact location on the server that you want to scan.

    You can filter by share, folder, and file property on CIFS server.

12 Click **Browse** to navigate to the location of the scan.

Alternatively, open the **Filter** category and set the options manually.

13 click the **Policies** tab and select policies whose rules will be applied against data at rest in the defined repositories.

14 Click **Save**.

Tagging and tracking

A tag is metadata that is added to the file in the form of a GUID that might also have a name and description. It is essentially an extended attribute that can be used to identify and track sensitive content on desktops, laptops, removable media, and other devices that contain data.

A tag label works as a classification device and stays with the content, even if it is copied into another document, moved to another location, attached to other files, or saved to another format.

The label can be either application- or location-based, and in McAfee Total Protection for DLP, might be applied in one of three ways:

- By rule (automatically)
- Directly (manually)
- By scanning a Windows repository (automatically)

After tags are created, the files to which they are applied can not only be tracked, but controlled by pre-programming **Data-in-Use** action rules that fire when tagged objects are found.

Using tags

In the McAfee Total Protection for DLP product suite, unified policy rules might contain location or application-based tags — and they might be used alone, or in combination with other Endpoint and network parameters to identify and apply actions to data at risk anywhere within the reach of the McAfee DLP Manager.

Users who have administrative privileges can create **Tag Labels** on the **Endpoint Configuration** page, then select them from menus on **Edit Rules** pages to define a condition for automatically applying them. If used on those pages, they can also be automatically to CIFS (Windows) repositories and endpoints through Discover scans.

When tag labels are used on unified policy rules pages, they can be applied as needed to files that match the conditions of the rules, or existing tags can be applied to a specific set of files that are defined by the rule.

For example, the Pharmaceutical Industry *Drug Code Data* rule might be modified to include an **Existing Tag Label** that identifies and tracks any document containing that code. An *Email Protection Rule* might then be added to prevent users from sending those documents to competitors.

> This rule applies only to data in motion, but email protection is covered by both network and endpoint products.

Applying tags with rules

Many files can be tagged in a single operation by using tags in combination with unified policy rules. When a tag is added to a network rule, its reach is not only extended to endpoints, but it can be used to impose a wide variety of conditions on the targeted data before the tag is applied. Many different network and endpoint parameters might be used to automatically apply tags when sensitive data is detected — and if specific conditions are not met, they might not be applied at all.

For example, a network rule might be used in an Asian bank to find and apply privacy tags to all files that contain *China UnionPay* credit card numbers. But those files might be tagged only if they are being posted to a known "carders" web site by an insider who is under investigation.

In such a case, the rule might contain a user name selected from the bank's Active Directory server, and the HTTP-Post protocol might be added to establish criminal intent. If both of those conditions are found, an Existing Tag Label might be automatically applied, and a Web Post Reaction action rule might be automatically applied to block the attempt and store evidence.

Applying tags manually

Tag labels can be added by any user who has administrative privileges. If the **Allow Manual Tagging** checkbox is selected during that process, the tag is visible to trusted users, who can use it to classify specific documents by applying the appropriate tag. After they are created, manual tags are pushed to users at endpoints by McAfee DLP Agent.

The ability to classify documents with tags encourages users to take independent action to protect files within their areas of responsibility. For example, users at medical facilities might be trusted to apply HIPAA tags to patient records that must be kept confidential by law.

> If the **Allow Manual Tagging** checkbox is not selected, file tagging can still be done manually — but only by administrative users, who can tag or remove files individually or in groups.

Apply tags by scanning

Many files can be tagged in a single operation by using a Discover CIFS scan to crawl Windows shares that serve laptops, desktops and mount volumes. The unified policies defined in the Discover operations apply rules against the data at rest on those endpoints, and when a match is found, a tag is added as metadata to any file that meets the conditions of the rule.

When a McAfee DLP Manager Discover scan is run on a CIFS share, endpoints are automatically included in the network scan by virtue of the unified policy design.

> Tagging files in data at rest or in use is a two-phase process when McAfee DLP Discover is used to apply tags. Although the definition of the scan and the policies to be used to detect sensitive data are set on the network side, the scheduling of the scan, the credentials used, and other scan definitions must be set through ePolicy Orchestrator on the McAfee DLP Agent configuration page.

Application-based tagging

Tags that identify applications are applied when a file is saved using a specific application, and the tag displays whenever the user opens the file. When used with other properties of a unified rule, they can be used to control files created by that application.

Simple application-based tagging rules monitor or block all files created by the application, but addition of other rule parameters can qualify or extend those actions when used in a more specific context.

Application tagging might be only one property of a unified rule. When an application definition is applied, or applications sharing a particular strategy are used (for example, all applications are editors), an application tag might be applied to a group of documents.

When documents of a specific type violate any property of a rule, one or more action rules can be used to control them.

The **Document Scan Scope** endpoint parameter might be used to extend protection to specific portions of a Microsoft Office document. For example, when users at network endpoints start Microsoft Word, the system might look only in headers or footers for specific content (such as "top secret"). If the document contains sensitive content in these areas of a document, users might be prevented from reading, writing, or deleting it.

How application tagging works

Applications can be deployed with tagging and protection rules by creating application definitions, then applying them to unified rules. They can also be applied manually, or by using a Discover CIFS scan.

Importing an applications list and creating application definitions are efficient ways of handling application-related tagging and protection rules.

For example, system administrators might import a list of all relevant applications available within the enterprise, create application definitions based on their needs, and implement these definitions with relevant rules to maintain policies.

> When a user opens files with an application that is defined in a rule by an application definition, it produces one event on the McAfee DLP Monitor *per application session*, not per sensitive file opened. The event includes all files that matched the specified conditions in that application session.

This "aggregated event" behavior is new in McAfee DLP Endpoint. For example, if the **Store Evidence** action was selected, only files from that application session matching the conditions are stored.

The Enterprise Application list

The Enterprise Application List contains a set of commonly-used applications. You can add applications to the list, delete them, or add an application definition that bundles related applications.

When an application is added to the Enterprise Application List, application-based tags are applied to matching files when they are found.

> Applications must be defined in the Enterprise Applications List before they can be referenced in a rule. If the applications you want to use do not appear on the list, you must add them.

When an Endpoint application tag is used with unified rule parameters and associated action rules, files that are detected on endpoints, in network traffic, and repositories can be controlled with one rule. Application-based tags might be used alone or collected in application definitions.

For example, users who open Adobe Photoshop files on endpoints or on network shares might be allowed those users to view, but not modify those files — or they might not be visible at all. But before building that rule, the .psd executable file must be added to the Enterprise Action List so that it is available for use in a unified rule. After Photoshop files are defined as significant objects and supplemented with other parameters, they can be detected and tagged when the unified rule is run, and an appropriate action might be taken at that time.

Strategies for categorizing applictions

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

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

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

- **Trusted** — An application that needs unrestricted access to files for scanning purposes. Examples are McAfee® VirusScan® Enterprise, backup software, and desktop search software (Google, Copernic, and so forth).
- **Archiver** — An application that reprocesses files. Examples are compression software such as WinZip, and encryption applications such as McAfee® Endpoint Encryption for Files and Folders™ software or PGP.

Change the strategy as necessary to optimize performance. For example, the high level of observation that an editor application receives is not consistent with the constant indexing of a desktop search application. The performance penalty is high, and the risk of a data leak from such an application is low. Therefore, you should use the trusted strategy with these applications.

Add a file extension parameter

File extensions can be defined along with other endpoint parameters to control applications by type.

Before you begin

Check to see if the file extension parameter already exists on the **Endpoint** file extension popup. If not, you must first create an **Application Definition** to add it to the **Enterprise Application List**.

Suppose you want to implement role-based access on a Windows network engineering share. You might have developers who have full access, users who are allowed to manage the contents of the site, and users who have special skills that are needed on specific document types.

For example, a group of technical illustrators might need access to the Adobe Photoshop and Illustrator files on that share. You could create a rule that would allow only those users access to those files.

Task

1. On your DLP appliance, select **Policies**.
2. Click a policy and a rule, or create new ones.

   Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.
3. On the **Add Rule** or **Edit Rule** page, select **User Groups** from the **Source/Destination** menu, and click **?**.
4. From the directory server pop-up, click **Find** and click the technical illustrators' user group.
5. Click **Apply**.
6. From the **Endpoint** menu, select **File Extension**, click **?**, and select the applications from the popup.

   In this use case, the PSD file type is listed, but you would have to add the AI file type in advance.
7. Click **Apply**.
8. From the **Endpoint** menu, select **Network Path**, click **?**, and use **Find** to select the share that contains the files.
9. Click **Apply**.
10. Click **Save**.

Protect data using an application-based tag

You can use an application protection rule to keep users from modifying or distributing all Microsoft Office documents on a protected Windows share.

> **Before you begin**
>
> If you want to use an **Existing Tag Label**, you must first create one on the **Endpoint Configuration** page.

Suppose you have a collection of *Health Insurance Portability and Accountability Act Compliance* documents that must be not only be kept confidential, but must not be modified in any way.

Task

1 On your DLP appliance, select **Policies**.

2 Click a policy and a rule, or create new ones.

> Make sure the policy and rule are in an **Enabled** state.

3 On the **Add Rule** or **Edit Rule** page, select **Concept** from the **Content** menu and click **?**.

The concepts palette appears.

4 From the **Source/Destination** menu, select **User Group** and click "**?**".

5 Click **Find**, then click the user group that is to be restricted.

The user group is added to the value field.

6 From the **Endpoint** menu, select **Network Path** and click **?**.

7 Click **Find**, then click the share containing the HIPAA documents.

8 Click **Apply**.

The share is added to the value field.

9 Add an **Endpoint** parameter by clicking the green plus icon.

10 Select **Tags — Application Based** and click **?**.

The **Application Definition** pop-up appears.

> The **Application Definition** condition can be used for the *Application Protection Rule* or combined with application tagging.

11 Click **Apply**.

12 Click the green plus icon to add another element.

13 Select **Apply Tag Label** and select a tag from the pop-up.

14 Click **Apply**.

15 Click **Save**.

Application definitions

Application definitions consist of groups of related applications. They are bundled by type to facilitate their use in unified rules.

When an application definition is created, it is automatically added to a template that can be used in rules to find any files created by the applications in the defined group.

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

- Command line — Allows command line arguments, for example: `java-jar`, that can control previously uncontrollable applications.
- Executable file hash — The application display name, with an identifying 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 name — Identical to the executable file name, unless the file has been renamed.
- Product name — The generic name of the product, for example Microsoft Office 2003, if listed in the executable file's properties.
- Vendor name — The company name, if listed in the executable file's properties.
- Window title — A dynamic value that changes at runtime to include the active filename.
- Working directory — The directory where the executable is located. One use of this parameter is to control U3 applications.

With the exception of the SHA-2 applications, all parameters accept substring matches.

You can add applications to application definitions from the Enterprise Applications List, or create them directly.

> The same application can be included in several application definitions, and can therefore be assigned more than one of the four strategies. McAfee DLP Endpoint software resolves potential conflicts according to the following hierarchy of application types: archiver > trusted > explorer > editor. In other words, editors have the lowest ranking. For example, if an application is an editor in one definition and anything else in another, McAfee DLP Endpoint software does not treat the application as an editor.

Default application definitions

A set of default application definitions, which consist of related applications that share certain characteristics, is included with the products. They are used to detect the application types in use at endpoints.

Email client applications

The email client applications definition includes the following standard email applications:

- Becky! Internet Mail
- Eudora
- Foxmail
- Microsoft Office Outlook
- Mail Warrior
- Mulberry
- Sylpheed
- The Bat!
- Thunderbird

Encryption applications

The encryption applications definition includes the following standard encryption applications:

- Advanced File Security
- BCArchive
- BCArchive UnPack Application
- Dekart Private Disk Light
- EasyEncipher
- File Manager

- Cryptainer
- Cryptainer LE
- CryptoForge
- CryptoMailer
- MegaCipher
- Personal Data Vault
- Secure IT
- Universal Shield

IM applications

The instant messaging applications definition includes the following standard IM applications:

- AIM
- ICQ
- Skype
- Windows Live Messenger
- MSN Messenger
- Microsoft Office Communicator
- Yahoo! Messenger

Media burner applications

The media burner applications definition includes the following standard burning applications:

- Nero Burning
- Roxio Creator
- Express Burn
- Power2Go
- DVD Movie Factory
- NTI Media Maker
- Gear CD-RW
- Acoustica MP3 CD Burner
- Slysoft CloneCD
- Alcohol 120%

Microsoft Office applications

The Microsoft Office applications definition includes the following standard Microsoft Office applications:

- Microsoft Office 2003
- Microsoft Office 2007
- Microsoft Office 2010
- Microsoft Office Outlook

P2P applications

The peer-to-peer applications definition includes the following standard P2P applications:

- Bittorrent
- eDonkey
- eMule
- iMesh
- KaZaa
- Maketorrent
- QT2
- Shareaza
- WinMX

Scanners and indexers

The scanners and indexers applications definition includes the following standard search applications:

- Copernic Desktop Search
- Google Desktop
- Microsoft Windows
- SFXCAB
- X1 Technologies

Web browsers

The web browser applications definition includes the following standard browser applications:

- Amaya
- Firefox
- Google Chrome
- Opera
- Safari
- Windows Internet Explorer

Zip applications

The zip applications definition includes the following standard compression applications:

- WinRAR
- WinZip
- Zipper

Add an application definition

Application definitions control related applications and can be used in rules to control files created by those applications. For example, you might add a definition that includes all applications published by a single vendor, such as Adobe Systems.

You can add application definitions by first adding their executables to the **Enterprise Application List**, then collecting them in an application definition for use in unified rules.

> The Edit Definition Parameter value fields can contain only one value per field. AND and OR conditions are not supported.

Task

1. On your DLP appliance, select **System** | **Endpoint Configuration**.
2. In the navigation pane under **Application Definition**, select **Application Definition List**.

   The available application definitions appear in the right pane.
3. From the **Actions** menu, select **Add New**.

   The **Add Application Definition** window appears.
4. Enter a name and optional description for the new application definition.
5. Select a **Parameter Name** checkbox from the available list.

   This defines the characteristics of the applications being defined. For example, you might select **Vendor Name** for all applications published by Adobe Systems.

   The **Edit Definition Parameter** dialog box appears.
6. Click **Save**.

7 On the **Application Definitions** page, select the checkbox of the new definition.

8 From the **Actions** menu, select a **Process Strategy**.

This assigns the definition to a group of application types.

Add a web definition application

Web application definitions allow you to create URL-based templates that enable tagging of files, screenshots, or clipboards saved from one or more web sites.

Task

1 On your DLP appliance, select **System | Endpoint Configuration**.

2 In the navigation pane under **Application Definition**, select **Application Definition List**.

The available application definitions appear in the right pane.

3 From the **Actions** menu, select **Add New**.

The **Add Web Application Definition** window appears.

4 Enter a name and optional description for the new web application definition.

5 Select a **Parameter Name** checkbox from the available list.

The **Edit Definition Parameter** dialog box appears.

6 Select or enter values that define the parameter.
Click the green plus icon to add additional parameters.

7 Click **Apply**.

8 Click **Save**.

Location-based tagging

Location-based tags identify protected shares that contain confidential files. If downloaded to desktops, those files are automatically tagged.

For example, users who do not belong to an executive group might attempt to copy and distribute documents from a restricted executive share. In that case, location-based tags are automatically applied to record the attempt to access confidential information. Pre-programmed actions, such as block, notify, and store evidence, might also be activated when the location tag is applied.

Location-based tags are most often implemented to prevent unauthorized users from accessing shares that must remain confidential.

Protect data using a network path

The **Network Path** or **Tags - Location Path** parameters can be used to ensure that a location containing confidential files are tagged and protected. The **Network Path** parameter is used to prevent modification of all documents on a share, and location tags are used to identify specific collections of documents as sensitive.

> **Before you begin**
>
> If you want to tag sensitive files, create a tag label under **Endpoint Configuration** , or use an existing one. If you want to trigger an action when the rule hits, make sure that the action rule you intend to use has the right action settings. If not, add a **Data-in-Use** action rule, or create a new one.

If you have to keep a specific file system secure (for example, a share containing forensic records that must be preserved intact), you can type in a network path, or select one from a directory server, and use an action rule to prevent them from being modified.

If you want to keep sensitive documents from being downloaded or compromised in any way, you can give them a collective tag (for example, *Human Resources*) that can be used in combination with an action rule to keep them from being downloaded to desktops. Instead of tagging documents one by one, you might use that tag to scan for similarly-tagged documents in unknown locations.

Task

1. On your DLP appliance, select **Policies**.
2. Add a new policy and rule, or open existing ones.

   > Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.

   The **Edit Rule** page appears.
3. Open the **Endpoint** category and select **Network Path** or **Tag - Location Path**.

   The **Edit Rule** page appears.
4. Click **?**, click **Find** on the AD pop-up, and select a network location.
5. Click **Apply**.
6. Click the **Action** tab, click **Add Action**, and select an action from the **Data-in-Use** actions.

   In this case, you might want to block the documents, whether they are found online or offline (in computers that are on-site, or disconnected from the network), and notify a manager.
7. Click **Apply**.
8. Click **Save**.

Protect data using a location-based tag

You can use location-based tags to ensure the protection of privileged information from copying or distribution.

> If you use a location tag to protect a location, you must define two **Endpoint** parameters: the tag and the location path.

For example, a manufacturing organization might have process engineers working on design documents on laptops and desktops that are accessed through a share on a Microsoft Windows server. If users who attempt to access and email those documents are not authorized members of that group, their attempts would be tagged and reported to a manager responsible for that department.

Task

1. On your DLP appliance, select **Policies**.
2. Click a policy and a rule, or create new ones.

   > Make sure the policy is active and the **Inherit Policy State** state of the rule is set to **Enabled**.
3. On the **Add Rule** or **Edit Rule** page, select **User Groups** from the **Source/Destination** menu, select **sender is none of** and click **?**.
4. From the directory server popup, click **Find** and click the process engineers' user group.

5 Click **Apply**.

6 From the **Endpoint** menu, select **Apply Tag Label**, click **?**, and select the relevant tag from the popup.

7 Click **Apply**.

8 From the **Endpoint** menu, select **Tags - Location Path**, click **?**, and use **Find** to select the protected share.

9 Click **Apply**.

10 Click **Save**.

Controlling devices

McAfee DLP Endpoint can control any number of devices attached to enterprise managed computers by using device rules to detect, then react to significant events on devices used at network endpoints.

Devices attached to enterprise managed computers — such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or Plug and Play devices — can be monitored or blocked using device rules, allowing you to control their use in the distribution of sensitive information. For example, a global company might use networked McAfee DLP Endpoint to protect sensitive data on USB drives issued by branch offices in other countries - even if the user of that device is on the road.

A device rule consists of a list of the device definitions and actions that might be pre-programmed to affect specific users. When sensitive content is detected in transit to or from endpoint devices, the rule can be pre-programmed to take an appropriate action.

Role-based device rules can be created for the enterprise workforce. For example, while the majority of workers might not be allowed to run executables from flash drives, IT and sales force might need that privilege to bypass operating systems so they can reformat hard drives.

By using role-based access control with device rules, a variety of users can be monitored or excluded from supervision, securing sensitive data without creating roadblocks to their productivity.

Device classes

Device classes are used to control groups of related devices. Each class of devices is identified by a name, an optional description, and one or more Globally Unique Identifiers (GUIDs).

If you are using McAfee DLP Endpoint with McAfee DLP Manager, you can find built-in *device classes* listed on the **Device Management** page. The devices are categorized by *status*:

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

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

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

Classifying devices

Every endpoint device has a unique set of parameters, and device definitions are used to identify each one.

Device parameters, such as Product ID/Vendor ID (PID/VID), or USB class code, are the components of the device definitions. A different set of properties for each device enables blocking or monitoring of specific devices by the system.

> Built-in definitions for McAfee Endpoint Encryption for Files and Folders and McAfee Endpoint Encryption for Removable Media facilitate the use of those products with McAfee DLP Endpoint

Defined devices are classified into two groups:

- **Plug and Play devices** — Devices that can be added to a managed computer without any configuration or manual installation of dlls and drivers. For example, the system can prevent loading of Plug and Play devices like Bluetooth, Wi-Fi, and PCMCIA devices. Most Microsoft Windows devices are PnP devices.
- **Removable Storage devices** — Removable external storage devices containing file systems that appear on the managed computer as drives.

> While the Plug and Play device definitions and rules include general device properties, the removable storage device definitions and rules are more flexible and include additional properties related to the removable storage devices. McAfee recommends using the removable storage device definitions and rules to control devices that can be classified as either PnP or removable storage, such as USB mass storage devices.

Whitelisted Plug and Play devices

Certain Plug and Play devices are whitelisted because they do not handle device management well, and might cause the system to stop responding or cause other serious problems. McAfee recommends adding such devices to the whitelisted device list to avoid compatibility problems.

Whitelisted Plug and Play device definitions are added automatically to the **Excluded** list in every Plug and Play device rule. They are never managed, even if their parent device classes are.

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

Add a new device class

Device classes categorize device types used by the system. Each class of devices is identified by a name, optional description, and one or more Globally Unique Identifiers (GUIDs).

Task

1. On your DLP appliance, select **System** | **Endpoint Configuration**.
2. In the navigation pane under **Device Management**, select **Device Classes**.

   The available devices appear in the right pane.
3. From an **Actions** menu under **Managed** or **Unmanaged** device classes, select **Add New**.

   The appropriate device class window appears.

4 Enter a name, an optional description, and the device's Globally Unique Identifier (GUID).

A GUID in the correct format is required.

5 Click **Save**.

Change the status of a device class

Devices might be managed, unmanaged, or unmanageable. You can change the status of devices that can be managed or unmanaged.

Task

1 On your DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Classes**.

The available device classes appear in the right pane.

3 Select a device class checkbox.

4 From the **Actions** menu, select **Mark Status as Managed** or **Mark Status as Unmanaged**.

If unknown device classes (classes with no name) appear on the dashboard, add them to one of the lists.

Controlling devices with device definitions

Device definitions are collections of parameters that identify managed devices. They are used in device rules to detect significant events on those devices.

When you create a device definition with multiple parameters, each **Parameter Name** is added to the definition as a logical OR, and multiple **Parameter Names** are added as logical ANDs.

For example, the following parameter selection creates the device definition shown below:

Table 9-2 Device definition example

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

- Bus Type is one of: Firewire (IEEE 1394) *OR* USB
- *AND* Device Class is one of Memory Devices *OR* Windows Portable Devices.

Add a device definition group

Device definition groups can be used to control related devices.

Task

1 On your DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**.

The available devices appear in the right pane.

3 Locate the **Plug and Play Device Definition Group** or **Removable Storage Device Definition Group** section.

The **Add Plug and Play Device Definition Group** or **Add Removable Storage Device Definition Group** window appears.

4 From the **Actions** menu, select **Add New**.

5 Enter a name and optional description for the new device definition group.

6 From the **Device Definitions** menu, select one or more device definitions from the available list.

7 Click **Save**.

Add a removable storage device definition

Removable storage devices can be identified by the parameters that define them. For example, PCI vendor IDs and USB serial numbers are unique parameters that identify only a single device.

Task

1 On your DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**, and locate the **Removable Storage Device Definition** section.

The available device definitions appear in the right pane.

3 From the **Actions menu**, select **Add New**.

The **Add Removable Storage Device Definition** window appears.

4 Enter a name and optional description.

5 Select a **Parameter Name** checkbox from the available list.

The **Edit Definition Parameter** dialog box appears.

6 Select or enter values that define the parameter.
Click the green plus icon to add additional parameters.

7 Click **Save**.

Add a removable storage file access rule

Removable storage device file access rules are used to control data on Plug and Play devices that contain file systems. Other removable devices can be identified by serial numbers and other identifiers, but devices that contain data are more vulnerable and require special handling.

Task

1 On your DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**, and locate the **Removable Storage File Access Device Rule** section.

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

3 From the **Actions menu**, select **Add New**.

The **Add Removable Storage File Access Device Rule** window appears.

4 Enter a name and optional description, and select **Active** from the **State** menu.

5 Select the **Include** or **Exclude** checkboxes from the available list to define the device rule.

6 Define the user names, groups, and organizations to whom the device rule will be applied.

> Select the **user is none of** condition to exclude any of those parameters.

Click the green plus icon to add additional parameters.

7 Click **Save**.

Add a Plug and Play device definition

Plug and Play device definitions allow you to manage and control most available PnP devices.

Task

1 On your DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Definitions**.

The available device definitions appear in the right pane.

3 From the **Actions** menu, select **Add New.**

The **Add Plug and Play Device Definition** window appears.

4 Enter a name and optional description for the new device definition.

5 Select a **Parameter Name** checkbox from the available list.

The **Edit Definition Parameter** dialog box appears.

6 Select or enter values that define the parameter.
Click the green plus icon to add additional parameters.

7 Click **Save**.

Add a whitelisted application definition

File access rules prevent users from opening potentially harmful executables from removable storage media. But some applications, such as encryption software, must be whitelisted to exempt them from the blocking rule.

Task

1 On your DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Whitelisted Applications**.

The available whitelisted applications appear in the hand pane.

3 From the **Actions** menu, select **Add New.**

The **Add Whitelisted Applications** window appears.

4 Enter the name and file extension of the application to be whitelisted in the **Enter a valid Application Name** box.

5 Click **Add** to add the application to the list.

6 Click **Save**.

Add a whitelisted Plug and Play definition

Some Plug and Play devices might cause the system to stop responding or cause other serious problems if they are managed by device control software. McAfee recommends adding such devices to a whitelist to avoid compatibility problems.

Task

1. On your DLP appliance, select **System** | **Endpoint Configuration**.
2. In the navigation pane under **Device Management**, select **Device Definitions** and scroll down to the **Whitelisted Plug and Play Device Definition** section.

   The available definitions appear in the right pane.
3. From the **Actions** menu, select **Add New**.

   The **Add Whitelisted Plug and Play Device Definition** window appears.
4. Enter a name and optional description for the definition.
5. Select a **Parameter Name** checkbox from the available list.

   The **Edit Definition Parameter** dialog box appears.
6. Select or enter values that define the parameter.

   Click the green plus icon to add additional parameters.
7. Click **Save**.

Using device rules

Device rules are made up of *device definitions* and user assignment rules that can be used to control usage of groups of devices. They might be used to trigger actions or use whitelisted application definitions when the devices are used.

Devices attached to enterprise managed computers — such as smartphones, removable storage devices, Bluetooth devices, MP3 players, or Plug and Play devices — can be monitored or blocked using device rules, allowing you to monitor and control their use in the distribution of sensitive information.

Device rules must be activated before they can be used.

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

Plug and Play and **Removable Storage Device** rules can be programmed to execute actions when the rule is triggered by content being sent to or from the devices, and **Removable Storage File Access** rules might be used to control executables and to include or exclude whitelisted applications.

Types of device rule

Device rules are used to control sensitive data that can be compromised by use of devices at network endpoints.

There are three types of device rules: **Plug and Play**, **removable storage**, and **removable storage file access**.

Plug and play and **removable storage device rules** can be pre-programmed to monitor or block usage of endpoint devices by users, take action when violations occur, and alert other users to those events. **Removable storage device rules** can also prevent data on devices from being appended, modified, or copied. For example, users might be allowed to listen to MP3 players, but their potential use as storage devices can be disallowed.

Removable storage file access rules block executables on plug-in devices from running, and they can also be used to include or exclude whitelisted applications, depending on who is using them. For example, some applications, such as encryption applications on encrypted devices, must be allowed to run, and their executables can be exempted from the blocking rule.

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

> File access rules also block executable files from being copied to removable storage devices because the file filter driver cannot differentiate between opening and creating an executable.

Add a removable storage device rule

Removable storage device rules can be used to block, monitor, and assign read-only and user permissions to external storage devices. Although USB storage devices are Plug and Play as well as removable storage devices, these rules should be used to block their use.

> Using a Plug and Play device rule to block a USB storage device can result in blocking the entire USB Hub/Controller. McAfee recommends using removable storage device rules because they allow the device to initialize and register with Windows, and the USB device can also be set to **read only**.

Task

1. On your DLP appliance, select **System** | **Endpoint Configuration**.
2. In the navigation pane under **Device Management**, select **Device Rules**.

   The available rules appear in the right pane.
3. In the **Removable Storage Device Rule** section, select **Add New** from the **Actions** menu.

   The **Add Removable Storage Device Rule** window appears.
4. Enter a name and optional description.
5. From the **State** menu, select **Active** to activate the rule.
6. If **Device Definitions** are to be added to the rule, select **Include** or **Exclude** checkboxes to indicate if the devices are to be blocked or encrypted.
7. From the **Actions** menu, select the checkboxes of actions that are to be executed when the rule hits. Each action can be set to execute if the user is on or off the premises, or both.

   Action

   Select the **Block** checkbox if the device is to be blocked when the user is on- or offsite, or both.

Action

Select the **Monitor** checkbox if the device is to be monitored when the user is on- or offsite, or both. If either is selected, select a checkbox that indicates the **Severity** of the violation.

Select the **Notify User** checkbox if an alert is to be sent when users who are on- or offsite, or both, trigger the **Block** or **Monitor** actions.

Select the **Read only** checkbox if write access to the device is to be blocked when the user is on- or offsite, or both. This prevents copying to or from the device.

8. Set a **User Assignment** condition if an alert is to be sent to users when the device is used on- or offsite. Users can be identified positively or negatively by name or affiliation, and they can be retrieved from an LDAP server.

   Click the green plus icon to add multiple user assignments.

9. Click **Save**.

Add a removable storage file access rule

File access rules control the usage of removable storage devices on the network. They can be used to block or encrypt removable storage devices, prevent applications from being started, or restrict the actions of users.

Task

1. On your DLP appliance, select **System** | **Endpoint Configuration**.
2. In the navigation pane under **Device Management**, select **Device Rules** and scroll down to the **Removable Storage File Access Rule** section.

   The available device management rules appear in the right pane.
3. From the **Actions** menu, select **Add New**.

   The **Add Removable Storage File Access Rule** window appears.
4. Enter a name and optional description.
5. From the **State** menu, select **Active** to activate the rule.
6. If **Device Definitions** are to be added to the rule, select **Include** or **Exclude** checkboxes to indicate if the devices are to be blocked or encrypted.
7. If there are applications listed under the **Whitelisted Applications** section, select checkboxes to indicate which ones are to be included or excluded from the rule.
8. Set a **User Assignment** condition if an alert is to be sent to users when the device is used on- or offsite. Users can be identified positively or negatively by name or affiliation, and they can be retrieved from an LDAP server.

   Click the green plus icon to add multiple user assignments.
9. Click **Save**.

Add a Plug and Play device rule

Plug and Play device rules can be used to block, monitor, and assign read-only and user permissions to Plug and Play devices. Although USB devices are Plug and Play as well as removable storage devices, the latter should be used to block their use.

Using a Plug and Play rule to block a USB storage device can result in blocking the entire USB Hub/ Controller. Plug and Play rules are not very flexible; if we block a device, it is completely unavailable for use. It is an "all or nothing" rule, because if you allow a device it will be completely usable. You cannot block a particular feature of the device or keep the device from performing a particular action.

> McAfee recommends using removable storage device rules because they allow the device to initialize and register with Windows, and the USB device can be set to **read only**.

Task

1 On your DLP appliance, select **System** | **Endpoint Configuration**.

2 In the navigation pane under **Device Management**, select **Device Rules**.

The available device management rules appear in the right pane.

3 In the **Plug and Play Device Rule** section, select **Add New** from the Actions menu.

The **Add Plug and Play Device Rule** window appears.

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

4 Enter a name and optional description.

5 From the **State** menu, select **Active** to activate the rule.

6 From the **Device Definitions** menu, select device and device group definitions to be added to or excluded from the rule. The **Exclude** option is used to whitelist devices that should not be controlled.

7 From the **Actions** menu, select the checkboxes of actions that are to be executed when the rule hits. Each action can be set to execute if the user is on or off the premises, or both.

Action

Select the **Block** checkbox if the device is to be blocked when the user is on- or offsite, or both.

Select the **Monitor** checkbox if the device is to be monitored when the user is on- or offsite, or both. If either is selected, select a checkbox that indicates the **Severity** of the violation.

Select the **Notify User** checkbox if an alert is to be sent when users who are on- or offsite, or both, trigger the **Block** or **Monitor** actions.

8 Set a **User Assignment** condition if an alert is to be sent to users when the device is used on- or offsite. Users can be identified positively or negatively by name or affiliation, and they can be retrieved from an LDAP server.

Click the green plus icon to add multiple user assignments.

9 Click **Save**.

Device parameters

Device parameters are used to build device definitions, which are incorporated into device rules that secure sensitive data at endpoints.

The following table provides definitions for all parameters used in device definitions.

Device parameters cannot be imported in the McAfee DLP Manager implementation of McAfee DLP Endpoint.

Table 9-3 Device definitions for Plug and Play and removable storage devices

Parameter name	Found in...	Description
Bus Type	Both	Selects the device BUS type from the available list (IDE, PCI, and so forth.)
CD/DVD Drives	RS only	A generic category for any CD or DVD drive.
Content encrypted by McAfee Endpoint Encryption for Files and Folders	RS only	Select to indicate a device protected with McAfee Endpoint Encryption for Files and Folders.
Device Class	PnP only	Selects the device class from the available managed list.
Device Compatible IDs	Both	A list of physical device descriptions. Effective especially with device types other than USB and PCI, which are more easily identified using PCI VendorID/DeviceID or USB PID/VID.
Device Instance ID (Microsoft Windows XP; Microsoft Windows 2000) Device Instance Path (Microsoft Windows Vista; Microsoft Windows 7)	Both	A Windows-generated string that uniquely identifies the device in the system. For example, `USB\VID_0930&PID_6533\5&26450FC&0&6`.
Device Name	Both	The name attached to a hardware device, representing its physical address.
File System Type	RS only	The type of file system, for example NTSF, FAT32, and so forth.
File System Access	RS only	The access to the file system: read only or read-write.
File System Volume Label	RS only	The user-defined volume label, viewable in Windows Explorer. Partial matching is allowed.
File System Volume Serial Number	RS only	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	Both	The PCI VendorID and DeviceID are embedded in the PCI device. These parameters can be obtained from the Hardware ID string of physical devices, for example, `PCI \VEN_8086&DEV_2580&SUBSYS_00000000&REV_04`.
USB Class Code	PnP only	Identifies a physical USB device by its general function. Select the class code from the available list.

Table 9-3 Device definitions for Plug and Play and removable storage devices *(continued)*

Parameter name	Found in...	Description
USB Device Serial Number	Both	A unique alphanumeric string assigned by the USB device manufacturer, typically for removable storage devices. The serial number is the last part of the instance ID; for example, `USB\VID_3538&PID_0042\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.
USB Vendor ID / Product ID	Both	The USB VendorID and ProductID are embedded in the USB device. These parameters can be obtained from the Hardware ID string of physical devices, for example: `USB\Vid_3538&Pid_0042`.

10 McAfee DLP Discover

McAfee DLP Discover scans file systems, databases, and endpoints to identify and protect sensitive data at rest in file systems or databases. When incidents or events are reported, they can be automatically protected by moving, copying, encrypting, or deleting data that might compromise the security of the repository.

Contents

Configuring McAfee DLP Discover

Before McAfee DLP Discover can be configured, it must be registered to McAfee DLP Manager, and permissions must be set for users who will be setting up scans.

Registration to McAfee DLP Manager wipes the configuration on the Discover appliance. Only captured data and incidents are retained.

> If you are going to prepare a standalone system for managed mode, you must do a backup to preserve the following user-defined elements.

- Scan tasks
- Schedules
- Credentials
- Scan statistics
- Export locations
- Users and user preferences
- Custom rules and policies

Register McAfee DLP Discover to McAfee DLP Manager

You must add McAfee DLP Discover to McAfee DLP Manager so that it can work in synchronization with other McAfee DLP devices. If it has functioned as a standalone machine, its configuration will be wiped.

Back up and recreate scan tasks and other user-defined elements manually.

Task

1 On your DLP appliance, select **System** | **Devices**.

2 From the **Actions** menu, select **New Device.**

3 Enter the IP address or host name and password.

4 Click **Add**.

5 Wait for the **Status** icon in the device list to turn green. If registration seems to be taking a long time, try refreshing the page.

   If the **Status** icon changes to a **Critical** or **Unknown** state, you might have to overwrite an old configuration or re-synchronize the systems. Deregister the machine, then reregister it.

Republish McAfee DLP policies

Republish policies, rules, concepts and content capture filters after registering McAfee DLP Discover to McAfee DLP Manager.

Task

1 On your DLP appliance, select **Policies.**

2 Click a policy that will be used by McAfee DLP Discover.

   The process is the same for concepts and content capture filters.

3 Click a rule in the policy.

4 Select the McAfee DLP Discover device in the **Devices** box.

5 Repeat for each rule that is to be used.

6 Click **Save**.

McAfee DLP Discover scan permissions

McAfee DLP Discover scan permissions must be set before users can scan repositories.

Table 10-1 McAfee DLP scan permissions

Scan Permission	Definition
Manage Schedules	Create, edit, and delete schedules
Manage Credentials	Create, view, edit, and delete credentials
Manage Scans	Create, view, edit, activate, deactivate, and delete scans; register documents; view and export scan statistics, history, and registered files; add and view excluded text
Control Scans	Create new actions, view, start, stop, re-scan, and clone tasks; view and export scan statistics, history, and registered files; add and view excluded text

Set scan permissions

You must assign scan permissions privileges to users who will be using McAfee DLP Discover to scan repositories.

> **Before you begin**
>
> You must have administrator permission to perform this task.

Task

1. On your DLP appliance, select **System** | **User Administration** | **Groups**.
2. Click the **Details** icon of the user's group.
3. Click **Task Permissions**.
4. Open **Discover Scan Permissions**.
5. Select one or more permissions.
6. Click **Apply**.

   Users will need **View Dashboards** permission to see the **Incidents** dashboard.

McAfee DLP Discover registration permissions

McAfee DLP Discover registration permissions must be set before users can register data.

Table 10-2 Registration permissions

Registration Permission	Definition
Web Upload	Upload documents or structured data to be registered; no deletion or de-registration rights; view user's own registered documents
Manage Uploaded Documents	Upload documents or structured data to be registered; view and manage documents uploaded by all users; delete and deregister uploaded files; update and delete excluded text
Discover Registration	Register documents or structured data

Set registration permissions

Set registration permissions to assign privileges to users who will be using McAfee DLP Discover to register data.

> **Before you begin**
>
> Administrator permissions are needed for this task.

Task

1. On your DLP appliance, select **System** | **User Administration** **Groups**.
2. Click the **Details** icon of the user's group.
3. Click **Task Permissions**.
4. Open **Discover Registration Permissions**.
5. Select one or more permissions.
6. Click **Apply**.

   Users will also need **Incident Permissions** permission.

Preparing the scan

Before creating a scan, create a framework for your protection strategy by considering the following parameters:

- Scan mode (Inventory, Registration, Discover or Classification)
- Credentials to access the repository
- Database type and version (for database scans)
- IP address, subnet, or range of the targeted repositories, including required ports
- Login database or SID and SSL certificate (for database scans)
- File systems to be scanned
- Schedule for the scan
- Configuration of firewalls
- Bandwidth to be used
- Projected scan load

McAfee DLP Discover scan types support inventory, registration, discovery, and classification of sensitive data. These four scan types are used to crawl network file systems or database repositories.

Table 10-3 Types of scan

Scan type	Description
Classification scan	Use a classification scan to get a bird's eye understanding of the type of data that exists in the repository you are targeting. This scan type sorts crawled data into different content types and analyzes attributes like file size, location, type, and concepts that might be triggered during discovery. The results of this scan can help you to learn about potential rule violations before they are reported, enabling you to create more focused Discover or Registration optimized scans.
Inventory scan	Use this scan to crawl all directories and files residing on a targeted repository and generate an index, or manifest. For databases, an inventory scan produces a schema - the database structure and number of records. It can also help you to decide what needs protection before going ahead with a registration or discovery scan. The inventory scan also classifies the crawled data based on file extensions.
Registration scan	Use this scan to register sensitive data by generating digital fingerprints, or signatures, that identify documents to be protected. You can register partial documents by defining excluded text within the documents. When scanning large databases, McAfee recommends registering only the sensitive data, such as bank account numbers or Social Security numbers. Registering an entire database is neither practical nor useful.
Discover scan	Use this scan to find data that has been registered, or is residing on a file share in violation of a policy. In this mode, McAfee DLP Discover can monitor, encrypt, copy, delete, or move files to a secure location (quarantine). All actions produce incidents that are reported to dashboards. After an incident is reported to the dashboard, it can be sorted, filtered, exported, saved, and remediated to prevent future violations.

File system repositories supported

When you access a repository, you are connecting to a central network location where data is stored, organized, and maintained. McAfee DLP Discover supports most common file system repository types.

The repository type is determined by the protocol used to access data on the device.

Table 10-4 File system repositories supported

Repository type	Description
CIFS (Common Internet File System)	Formerly Microsoft SMB (Server Message Block) file system. Windows XP supported.
NFS (Network File System)	Sun Microsystems file system
FTP (File Transport Protocol)	Open source file transfer system
HTTP/HTTPS (Hypertext Transport Protocol/over Secure Sockets Layer)	Web server systems
Documentum 5.3, 6.0	EMC documentation server, access through the default docbase port. Supports Lotus Notes, SharePoint, Verity, Oracle, SAP, Google Search.
SharePoint 2007	Microsoft documentation server; SharePoint 2007 supported.

Database repositories supported

When you access a repository, you are connecting to a central network location where data is stored, organized and maintained. McAfee DLP Discover supports several common database repository types.

McAfee DLP Discover supports JDBC (Java Database Connectivity).

Table 10-5 Database repositories supported

Repository type	Description
DB2	Versions 5x iSeries, 6.1 iSeries, 7.x-9.x
MS SQL Server	Versions 2000, 2005, 2008, 7.0, MSDE 2000
My SQL (Enterprise)	Versions 5.0.x, 5.1
Oracle	Versions 8i, 9i, 10g, 11g

Scanning network attached storage

McAfee DLP Discover scans storage devices by using the protocols that are used to access them.

Table 10-6 Common network storage types

Storage type	Access method
Network Attached Storage	Network Attached Storage presents a conventional file system to the network, and can be accessed directly by McAfee DLP systems.
Storage Area Networks	Store data in an unusable format using physical blocks of disk space, but McAfee DLP Discover can connect through any server that owns a pool of data on that device.

Firewall options for scanning

Before scanning a repository, its firewall must be configured to allow scans.

Source ports are randomly chosen unless explicitly noted. Network and host-based firewalls typically permit connections only on certain ports and might have to be configured to permit connections on others.

Table 10-7 Firewall options

Repository type	Direction	Ports
CIFS	Discover to Server	TCP 139 and 445 on server
FTP Active Mode (tried by Discover if Passive Mode fails)	Discover to Server	TCP destination port 21 on server (control)
FTP Active Mode	Server to Discover	TCP source port 20 (from server), and destination port (on Discover) chosen by Discover (data)
FTP Passive Mode (tried first by Discover)	Discover to Server	TCP destination port 21 on server (control), and another port on server (data) chosen by the server
HTTP	Discover to Server	TCP destination port 80 on server, unless port is manually configured in the URL itself
HTTPS	Discover to Server	TCP destination port 443 on server, unless port is manually configured in the URL itself
NFS	Discover to Server	TCP and UDP destination ports 111; 2049 on server
Database	Discover to Server	Standard ports, by database: • DB2 - 50000 • Microsoft SQL - 1433 • MySQL - 3306 • Oracle - 1521 If the database server is running on a non-standard port, that port number must be punctured in a firewall.
EMC Documentum	Discover to Server	TCP destination port 1489 on server
Microsoft SharePoint	Discover to Server	TCP destination ports 80 (HTTP) or 443 (HTTPS) on server, unless port is manually configured in the URL itself

Defining scans

Scans can be run to take classify data, inventory and register documents, or discover incidents and events. Each parameter of a scan must be defined before it can be put into action.

Before a scan is run, you must configure the parameters that filter the content, define the policies that will be used to find, and set up registration if the files found are to be fingerprinted.

Classification scans are recommended before running Discover or Registration scans, because they provide information that allows you to focus on the most significant data types.

The scan definition must include the credentials to be used to access the repository, as well as a schedule that determines when the scan will be run.

Set up scans

Depending on your objective, you can set up scans that inventory, register, discover or classify data in file system or database repositories. Results from the classification scan type can be used to create optimized scans that produce better results faster.

Before you begin

Analyze your objective so that you will know what kind of scan to run. You will also need credentials for the file system or database repository you are crawling.

> Integrated Windows authentication is not supported for Microsoft SQL Server. If you are scanning a database server of this type, you must create an MS SQL Server user with the correct credentials.

> It is a good idea to include the scan mode in the name of a scan. For example, a name like *Finance_registration* will help you to remember what the scan does when it is used in a rule.

Task

1. On your DLP appliance, select **Classify** | **Scan Operations**.

2. In the **Actions** tab, select **New**.

3. Enter a scan task name and optional description.

4. From the **Repository Type** menu, select a file system or database type.

   The user interface offers different options for each type.

5. From the **Credential** menu, select from the list of authentication parameters that allow access to the repository, or click **New** to add a new one to the list.

6. From the **Schedule** menu, select from the list default schedules, or click **New** to create a new one.

7. From the **Mode** menu, select one of the four scan types.

8. Under **Devices**, select the appliance from which the scan will be run. Select **None** if you want to save a scan without deploying it.

9. In the **Node Definition** tab, define the server that is the target of your scan. Depending on the file system or database selected, you might enter a URL to define an FTP or web server instead of IP addresses or host names.

   If you are using IP addresses or host names to define the repository, you have several choices.

   - If you are setting up a database crawl, you must provide a port number, database login, and SSL certificate options along with an IP address or host name.

   - If you are setting up a file system crawl, you must provide one or more IP addresses, a subnet, or a range.

10. If you want to test the connection, select your device before clicking **Test**.

11. Click **Include** to add the defined node to the **Included** list.

    If you want to exclude one or more addresses from an IP adress range or subnet, click **Exclude**.

12. Click the **Filters** tab to define the exact location on the server that you want to scan.

    Depending on the repository type, you can filter by shares, folders, file properties on file system servers, or catalogs, schemas, tables, columns, and records and rows on database servers.

13 Click **Browse** to navigate to the location of the scan.

Alternatively, open the Filter category and set the options manually. If you choose this method, you can select **Preserve** to keep the original access times on the files. Otherwise, the operating system will change timestamps as the files are touched.

14 Click the **Advanced Options** tab to set the amount of bandwidth dedicated to the scan, and to set up email notifications to be sent when the scan starts or ends.

- If you choose to throttle the bandwidth available to the scan, enter a value in Kbps or Mbps.
- If you choose to send notifications of the start or end of a scanning process, you can use dynamic variables to provide scan details via email messages, but you cannot customize subject fields. There might be a lag of a few minutes between conclusion of the task and the posting of email notification, and file processing might continue after notification.

15 The next steps depend on what type of scan you are planning.

- If you are planning an Inventory or Classification scan, configuration is complete.
- If you are planning a Registration or Data Match scan of a file system or database, click the **Registration** tab and select the **Signature Type** and **Target Devices**.
- If you are planning a Discover scan, click the **Policies** tab and select policies whose rules will be applied against data at rest in the defined repositories.

16 Click **Save**.

Filter scans by browsing

Scans must be filtered to identify the locations to be scanned. You can set the shares, folders and file properties manually, or you can click **Browse** to set them by pointing and clicking.

Before you begin

Before filtering, you must identify the file system or database that contains the target of the scan. Identify the repository using the **Node Definition** tab.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 Enter a task name and select a **Repository Type**.

3 From the **Credential** menu, select **New**, enter the authentication parameters needed to access the repository, and save the credential.

4 From the **Schedule** menu, select **New**, set the scheduling parameters, and save the schedule.

5 Select the scan **Mode**.

6 Define the node to be scanned.

7 Click the **Filters** tab.

Set the scan location manually if a URL is needed to access the repository.

8 Click **Browse**.

9 Select the repository from the directory tree in the repository.

Define scan locations manually

Define scan locations manually if parameters are easier to set one by one.

Before you begin

Parameters in the **Advanced Options** and **Registration** tabs can be entered before or after the location is identified.

You can also browse to the location from the **Filters** tab.

Task

1. On your DLP appliance, select **Classify** | **Scan Operations**.
2. In the **Actions** tab, select **New**.
3. Enter a scan task name and select a **Repository Type**.
4. If you have already created a credential, you can select it from the menu.

   If not, you can create one while you are configuring the scan. Click **New**, enter the authentication parameters needed to access the repository, and **Save**.
5. If you have already created a schedule, or you want to use one of the default schedules, you can select it from the menu.

   Click **New**, set the scheduling parameters, and **Save**.
6. Select the scan **Mode**.

   You can inventory the scan target, register the data at that location, apply policies and rules, or classify the data.
7. Define the node to be scanned using an IP address, host name, or URL.
8. Click the **Filters** tab.
9. Expand the **Filter** menu.
10. Make selections from the menu categories to define the location of the scan.
11. Click **Save**.

Define IP addresses or host names for a scan

Define scan targets by entering IP addresses or host names of the file system or database repositories to be crawled.

Before you begin

Define the scan operation name, credential, schedule, mode, and devices.

IP addresses of host names are required for most file system and database repositories to be scanned. If you are scanning a file system, you might define ranges of IP addresses or subnets to be scanned in one operation.

HTTP/HTTPS, FTP, and SharePoint servers require a URL instead.

Task

1. On your DLP appliance, select **Classify** | **Scan Operations**.
2. From the **Repository Type** menu, select a file or database server.

3 Enter IP addresses, host names, or URLs, as appropriate, to define the node to be scanned.

If you are a **CIFS**, **NFS**, or **Documentum** file server, you can exclude IP addresses or ranges from the scan.

4 Click **Include** or **Exclude** to define the scan target.

5 Click **Test** to verify that the scan target is reachable.

6 Complete scan configuration by entering parameters in the **Filters**, **Advanced Options**, **Registration**, or **Policies** tabs as needed.

7 Click **Save**.

Define an IP address for a subnet scan

Define a subnet scan by entering the base IP address as the first host IP of the sub-network. For example, you might use 172.25.6.1 as the base IP address, and 255.255.255.0 as the network mask.

You must use a valid address in the subnet range that can be considered the "starting" address to be scanned in the subnet. For example, if 172.25.6.14 is the IP address defined, 172.25.6.14 through 172.25.6.254 will be scanned.

> You cannot use the broadcast IP address as the base IP.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 From the **Repository Type** menu, select a file or database server.

3 Enter the base IP address followed by the network mask (for example, 172.25.6.1/255.255.255.0).

4 Click **Include** to define the scan target.

5 Click **Test** to verify that the scan target is reachable.

6 Complete scan configuration by entering parameters in the **Filters**, **Advanced Options**, **Registration**, or **Policies** tabs as needed.

7 Click **Save**.

Define URLs for a scan

URLs are required to define the target of a scan if the repository type is HTTP, HTTPS, FTP, or Microsoft SharePoint.

> **HTTP incremental crawls** conserve bandwidth and other network resources. When HTTP servers are crawled the first time, every file is crawled and downloaded. In subsequent runs, only the files modified since the last run are downloaded. By dividing HTTP crawls into inventory and fetch phases that are run in parallel phases, only the fresh files, or those that have been modified, are downloaded.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 From the **Repository Type** menu, select **HTTP**, **HTTPS**, **FTP** or **Microsoft SharePoint**.

Other repository types do not support URLs.

3 Select **Test** to verify that the URL is working.

4 Click **Include**.

5 Enter parameters in the **Filters**, **Advanced Options**, and **Registration** tabs as needed.

6 Click **Save**.

Define file properties for a scan

Define file properties to be scanned if the targeted repositories are CIFS, NFS and Documentum repository types. HTTP, HTTPS, FTP and Microsoft SharePoint repositories allow use of file patterns and sizes as well as shares, folders and properties.

Parameters in the **Advanced Options**, **Registration** and **Policies** tabs can be completed before or after the location is identified.

File patterns, sizes, paths, and owners, as well as time of creation, modification and access can be defined.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 After completing the scan and node definitions, click the **Filters** tab.

3 Click **Filter** | **File Properties**.

If you are defining more than one file pattern, click the green plus sign to add more elements.

4 From the **Condition** menu, select **equals** or **not equals**.

Absolute Directory Path is recognized as the base directory. All subdirectories matching the pattern will be crawled.

5 Enter a value.

Sample file property patterns

- Absolute Directory Path > equals > `C$/Eng/Network/Drawings`
- File Pattern > equals > *.jpg
- File Owner > equals > bjones
- File Size > range > 1024-5000 (requires numbers expressed in bytes)
- File Creation Time > between > 16:30:00 and 17:00:00.
- Last Modification Time > after > 13:30:00
- Last accessed > before > 17:00:00

6 Click **Save**.

Define shares for a scan

Define shares to be scanned if the targeted repositories are CIFS, NFS and Documentum repository types. HTTP, HTTPS, FTP and Microsoft SharePoint repositories allow use of file patterns and sizes as well as shares, folders and properties.

Before you begin

Parameters in the **Advanced Options**, **Registration** and **Policies** tabs can be completed before or after the location is identified.

Task

1. On your DLP appliance, select **Classify | Scan Operations.**
2. After completing the scan and node definitions, click the **Filters** tab.
3. Open **Filters**, then open the **Folders** menu.
4. Select an **Element** and **Condition.**

   Absolute Directory Path is recognized as the base directory. All subdirectories matching the pattern will be crawled.
5. Enter a value.

   Examples
   - Absolute Directory Path > equals > `C$/Eng/Network/Drawings`
   - Directory Pattern > contains > Human Resources
   - Directory Pattern > does not contain > Employee Records
6. Click **Save.**

Define folders for a scan

Define folders to be scanned if the targeted repositories are CIFS, NFS and Documentum repository types. HTTP, HTTPS, FTP and Microsoft SharePoint repositories allow use of file patterns and sizes as well as shares, folders and properties.

Before you begin

When you scan all shares on a system, you do not have to define a filter at all. The default filter will always crawl all the shares on the system with the base directory (root).

Task

1. On your DLP appliance, select **Classify | Scan Operations**.
2. After defining the target of the scan in the **Node Definitions** tab, click the **Filters** tab.
3. Open **Filters**, then the **Shares** menu.

   There is only one option for scanning shares - **equals**.
4. From the **Condition** menu, select **All, Exact Match**, or **Pattern.**
5. The **All** condition is the default, and indicates that all shares will be scanned. If you select **Exact Match** or **Pattern**, enter a **Value** that defines a specific location on the share.
6. If more granularity is needed, define the folders and file properties of the scan.
7. Click **Save**.

Define policies for a scan

Define policies for a discovery scan to apply rules against the data at rest in targeted repository. When a match is found, an incident is displayed on the dashboard and stored in the database.

Task

1. On your DLP appliance, select **Classify** | **Scan Operations**.
2. Define all of the needed scan parameters on the **Node Definition**, **Filters**, **Advanced Options**, or **Registration** tabs, and select the device from which the scan will be deployed.
3. Click the **Policies** tab.
4. Click one or more policies.
5. Click **Add** or **Add All**.

   Depending on the size of the repository, you will get better results from the scan if you select fewer policies.
6. Click **Save**.

Using credentials to authorize entry

Credentials are needed to authorize entry to repositories that are to be scanned.

Before you run a scan on a repository, you must have an account on it for which you can provide credentials. Some systems might also require a domain name to complete the authentication process.

ⓘ If the data in a file system is openly accessible, you can use the default credential **None**.

Testing repository credentials

Repositories cannot be scanned without authentication. You can ensure that the repository is accessible by testing your credentials before you start the scan.

On the **Node Definition** page, you can click the **Test** button after defining the target of the scan. **Authentication failed**, **Success**, or **No Shares Detected** will appear.

If access to the repository is denied or the node definition is incorrect, the node will be highlighted in red; otherwise a green highlight will appear.

Add repository credentials

When you create a repository scan, you must already have a legitimate account on that repository. If you know what authentication parameters are required, you can use them to create a credential that will allow the scan to run.

Before you begin

Get the user name and password of an account on the repository that is to be scanned, or contact a system administrator to create an account for you.

Task

1. On your DLP appliance, select **Classify** | **Configuration** | **Credentials**.
2. From the **Actions** menu, select **New**.

   You can create a credential while you are configuring a scan by clicking the **New** button next to the **Credential** drop-down list.

   The **Create Credential** window will appear.
3. Enter a name and optional description.
4. Enter the user name of an account on the repository.

   Domain name requirements vary by repository.
5. Enter the account password and confirm it.
6. Click **Save**.

Modify repository credentials

Modify credentials if the authentication parameters for the repository account have changed.

> **Before you begin**
>
> An existing credential must be displayed in the **Credentials** list.

Task

1. On your DLP appliance, select **Classify** | **Configuration** | **Credentials**.
2. Click the **Name** of the credential to be modified.

   The credential you create will be added to the drop-down list for use in subsequent scans.

   The **Edit Credential** window will appear.
3. Edit the **User Name** and **Password** fields.

   Domain name requirements vary by repository. If the **Domain Name** has changed, you might also have to modify it.
4. Click **Save**.

Delete repository credentials

You can delete credentials that are no longer useful or valid.

> **Before you begin**
>
> An existing credential must be displayed in the **Credentials** list.

Task

1. On your DLP appliance, select **Classify** | **Configuration** | **Credentials**.
2. Select the credentials to be deleted.

   You can delete a single credential by clicking its trash can icon.
3. From the **Actions** menu, select **Delete Selected**.

   The credentials will disappear from the **Credentials** list.

Scheduling scans

Scans can be scheduled to run continuously, in periodic mode, or on demand. They can also be configured to run once, or not at all.

Daily, weekly and monthly scan schedules are provided for easy application to new scan operations. They can be used on an as-is basis, or modified and customized. New scans can be added on the **Create Schedule** page in the **Classify** tab.

Tasks

- *Add scan schedules* on page 165
  Add new scan schedules when needed by setting time parameters. Scans can be scheduled to run on a one-time basis, but they are often scheduled to run repetitively.
- *Modify scan schedules* on page 165
  Modify scan schedules by editing parameters. Scans can be scheduled to run on a one-time basis, but they can also be configured to run repetitively.
- *Delete scan schedules* on page 165
  Delete scan schedules when you no longer need them. You can delete them individually or in groups.

Add scan schedules

Add new scan schedules when needed by setting time parameters. Scans can be scheduled to run on a one-time basis, but they are often scheduled to run repetitively.

Task

1. On your DLP appliance, select **Classify** | **Schedules**.
2. From the **Actions** menu, select **New**.
3. Enter a name and optional description.
4. Set time parameters for the schedule.

   Setting end times is optional.
5. Click **Save**.

Modify scan schedules

Modify scan schedules by editing parameters. Scans can be scheduled to run on a one-time basis, but they can also be configured to run repetitively.

Task

1. On your DLP appliance, select **Classify** | **Schedules**.
2. Click a schedule and modify the parameters.
3. Click **Save**.

Delete scan schedules

Delete scan schedules when you no longer need them. You can delete them individually or in groups.

> Delete schedules one by one by clicking on the trash can icon.

Task

1 On your DLP appliance, select **Classify | Schedules**.

2 Select scans to be deleted.

3 From the **Actions** menu, select **Delete Selected**.

Scan statistics and reporting

When you run a scan operation, files that have been registered or matched to rule conditions are indexed and fetched from the repository. Incidents found by the crawler are displayed under the **Data-at-Rest** vector.

Scan results are first displayed on the **Scan Statistics** dashboard. Statistics describing the status of the scan are displayed under the **Statistics** icon on the **Scan Operations** page.

Incidents found by a scan operation are reported on the **Data-at-Rest** dashboard. Files are downloaded directly to McAfee DLP Discover from the host on which they were detected, but the files are not saved indefinitely. They are fetched from the source when needed and the cache is flushed regularly to optimize disk utilization.

The index keeps running in the background until all files are reported, even if the task has completed.

> To maximize performance during CIFS, NFS, or Documentum inventory scans, the crawler updates the database only after 100,000 files have been processed. If fewer files are detected, the counters are updated after the scan has been completed.

Scan results are reported on the **Data-in-Use** dashboard, but the scan metadata is available on the **Scan Operations Statistics** page.

Statistics include the parameters defined in the scan and processing information about the crawl, such as files processing, number of incidents retrieved, and success of the run.

When you run a scan operation, files that have been registered or matched to rule conditions are indexed and fetched from the repository. While files are being fetched, counters increment as nodes are identified and shares are authenticated. The incident database is updated every 15 minutes until the conclusion of the task.

Incident files are downloaded directly to McAfee DLP Discover from the host on which they were detected, but the files are not saved indefinitely. They are fetched from the source when needed and the cache is flushed regularly to optimize disk utilization. The index keeps running in the background until all files are reported, even if the task has completed.

To maximize performance during CIFS, NFS, or Documentum inventory scans, the crawler updates the database only after 100,000 files have been processed. If fewer files are detected, the counters are updated after the scan has been completed.

Types of scan statistics report

Three types of scan statistics report can be generated.

Table 10-8 Types of scan statistics report

Report type	Description
Current statistics	Reports statistics which are currently viewable. They could be from the current scan, the last one run, or any other historical scan.
All statistics	Reports all the statistics of all the runs of the scan task
Export file list	Reports the file list at share level (only files of the required share), IP level (only files of a required host), or task level (all files detected by the task across hosts and shares). If there is a single host with a single share, all three reports will be the same.

Determining access to scanned files

When incidents are reported, the **Access Control List** for each file can be viewed in incident details.

During scans, file metadata and permissions are fetched first, and permissions are reported on the **Incident Details** page.

Get historical scan statistics

You can get historical statistics from previously completed scans by selecting an export option from the **Report Options** menu in McAfee DLP Discover.

Task

1. On your Linux-based appliance, select **Classify** | **Scan Operations**.
2. Click the **Statistics** icon.
3. From the **History** menu, select a scan.

Get reports of scan statistics

The results on the **Scan Operation Statistics** page can be exported to reports.

All results generated during a scan are saved and displayed to dashboards.

Because CSV is a generic ASCII format, it can be opened with any text editor, spreadsheet or database program. If the CSV file is very large (50,000+ records), it will be compressed into a zip file before it is available for opening or saving.

If you have Microsoft Excel installed and are using Internet Explorer, the reports will automatically open in Excel. If not, a CSV (comma-separated values) text file will open.

> Export from the dashboard is limited to 5 KB. Although the dashboard incident list is limited to 5,000 results, up to 150,000 results can be exported.

Task

1. On your Linux-based appliance, select **Classify** | **Scan Operations**.
2. Click the **Statistics** icon.
3. From the **Reports** menu, select a report.
4. Click **Save**.

View scan results

When you run a scan, files that have been registered or matched to rule conditions are indexed and fetched from the repository, and any incidents detected are displayed on the **Incidents** dashboard under the **Data-at-Rest** vector.

You can find the results of in-progress or completed scans on the **Scan Statistics** page. View specific matches for each incident by clicking its **Details** icon.

> ℹ After a standalone McAfee DLP Discover is registered to McAfee DLP Manager, the number of total incidents displayed will not include incidents that were reported before the appliance was added to the network. Because a few documents might be re-registered after a reboot or restart, duplicate incidents might be reported.

Task

1. On your Linux-based appliance, select **Classify** | **Scan Operations**.
2. Click the radio button of the scan.
3. Click its **Statistics** icon.
4. View the details in the **Job Summary** tab.
5. Click the **Repository Detail** tab for more information.

   The **Host Summary** and **Share Details per Host** drop-down menus appear.

6. Open the menus and click the underlined values for more information.

   If useful information is reported, select **Export** to save it to a CSV file.

Types of task status message

McAfee DLP Discover task status messages advise users of scan anomalies.

Table 10-9 Types of task status message

Status Message	Definition	Remedy
Resource Missing	The path does not exist, or the file might be missing. It was found during the investigation phase (indexing), but is missing during the crawling phase.	Check on the repository to see if it is really missing. If not, restart the scan.
Configuration Error	The task database might have been corrupted.	Recreate the task. Call McAfee Technical Support if that does not resolve the problem.
Connection timed out - Incomplete Listing	Cannot connect to the repository while investigation phase is in progress.	Wait for awhile, then try again.
Complete	The scan is complete.	
Incomplete	The scan is incomplete, probably due to a network error. The repository might have become unavailable.	Reconnect and restart the scan.
Incomplete Listing	The node is down, there was a network failure, credentials were changed between tasks, or the server is busy.	Wait for awhile, then rescan.
Server stopped responding	The server is busy.	Wait for awhile, then resume the task.

Table 10-9 Types of task status message *(continued)*

Status Message	Definition	Remedy
Task Terminated	The Stop action was applied to the scan operation, the task stopped according to schedule, or it was killed by some extraneous means (for example, a system crash or health check).	Wait for awhile, then rescan.
Task Terminated - Incomplete Listing	The task stopped (or its scheduled end time arrived) during investigation phase.	Restart the task.
Waiting - crawlers busy	The system has reached the maximum limit.	The task will continue when the system is free.

Types of system status message

McAfee DLP Discover system status messages advise users of scan anomalies.

Table 10-10 Types of system status message

Status Message	Definition	Remedy
Connection Timed Out	The repository is busy, too many connections have been made to the repository, or the network is down.	Wait for the network or repository to idle, then restart the scan.
Account is locked	The account (username) is locked.	Provide a valid account, or contact administrator of the repository.
Authentication Failed	An incorrect credential has been entered.	Check the user name, password and domain in the credential, or try another one.
Authentication OK	Authentication was successful.	
Permission Denied	Although authentication was successful, you do not have the privilege needed to use the resource.	Contact your administrator.
Do not have permission to update last access time on repository	Permission to access the repository is needed.	Supply the correct credentials (read/write access) and restart the task.
Share (or Shares) Inaccessible	A share might be inaccessible because of insufficient user privilege, or because the share is being used exclusively by another process.	Select the **Filters** tab and try to browse to the share.
Socket Communication Failure	Could not establish socket connection to the database.	Verify the IP address and port, then restart.
Unknown	This error is rare, but might be related to a configuration error.	Call McAfee Technical Support if the error persists.
Unknown database	The login database given was wrong.	Provide correct login database, then restart.
Unsupported database version	Database version on the repository is not supported.	Check documentation for supported version.

Registering documents and structured data

Data in documents and databases can be registered by uploading files or structured data or by using a Registration scan to create signatures for many files in a defined location. You can also register files using a McAfee DLP Discover scan to match rules to data at rest to tag sensitive data, embed signatures in rules that run on a regular basis, or deploy signatures to endpoints through McAfee DLP Agent.

Signatures that identify sensitive documents are stored in the DocReg or DBReg concepts. For McAfee DLP Endpoint scans, the signatures are stored in registered document packages that are deployed to endpoints.

When data is registered by the web upload method, all devices registered to McAfee DLP Manager at that time will receive the signatures. When data is registered by scanning, you can choose the device that will store the signatures.

There are four ways to register content:

- Uploading files or structured data
- Applying policies to data at rest in repositories
- Using signature collections (DocReg or DBReg) or signatures created with a SHA-2 sum utility in rules
- Scanning endpoints and deploying the signature package to McAfee DLP Agent.

Signatures that identify sensitive data are generated by complex algorithms during a registration scan or by uploading documents. Each protected document might contain hundreds of overlapping signatures, which are expressed as hexadecimal numbers. The density, or fidelity, of the signature tiling depends on the level of detection needed.

Typically, the registration process runs whenever a document is uploaded to a McAfee DLP Discover appliance, or when a Registration scan runs on a designated file system or database.

Types of signatures

The signature type selected when data is registered determines the density of signatures generated during registration.

Signature types vary depending on usage and available memory.

When registered text is plagiarized, it is unlikely that a 100 percent match will be found to the original document. Therefore, searching for a percentage match of the registered material is more likely to expose intellectual property theft.

Use the high granularity signature type to detect percentages of matching signatures.

Table 10-11 Definitions of signature types

Signature type	Definition
High granularity	High granularity signatures provide full plagiarism detection and protection by generating overlapping tiles over every bit of text. The original document can be identified, even if words are transposed or the contents differ by a couple of lines of text. Only High Granularity signature types are generated for Web Uploaded documents.
Medium granularity	Medium granularity signatures provide basic plagiarism detection and protection by generating tiles over every eighth word. The original document can be identified even if the contents differ by a couple of pages of text.
Low granularity	Low granularity signatures include a single compact digital signature for each document registered. Exact copies of the file can be detected.

How signatures are shared with managed systems

When McAfee DLP Discover is managed by McAfee DLP Manager, the signatures generated from scans or web uploads are distributed to other McAfee DLP appliances in the built-in concepts DocReg and

DBReg. The signatures stored in those concepts are used to locate registered data in network traffic and remote repositories.

When McAfee DLP Discover and McAfee DLP Monitor are in communication through McAfee DLP Manager, the registration records produced on a McAfee DLP Discover appliance are automatically shared with the McAfee DLP Monitor signature agents.

> Signatures are automatically transferred from the McAfee DLP Discover appliance to any managed McAfee DLP Monitor or McAfee DLP Discover when a registration scan is run. Rescanning is not necessary.

When signatures are shared, protection for content that has been identified in data at rest is extended to **Data in Motion** and **Data in Use** on the network.

Add DocReg or DBReg to a rule

Add the DocReg or DBReg concepts to a rule to match signatures to data at rest in file systems and database repositories.

> You can add up to two scan tasks to a rule, but only one of each type (**Data-in-Motion** or **Data at Rest**). The definition of the rule determines which type is targeted.

If you add a scan task to a rule after the DocReg or DBReg concept is added, you can apply existing signatures to the data that was registered or discovered by that task.

> If a Registration task is used with the DocReg or DBReg concepts, the rule will also be evaluated by any Discover scan that uses its policy. You must manually configure the rule to include the concept if you want to register the same document across multiple rules.

Task

1. On your DLP appliance, select **Policies**.
2. Select a policy, then click a rule.
3. Select **Content**.
4. Click the plus icon to add an element.
5. In the new element, select **Concept is any of**.
6. Click **?**, then open **Corporate Confidential** and select **DocReg** or **DBReg**. This instructs the rule to match all existing signatures to the content you defined.
7. Click **Save**.

   Alternatively, click **Save as Rule** to open a rule definition page. Adding this rule to a policy allows you to use the DocReg or DBReg concepts to identify sensitive data automatically whenever that policy is used to find incidents.

Examples

If DocReg is added to the PII Social Security Number in Documents, it will find signatures only in stationary documents.

If DBReg is added to Social Security Number in Email and Instant Messaging Conversations, it will find signatures only in streaming network data.

Register data by uploading

Register data in repositories by uploading files to McAfee DLP Discover. If they are registered through McAfee DLP Manager, the files will automatically be registered on all managed devices.

Role-based access control determines which users will be empowered to register data.

> If you want to upload a CSV (comma-separated values) file larger than 100 MB, compress the data file (zip, jar, gzip, tar, etc.) before uploading.McAfee DLP Discover caps the size of uploaded files from browsers to 100 MB. However, a larger data file can easily be compressed into an archive smaller than 100 MB. There are no size limits on files after they are uploaded and uncompressed.

Task

1. On your DLP appliance, select **Policies** | **Registered Documents** | **Web Upload**.
2. From the **Actions** menu, select **Upload New File**.
3. Browse to the file you want to register.

   The file to be registered cannot be over 10 MB.
4. Select the policy and rule you want to use to detect the document.
5. Click **Save**, or **Save, Upload Another**.

   > You need not define the McAfee DLP device that will store the uploaded data. When documents are registered by uploading, all devices are automatically selected by default.

Example

If your goal is to protect design documents, you might select the High Technology Industry IP policy and the Design Documents Emailed to Competition rule.

When you click **Save**, the signature of the document is added to the DocReg concept. All web uploaded documents are collected in that concept; they are treated as a group, not registered individually.

> If you are using Mozilla Firefox 3.x, you might get an error message advising you of a security risk after clicking **Save**. The file will be uploaded anyway, but unless you reconfigure Firefox, the complete path to it will not be recorded when using that browser.

Reconfigure Firefox 3.5.x to view complete paths

Reconfigure Firefox 3.5.x to view complete paths when a file is discovered. Other browsers do not provide security alerts when uploading files, so they do not require reconfiguration to display complete paths.

> Firefox 3.5.x does not display complete paths for security reasons.

Task

1. Enter `about:config` in the Firefox address bar.

   Click the button acknowledging the warning.
2. Double-click `signed.applets.codebase_principal_support`.
3. Close and re-open Firefox.

4 Upload a file.

5 Click **Allow** on the **Internet Security** pop-up.

Exclude text from registration

Exclude text from registration to improve performance and clear the dashboard for significant results. Text that is excluded might include boilerplates files or other innocuous content.

Task

1 On your DLP appliance, select **Policies** | **Registered Documents** | **Excluded Text**.

2 From the **Actions** menu, select **New Text.**

3 Open the document containing the text to be excluded.

4 Cut and paste the text into the **Text to Exclude** box.

5 Click **Save.**

Re-register content

Re-register content that has been de-registered.

Task

1 On your DLP appliance, select **Policies** | **Data Registration**.

2 From the **Actions** menu, select **Reregister**.

The registration crawler will restore the document or data from future registration.

Unregister content

You can unregister content that is not relevant to your results.

Task

1 On your DLP appliance, select **Policies** | **Data Registration**.

2 From the **Actions** menu, select **Unregister**.

When this is done, the registration crawler will exclude the document or data from future registration.

Crawling databases

Dynamic Data Registration is a method of fingerprinting large volumes of data using the **Data Match** function. The type of data registered might include extended caches of customer names and account numbers, credit card numbers, patient records, or any other type of structured data.

Up to 300 million records can be registered and tracked as they are moved. In addition, data that has been identified can be associated with a rule to provide long-term protection.

The data retrieved using this method matches specific data values, not just patterns that describe the data, and fine distinctions can be made between matches. For example, customer credit card numbers might be reported as privacy violations, but an employee's own credit card number can be defined as an exception and ignored.

The same mechanisms that support registration of flat files also support registration of database records. For example, the signatures produced by data matching are stored in a factory default concept, DBReg, which collects structured data in the form of comma-separated values found in databases.

The DocReg concept performs the same function for documents.

Database terminology

Terminology that identifies database properties is determined by database types, which vary by vendor. McAfee DLP Discover uses the appropriate object hierarchy when setting up filtering options for scans.

The object hierarchy used by the supported database types varies. The five filtering components supported by McAfee DLP Discover are catalogs, schemas, tables, columns, and records and rows.

Schemas are collections of database objects that are owned or have been created by a particular user, and catalogs are collections of related schemas.

But these terms are used interchangeably in MySQL databases, and Microsoft SQL Server defines a catalog/schema model for data stores. In this model, catalogs contain schemas. By contrast, Oracle and DB2 database use only the term schemas.

Whether the term schema or catalog is used, all databases contain tables, which contain records and rows. McAfee DLP Discover database scanning extends to the records and rows level.

Types of database repository supported

In addition to large volumes of unstructured data in file system repositories, McAfee DLP Discover protects databases containing up to ten million records.

McAfee DLP Discover supports ODBC (Open Database Connectivity), and crawls the following structured databases:

- DB2, versions 5x iSeries, 6.1 iSeries, 7.x-9.x
- My SQL Server, versions 2000, 2005, 2008, 7.0, MSDE 2000
- My SQL (Enterprise), versions 5.0.x, 5.1
- Oracle, versions 8i, 98, 10g, 11g

How database content is registered

Database content is registered by uploading structured data, scanning a database, or deploying rules that identify sensitive data during the discovery process.

You can use McAfee DLP Discover to register database content using one of three methods.

- Upload data in structured format on the **Web Upload** page.
- Create a Registration database scan on the **Scan Operations** page
- Embed the DBReg attribute in one or more rules on the **Edit Rule** page.

The structured data found can be saved to your desktop and uploaded, so that it can be used in subsequent scans.

Register structured data by uploading

Register structured data found in a database by uploading it to McAfee DLP Discover. You can use the registered objects to detect similar content in other repositories.

> If you use McAfee DLP Manager to upload structured data, it will automatically be registered on all managed devices.

Task

1. On your DLP appliance, select **Classify** | **Registered Documents**.
2. In the **Actions** tab, select **Upload New File**.
3. Click **Browse** to locate the data that needs protection.
4. Enter a file name.

   The **Signature Type** field defaults to **High Granularity**, which is the only choice for documents that are registered by uploading.
5. From the **Policy** menu, select a policy.
6. From the **Rule** menu, select a rule.

   The rules listed are the only ones available, because they are the components of the selected policy.
7. From the **Devices** box, select the device that will receive the uploaded data.
8. Click **Save** or **Save & Upload Another**.

Database filtering options

The hierarchical structure of the targeted database determines the filtering options available.

Table 10-12 Filtering options by database type

Database type	Filtering options
MySQL	Catalogs, tables, columns, records/rows
Oracle	Schemas, tables, columns, records/rows
DB2	Schemas, tables, columns, records/rows
MS SQL Server	Catalogs, schemas, tables, columns, records/rows

> For MySQL, only the Enterprise version is supported. MySQL CE (Community Edition) cannot be used for a database scan task because DataDirect, publisher of the JDBC driver used in DLP products, does not support free GPL (General Public License) database versions.

Defining the database to be scanned

Before a database can be scanned, its host name or IP address must be defined to identify the targeted repository.

> When you have completed the node entries, click **Include**. You can also **Test** the database connection.

Table 10-13 Node definition settings for database scans

Option	Definition
IP Address	Host names or single IP Addresses are allowed. For Oracle Real Application Clusters, use the VIP (virtual IP address) of node1 (or node2 of RAC) For MS SQL Server databases with multiple instances, use `<host ip>\\<db instance name>` (for example, `172.20.242.151\\N14N`).
Port	Ports are automatically configured, according to the database type: • DB2 - 50000 • Microsoft • Server - 1433 • MySQL - 3306 • Oracle - 1521 Enter non-standard ports in the text box.
SID	For Oracle RAC, use the service name of the RAC.
Login Database	Type the name of the login to the database. For SQL, this is the database instance. For Oracle, use the SID (System ID).
SSL Certificate	Certificates are created and saved on the Discover configuration **SSL Certificates** page. Click **New** to create a new certificate, or use an existing one.

Catalog options for database scans

Catalog options are available for use in SQL database scans.

Table 10-14 Catalog options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the catalog name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the catalog name entered in the VALUE parameter.

Schema options for database scans

Schema options are available for use in all types of database scans except for MySQL.

Table 10-15 Schema options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the schema name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the schema name entered in the VALUE parameter.

Table options for database scans

Table options are available for use in all types of database scans.

Table 10-16 Table options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the table name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the table name entered in the VALUE parameter.

Column options for database scans

Column options are available for use in all types of database scans.

Table 10-17 Column options

Option	Definition
All	Default value; equivalent to no filtering.
Exact Match	Filters by exact match to the column name entered in the VALUE parameter.
Pattern	Filters by text pattern match to the column name entered in the VALUE parameter.

Record and row options for database scans

Database scans can be run on a specified number of records or rows, allowing definition of a very narrow range of data. In SQL databases, patterning can be used to retrieve specific results from columns.

Table 10-18 Record and row options for database scans

Option	Definition
Where	Allows entry of any SQL **where** clause. For example, retrieve matching names from columns in a table by entering surname like `'%lang';` .
Limit (number of rows)	Limits the number of rows fetched from each table. If you set a limit of 100, it means at most one hundred rows will be fetched from each table crawled.

Setting conditions in database scans

When a scan task is set up, conditions are used to constrain the scan to a specific portion of the database component being filtered.

For example, McAfee DLP Discover might be configured to crawl all columns and rows of one table in a single schema of an MS SQL catalog. Such a configuration might be useful for finding all employees in a group under a single department manager of a business unit.

Set the conditions in the **Filters** tab on the **Add Scan Operation** page.

Login options for database scans

Logins authenticate users to the databases to be scanned, and options vary according to database type.

Table 10-19 Login options for database scans

Option	Definition
Login	• For SQL databases, use the database instance. • For Oracle databases, use the System ID.

Port options for database scans

Port numbers for each of the database types are already set. If a different port is to be used for the scan, it can be defined in the Node Definition tab.

Table 10-20 Port options for database scans

Option	Definition
Port	Ports are automatically configured according to database type. Enter non-standard ports in the Node Definition **Port** box. • DB2 - 50000 • Microsoft SQL Server - 1433 • MySQL - 3306 • Oracle - 1521

Advanced options for database scans

McAfee DLP Discover supports configuration of bandwidth and email notification in addition to routine scanning tasks. These options are available on the **Add Scan Operation** page in the **Advanced Options** tab.

Bandwidth throttling allows you to set a specific data transfer rate for a scan. Email notification allows set up of notification when a scan has started, stopped or both.

> Email subject fields are not customizable. There might be a lag of a few minutes between the actual task start-stop time and the email posting. The end notification is sent at the end of scanning. File processing might continue after notification.

Table 10-21 Schema options for database scans

Option	Definition
Bandwidth	When throttling is activated, allows users to set bandwidth allocated to a scan.
Last Access Time	Microsoft Windows updates files with the last access update time when they are opened by any application unless the **Preserve** option is selected.
Email Notification	Notifies users of scanning operations if **On Start** or **On End** is selected.
Email To / On Start	Sends customized email to a user when a scan starts.
Email To / On End	Sends customized email to a user when a scan is complete.

Using SSL certificates

Like credentials, SSL certificates authenticate users to repositories that are to be crawled. Unlike credentials, they encrypt the channel between the database server and the McAfee DLP Discover appliance.

Database scans using SSL certificates enforce host name verification while negotiating a SSL connection with a database server. Host name verification ensures that the host name in the database server URL to which the crawler (client) connects matches the host name in the digital certificate that the database server sends back as part of the SSL connection.

This helps to prevent man-in-the-middle attacks. But in some situations, the host name in SSL certificate might differ from the host name of database server (for example, a certificate might be issued to an alias/subdomain like `xyz.mcafee.com`, but the database server given (in URL) is `xyz1.mcafee.com`).

The database crawler will fail to crawl such SSL setups. The workaround is to either use the correct hostname in the database host name while configuring the scan, or configure the correct SSL certificate on the database server and upload it to McAfee DLP Manager.

SSL certificate settings

SSL certificates identify the database server host and encrypt the data exchanged between database server and the McAfee DLP device.

Databases must be set up to allow the McAfee DLP Discover client to connect using an SSL socket.

All of the database types different configuration requirements for SSL, and if a certificate is required, it must be exported from the server that is to be scanned. The services of a database administrator will be needed to handle these tasks.

McAfee DLP Discover client certificate handling is currently not supported.

After the certificate is exported, it is imported into the TrustStore of the McAfee DLP Discover appliance.

Table 10-22 SSL certificate settings for database scans

Option	Definition
No SSL Certificate	The scanned data need not be encrypted.
Any SSL certificate	A certificate is required, but it can be non-standard or self-signed.
Signed SSL certificate	The certificate must be verified by a legitimate authority.

Add an SSL certificate

If a secure channel is needed for a database crawl, an SSL certificate might be used to encrypt traffic between the repository and the McAfee DLP Discover client.

Before you begin

If a certificate is to be used, the Database Administrator of the targeted repository must first configure the database to use SSL for authentication and data exchange with clients. This involves exporting the public key of the SSL certificate to a file that the McAfee DLP administrator will downloads for later upload to McAfee DLP Discover.

DBAs should refer to the appropriate database user manual for details. The certificate must be PEM/X.509 standard, and in one of two formats: .cer (Base64 encoded) or .der (Windows encoded).

This procedure explains only the SSL certificate portion of the creation of a database scan. When this part of the process is complete, the SSL certificate will have been uploaded to the McAfee DLP Discover appliance.

Task

1. On your DLP appliance, select **> Classify | Discover Scan Operations | SSL Certificates.**
2. Create a database scan operation.
3. Enter a name and optional description for the certificate.
4. Browse to the location of the certificate on your desktop.

   You can click the magnifying glass icon to get the **Certificate Details** before you save it.

   If the certificate hasn't yet been exported from the repository to be scanned, contact the database administrator.

5 Enter the **Host Name** or IP address of the database server.

6 Click **Save**.

The certificate be uploaded to the McAfee DLP Discover appliance and stored in the TrustStore of the database crawler, and its identifying characteristics will appear in the **Edit SSL Certificate** window.

After you have added the certificate and saved the task, you can start it. If the certificate matches the exported from the database, the crawler will start.

Troubleshooting the SSL certificate

If the crawl fails to validate the certificate, you can log on as root to the McAfee DLP Discover appliance to examine the certificates in the TrustStore.

Change directory to `/data/stingray/python`, then view the contents of the certificate file by running this command:

```
# ./certificate_ct1.py LIST
```

You can match up the information in this file to the **Certificate Details** pane of the **Edit SSL Certificate** window.

Optimizing scanning with data classification

The **Data Classification** feature sorts crawled data into different content types and evalutes the likelihood of potential rule violations before they are reported. That knowledge can be used to create new protection strategies and optimized, more effective scans.

Without enough information about the characteristics of data in a repository, constructing a protection strategy for the data involves trial and error. Sensitive data might be sampled with different types of crawls, and trial runs might be done using different combinations of rules and policies.

Data Classification uses an OLAP data model to obviate the need for such time-consuming tactics, producing comprehensive and useful information so that new strategies can be devised and significant results can be retrieved more quickly.

Once data has been classified for use in optimized scans, OLAP tools can be used to manipulate and record it.

How McAfee DLP Discover uses OLAP

McAfee DLP Discover databases are configured to use *Online Analytical Processing*, a data model that enables processing of metadata at rapid rates from many different viewpoints. The process creates multidimensional relationships between data values.

When McAfee DLP Discover scans a file system repository, each value, or *hypercube*, is compared to many others in the database. A web of relationships between data values produces previously unknown data patterns that can be used to protect data at rest quickly and more effectively.

When an optimized Discover scan is run after data has been classified and stored in a multidimensional OLAP database, new knowledge about the data can be used to estimate potential violations. Using data that describes the context of data values amplifies its usabilty and extends the effectiveness of discovery.

McAfee DLP Discover includes OLAP tools that enable users to explore all aspects of the scanned data. Evaluating the contents of a repository or share before scanning makes it possible to invent new protection strategies that will focus efforts more precisely on data at risk.

The OLAP Navigator

The **OLAP Navigator** displayed on the **Predefined View** and **Task View** pages provides tools that allow users to manipulate classified data.

The OLAP tools give you the ability to explore, drill down, chart, print and report classified data in an infinite number of configurations.

ℹ You must be authorized to view **Data Classification** results. An administrator must add that privilege to the your user group under **Discover Scan Permissions**.

Each of the attributes listed under **Columns** and **Rows** offer an opportunity to explore the classified data produced by the scan you are analyzing.

After you have analyzed a view, you can clear it by selecting the red **X** icon.

Table 10-23 OLAP Tools

OLAP Tool	Function
OLAP Navigator	Displays potential rule hits using the classified data available for each.
Drill position	Offers the ability to drill down to finer granualarity data levels by clicking plus icons.
Show/Hide Chart	Use the values to show or hide the default chart.
Chart Configuration	Use chart settings to create a new chart.
Configure Print Settings	Use print settings to print a new chart.
Print to PDF	Save the results in a PDF report.
Export to Excel	Save the results in a CSV report.

How the classification engine works

The data classification engine operates on two levels: during scan operations, and on the McAfee DLP device.

When inventory and classification scans run, the classification engine crawls the defined repository, reports the files and directory attributes (file name, size, path, etc.) found at that location, classifies them by file type, and reports the results in a several different predefined views.

During a classification scan, the inventory phase is followed by fetching and classifying the content that is found in the repository. The classification engine then stores the existing information about the data (metadata) in a classification database, and it is available on the **Data Classification** dashboard.

The data can then be used to add refined Discover and Registration scans that allow targeting of specific content types and policies.

! Classification scans do not generate incidents on **Data-at-Rest** dashboards.

How data classification scans work

Data classification scans can be used as an interim step between Inventory and Discover scans. They build on inventoried data, classifying it by content type and predicting the type of violations that are likely to be found in the repository.

When the results of a classification scan are used as a starting point for new scans, investigation of a repository returns multidimensional results that offer users more ways to protect data and better results.

Classification scans are especially useful because of their speed and flexibliity. Manifests of file systems produced by Inventory scans are made up of long lists of data that is difficult and time-consuming to analyze. Doing full Discover scans of large repositories might produce so much data that significant patterns might go unrecognized, and the lack of information about the data might lead to incorrect protection strategies.

Classification scans run after repository data has been indexed and before incidents are discovered. This interim step reduces overhead of the scan on the targeted server while increasing the value of reported results.

> Currently, the **Data Classification** feature supports only file-based scans (CIFS, NFS, HTTP, HTTPS, FTP, Documentum, and SharePoint).

How categories are used to forecast rule hits

Categories displayed on the **Task View** page contain rules that could potentially be violated if a Discover scan were run on that share or repository. By exploring each available option, you can figure out what combination of scan parameters will give you the best results.

Other attributes include the share, file types, and owners of the classified data. The **Measures** attributes include the number and size of the files that might be discovered.

Data classification workflow

The **Data Classification** workflow objective is to prepare data found on a repository for optimized scans that can produce significant results quickly.

After you create a classification scan that crawls a specified repository, the classification engine sorts the scanned data and displays it in graphical form on the **Data Classification** page.

Data displayed in the **Predefined View** is made up of any classified data resulting from all scans performed on the McAfee DLP Discover appliance.

Data displayed in the **Task View** is made up of any classified data resulting from a single scans performed by the McAfee DLP Discover appliance. In this view, the sorted data is available for use in subsequent scans by content type (and in the case of a Discover scan, by policy), making it possible to create a refined scan that runs on a very narrow range of data.

How classified data is displayed

Classified data is displayed in two different views. **Predefined Views** can be used for common scenarios, and **Task Views** are user-configurable.

The **Predefined View** is at the McAfee DLP device level, and shows all possible data that has been collected by various scans. The **Task View** is at scan task level, and shows data that has been collected by specific scan operations.

In the **Predefined View** , you can use the **OLAP Navigator** to review many different aspects of the classified data. You can examine discovered data in graphical format, export to a report, or save to a CSV file format.

The results on the **Predefined** dashboard contain all possible data that has been collected by varous scans in a variety of formats, and they are displayed in ways that many users will find helpful. These useful views are provided for user convenience.

In the **Task View**, you see a list of all scans that are doing classification. You can select the **Analysis** icon to find the data classified by that scan, then select aspects of it that can be used in additional scans.

As in the **Predefined View**, when you see the data from those scans in the **Task View**, you can graph, export, or save them to a CSV file format.

Predefined views of classifed data

The **Predefined View** is device-based. It contains classified data gathered from all McAfee DLP devices on the network that have stored results of multiple scans.

These contextual views display classified data in a variety of formats.

Table 10-24 Device data classification views

Device context view type	Data types displayed
Global	Classification on all dimensions like device, task, repository, share and file type
Repository-Share-File Type view	Classification on repository, share and file type
Device-File Type view	Classification on device and file type
Device-Task-File Type view	Classification on device, task and file type
Task-File Type view	Classification on task and file type
File Type-Repository-Share view	Classification on file type and repository
File Type-Device view	Classification on file type and device
Category-Owner view	Classification on category and owner
Category-Repository view	Classification on repository
Category-Repository-Share view	Classification on repository and share
File Type-Share view	Classification on file type and share
File Type-Owner view	Classification on file type and owner

Task view of classified data

The **Task View** page lists all classified and inventory scans. **Statistics** and **Analysis** options are available for each scan.

Selecting **Statistics** on the **Task View** page opens the **Scan Statistics** page. The results of the scan are displayed in the same way as scans that do not create classified content.

Selecting **Analysis** on the **Task View** page opens the **Data Classification** page for that scan. The results of that scan are not only displayed as statistics, but they are also highly configurable. The OLAP tools offer exploration, drilldown, charting, printing and reporting options.

Creating optimized scans from the Task View page

After a classification scan is defined, an optimized scan can be created from the **Task View** page. All of the values defined in the classification scan populate matching fields in the optimized scan.

Even after values from the **Select Classified Data** menu are applied to an optimized scan, it can still be edited on the **Edit Scan Operation** page. The existing applied filters can be used or excluded as needed.

Create an optimized scan from classified data

When you evaluate classified data before creating a new scan, you can refine scan filters to produce more effective results.

Before you begin

Create and run a data classification scan to provide content and context for the optimized scan.

Task

1 On your DLP appliance, select **Classify | Data Classification**.

2 On the **Task View** page, select an Inventory or Classification scan that might have the type of classified data you need to get optimized results.

3 Click the **Analysis** icon of the selected scan.

A page of sorted and configurable results appears.

4 From the drop-down list, select a scan mode.

5 Click **Create Task**.

A window titled **Select Classified Data** appears.

6 Select the checkboxes of file extensions to define the classified content, then select the shares you want to scan.

If you are creating a Discover scan, you must also select one or more policies to indicate what rules you want to match to the classified data.

7 Click **Generate**.

The **Add Scan Operation** page appears.

8 If you click the Policies and Filters tabs, you will see that the policies and filtering options you selected have already been added to the scan definitiion.

9 Click **Save**.

Managing scans

Scan operations are managed by applying different statres from the **Actions** menu on the **Scan Operations** page.

Scan operations can be paused and resumed, and notification can be set up to inform users that a crawl has started and stopped.

Table 10-25 Scan actions

Scan Action	Description
New	Opens the Add Scan Operation dialog box
Clone	Copies the selected scan and opens the Edit Scan Operation dialog box; allows name and other parameters to be changed
Activate	Activates the selected scan; causes system to fetch files and analyze content
Deactivate	Deactivates the selected scan (keeps it from running)
Start	Starts the scan; fetches only new content
Stop	Stops the scan
Abort	Stops the scan abruptly
Rescan	Resubmits the scan for tasks that are not running, but are in a Ready state - re-fetches files and re-analyzes all content, and generates new incidents
Delete	Deletes the scan

Scan states

The status of each scan is displayed in the **Status** column on the **Scan Operations** page.

Table 10-26 Scan states

Scan status	Definition
Ready	Task is ready to run and user can start tasks.
Running	Task (crawler) is running.
Inactive	Task has been removed from the schedule queue and tasks cannot be run (even manually). Such tasks must be activated before they can be run.
Starting	Task is starting and about to run.
Stopping	Task is stopping.
Stopped	Task was killed/crashed by some unforeseen situation. Such tasks can be started again. (Rare)
Aborting	Task is aborted immediately, discarding already fetched and queued objects, if any. This might lead to incorrect scan statistics (object counters) when the scan is next run.

Activate or deactivate scans

Scans must be in an active state before they can be run, and new scan operations are activated by default.

If you deactivate a scheduled scan, it will not run at the appointed time.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 From the **Actions** menu, select **Activate** or **Deactivate**

Start scans

Start scans on demand, or by scheduling them to start at a specific time.

Scans that are to be started must be in a **Ready** state.

A new scan will remain inactive until its associated policies are published.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 Select the scan to be started.

3 From the **Actions** menu, select **Start**.

Stop scans

Scans that are stopped shut down cleanly.

Before you begin

Scans that are to be stopped must be in a **Running** state.

Depending on the number of queued files and load on the server, it could be a few minutes to several hours before the the processing of the crawled files is completed, and the task actually stops.

Stop does a clean shutdown of running tasks. When you stop a scan, the process pauses and the existing data is saved. All fetched files are processed, and all counters are updated before the scan exits and the system returns to readiness. Because of this, using **Stop** will not lead to missed files from processing.

Select **Start** from the **Actions** menu to resume the scan. Restarting the device is not necessary.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 Select the radio button of the scan to be stopped.

3 From the **Actions** menu, select **Stop**.

Abort scans

Use the **Abort** function to stop scans quickly.

Before you begin

Scans that are to be aborted must be in a **Running** state.

Abort immediately kills a running scan without completing processing of files already fetched by the crawler. Some files might go missing due to the abrupt stop.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 Select the radio button of the scan to be aborted.

3 From the **Actions** menu, select **Abort**.

Rescan a repository

Rescanning might be needed after a scan is stopped, aborted, when policies are changed, or file filters are updated.

When a repository is rescanned, the saved manifest is destroyed. Rescanning might result in duplicate incidents.

Task

1 On your DLP appliance, select **Classify** | **Scan Operations**.

2 Select the radio button of the scan task you want to use to rescan the repository.

3 From the **Actions** menu, select **Rescan**.

Set bandwidth for a scan

No Throttling is the default for scanning, which means all available bandwidth will be used. But you can allocate only a portion of the spectrum to the scan by setting bandwidth limitations.

Before you begin

Consider the transmission capacity of your network and the amount of network traffic before deciding how much bandwidth to allocate to the scan.

Task

1. On your DLP appliance, select **Classify | Scan Operations**.
2. Select a scan and click the **Advanced Options** tab.
3. Pull down the throttling menu and choose one of the following.
   - **No Throttling** (default)
   - **Kbps** (kilobits per second)
   - **Mbps** (megabits per second)
4. Click **Save**.

> On a 100-Mbps LAN, limit bandwidth to 50 Mbps to limit the crawler to half of the bandwidth available. If bandwidth is throttled correctly and there is L3 connectivity between networks, McAfee DLP Discover can be deployed across a WAN, though object viewing might be slower due to WAN latency. For example, if a 1 Gbps link between Tokyo and London is used, only ~10 Kbps throughput might be available for a CIFS scan.
>
> Bandwidth throttling is applied as an average across the entire scan rather than as each individual file is being fetched. A Discover scan might burst above or below the configured throttle limit, but the average throughput measured across the entire scan will remain very close to the configured limit.

Scanning in full duplex mode

McAfee DLP Discover must be deployed in full-duplex mode.

Every interface between the Discover appliance and target nodes (intermediary switch, router, firewall, etc.) cannot be set to half-duplex mode.

Guidelines for Fast Ethernet networks

- Hard-code the speed and duplex of the Discover appliance to 100 Mbps and full duplex.
- Ensure that all intermediary devices are either hard-coded to 100 Mbps and full duplex, or validate that all intermediary devices have negotiated to full duplex if configured for automatic negotiation.

Guidelines for Gigabit Ethernet networks

- Set the speed and duplex of the Discover appliance to 1000 Mbps and full duplex or to auto-detect.
- Ensure that all intermediary devices are either hard-coded to 1000 Mbps and full duplex, or validate that all intermediary devices have negotiated to full duplex if configured for automatic negotiation

Managing scan load

Scan load might have an impact on performance of McAfee DLP systems. If too many operations are running concurrently, a scan might appear to be stalled.

Operations that add load to the system include:

- Deleting or creating scans in the same time frame
- Crawlers running and processing files from an extended scan

- Multiple policies and rules being decoupled from deleted scans
- Rescanning, which republishes associated policies and rules

If a scan appears to have stopped, wait for 30 minutes. If the task does not reactivate, select it and **Activate** from the **Actions** menu.

If several retries fail, save the scan as a new task to republish all policies, and delete the old task.

Deploy scans

Scans that are deployed can be run from any of the defined appliances.

Signatures generated from managed McAfee DLP Discover devices are immediately loaded into DocReg when registration tasks conclude. They are automatically stored on other managed appliances to extend their usability.

Task

1. On your DLP appliance, select **Classify** | **Scan Operations**.
2. Select the scan to be deployed.

   Scans are usually deployed when they are created, but not always. Deploying a scan to **None** saves it for later deployment.
3. On the **Edit Scan Operation** page, select one or more devices in the **Devices** box.
4. Click **Save**.

Modify scans

Modify scans if any of the defined parameters have changed.

Task

1. On your DLP appliance, select **Classify** | **Scan Operations**.
2. Select the scan to be modified.
3. On the **Edit Scan Operation** pages, make changes to the scan parameters.
4. Click **Save**.

Delete scans

You can delete scans that are not producing the desired results.

Before you begin

A scan that is in a **Running** state must be stopped before it can be deleted.

When a scan is deleted, the incidents produced by that scan are saved.

Task

1. On your DLP appliance, select **Classify** | **Scan Operations**.
2. Select the radio button of the scans to be deleted.
3. From the **Actions** menu, select **Delete**.

   The scans immediately disappear from the list.

Remediating incidents

McAfee DLP Discover protects data by finding and displaying sensitive data. Remedial actions can be pre-programmed to resolve any problems found.

When a violation is found, you can use a **Data-at-Rest** action rule to prevent or resolve the problem.

Use the **Remediation** button on the **Incident Details** page to resolve incidents as their components are reviewed.

> Remediation is part of the incident workflow, and any time incidents are wiped from the system, remediated files will also be wiped.

When violations are found in **Data-at-Rest**, the remediation feature might be used to do the following:

- Copy files containing violations to another location on the network
- Move files containing violations to another location on the network
- Password-protect files containing violations
- Delete files containing violations

Each of these actions also includes the capability to do the following:

- Notify users of violations found in scanned data
- Record violations found in scanned data in a system log
- Assign incidents to one or more reviewers
- Set a status that indicates the state of resolution

Remediation can be applied directly to incidents reported on the **Data-at-Rest** dashboard, or pre-programmed by attaching an action rule to rules that produce incidents.

Types of remedial action

Remedial actions can be set up to copy, move, encrypt and delete incidents found in **Data-at-Rest**.

Incidents found by a Discover scan might be processed using one of four remedial actions.

- Copy the file to another location
- Move the file to another location
- Encrypt the file
- Delete the file

Each action can be configured to automatically notify users that a remedial action has been applied to a violation found in **Data-at-Rest**.

Each action can also be configured to place a record in a system log, assign the incident to one or more reviewers, or apply a status that indicates its stage of resolution.

Compliance with FIPS standards

With this release, best practices for implementing cryptographic algorithms, which handle key material and data buffers, are supported by compliance with FIPS standards.

The Federal Information Processing Standard (FIPS 140-1) and its successor (FIPS 140-2) are U.S. government standards that provide a benchmark for implementing cryptographic software. Algorithms used for encryption, hashing, and signing are enabled to secure the McAfee DLP Discover remediation processes.

Review remedial actions

You can review remedial actions that have been applied to an incident on the **Incident Details** page.

> Click **Columns** to add the three **Rem** columns to the dashboard.

Task

1 On your DLP appliance, select **Incidents**.

2 Select **Data-at-Rest** from the display thumbwheel.

3 Click the Details icon for an incident.

The **Incident Details** page appears.

4 Review the remedial actions that have been applied.

Add columns to display remedial actions

Add columns to configure the **Data-at-Rest** dashboard to display remedial actions that have been applied to incidents.

> If you make a mistake, you can move column headers out of the **Selected** list by selecting them and clicking **Remove**.

Task

1 On your DLP appliance, select **Incidents**.

2 Select **Data-at-Rest** from the display thumbwheel.

3 Click **Columns**, then scroll down the list of **Available** columns.

4 Select one or more of the **Remediation** column headers:

- RemActionRule
- RemActionType
- RemTaskStatus

5 Click **Add** to move the column headers to the **Selected** list.

6 Use the **Move Up** and **Move Down** buttons to position the columns on your dashboard.

Moving column headers to the top of the window positions them on the right side of the dashboard.

7 Click **Apply**.

The **Incidents** dashboard displays the added columns.

Add remedial action rules

Add remedial action rules to rules that will be used in a Discover scan. When the rule hits, the action will be applied.

Task

1 On your DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu under **Data-at-Rest**, select **Add Action Rule**.

3 Enter a name for the action rule.

4 Open **Email Notification** to alert one or more users to the action.

5 Open **Syslog Notification** and select **Enable** to log the incident.

6 Open **Incident Reviewer** and select **Incident Status** to assign a reviewer.

7 Open **Incident Status** to define its stage of resolution.and select **Enable** to log the incident.

8 Open **Remediation Policy** and select the corrective action that is to be taken.

9 Click **Save**.

Apply remedial action rules

Apply remedial actions to discovered incidents by adding them to rules. The actions are applied when the rule is matched against on data at risk. If the rule detects sensitive data, the action defined in the rule will be taken.

> If McAfee DLP Discover and McAfee DLP Monitor devices are managed by McAfee DLP Manager, every rule can be configured to deploy one action to each of the three incident types.

> Rescan to produce updated results, then verify that the action rule applied to the rule implements the correct remedial action.

Task

1 On your DLP appliance, select **Policies**.

2 Click the policy defined in the scan, then click a rule.

3 Click the **Actions** tab.

4 Click **Add Action**.

5 Select a remedial action from the **Data-at-Rest** menu.

6 Click **Save**.

Set up locations for exported files

Set up locations for exported files so that when sensitive files are found in a database or repository, they can be copied or moved to a shared folder.

Export locations are used in file remediation and action rules.

> Only Windows shares (CIFS) are supported.

Task

1 On your DLP appliance, select **Classify** | **Export Locations**.

2 From the **Actions** menu, select **New**.

3 Enter a name on the **Create Export Location** page.

If the folder does not already exist, it is created.

4 Select a credential to access the repository, or click **New** to create a new using the authentication parameters of an existing account.

5 Click **Test** to verify read/write access to the repository. If the credential is correct but the test is negative, use Windows Explorer to verify that sharing is enabled and read/write privilege has been granted.

6 In Microsoft Windows Explorer, right-click the target folder and select **Properties.**

7 In the **General** tab, deselect the **Read-only** checkbox.

8 In the **Sharing** tab, select **Share this folder.**

9 Click **OK**

10 Click **Save**, then re-test.

Copy discovered files

Copy discovered files to a quarantined export location after a remedial action has been applied to an incident.

> When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

> You can use **Dynamic Variables** to automatically inform users that the file has been copied to an export location.

Task

1 On your DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule.**

- If you want to copy an incident from the dashboard, select its **Detail** icon, select **Remediate** | **Action** and select the **Copy** action rule from the sub-menu.
- If you want an incident to trigger a copy action, add the <copy action rule> to the rule and click **Save**, then start a Discover scan that applies the rule containing the action rule.

3 Enter a name for the action rule.

4 Open **Email Notification** to alert one or more users when the action is triggered.

You can use **Dynamic Variables** to inform users of the prevented action automatically.

For example, `##Filename` found by the `##Rule` violated the `##Policy` and was copied to <export location>.

For example, `##Filename` found by `##ScanOperation` violated the `##Policy` and was copied to <export location>.

5 (Optional) Open **Syslog Notification** and select **Enable** to log the incident.

6 Open **Incident Reviewer** to assign a reviewer when the action takes place (recommended).

7 Open **Incident Status** to change the stage of resolution when the action takes place (recommended).

8 Open **Remediation Policy** and select **Copy** from the **Action** list.

9 Select the export location from the **Destination** drop-down list.

10 Click **Save**.

Move discovered files

Move discovered files to a quarantined location after a remedial action has been applied to an incident.

> When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

> You can use **Dynamic Variables** to automatically inform users that the file has been moved to a quarantined location.

Task

1 On your DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule**.

- If you relocate an incident from the dashboard, select its **Details** icon and select **Remediate** | **Action** and select the **Move** action rule from the sub-menu.
- If you want an incident to trigger a move, add <move action rule> to the rule and click **Save**, then start a Discover scan that applies the rule containing the action rule.

3 Enter a name for the action rule.

4 Open **Email Notification** to alert one or more users when the action is triggered.

You can use **Dynamic Variables** to inform users of the prevented action automatically.

For example, `##Filename` found by the `##Rule` violated the `##Policy` and was quarantined.

For example, `##Filename` found by `##ScanOperation` violated the `##Policy` and was moved to <export location>.

5 Open **Syslog Notification** and select **Enable** to log the incident (optional).

6 Open **Incident Reviewer** to assign a reviewer when the action takes place (recommended).

7 Open **Incident Status** to change the stage of resolution when the action takes place (recommended).

8 Open **Remediation Policy** and select **Move** from the **Action** list.

9 Select the quarantine location from the **Destination** drop-down list.

10 Click **Save**.

Encrypt discovered files

Encrypt discovered files when they are found by providing passwords that must be used to access them. With this release, the default *openssl* utility used to encrypt discovered files is replaced with the McAfee® Endpoint Encryption for Files and Folders™ algorithm.

The encryption key is stored in ePO databases and an ePO extension is used to display the list of keys stored.

> When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

> You can use **Dynamic Variables** to automatically inform users that the file has been encrypted.

Task

1 On your DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule.**

3 Enter a name for the action rule.

4 Open **Syslog Notification** and select **Enable** to log the incident (optional).

You can use **Dynamic Variables** to inform users of the encryption automatically.

For example, `##Filename` found by the `##Rule` found by the `##ScanOperation` was encrypted.

5 Add **File Marker Text** to change the stage of resolution when the action takes place (recommended).

6 Open **Incident Reviewer** to assign a reviewer when encryption occurs (recommended).

7 Open **Incident Status** to change the stage of resolution when encryption occurs (recommended).

8 Open **Remediation Policy** and select **Encrypt** from the **Action** list.

9 Enter a password and confirm it.

10 Click **Save**.

Delete discovered files

Delete discovered files by a delete action when they are found by a Discover scan. After this is done, the file cannot be recovered.

When you copy, move, delete or encrypt a file, McAfee DLP Discover leaves a trace file at the original location to leave a record of the remedial process that has been applied.

You can use **Dynamic Variables** to automatically inform users that the file has been deleted.

Task

1 On your DLP appliance, select **Policies** | **Action Rules**.

2 From the **Actions** menu, select **Add Action Rule.**

- If you relocate an incident from the **Incident Details** page, select its checkbox and select **Remediate** | **Action** and select the **Move** action rule from the sub-menu.

- If you want an incident to trigger a move, add the <delete action rule> to a rule and click **Save**, then start a discovery scan that applies the rule containing the action rule.

3 Enter a name for the action rule.

4 Open **Remediation Policy** as appropriate.

You can use **Dynamic Variables** to inform users of the prevented action automatically.

For example, `##Filename` found by the `##Rule` found by the `##ScanOperation` was deleted.

5 Add **File Marker Text** to change the stage of resolution when the action takes place (recommended).

6 Click **Save**.

7 Apply the new action rule to one or more rules.

8 On your DLP appliance, select **System** | **Discover Configuration**.

9 When the **Scan Operations** page appears, select a scan.

10 From the **Actions** menu, select **Rescan**.

11 Check the results to verify that the file has been deleted.

Revert remediated files

Revert remediated files to reverse an action that has been applied to a file that was found during a scan.

Deleted incidents cannot be reverted or recovered.

> If data is moved to quarantine an incident, the action can be reverted. If remediation actions fail, error messages appear.

Task

1 On your DLP appliance, select **Incidents**.

2 Select one or more incident checkboxes.

3 From the **Remediate** menu, select **Revert**.

4 Click **OK** to confirm, or **Cancel**.

5 You might want to rescan to verify that the action has been reverted.

Searching discovered data

Sensitive data that has been discovered in network repositories is stored in the McAfee DLP Discover database, and is searchable through McAfee DLP Manager.

The **Advanced Search** and **Edit Rule** pages list a **Discover** category that includes a list of options for searching discovered data.

Those parameters can be used alone or in combination with other attributes to retrieve narrow ranges of discovered data.

Find registered files in data at rest

Find registered files in discovered data by using the **DocReg** concept with one of the **Discover** parameters.

> Use **Share Name** or **File Path** to define a location at which you want to find registered data.

Task

1 On your DLP appliance, select **Capture** | **Advanced Search**.

2 From the **Discover** menu, select **Share Name** or **File Path**.

3 Enter the share name or file path into the value field.

4 Click **Search**.

Find scan operations in data at rest

Find scan operations in discovered data by using the **Scan Operation** attribute in a query.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, accept the default **Scan Operations**.
3. Click **Search**.

Find IP addresses in data at rest

Find IP addresses in discovered data by using the **Host IP** attribute in a query.

> You can search for single IP addresses, ranges, subnets, and addresses expressed in CIDR notation.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **Host IP**.
3. Enter the IP address, range, or address and subnet of the repository in the value field.
4. Click **Search**.

Examples

192.168.3.225

10.1.0-10.0.1-255

172.16.1.1/24

Find host names in data at rest

Find host names in discovered data by using the **Host Name** attribute in a query.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **Host Name**.
3. Enter the host name in the value field.
4. Click **Search**.

Find domain names in data at rest

Find domain names in discovered data by using the **Domain Name** attribute in a query.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **Domain Name**.
3. Click **Search**.

Find share names in data at rest

Find share names in discovered data by using the **Share Name** attribute in a query.

Use this task to find share names in discovered data by using the **Share Name** attribute in a query.

> On Microsoft Windows computers, the default share is C$.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **Share Name**.
3. Click **Search**.

Find file name patterns in data at rest

Find file name patterns in discovered data by using the **File Name Patterns** attribute in a query.

You can also use this attribute in a **Basic Search** to find files in network data.

> The only metacharacter supported is a single asterisk. Comma- and space-separated values signifying AND and OR are not supported.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **File Name Pattern contains any of**.

   You can use a keyword with an asterisk (for example, Financ*), but a **File Name Pattern** search is faster.
3. Enter a name or file type extension into the value field.
4. Click **Search**.

Find repository types in data at rest

Find repository types in discovered data by using the **Repository Type** attribute in a query.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **Repository Type**.
3. Click **Search**.

Find file paths in data at rest

Find file paths in discovered data by using the **File Path** attribute in a query.

> Absolute or relative file paths in Microsoft Windows (\) or UNIX (/) systems are indexed in the database, but only UNIX paths are supported when searching.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **File Path is any of**.

3. Enter the file path in the value field.
4. Click **Search**.

Find file owners in data at rest

Find file owners in discovered data by using the **File Owner** attribute in a query.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **File Owner is any of**.
3. Enter the file owner in the value field.
4. Click **Search**.

Find catalogs in data at rest

Find catalogs in discovered data by using the **Catalog** attribute in a query.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**..
2. From the **Discover** menu, select **Catalog**.
3. Click **Search**.

Find schema names in data at rest

Find schema names in discovered data by using the **Schema Name** attribute in a query.

> Database design varies by vendor, but all vendors use schemas.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **Schemas**.
3. Click **Search**.

Find table names in data at rest

Find table names in discovered data by using the **Table Name** attribute in a query.

Task

1. On your DLP appliance, select **Capture** | **Advanced Search**.
2. From the **Discover** menu, select **Table Name**.
3. Click **Search**.

Find column names in data at rest

Find column names in discovered data by using the **Column Name** attribute in a query.

> Database design varies by vendor, but all vendors use columns.

Task

1. On your DLP appliance, select **Capture | Advanced Search**.
2. From the **Discover** menu, select **Column Name**.
3. Click **Search**.

Find records and rows in data at rest

Find records and rows in discovered data by using the **Records and Rows** attribute in a query.

> Database design varies by vendor, but all vendors use records and rows.

Task

1. On your DLP appliance, select **Capture | Advanced Search**.
2. From the **Discover** menu, select **Records and rows**.
3. Click **Search**.

Find signature percentage matches in data at rest

When registered text is plagiarized, it is unlikely that a 100 percent match will be found to the original document. Finding only a percentage of the registered material is more likely to expose intellectual property theft.

The **Signature Percentage Match** parameter can only be added to a rule to supplement other parameters that have been defined. It is not possible to find percentage matches of registered data in a search.

Task

1. On your DLP appliance, select **Policies**.
2. Open a policy, or add a new one.
3. From the **Actions** menu, select **Add Rule**.
4. Open the **Content** category.
5. From the drop-down lists, select **Concept is any of** and click **?**.

   The Concepts palette appears.
6. From the **Corporate Confidential** category, select DocReg.

   The DocReg concept contains all of the signatures that were added during document registration.
7. From the **Discover** menu, select **Signature Percentage Match**.

   Because an exact percentage match is unlikely, the match can only be greater than the percentage you specify.
8. Enter an integer in the value field.
9. Click **Save**.

   When the rule is run, the DocReg signatures are matched against data in network file systems, and results are reported on the **Data-at-Rest** dashboard.

Search with the DocReg concept

Searching with the DocReg concept applies all existing signatures to the network data stream, network repositories, and endpoints.

Task

1. On your DLP appliance, select **Policies**.
2. From the **Content** menu, select **Concept is any of.**
3. Enter `DocReg` in the value field.
4. Click **Search**.

Use cases for scanning data at rest

The following use cases are typical scenarios used when scanning data at rest.

Identify and track sensitive documents

McAfee DLP systems help you to identify and track fragments of data at risk. When you upload data to McAfee DLP Discover, the system registers it by generating overlapping tiles with unique hexidecimal numbers that identify every bit of text. Even if words are transposed or contents differ by a few lines of text, it can be easily tracked.

> If you can't upload all of your sensitive data because you can't identify it all, run a Discover scan that applies a generic set of rules against the data in your repository. You can set it up so that it will generate incidents that violate many different policies, and when you evaluate the results you can devise a more targeted strategy.

Task

1. On your Linux appliance, select **Policies** | **Registered Documents**.
2. From the **Actions** menu, select **Upload New File.**
3. Browse to locate a sensitive file that must be protected.

   > Mozilla Firefox 3.5 will not include the path to the uploaded document unless you reconfigure it before scanning.

4. Select a policy and rule to guide the search.

   For example, select the *Financial and Security Compliance* policy and the *Financial Statement Documents* rule to protect a document that contains sensitive financial information.

5. Define the device that will receive the uploaded file by selecting checkboxes of one or more McAfee DLP appliances.
6. If more documents need protection, select **Save & Upload Another** and repeat the process.
7. Click **Save**.
8. After some time, check the **Data-at-Rest** vector on your McAfee DLP Manager dashboard. For full coverage, add the content to a rule and schedule it to run at regular intervals.

   Remember to select an appropriate time filter. The system cannot track data before it was uploaded.

Find files that have been copied or moved

This case helps you to control copies of sensitive documents.

Confidential documents often proliferate over networks, because employees can copy or move them to insecure locations to work on them, or share them with other staff members. Even when confidential information is accessed only by those who have the proper privileges, finding, registering, and controlling every copy is the only way to protect it.

Task

1. On your DLP appliance, select **Policies | Registered Documents**.
2. From the **Action** menu, select **Upload New File**, and browse to the file you want to track.

   The web upload feature supports only high granularity mode, which provides full plagiarism detection and protection by generating overlapping signatures over every bit of text in a file. The original document can be identified, even if words are transposed. The contents might differ by a couple of lines of text.
3. Select a signature type.

   The web upload feature supports only high granularity mode, which provides full plagiarism detection and protection by generating overlapping signatures over every bit of text in a file. The original document can be identified, even if words are transposed. The contents might differ by a couple of lines of text.
4. Select a policy and rule that fits your objective.

   For example, you might use the *Competitive Edge* policy if your goal is to protect sensitive sales documents, and the *Pricing Information* rule if you want to protect your price lists.
5. Click **Save**.

   You need not define the McAfee DLP device that will store the uploaded price list. When documents are registered by uploading, all devices are automatically selected by default.
6. On the **Web Upload** page, click the **Details** icon of the price list to view the **SHA-2** signature number.

   This unique number is used to find sensitive data during any scan or search of data at rest.
7. Configure a Discover scan and start it, allow some time for processing, then select **Incidents** and click the **Columns** button.
8. Add the **Signature** and **Path** columns to your dashboard, then click **Apply**.
9. Go to the **Incidents** page and select **Data-at-Rest** from the vector thumbwheel. Look for the signature number of the document in the results under the added columns.
10. Right-click the signature number and select **Copy**.
11. Go to the **Advanced Search** page and open the **File Information** category.
12. Select **SHA-2 | is any of** and paste the signature number in the value field and click **Search**.

    You might find that you are inadvertently pasting in unrelated text. If so, close the program that contains that text and repeat the process.
13. On the **Data-at-Rest** dashboard, view the **Signature** and **Path** columns, which will tell you the exact locations of the file.

Match existing signatures to data in a scanned repository

Suppose you have completed several registration scans of file systems or databases that have produced an extensive collection of signatures that contain protected content. You can use the signatures from one or more of those scans to determine if the same content is found in a share that has already been crawled.

Task

1. On your DLP appliance, select **Policies**.
2. Open a policy, or add a new one.
3. From the **Actions** menu, select **Add Rule**.
4. Open the **Content** category.
5. From the drop-down menus, select **Concept is any of**.
6. Click **?**, open **Corporate Confidential**, and select DocReg or DBReg, depending on the target of your scan.
7. Click **Apply**.
8. Open the **Discover** category.
9. From the drop-down menus, accept the default, **Scan Operation is any of**.
10. Click **?** and open the **Database Registration** or **Document Discovery** categories, depending on the target of your scan.

    If Discover scan is listed, do not select it. Referencing Discover scan results will not apply the rule parameters to the original location of the scan.
11. Click **Apply**.
12. Click the green plus icon to add a new element.
13. From the drop-down menus, select a parameter that can be used to define the location of the targeted repository.

    For example, use **Share Name** or **File Path** to define the location of the files to be matched against the signatures generated by the registration scans or web uploads.
14. Click **Save**.

When the rule runs, the registered content contained in the signatures will be compared to the files in the location in the repository. If there are any matches, they are displayed under the **Data-at-Rest** vector on the **Incidents** dashboard.

11 McAfee DLP Prevent

McAfee DLP Prevent provides protection for email and webmail by analyzing traffic and applying preventive action rules to mail that violates policy.

The multi-threaded support feature of McAfee DLP Prevent allows traffic to pass more quickly through the monitor port. This improves performance and increases response time.

Contents

How McAfee DLP Prevent protects data

McAfee DLP Prevent protects data by deployment with an MTA (Mail Transport Server) or proxy server. Communications are forwarded over SMTP or ICAP, depending on whether an email or web gateway is used. When a violation is found in network communications, the software triggers an optional action rule to resolve the incident.

McAfee DLP Prevent uses a rules evaluation mechanism with applied actions to provide automatic resolution of problems found in email and webmail that is circulating on a network.

When violations are found in webmail, the seven actions are attenuated to BLOCK and ALLOW. When violations are found in network email, McAfee DLP Prevent can take more actions.

- block confidential data breaches
- encrypt authorized transmissions
- quarantine suspicious traffic
- bounce email that violates policies
- notify supervisory personnel
- record incidents in a system log
- allow email that is determined to be legitimate.

Use McAfee DLP Prevent to capture network traffic for later forensic analysis or block the transmission of sensitive data sent using specific mail protocols (for example, HTTP POST, SMTP_Request, etc.).

The role of McAfee DLP Prevent in a managed system

When McAfee DLP Prevent is managed by McAfee DLP Manager, the software deploys preventive actions to **All Devices** that are managed by the system. Use of multiple systems with McAfee DLP Prevent ensures that enterprise networks prevent security leaks more efficiently.

If McAfee DLP Monitor, McAfee DLP Discover, and McAfee DLP Endpoint devices are managed by McAfee DLP Manager, every rule can be configured to deploy one action of each of the three incident types (**Data-in-Motion**, **Data-at-Rest**, **Data-in-Use**).

McAfee DLP Monitor is a passive component on the network, so the default preventive action has to be set to ALLOW. This setting changes only if McAfee DLP Prevent is installed. Preventive actions are not supported without it.

Types of preventive actions

Preventive actions are added to rules that are matched to data in motion on the network. When a rule hits, the action is applied.

Each action can be configured to automatically notify users that a preventive action has been applied.

Each action can also be configured to place a record in a system log, assign the incident to one or more reviewers, or apply a status that indicates its stage of resolution.

- Allow
- Block
- Bounce
- Encrypt
- Monitor
- Notify
- Quarantine
- Redirect

MTA requirements to interoperate with McAfee DLP Prevent

The capabilities of generic MTAs determine whether it is feasible to have interoperability with McAfee DLP Prevent.

The following distinguishes between the terms incoming/outgoing and entering/leaving for emails.

- By incoming and outgoing, we mean emails that are either being sent to or received from the outside world.
- By entering and leaving, we mean emails that are entering or leaving the MTA.

Any MTA that is expected to inter-operate with Prevent must comply with the following requirements.

1. Must be capable of sending either all or a portion of outgoing traffic to the McAfee DLP Prevent application. McAfee DLP Prevent is not typically used to inspect incoming email. Examples of a requirement where only a portion of the traffic needs to be scanned may be in environments where only traffic with attachments is to be scanned, or where scanning is limited to traffic directed to public sites (for example, Yahoo).

2. Must be capable of inspecting email headers of messages entering the MTA.

3. Must be capable of taking actions based on specified match expressions for email headers. The specific header strings received from McAfee DLP Prevent are the X header X-RCIS-Action header with values ALLOW, BLOCK, QUART, ENCRYPT, BOUNCE, REDIR and NOTIFY.

4 Based on entering port or some other metric, must be capable of distinguishing between all emails arriving from the McAfee DLP Prevent appliance, then applying header inspection and header-based action rules exclusively to incoming email from McAfee DLP Prevent.

5 Must be capable of ensuring that emails arriving from the McAfee DLP Prevent appliance are not routed back to the McAfee DLP Prevent appliance. This can be done either by using port / srcIP-based mail routing, checking to see if an X-RCIS-Action header already exists in an email scheduled to be routed to the McAfee DLP Prevent appliance, or by some other means.

6 Must be capable of implementing all of the McAfee DLP Prevent-based actions. If the MTA does not have all of the required capabilities, inter-operation is still possible - but in that case, the actions that can be set when rules are created must be limited to those supported by the MTA.

7 Must be able to inter-operate with an email encryption appliance (if this capability is needed) and instruct the encryption appliance to encrypt specific messages based on header information or other metrics.

McAfee DLP Prevent email and webmail processes

McAfee DLP Prevent follows standard processes when processing email and webmail.

Email process

This is how the McAfee DLP Prevent email process works:

1 A host sends an email message to an email gateway.

2 The message is relayed to the smart host, which routes it to the McAfee DLP Prevent appliance.

3 On receiving the email, the McAfee DLP Prevent appliance compares it to existing rules.

4 If a rule matches, McAfee DLP Prevent adds an X-RCIS-Action header and stores the event in its database.

5 The McAfee DLP Prevent then sends the email back to the smart host, and it is relayed back to the email server.

6 Based on the action specified in the X-RCIS-Action header appended by the Prevent appliance, the message is allowed, blocked, bounced, encrypted, monitored, quarantined or redirected.

7 The software sends notification of the action to the defined user.

Webmail process

This is how the McAfee DLP Prevent webmail process works.

> ℹ Although McAfee DLP Prevent supports block, bounce, encrypt, monitor, quarantine and redirect actions, proxy servers can only BLOCK or ALLOW webmail.

1 A host sends a webmail message to a network address.

2 If a web proxy server is set up, it intercepts the message and routes it to the McAfee DLP Prevent appliance.

3 On receiving the email, the McAfee DLP Prevent appliance compares it to existing rules.

4 If a rule matches, McAfee DLP Prevent adds an X-RCIS-Action header and stores the event in its database.

5 The McAfee DLP Prevent then sends the webmail back to the proxy server, and it is either blocked or delivered to its addressee.

6 The software sends notification of the action to the defined email address.

Configuring McAfee DLP Prevent

Configure the software to provide protection for email and webmail by analyzing traffic and applying preventive action rules to mail that violates policy.

McAfee DLP Prevent automatically resolves problems found in network email and webmail.

Tasks

- *Add McAfee DLP Prevent action rules* on page 206
  Add McAfee DLP Prevent action rules, then apply them to standard or customized rules that are matched to data in motion on the network. When the rules hit, the actions rules resolve problems in email communications.
- *Apply McAfee DLP Prevent action rules* on page 207
  Apply McAfee DLP Prevent to international rules to take action when the rules hit on sensitive data in email.
- *Configure McAfee DLP Prevent for email* on page 207
  When configured with an email gateway, McAfee DLP Prevent monitors transmissions and applies preventive actions to sensitive data found in network communications.
- *Configure McAfee DLP Prevent for webmail* on page 208
  When configured with a web proxy server, McAfee DLP Prevent monitors transmissions and identifies data in wikis, portals, blogs and other collaborative sites using HTTP and HTTPS protocols.
- *Review McAfee DLP Prevent action rules* on page 208
  Review McAfee DLP Prevent action rules by viewing the **Incident Details** page.

Add McAfee DLP Prevent action rules

Add McAfee DLP Prevent action rules, then apply them to standard or customized rules that are matched to data in motion on the network. When the rules hit, the actions rules resolve problems in email communications.

Task

1 Select **Policies** | **Action Rules**.

2 In the **Data-in-Motion** section, select **Actions** | **Add Action Rule**.

3 Type a name for the action rule.

4 Open **Email Notification** and fill in the value fields to alert one or more users when the action is triggered.

   You can use **Dynamic Variables** to inform users of the pre-defined action automatically.

   For example, `##Filename` found by the `##Rule` violated the `##Policy` was redirected to <Manager>.

   The Manager of record is identified through Active Directory user IDs.

5 **Optional:** Open **Syslog Notification** and select **Enable** to log the incident.

6 **Recommended:** Open **Incident Reviewer** to assign a reviewer when the action takes place.

7 **Recommended:** Open **Incident Status** to change the stage of resolution when the action takes place.

8 Select an action from the **Data-in-Motion Prevent Action** menu.

9 Click **Save**.

Apply McAfee DLP Prevent action rules

Apply McAfee DLP Prevent to international rules to take action when the rules hit on sensitive data in email.

Apply a McAfee DLP Prevent action rule to a rule.

Task

1 On your Linux-based appliance, select **PoliciesAction Rules**.

2 Click a rule to open it.

3 Select an action from the **Data-in-Motion Prevent Action** menu.

4 Click **Save**.

Configure McAfee DLP Prevent for email

When configured with an email gateway, McAfee DLP Prevent monitors transmissions and applies preventive actions to sensitive data found in network communications.

> Both MTA and proxy servers can be handled by one McAfee DLP Prevent system, but contact a McAfee Service Representative to assure proper performance.

Task

1 On your Linux-based appliance, select **System | System Administration | Devices**.

2 Add the McAfee DLP Prevent appliance to McAfee DLP Manager:

a Select **Actions | Add New Device**.

b Enter the **Device IP or hostname** and **Password** in the value fields.

c Click **Add**.

3 Select the McAfee DLP Prevent appliance and click **Configure**.

4 Scroll down to the **Smart Host** section of the page and enter an IP address to which the processed email will be routed.

Host names are not supported; an IP address is required. A smart host is configured only if SMTP email is being processed, and configuring more than one is not supported.

5 If you configured a rule and you want email notification when the rule hits, you must add an email address. The mail server sends notification to that address after the action is taken.

6 Click **Send test mail** to verify that the smart host connection is alive.

7 Click **Update**.

Configure McAfee DLP Prevent for webmail

When configured with a web proxy server, McAfee DLP Prevent monitors transmissions and identifies data in wikis, portals, blogs and other collaborative sites using HTTP and HTTPS protocols.

> McAfee Email Security Appliance is set to handle up to 30 concurrent SMTP connections - but McAfee DLP Prevent exceeds this limit. To get these two appliances to work together, you must modify the ESA configuration files.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. Add the McAfee DLP Prevent appliance to McAfee DLP Manager:
   a. Select **Actions** | **Add New Device**.
   b. Enter the **Device IP or hostname** and **Password** in the value fields.
   c. Click **Add**.
3. Select the McAfee DLP Prevent appliance and click **Configure**.
4. Scroll down to the Email Settings section of the page and add an email address for notification.

   If you are monitoring traffic through a proxy server, no configuration is needed because that server is already part of the network, so smart hosts are not used when DLP Prevent is configured with a proxy server. Do not enter anything in this box.
5. Click **Update**.

   SSL-encrypted webmail transmissions might become visible during this process.
6. The web proxy server captures outgoing HTTP traffic (including webmail) and sends that the McAfee DLP Prevent over ICAP (Internet Control Adaptation Protocol).
7. If a rule matches, McAfee DLP Prevent adds an X-RCIS-Action header and stores the event in its database.
8. If the action specified in the header is not ALLOW, the webmail is BLOCKED.
9. Click **Update**.
10. Notification of the action is sent to the defined user.

Review McAfee DLP Prevent action rules

Review McAfee DLP Prevent action rules by viewing the **Incident Details** page.

Task

1. On your Linux-based appliance, select **Policies**.
2. Click on the magnifying glass icon of an incident.

   The **Incident Details** page launches.
3. Check the details to see if an action has been applied.

12 Managing McAfee DLP systems

All DLP setup, configuration and management tasks are handled by McAfee DLP Manager, which coordinates all DLP systems.

Managed devices may include the DLP product appliances and servers that provide added functionality.

If you have the proper administrative permissions, you can monitor and manage your DLP systems from the **System Administration** dashboard.

Contents

Working with McAfee DLP devices

Use the McAfee DLP Manager to add, configure, back up, and manage DLP systems.

Proper management of your DLP systems is essential for the software to operate well.

Add McAfee DLP devices

Add McAfee DLP appliances to McAfee DLP systems through McAfee DLP Manager. When new appliances are added, an SSH communication tunnel is created between them.

Adding a McAfee DLP appliance wipes the current configuration of that machine, but captured data, cases, and incidents will not be lost. Unless you have previously deployed policies to **All Devices**, you will have to edit them to add the device.

If a device is registered with McAfee DLP Manager, the device cannot be brought back to standalone mode after deregistering it, and it will have to be reinstalled.

> On some networks you can choose a port configuration. The McAfee DLP appliance is a Gigabit network device, so it is possible to bring it down.

The **Add Device** page is also used to add an ePolicy Orchestrator server (ePolicy Orchestrator GUI IP Address) and database (ePolicy Orchestrator Database IP or hostname). If the ePolicy Orchestrator device checkbox is selected, the options change.

> If **Incident Copy Only** is selected from the **Type** menu, there is no integration with unified policy, and you must use the McAfee DLP Endpoint Policy Manager to update the policy.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. Select **Actions** | **New Device**.
3. Enter the **Device IP or hostname** and **Password**.

   Use the root user account for association. McAfee recommends that you change the root password on the appliance before adding it to McAfee DLP Manager. If you change the IP address, the network service needs to be restarted. Stingray automatically restarts the box to register the change.
4. Click **Add**.
5. Click **OK** to confirm or **Cancel** the registration.
6. Wait for the **Status** icon in the device list to turn green.

   The CPU usage display indicates that the registration tasks being performed. McAfee DLP Manager does not display any CPU activity, because it serves only as a collection point for the data. Other machines are capturing and indexing data and the processor indicates the CPU utilization. It should not go over 70-80%.

   If registration seems to be taking a long time, try refreshing the page.

   When devices are added successfully, their status icons will turn green.

Configure McAfee DLP devices

Configure McAfee DLP devices during installation by running the **Setup Wizard**, or after installation by making changes on the **System Configuration** page of the device.

With this release, the **Devices** page is refreshed automatically every two minutes to reflect the new status of the devices and statistics.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. Select a device and click **Configure**.
3. Change parameters on the **System Configuration** page.
4. Click **Update** after each change is made.

Back up McAfee DLP systems

Back up McAfee DLP systems regularly so they can be restored, if necessary. Maintain a backup archive to ensure that configuration files, users, logs and cases are not lost during daily system operations.

Depending on the volume of data to be backed up, processing time might be lengthy.

> After 30 days or 150,000 incidents, the oldest incidents are lost, and if a managed mode device is deregistered, all incidents are lost. Backing up whenever there is a change in content or configuration is recommended.

Archive contents:

- Active configuration files (policies, rules, action rules, concepts, templates, network and content capture filters, DHCP settings, schedules, task definitions and credentials)
- Local and Active Directory users
- Network settings
- User Action Logs
- Cases

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Backup**.
2. Enter the **Remote Host Name** of an external storage device.

   Only Linux devices are supported. Microsoft Windows computers have not been tested.
3. Enter the **User Name** and **Password** required to log on to that machine.
4. **Browse** to the directory (**Location**) that will receive the backup.
5. Select the **Port** to be used to connect to the remote host.
6. Click **Backup**.

   Click **Refresh File List** and select the archive with the latest date and highest backup number. You will be able to verify the build number after extraction. The local archive filename will be made up of a date and backup number (for example, 20091030-1346). But on the Remote Host and other McAfee DLP devices, the filename will also include the FQHN (fully-qualified host name) and device type (inSight = Manager, iGuard = Monitor), followed by `<date_backup#>.tar`.

   When the process is complete, email is sent to the address in the user's profile, and the file list is populated with the name of the new archive.

FQDN filename example

```
abc-123.lab.company.net-inSight-20091030-1346.tar
```

Restart McAfee DLP appliances or services

Restart, shut down or reboot McAfee DLP appliances to clear problems.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. In the **Advanced** column, click **More** for a specific device.
3. Scroll down to **Restart/Shutdown**.
4. Click either the **Restart console server**, **Reboot device**, or **Power-down device** command.

Unregister McAfee DLP devices

Unregister McAfee DLP devices if you need to re-synchronize a timed-out system, overwrite an older configuration, or register a device to a different McAfee DLP Manager.

> If the device is to be reconfigured as a standalone system, you must reinstall it.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. In the **Advanced** column, click **More** for a specific device.
3. Scroll down to the **Restart/Shutdown** section and select **De-register device**.
4. Click **OK** or **Cancel**.

   Because the messaging service must be restarted whenever a device is deregistered, you might get a logon error message like "could not connect to service" before you can log on again. If so, the messaging service will generally be back up in 1-3 minutes.
5. Confirm that the deregistered device has been removed from the list on the **Devices** page.

Change link speed

Change link speed if devices installed on the network have specific speed and duplexing requirements. McAfee DLP Monitor might not be able to auto-negotiate traffic to capture interfaces.

> Depending on your network configuration, you might have to replace your standard Ethernet cable with one that is appropriate for your network.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. Select a device from the list.
3. Click **Configure**.
4. In the **Capture Interfaces** section, select link speeds for each capture interface from the **Speed and Duplex** menus.
5. Click **Update**.

   A notification message appears to verify the change.

Setting wiping policies

Wiping policies set the standard for usage of disk space on the McAfee DLP appliances. You can wipe captured data depending on how much space is used, or at fixed time intervals.

Wiping policies are set on the **System Configuration** page, which is accessible from the **Configure** link of each registered device.

Wiping policy types

Space-based wiping is the default policy. It erases the earliest results after 80% of the disk is used. When that threshold is reached, the system erases data to the 70% watermark.

Time-based wiping is configurable from 30 to 180 days.

Manage McAfee DLP appliance disk space

McAfee DLP appliance disk space varies from 0.5 to 10TB, depending on whether legacy or Intel appliances are used, and the configuration of each device. You can determine disk space by retrieving disk usage information on the appliances registered to McAfee DLP Manager.

The Reconnex file system (RFS) divides the McAfee DLP Monitor disk into partitions. Capture partitions hold all the content captured, which is organized by type. Non-capture partitions contain the operating system and the results partitions (A-Z), which fill sequentially.

The capacity of the capture partitions in the Intel Server System SR2612SR is 7.2TB (across 12 disks).

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. In the **Advanced** column, click **More** for a specific device.
3. Scroll down to **Application Information**.
4. Click **Disk usage**.

   The `show_rfs_df` command runs, and the results are displayed on the page that opens.

Servers and DLP

Systems that are deploying McAfee Total Protection for Data Loss Prevention support several types of servers that extend their functionality. Enterprise DLP configurations usually have DHCP, DNS, and Active Directory services configured, as well as connections to mail, NTP, and syslog servers. If Active Directory servers are used, McAfee Logon Collector can be used to extend DLP functionality by resolving the identities of specific users.

Server connections can be made from the native DLP Manager interface, or through ePolicy Orchestrator. If the applications are set up to work through ePolicy Orchestrator, a DLP Host server and McAfee Agent will also have to be installed.

- Adding a DHCP server supports accurate resolution of the sources and destinations of network transmissions.
- Adding an LDAP server supports integration with existing user systems, enables notification of users, and authenticates user accounts. DLP supports Microsoft Active Directory LDAP services.
- McAfee Logon Collector can be configured with DLP Manager to resolve user identities by retrieving collections of user account information from all Active Directory servers that have been added to the DLP system.
- Adding a Host DLP server supports integration with McAfee ePO.
- Syslog servers receive DLP error messages.
- NTP servers make it possible to synchronize DLP systems.

Contents

Adding DHCP servers to DLP systems

DLP systems can accurately resolve the sources and destination of network transmissions by using DHCP (Dynamic Host Configuration Protocol) services. A DHCP server might be added to the system to provide those services.

Senders and recipients can be easily identified if they have static IP addresses, but dynamic addresses are more commonly used. Because they change frequently, it is often difficult to pinpoint the sources and destinations of transmissions.

DHCP servers automatically assign IP addresses from an appropriate pool to the clients connecting to the system. The server then extracts, parses and loads log files to resolve the address to a host name, and the information is passed along to the DLP system.

> If McAfee Logon Collector is used with an Active Directory server, user mapping returns better results.

Add DHCP servers to DLP systems

Add DHCP (Dynamic Host Configuration Protocol) servers to DLP systems to provide accurate location information about incidents that have been identified by DLP systems. If there is no Active Directory server, DLP processes query the DHCP server to map IP addresses to users.

DHCP servers are used by most ISPs (Internet Service Providers) to assign dynamic addresses to the hosts they administer. Because dynamic addresses expire at specified times, hosts using them can be tracked only through DHCP server records.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **DHCP Servers**.
2. Select **Actions** | **Add DHCP**.
3. Enter a name for the server and an optional description.
4. Select the **Server Type**.

   Internet Systems Consortium, Solaris and Microsoft Windows types are supported.
5. Select an **Access Mode** to retrieve directory information, get and put log files, and perform related transfer tasks.

   The access mode determines the method of transfer. SMBClient access mode is supported only for Windows Server.
6. Enter the **IP Address/Name**, **Username**, and **Password** to log on to the server.
7. Enter the **Folder/Share** name, if needed.
8. Add the **File Name/Pattern** to enable DHCP logging.

   The DHCP log file name depends on the DHCP server operating system. `DhcpSrvLog` is a Windows file name pattern. Use `dhcpd*` for ISC and Solaris DHCP logs (`dhcpd.leases`).

   Matching this pattern enables DHCP logging. For the SMB client, `mget DhcpSrvLog*` can be used from the SMB prompt to link to Windows files such as `DhcpSrvLog-Wed.log` or `DhcpSrvLog-Sun.log` . For SCP or SFTP, use `/var/state/dhcp/dhcpd.leases` or `/var/state/dhcp/dhcpd*`.
9. Set the **Frequency** to indicate how often the server should be polled to pull down new information.
10. Select the checkboxes of devices to be connected to the DHCP server.
11. Click **Save**.

Adding directory servers to DLP systems

DLP products use LDAP services to integrate with existing user systems, authenticate user accounts, extend notification to users by role, and support other objects that might be imported from an LDAP server. LDAP servers are needed to support those functions.

Microsoft Active Directory and OpenLDAP servers are supported.

Importing multiple user accounts is a common task that is enabled by adding directory servers to DLP Manager. If customized attributes are added to the directory database, the information in those fields will automatically populate the default user fields on the DLP dashboards.

> LDAP users must be assigned to existing groups. If you have not yet decided on a user group design, review user group management.

Contents

Add Active Directory servers

Active Directory or OpenLDAP servers must be added to support integration with existing user systems. After the server is configured and users are added, significant incidents can be detected through the user accounts on the servers.

> More than one directory server can be added to DLP, but they must be of the same type. If an Active Directory server is added, you cannot also add an OpenLDAP directory server.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Directory Services**.

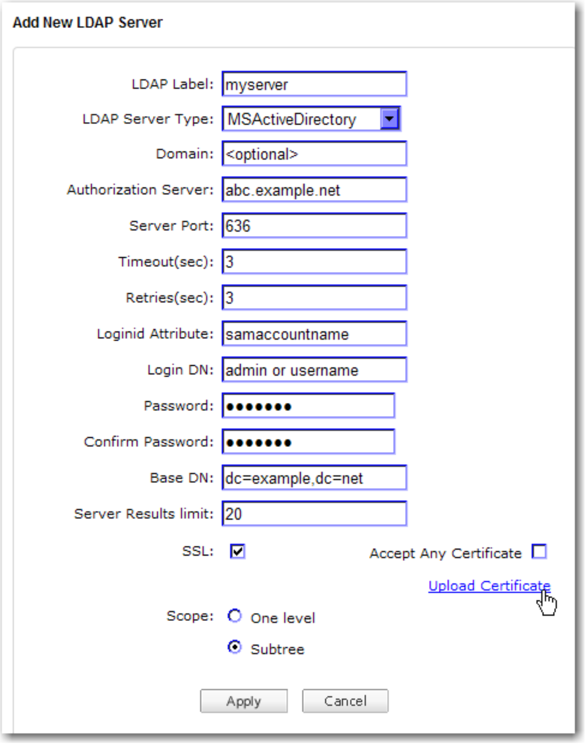
2. Select **Actions** | **Create Directory Server**.

3. Enter a label to identify the LDAP server.

4 Do one of the following:

- Enter the **Domain** of the LDAP server.

  If you use this option, you must log on to an administrative account on the LDAP server. The system will then query the Domain Name Server to find the domain controller for the Active Directory domain.



Add New LDAP Server

LDAP Label:	myserver
LDAP Server Type:	MSActiveDirectory
Domain:	<optional>
Authorization Server:	abc.example.net
Server Port:	636
Timeout(sec):	3
Retries(sec):	3
Loginid Attribute:	samaccountname
Login DN:	admin or username
Password:	•••••••
Confirm Password:	•••••••
Base DN:	dc=example,dc=net
Server Results limit:	20
SSL:	☑
Accept Any Certificate	□

Figure 12-1 Add New LDAP

- Enter the name or IP address of the **Authorization Server**.

  If you are using SSL (Secure Sockets Layer) to encrypt the connection, you must enter the FQDN (fully qualified domain name) cited in the uploaded certificate.

  Unlike the LDAP server domain name, you can use any valid account that has permission to read from the LDAP server (an administrative account is not necessary). If you have already entered the domain name of the LDAP server, any information you enter here will be ignored.

5 Enter the **Server Port** to be used for the connection.

6 Set intervals for connection **Timeout** and **Retries** (in seconds).

7 Enter the **Loginid Attribute**.

Use `samaccountname` to retrieve user names from the server.

8 Enter the user name (**Login DN**) and **Password**.

9 Identify the local domain components in the **Base DN** field (for example, `dc=mydomain,dc=com`).

Use an administrative account whose password does not expire to maintain the connection, but a non-administrative account name is acceptable when using an authorization server.

10 Enter the number of records you want to retrieve at one time in the **Server Results limit** field.

Before entering a value higher than 10, consult the administrator of the Active Directory server to find out how many records can be served per request.

11 Select the **SSL** checkbox to encrypt the connection and enable LDAPS (LDAP over SSL).

A secure connection is not required, but is strongly recommended. Accept any available certificate, or select one by uploading it. If you upload, you must find the FQDN name of the authorization server in the encrypted file by logging on to the back end of the McAfee DLP appliance and running the following.

```
# openssl x509 -noout -in <filename>.cer -subject
```

The FQDN will be returned in reverse order:

```
subject= /DC=net/DC=reconnex/CN=tyche
```

Read from left to right to get the name of the authorization server:

```
tyche.reconnex.net
```

Enter the name into the **Authorization Server** field.

12 Select a **Scope** to set the directory depth to be accessed on the server.

13 Click **Apply**.

Configure Active Directory servers

Configure Active Directory servers by installing the LDAP RWL (Real World Locality) client, which works with directory services to enable retrieval of all LDAP data.

> The RWL client must be configured before LDAP functions can be utilized.

Task

1 Log on to McAfee DLP Manager.

2 Get the integration files by typing the file location into the browser address bar.

`https://<DLP_address>/activedir/ADintegration.zip`

3 Save the file to your desktop and extract the two files in the archive to your desktop.

4 On the Windows server desktop, click **Start** | **Administrative Tools** | **Active Directory Users and Computers**.

5 In the navigation bar, right-click the domain name and select **Properties** | **Group Policy** | **Default Domain Policy** from the pop-up menu

6 Select **Edit**.

7 Under **User Configuration**, select **Windows Settings** | **Scripts** | **Logon**.

8 In the Scripts tab, click **Show Files**.

9 Drag the `rwl_client.exe` and `logon.bat` files from your desktop to the **Group Policy Object Editor** window.

10 Right-click the `logon.bat` file and select **Edit** | **Run** from the pop-up menu.

11 After `rwl_client.exe`, enter the IP address of the DLP Manager or Monitor (if you are on a standalone system).

When the batch file gets executed, DLP Monitor is notified that a user has logged on.

```
REM Substitute the following 'hostname.example.org' argument
REM with the hostname or IP address of your Monitor
rwl_client.exe iGuardHostname.reconnex.net
```

12 Click **Save**.

13 Close the window containing the `rwl_client.exe` and `logon.bat` files.

14 Click **OK** on the **Scripts** tab of the **Logon Properties** dialog box.

15 Close the **Group Policy Object Editor** window.

16 Click **OK** on the **Group Policy** tab of the reconnex.net **Properties** dialog box.

17 Close the **Active Directory Users and Computers** window.

18 Register the server to DLP Manager.

Add Active Directory users

Add LDAP users from Active Directory or OpenLDAP servers, which must first be added to a DLP system to support integration with existing user systems. After the server is configured and users are added, significant incidents can be detected through the user accounts on the servers.

> LDAP users must be assigned to existing groups. If you have not yet decided on a user group design, review user group management.

Task

1 On your Linux-based appliance, select **System** | **User Administration** | **Users**.

2 Click **Actions** | **Create LDAP User**.

3 Select the **LDAP Host**.

4 Retrieve one or more users with one of the following techniques.

User names containing special characters cannot be retrieved.

- Enter an asterisk (*) to retrieve a list of all users on the server.
- Enter a known **Login ID** or **User Name**.
- Use an asterisk (*) as a metacharacter to retrieve related users (for example, R* or *st*).

5 Click **Find**.

6 Select a user from the list.

7 Select one or more groups from the **Available** groups for the new user and **Add** the users to the groups.

8 Click **Apply**.

To make changes to the user's status later, go to **System** | **User Administration** | **Users** and select the **Detail** icon of the user. For example, you can use the **Action** menu to **Disable** or **Delete** the user.

Export certificates from Active Directory servers

Export certificates from Active Directory servers to secure connections to DLP systems.

This task retrieves a certificate from a Microsoft Active Directory server, exports it, and adds it in the McAfee DLP Manager interface.

> By default, LDAP traffic is transmitted unsecured, but using secure LDAP over SSL technology encrypts the connection.

Task

1. Log on as a member of one of the following:
   - the local Administrator security group for standalone computers
   - a member of the Domain Administrator security group for any computers that are connected to the domain.
2. Install the certificate on the Windows server, which will install the server certificate on the Active Directory server.
3. Start the Microsoft Management Console: click**Start** | **Administrative Tools** | **Certificate Authority**.
4. Select the CA system, then right-click and select **Properties**.
5. From the **General** menu, select **View Certificate**.
6. Select the **Details** view.
7. Click **Copy to File** on the lower right corner of the window.
8. Use the **Certificate Export Wizard** to save the CA certificate in one of the following formats:
   - DER Encoded Binary X-509 format
   - Base-64 Encoded X-509 format
9. Verify that SSL is enabled on the Active Directory server:
   - Windows 2000
   - Windows 2003

   a. Ensure that **Windows 2000 Support Tools** (**Windows Support Tools** on Microsoft Windows 2003) is installed on the Active Directory server.

   b. Find the `suptools.msi` setup program in the `\Support\Tools\` directory on your Windows CD.

   c. Start the ldp tool.

   For Microsoft Windows 2000 systems, go to **Start** | **Windows 2000 Support Tools** | **Tools** | **Active Directory Administration Tool**. For Windows 2003, go to **Start** | **Windows Support Tools** | **Tools** | **Command Prompt**.
10. Select **Connection** | **Connect** from the ldp window.
11. Enter the host name and port number (secure port 636 is required).

    If the connection is successful, a window is displayed listing information related to the Active Directory SSL connection. If it is unsuccessful, restart your system and repeat the procedure.

How ADAM servers extend DLP Manager

ADAM (Microsoft Active Directory Application Mode) servers allow DLP to access objects in customized database schemas. Default attribute mappings are modified to recognize the names of equivalent fields in existing LDAP databases.

DLP products enable retrieval of information from Microsoft ADAM servers, making it possible to customize existing attributes to map to DLP settings.

- Use of a Certificate Authority supports secure transmissions through LDAPS or HTTPS. Verification can be disabled by selecting **Accept Any Certificate** when adding the server.

Whenever SSL communication is requested, the host name should be name of the server with domain clearly specified. An IP address will not work.

Default attribute mappings

DLP defaults can be mapped to existing databases with different sets of attributes to customize retrieval of records from LDAP servers. When existing attributes are remapped, incidents reported to the dashboard contain the user information found in the corresponding fields on the existing LDAP server.

Use these mappings to customize directory attributes.

Table 12-1 Default Attribute Mappings

Default attribute mapping
UserName=cn
UserID=sAMAccountName
UserTitle=title
UserCompany=company
UserDepartment=department
UserCity=givenName
UserZipcode=postalCode
UserCountry=countryCode
UserManager=manager
UserGroups=memberOf
UserEmail=proxyAddresses

Map LDAP directory attributes

Map LDAP directory attributes to DLP defaults to customize retrieval paths to existing server configurations.

Task

1. On your Linux-based appliance, go to **System** | **DHCP Servers** | **Directory Services**.
2. Click on **Edit**.
3. Enter new attribute names in the **Directory Server Mapping Attributes** fields.
4. Click **Apply**.

Adding McAfee Logon Collector servers to DLP systems

DLP products use McAfee Logon Collector servers to identify remote users definitively.

With McAfee Logon Collector, remote users are identified through SIDS (Security Identifiers) instead of IP addresses, host names, or other user parameters that are subject to change.

Connect McAfee Logon Collector to McAfee DLP Manager

Connect McAfee Logon Collector to McAfee DLP Manager by using certificates to authenticate them to each other. When the process is concluded, an SSL connection is established between the servers.

Task

1. Open a web browser, type the IP address of the McAfee Logon Collector into the address bar, and logon.
2. Go to **Menu** | **Configuration** | **Server Settings** | **Identity Replication Certificate**.
3. Select and copy all text in the **Base 64** field and paste it into a text editor.
4. Add the following beginning and ending lines to the document, then paste in the Base 64 text.

   ```
   -----BEGIN CERTIFICATE-----
   <pasted Base 64 field text>
   -----END CERTIFICATE-----
   ```

5. Highlight and copy the entire text, including the BEGIN and END CERTIFICATE lines.
6. Open a web browser and logon to the Network McAfee DLP Manager.
7. On your Linux-based appliance, select **System** | **System Administration** | **Directory Services**.
8. Select **Actions** | **Create McAfee Logon Collector**.
9. Enter the IP address of the McAfee Logon Collector into the **Export NetDLP Certificate** field.
10. Select the **Paste from Clipboard** option and paste the Base 64 text into the box.

    Alternatively, you can export the certificate from McAfee Logon Collector to your desktop, then **Browse** to it from the **Import MLC Certificate** | **From File** field.

11. Click **Apply**.

    This authenticates the McAfee Logon Collector to McAfee DLP Manager.

12. Click the **Export** link to save the NetDLP certificate to your desktop.

    The file name is `netdlp_certificate.cer`.

13. Open a web browser, enter the IP address of the McAfee Logon Collector in the address bar, and log on.
14. Select **Menu** | **Configuration** | **Trusted CA**.
15. Click **New Authority**.
16. Browse to the `netdlp_certificate.cer` file you saved to your desktop.

17 Click **Open**, then **Save**.

This authenticates the DLP Manager to McAfee Logon Collector.

18 Open a Remote Desktop session on the McAfee Logon Collector server and restart it.

When the server comes up, the SSL connection between the servers is complete.

How McAfee Logon Collector enables user identification

McAfee Logon Collector is used to map IP addresses to user identities within Active Directory servers. Without it, users may be hard to identify because they may be logged into different or multiple workstations. IP addresses change when DHCP servers assign new addresses, and more than one user might be logged on to the same workstation.

When a McAfee Logon Collector is configured with McAfee DLP Manager, it resolves user identities by retrieving collections of user account information from all Active Directory servers that have been added to the DLP system. Supporting multiple domain controllers means that large-scale enterprise operations can be served by McAfee applications.

For McAfee DLP, that means that after McAfee Logon Collector is enabled, DLP administrators can configure Active Directory-based queries and rules to find out what activities specific users are engaging in on the network.

How McAfee DLP uses SIDs

Because McAfee Logon Collector allows DLP to key on SIDs (Security Identifiers) instead of sAMAccountnames, the identities of individual users can be resolved and their traffic can be monitored. By leveraging multiple user attributes, it is now possible to identify end users conclusively, regardless of what email or IP addresses they are using.

When a SID is retrieved from the Active Directory server, all of its associated attributes, such as domain name, location, department and user group, come with it. That collection of information can then be used in rules, templates, action rules, and notifications to find and stop security violations by specific users.

Track IP violations with McAfee Logon Collector and McAfee DLP

Suppose you know that your company has lost intellectual property to a Chinese firm, and you suspect that the leak came from an insider in your Shanghai branch. You can create rule parameters that find the leaked documents and the suspected violator, then monitor his or her activities to build a legal case and prevent any more data loss.

Before you begin

You must have an Active Directory server and McAfee Logon Collector connected to the McAfee DLP system.

You can track down the violation by identifying the information compromised, the recipient of the information, and the suspected user by creating rules with parameters that will pull related information from the directory server.

If you don't know the user's name, you can gradually develop his identity by searching for users in Shanghai, searching the user groups in your Engineering division, and identifying a sub-group that may contain the user. You might not know in advance what you might find, but you can use what you discover to ask the next logical question.

Task

1. Create a new rule.
   1. On your Linux-based appliance, select **Policies** | **Policies**.
   2. Open a suitable policy or create a new one.
   3. Select **Actions** | **Add Rule**.
2. Name the rule, then add **Content** parameters that describe the intellectual property lost.

   You might add keywords, an exact phrase found in the leaked documents, a file type, or a concept that will retrieve similar content.
3. Add **Destination** parameters that describe the recipients of the data.

   You might have an IP addresses, domains, or a geographic locations that will help to define the recipient. When you have finished, click **Save**.
4. After the rule retrieves some results, click the **Details** of an incident or event.

   You might find that a user ID is listed.
5. Click on any link on the **Details** page that provides more information.

   If a user ID or email address is reported, you can add that information to your rule so that you can monitor all of that user's transactions.
6. Edit the rule by adding an action rule (on the **Actions** tab) to block, quarantine, redirect, or notify an administrator of all subsequent activity.

Synchronizing DLP with network devices

DLP uses Network Time Protocol servers and syslog servers to synchronize and troubleshoot its connections to the network.

Correct time in the McAfee DLP Manager interface

Correct time settings in the McAfee DLP Manager interface to re-synchronize with the network.

> This procedure might clear the synchronization error message displayed when logging on. If this doesn't work, log on to the back end as root and reset the time from the McAfee DLP Monitor command line.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. Click the **Configure** link for a specific device.
3. Scroll down to **Time** and select **Manual**.
4. Enter the correct date and time.
5. Click **Update**. **Logout** of McAfee DLP Manager, then log on again.

Synchronize McAfee DLP devices with NTP servers

Synchronize McAfee DLP devices with network time servers if they lose their connections to the network.

Use this task to re-synchronize McAfee DLP device time with your desktop.

> This is one way to clear a system time error that might prevent you from logging on.

Task

1 Open the **Date/Time** display on a Windows desktop.

2 Adjust local time to Greenwich Mean Time.

3 Log on as root to the McAfee DLP appliance.

4 Type the date - -utc command to enter the correct date and time.

```
 # date --utc MMDDhhmmCCYY
```

5 Type the hardware time command to reset the clock.

```
# hwclock -w
```

6 Type the date command.

```
 # date
```

7 If the correct date is returned, reset Stingray.

```
 # service stingray reset
```

8 Find and kill the current process.

```
# ps -ef | grep java
# kill -9 <process id number>
```

9 Log on again as root to the McAfee DLP appliance.

10 Restart Stingray and reboot the machine.

```
# service Stingray restart
# reboot
```

11 Open a web browser and enter the address of the McAfee DLP appliance in the address bar.

12 Return the Windows clock setting to the correct time zone.

Reset time manually

Reset time manually by stopping and restarting NTP services.

Stop and restart the NTP daemon to manually reset the time.

Task

1 Log on as root to the McAfee DLP appliance.

2 Stop the NTP daemon.

```
# service ntpd stop
# chkconfig --level 2345 ntpd off
```

3 Restart the NTP daemon.

```
# service ntpd start
 # chkconfig --level 2345 ntpd on
```

The service command will control the service while the system is running; the `chkconfig` commands will control what happens at boot time.

Syslog server message structure

Syslog servers are automatically recognized if they reside on the same network as DLP devices; no special connection is needed. If a syslog server is installed on the network, DLP automatically sends messages about significant events in the following format.

The health of the DLP appliances, as well as the rule hits, are automatically transferred to the syslog server.

Table 12-2 Syslog server message definitions

Message field	Definition
Date	Date the event was logged
Host name	Name or IP address of the machine that logged the event
Component	Component or process that generated an alert
Format	Format version of the syslog output
Device vendor	Vendor name
Device product	Manager, Monitor, Discover, Prevent or Endpoint
Device version	Product version
Rule	Search rule
Severity #	Critical, High , Medium, Low, Informational
Policy	Policy name
Policy label	Type of object
Match count	Matches found
Match count label	Type of object
Source IP	Source IP address
Destination IP	Destination IP address
Source Port	Source port
Destination port	Destination port
Source user name	Source user name
Destination name	Destination user name
Email subject	Email subject
File name	File name

Using DLP on remote directory servers

The ability to monitor user traffic on Active Directory servers now has been extended to directory servers, making global user management a reality.

The ability of McAfee Total Protection for Data Loss Prevention to connect to multiple domain controllers makes it possible to capture data on local networks and up to two LDAP servers.

When users can be recognized by name, group, department, city or country, a DLP administrator can extract a great deal of significant information by using a few seminal facts to gradually gather more details about potential violations.

OpenLDAP and Active Directory server differences

McAfee Total Protection for DLP now supports OpenLDAP as well as Active Directory servers.

OpenLDAP and Active Directory produce different user schemas. Active Directory has a constrained set of parameters, but OpenLDAP is completely customizable, so user implementations may vary widely.

OpenLDAP and Active Directory servers identify users by using different means of user identification. Active Directory uses *sAMAccountName*, and OpenLDAP uses *UID*. LDAP queries for sAMAMccountName 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.

How directory server accounts are accessed

Historically, McAfee DLP Manager has been linked to sAMAccountName as the main user identification element. But if that attribute is applied to users in the same domain who have similar or matching user names, they cannot be identified conclusively.

McAfee DLP keys on the unique alphanumeric SID (Security Identifier) that is assigned to each user account by the Windows domain controller.

Because McAfee Logon Collector allows McAfee DLP to key on SIDs (Security Identifiers), the identities of individual users can be resolved and their traffic can be monitored. By leveraging multiple user attributes, it is now possible to identify end users precisely, regardless of what email or IP addresses they are using.

When a SID is retrieved from the Active Directory server, all of its associated attributes, such as domain name, location, department and user group, come with it. That collection of information can then be used in rules, templates, action rules, and notifications to find and stop security violations by specific users.

For example, the user name jsmith may belong to John Smith or Jack Smith, so more information would be needed to distinguish between those two users. They may even be using the same IP address, which would amplify the problem of discovering the identity of the actual user.

Each account on an Active Directory server is made up of attributes that identify the individual who owns the account. McAfee Logon Collector matches the unique SIDs that are assigned to each Active Directory user to IP addresses, and all of the parameters associated with that SID are extracted when MLC moves binding updates from the Active Directory server to McAfee DLP.

> Because sAMAccountName was used to index data in earlier releases, that information may be lost during ad hoc searches when the user upgraded, or the data residing in the capture database pre-dates the upgrade.

How directory servers are used with DLP systems

If a directory server is added to McAfee Data Loss Prevention Manager, DLP can use the data on the server to identify remote users and manage their data.

Directory servers enable enterprise users to locate users through their logins, email or IP addresses, or by compound rules that combine user logins with locations or affiliations.

How remote user accounts are monitored

Historically, DLP Manager has been linked to sAMAccountName as the main user identification element. But if that attribute is applied to users in the same domain who have similar or matching user names, they cannot be positively identified.

McAfee Total Protection for Data Loss Prevention now keys on the unique alphanumeric SID (Security Identifier) that is assigned to each user account by the Windows domain controller.

For example, the user name `jsmith` may belong to John Smith or Jack Smith, so more information would be needed to distinguish between those two users. Those individuals may even be using the same IP address, which would aggravate the problem of discovering the identity of the actual user.

But each account on an Active Directory server is made up of attributes that identify the individual who owns the account. McAfee Logon Collector matches the unique SIDs that are assigned to each Active Directory user to IP addresses, and all of the parameters associated with that SID are extracted when MLC moves binding updates from the Active Directory server to DLP.

> Because sAMAccountName was used to index data in earlier releases, that information may be lost during ad hoc searches when the user has upgraded, or when the data residing in the capture database pre-dates the upgrade.

Monitoring LDAP users

The ability to monitor user traffic on LDAP servers has extended the reach of McAfee DLPtools to directory servers used by enterprise-sized organizations. Connections through multiple domain controllers makes this possible.

Data on local networks is captured and the software extends this capability to all traffic on up to two remote LDAP servers.

When users can be recognized by name, group, department, city or country, a DLP administrator can extract a great deal of significant information by using what little information is known about those users to gradually gather more details about a potential threat.

For example, suppose you know that your company has lost intellectual property to a Chinese firm, and you suspect that the leak came from an insider in your Shanghai branch.

Because McAfee DLP Monitor captures all traffic on your company's network, you can add an Active Directory server that contains the user account of that insider to McAfee DLP Manager, then search for the UserName of that individual and monitor his communications.

You might then search his communications for the name of the lost component, then find the email address and geographical location of users outside the company who may have received the information. You might not know what will be in those communications, but you can use what you find to form the next question.

Using Active Directory attributes

Active Directory attributes can be used for queries and rules, but incidents that are reported on the dashboard may have more objects available in the database. That information can be viewed by adding columns that can display those fields.

All Active Directory elements are treated as word queries, and can be directed to specific LDAP servers. When Active Directory elements are used in a query, columns supporting the parameter are configured in the search popup and on the dashboard.

Each of the user elements retrieves the following attributes.

- User Name: user's name, alias, department, location
- User Groups: user's group
- User City: user's city
- User Country: user's country
- User Organization: user's company or organization

Viewing Active Directory incidents

All Active Directory incidents are reported to the dashboard.

When Active Directory elements are used in a query, columns supporting the parameter are configured in the search popup and on the dashboard.

When you get results from querying a directory server, you can view them on the **Data-in-Motion** dashboard or the corresponding ePolicy Orchestrator dashboard. Clicking the **Columns** icon will show you what other data categories are available for display.

Not all of these parameters can be used for queries. This accounts for the disparity of data categories on search and rule pages.

Search for user attributes in LDAP data

If a directory server is registered to McAfee DLP Manager, you can search the imported data to find incidents by keying on user attributes.
Directory server data can be searched by source or destination IP and/or port.

Use **Basic Search** to do exploratory searches, and **Advanced Search** to create complex searches or rules.

Task

1 On your Linux-based appliance, select **Capture**.

2 Click either **Basic Search** or **Advanced Search**.

3 From the **Basic Search** | **Input Type** or **Advanced Search** | **Source/Destination** menu, select a user attribute.

4 Click **Search** or **Save as Rule**.

Find user attributes in LDAP data

If a directory server is registered to McAfee DLP Manager, you can use the imported data to find incidents by keying on the user attributes.

Before you begin

One or more dashboards must display incidents retrieved from a directory server attached to the McAfee DLP system.

Use the filtering process to locate user attributes in dashboard results.

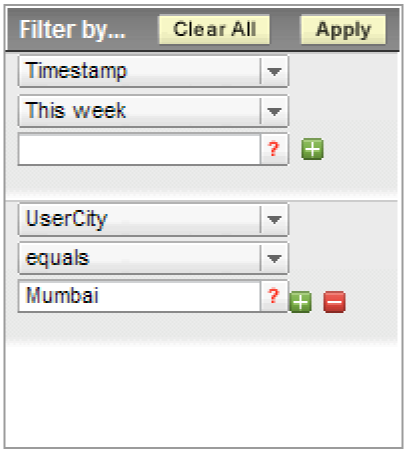


Figure 12-2 Filter for user attributes

> Before filtering, add columns to the dashboard to display the user attribute results you are looking for.

Task

1. Select **Incidents** | **Incidents**.
2. At the top of the **Incidents** page, select a vector: **Data-in-Motion**, **Data-at-Rest**, or **Data-in-Use**.

   These dashboards display incidents or events from McAfee DLP Monitor, McAfee DLP Discover, or McAfee DLP Endpoint, respectively.
3. In the **Filter by** pane, select a time frame.
4. Click the green plus icon to add a filter.
5. From the filter list, select a user attribute from the list.

   If customized attributes are used on the directory server, they must be mapped to those in this list.
6. Select a comparator such as **equals** or **not equal** and enter required information in the value field.
7. Click **Apply**.

LDAP columns available for display

The columns available reflect the scope of data available. Not all of these parameters can be used for searching captured data or implementing rules. In an ad hoc search, some Active Directory attributes (user names, companies, email, managers, titles) are not displayed.

There are many more columns available than there are searchable network elements. They were added to the interface to accommodate Host DLP. You can use them to display additional attributes that are reported, but not displayed by default.

The following columns are available.

- User Custom
- UserCity
- UserCompany
- UserCountry
- UserManager
- UserName
- UserGroup
- UserOrganization

- UserEmail
- UserGroups
- UserID
- Network printer
- Network path
- Location Tag Path

Add columns to display user attributes

Add columns to display the relevant user attributes that were retrieved from your directory server.

The columns available reflect the scope of data that might be available on the directory server. Not all of these parameters can be used for searching captured data or implementing rules. In an ad hoc search, some attributes (user names, companies, email, managers, titles) may not be displayed.

Task

1. Select **Incidents** | **Incidents**.
2. Click **Columns**.
3. From the **Available** list, select the relevant user attributes.

   If customized attributes are used on the directory server, they must be mapped to those in this list.
4. Click **Add** to move them to the **Selected** box.
5. Select the navigation buttons to determine the placement of the user attributes in the dashboard display.
6. Click **Apply**.

Installing McAfee DLP on ePolicy Orchestrator

McAfee DLP products can be installed as a frame-in on ePolicy Orchestrator 4.5 or 4.6 servers. For instructions, download the McAfee Installation Guide for McAfee DLP on ePolicy Orchestrator for the appropriate version from the ServicePortal.

If the ePolicy Orchestrator server loses connection to the database, you cannot use `https://servername:port/core/config` to reconnect to the database. Refer to KB66320 in the McAfee Knowledgebase for more information.

Create ePolicy Orchestrator database users

Create ePolicy Orchestrator database users to authenticate connections from McAfee DLP Manager to ePolicy Orchestrator servers. ePolicy Orchestrator servers are Windows-based, but a McAfee DLP Manager is a Linux servers that doe not support Windows-based authentication of users. Database user accounts are used to make the connection.

> Creating an ePolicy Orchestrator database user is only one aspect of establishing a connection to the ePolicy Orchestrator server, which is required to support McAfee DLP Endpoint features. Consult *Installing McAfee Host and Network Data Loss Prevention on ePolicy Orchestrator* for more information.

Task

1. On your Linux-based appliance, select **System** | **User Administration** | **DB User**.
2. On the **ePO User Information** page, enter and confirm a password.

   The ePolicy Orchestrator **User Name** is not configurable.

3. Type an **IP Address** for the ePolicy Orchestrator user's account and **Add** it to the **Selected IP Addresses** box.

   Repeat if more than one ePolicy Orchestrator user is needed.
4. Click **Apply**.

Add a McAfee DLP Endpoint evidence server

Add an evidence server to support reporting of endpoint events to McAfee DLP dashboards. Transmission of the events found by the McAfee Agent depends on the connection between McAfee DLP Manager and the evidence server, where the database of events resides.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. Select **Actions** | **New Evidence Server**.
3. Type the **Hostname**, **IP Address**, **Username** and **Password** in the value fields.
4. Click **Add**.
5. Wait for the **Status** icon to turn green.

   If registration seems to be taking a long time, try refreshing the page.

Managing the Intel server system

With this release, Simple Network Management Protocol is supported, making it possible to manage the Intel server system efficiently.

The Intel server system polls the conditions of the network devices, receives traps from the SNMP agent, and reports anomalies.

Conditions monitored include the following:

- Loss or removal of hard drives from the DLP appliances
- Failure of the system fan
- Loss of one of the redundant power units
- Disk usage exceeds the threshold
- Memory usage exceeds the threshold
- CPU usage exceeds the threshold
- System temperature exceeds the threshold

Configure SNMP Traps

You can configure the traps that are received from the SNMP agent when the network devices are polled.

SNMP traps are thresholds that trigger notifications when they are detected by monitoring of the McAfee DLP system.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Devices**.
2. Select a device from the list.

3. Click **Configure**.
4. Scroll down to the **SNMP Trap Configuration section.**
5. Complete the settings in the section.
6. Click **Update**.

   A notification message appears to verify the change.

Using network statistics

The **Network Statistics** page displays status information on all of the data captured on your McAfee DLP devices, including traffic and other relevant systems data. If you have system administrators' permissions, you can view this page and reconfigure the views to reveal significant patterns.

Each of the statistical panes contains a different type of data, and clicking on the **Details** icons gives access to more granular results. For example, you might want to know how much data one of your managed appliances captures in a specific period of time, how much *Yahoo_Chat* traffic there is on the network, or what percentage of the captured data consists of office documents. The graphical views on the page reveal answers to those questions and more at a glance.

> In this release, network statistics are available only on **Data in Motion** devices (McAfee DLP Monitor, McAfee DLP Prevent).

Types of network statistics

Network statistics are generated as the data is collected, analyzed and displayed. They are useful for getting a comprehensive picture of your McAfee DLP systems.

Network statistics are summarized in three related analysis views:

- Protocol summary
- Content summary
- Source/Destination Summary

Click the **Details** icon in the head of each view for more information.

Filter network statistics

Network statistics can be filtered like any other data reported to McAfee DLP dashboards.

Use the **Filter by** and **Order by** menus to configure network statistics.

With the **Filter by** options, you can examine results on one or more registered devices within specific time ranges.

- Devices
- Time ranges

With the **Order by** menu, you can examine the results being returned from the systems within specific time ranges:

- Time Trend (Hourly, weekly, etc.
- Counter Trend (Incidents, Size, Count).

Setting up system alerts

Device down alerts notify administrators at defined intervals whenever McAfee DLP appliances go down and come back up.

If you have a syslog server, system events are regularly reported to the events database. The database is polled every 2 minutes, and every alert in the database is sent to the dashboard within this interval.

A timestamp is reported for each alert.

Types of device down alerts

Three device down alert types can be used to notify administrators that there might be a problem with McAfee DLP appliances.

Device down alerts can be customized depending on timing and intervals.

- Notification that the device has recovered and has been up for X minutes
- Notification that the device was down for X minutes
- Notification is sent every X minutes after the device went down

Configure device down alerts

Configure device down alerts to notify administrators when McAfee DLP appliances go down. The software sends notification about whether the devices are disconnected or just turned off.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **System Alerts**.
2. Enter the email addresses of the users to be notified.

   Up to 25 email addresses are supported.
3. Select the alert types to be sent.
4. Click **Apply**.

Technical specifications

McAfee DLP appliances meet all safety and operational standards and are in compliance with FCC standards.

McAfee DLP rack mounting requirements

McAfee DLP hardware must be rack-mounted properly to ensure safe configuration.

Elevated Operating Ambient Temperature

If installed in a closed or multi-unit rack assembly, the operating ambient temperature of the rack environment may be greater than room ambient. Therefore, consideration should be given to installing the equipment in an environment compatible with the MAT (maximum ambient temperature) specified by the manufacturer.

Reduced Air Flow

Installation of the equipment in a rack should be such that the amount of air flow required for safe operation of the equipment is not compromised.

Mechanical Loading

Mounting of the equipment in the rack should be such that a hazardous condition is not created due to uneven mechanical loading.

Circuit Overloading

Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of the circuits might have on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings should be used when addressing this concern.

Reliable Earthing

Reliable earthing of rack-mounted equipment should be maintained. Particular attention should be given to supply connections other than direct connections to the branch circuit (use of power strips).

McAfee DLP power redundancy

McAfee DLP appliances with more than one power supply must be configured to provide redundancy by sharing the load while operating at nominal power. Additional protection is provided if two electrical outlets that are on different circuit breakers are used.

Should one power supply fail, a back-up fan automatically turns on, an alarm sounds and a warning LED is illuminated. If this occurs, contact McAfee for a replacement unit.

ℹ If a McAfee DLP appliance loses power for any reason, it will not come back up unless you change the BIOS setting in advance. The motherboard is set to **off** by default.

McAfee DLP FCC compliance

McAfee DLP hardware has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 16 of the Federal Communications Commission rules. Any modifications to McAfee DLP equipment, unless expressly approved by the party responsible for compliance, could void authority to operate the equipment.

Operation of the McAfee DLP appliances is subject to the following conditions:

- The device may not cause harmful interference, and
- The device must accept any interference received, including interference that may cause unwanted operation.

These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment.

McAfee DLP equipment generates, uses, and can radiate radio frequency energy. If not installed and used in accordance with the instruction manual, it might cause harmful interference to radio communications. If operation of this equipment in a residential area causes harmful interference, it must be corrected at owner expense.

McAfee DLP safety compliance guidelines

McAfee DLP appliances must be operated in compliance within strict safety guidelines.

McAfee DLP hardware must be installed only in **Restricted Access** locations (dedicated equipment rooms, electrical closets, or the like).

❗ Disconnect all power supply cords before servicing. There is a RISK OF EXPLOSION if a battery is replaced by an incorrect type. Dispose of used batteries according to industry standards.

Users and groups

McAfee DLP is based on the Role-Based Access Control (RBAC) system, which is used to assign access to users based on the privileges they need to do their jobs. Users inherit their privileges from group membership.

The primary administrator of a McAfee DLP Manager has all privileges needed to grant access to users and groups, and can assign those rights to other administrators. They may also create failover accounts to allow access if a system component goes down.

Because all content is indexed, a capture filter can be used to filter out large portions of network traffic that do not need to be analyzed by the capture engine.

Administrators can create system or ePolicy Orchestrator database users locally on McAfee DLP Manager, or their accounts can be imported from LDAP servers. They must be associated with groups to acquire privileges.

Administrators can assign users to the role-based groups installed on McAfee DLP Manager, customize those groups, or add new groups.

Administrators can also audit user activity, save user logs, or customize their logins and passwords.

Contents

Managing user accounts

User account types can be reconfigured to assign different privileges, customize login and password settings, or change the account type.

Administrators can customize login and password settings for local users, configure different types of administrator account, or add configure failover accounts if needed.

Configure primary administrator accounts

Configure additional administrator accounts if you are the primary administrator. Do this immediately after the first login to preserve the integrity of the default account.

> Primary administrators have complete access to all task and policy permissions and are responsible for creating users and custom user groups. Dividing responsibilities by allocating specific tasks to additional administrators is recommended.

Task

1. Select **System** | **User Administration** | **Groups**.
2. Click the **Details** icon of the **Administrator** group.
3. Edit the **Group Name**, **Description**, and **Email** address as required.
4. From the **Available Users** menu, select the users to be added to the group.
5. Click **Apply**.

Configure failover accounts

Configure failover accounts to allow back door access to McAfee DLP Monitor if McAfee DLP Manager goes down. Failover accounts are disabled by default because if the link between McAfee DLP Manager and McAfee DLP Monitor is open, the default failover account could be used to logon to the system.

Task

1. Select **System** | **User Administration** | **Failover Account**.
2. Type a **Login ID** for the failover account administrator.
3. Type a **Password** for the failover account administrator.
4. Set **Allow Login** to **On**.
5. Click **Update**.

Customize login settings

Customize login settings to discourage unauthorized logins. Lockout is disabled by default, but should be enabled to prevent cracking attempts.

Task

1. Select **System** | **User Administration** | **User Settings**.
2. Select the **Enable lockout** box.
3. Enter the **Maximum number of failed attempts** to be allowed.
4. Set the **Mode of disabling lockout** to `Automatic` or `Manual`.
5. Set the time frame (in minutes) to reset login for locked-out users.
6. Click **Submit**.

Customize password settings

Customize password settings to discourage unauthorized logins. Lockout is disabled by default, but should be enabled to prevent cracking attempts.

Task

1. Select **System** | **User Administration** | **User Settings**.
2. Type the minimum and maximum length of characters allowed for passwords.
3. Type the minimum number of upper- and lowercase alphabetic, numeric and special characters to be allowed.
4. Click **Submit**.

Managing user groups

McAfee DLP systems user Role-Based Access Control (RBAC) to match the rights of individual users to their roles, which are defined by user group permissions.

Administrators can utilize the default pre-configured groups, edit them, or create new groups as needed.

Add user groups

Add user groups to define user roles, and assign users to the groups that correspond to their organization tasks.

> It is not necessary to create a group before adding a user.

Task

1. Select **System** | **User Administration** | **Groups**.
2. Select **Actions** | **Create New Group**.

   Alternatively, select **Details** and rename a pre-configured group.
3. Enter a **Group Name** and optional **Description**.
4. Enter an **Email** address for the group.
5. From the **Available Users** box, select users and **Add** them to the **Current Members** box.

   Remove or **Remove All** users as needed.
6. Click **Apply**.
7. Click the **Task Permissions** tab, open each category, and select the check boxes of task permissions to be assigned to the group.

   View Dashboard permission is required to see the **Incidents** dashboard; **Execute** Policy Permission is also required for that task.
8. Click **Apply**.
9. Click the **Policy Permissions** tab, open the **Policies** category, and select the check boxes of permissions for each policy to be assigned to the group.

   Minimum permissions for policies are **View** and **Execute**. Others will not be available to group users unless these two boxes are checked.

   Consider selecting the **Delete Policy** column header to keep users from deleting policies.
10. Click **Apply**.

Delete user groups

Delete user groups that are not needed or no longer useful. Only administrators can delete user groups.

Task

1. On your Linux-based appliance, select **System** | **User Administration** | **Groups**.
2. Click the **Details** icon of the group to be deleted.
3. By the **Action** | **Delete**field, click **Go**.
4. Click **OK** to delete or **Cancel**.

Setting permissions

Permissions are assigned through group membership. Administrators can customize group permissions by adding specific policy and task permissions that individuals need to perform their tasks.

Assign task and policy permissions

All user rights are inherited from group affiliations. Assign permissions to individual users by adding them to the appropriate groups.

> If group permissions are modified, all of its members will have to log out and re-login.

Task

1. Select **System** | **User Administration** | **Groups**.
2. Click the **Details** icon of a group.
3. Click the **Task Permissions** tab, open each category, and select the check boxes of task permissions to be assigned to the group.
4. Click **Apply**.
5. Click the **Policy Permissions** tab, open the **Policies** category, and select the check boxes of permissionsfor each policy to be assigned to the group.
6. Click **Apply**.

Assign incident permissions

In a role-based access control systems, not all users should have privileges to view all types of incidents produced by the DLP system.

For example, as a member of the group responsible for reviewing evidence of non-compliance with SOX policy, an accountant might have access only to incidents produced by the rules of that policy.

Task

1. Select **System** | **User Administration** | **Users**.
2. Click the **Details** icon for a user.
3. Click the **Incident Permissions** tab.
4. Click **Add**.
5. Select **Reviewer**, **Rule**, or **Devicename** from the drop-down menu.
6. Select an **equals** or **not equals** condition.
7. Click "?".

   A palette containing the values available for the selection appears.
8. Select one or more value check boxes.
9. Click **Apply**.

Check user permissions

Check user permissions to determine access to McAfee DLP features. Because all rights are inherited from group affiliation, users must determine their group affiliations first.

> This procedure works only if an administrator has given the user's group permission to view permissions.

Task

1. On your Linux-based appliance, select **System** | **User Administration** | **Groups**.
2. Select the **Details** icon of the user's group.
3. Click the **Task Permissions** tab, open each category, and view the boxes of task permissions assigned to the group.
4. Click the **Policy Permissions** tab, open each category, and view the boxes of policy permissions assigned to the group.

Check group incident permissions

Check group incident permissions to determine the dashboards the members of a group can see, and the features they can use.

Task

1. On your Linux-based appliance, select **System** | **User Administration** | **Groups**.
2. Click the **Details** icon of the user's group.
3. Click the **Task Permissions** tab, then open the **Incident Permissions** category and view the permissions assigned to the group.

Monitoring audit logs

Audit logs record all user activity on the McAfee DLP systems. Administrative permissions are required to view the logs.

Audit logs are located on the **User Administration** pages. The log elements can be rearranged by clicking headers, and the **Filter by** feature in the navigation pane can be used to sort the results.

Auditing live users

The Live Users feature records all activity in all live sessions. Administrator permissions are required to view the live user records.

Live user records are available on the **User Administration** | **Live Users** page. The **Session Id** links directly to the records of the users who are logged in.

Audit log actions

All user actions are sorted into categories when they are logged.

Table 12-3 Summary of Audit Log Actions

Category	Actions
Devices	View, add, edit, delete
Statistics	View, view details, view system logs, delete system logs
Alias	Create, modify, delete alias; view alias list
Capture filters	Create, modify, delete, update, apply capture filters; view capture filter list; restore factory defaults
Configuration	Show, modify system configuration; modify IP management
Users and user groups	View, delete user audit logs; view user and use group accounts; add local and LDAP users; add, modify, delete, view, search for users; add, modify, delete user groups; view users group members and group lists
Permissions	View group, task, policy, user permissions; update user and task permissions; view, update failover setup

Table 12-3 Summary of Audit Log Actions *(continued)*

Category	Actions
Servers	View, create, modify, delete, update DHCP and LDAP servers; add LDAP domain
Cases	View cases, view opening of cases
Policies/rules	Create, modify, delete, view policies; export/import policies and rules; view, download exported policies, rules, reports; view runtime, configuration of rules; view policy deployment status and error; view policy schedule
Search	Create, view, schedule, deschedule search; view search list, details, document, object; create document, email, FTP, image search; view search detail
Discover	Fetch, upload, attach file; show, cancel file upload
Summaries	View incident, user, location, risk, network, case summaries
Dashboard	Display, delete, save, create dashboard views; export dashboard
Incidents	Detect view incident annotations, history, attributes, matches; mark incident for deletion, as false positive, as read/unread
Reports	View, create, show reports and scheduled reports
Login	Log on, logout
Statistics/Results	View, delete, modify, who exports files/results, modify results per page
Utilities	View utilities, kernel version, system uptime, application version; show help, view status/version information; show disk capacity; display flow statistics

Generate audit log reports

Generate audit log reports to save them for future reference. Reports are saved in CSV (comma-separated values) format.

Task

1 On your Linux-based appliance, select **System | User Administration | Audit Logs**.

2 Select **Actions | Export as CSV**.

3 Open or save the log.

If Microsoft Excel is installed and you select **Open**, the report will open in spreadsheet format.

Filter audit logs

Filter audit logs to troubleshoot systems that have been changed, or discover patterns in usage.

> Click on the Session ID link of a user to see what actions the user has taken.

Task

1 On your Linux-based appliance, select **System | User Administration | Audit Logs**.

2 Determine which cell in the audit log table will act as the primary key.

3 Click the cell to automatically create a filter in the **Filter by** pane.

The dashboard data immediately changes to reflect the selection.

4 Click **Clear All** in the **Filter by** pane before creating another filter.

Sort audit logs

Sort audit logs to rearrange the entries so that you can discover usage patterns or troubleshoot the system if it has been reconfigured.

Task

1. On your Linux-based appliance, select **System | User Administration | Audit Logs**.
2. Determine which column in the audit log table will act as the primary key.
3. Click a column header to rearrange the log entries.

   For example, you might select the **Timestamp** column header to find out what actions were taken in a specific time frame, or on the **User** column to find out who took those actions.

How capture filters work

McAfee DLP Monitor classifies and analyzes captured objects into three different databases, from which relevant objects can be retrieved.

The capture engine captures and indexes all TCP/IP traffic, breaking it down into content types. Anything that cannot be identified is tagged Unknown Protocol.

Because all content is indexed, a capture filter can be used to filter out large portions of network traffic that do not need to be analyzed by the capture engine.

Filtering network data can cut down on the vast amounts of data captured and analyzed, so it is important to tune the system using capture filters when it is set up.

This not only improves performance, but makes it easier to expose only the most significant data for investigation.

> Under certain circumstances, capture filters can also be used to store critical sessions and applications-level data.

Contents

Filter out traffic using common IP addresses

Filter out portions of traffic using one or more IP addresses that comprise a large portion of your network traffic. Drop or store that data to reveal more significant traffic.

> For example, you may drop specific IP addresses that are well-known within your intranet, a range of addresses, or all addresses on a subnet. These addresses, also known as elements, will be removed from consideration by the capture engine. In addition, you may expand drop all of the sessions containing those elements, or you may opt to store only the metadata defining them.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
2. Click **Create Content Filter**.
3. Enter a **Filter Name** and optional **Filter Description**.
4. Select the devices on which the capture filter is to be deployed.
5. Select a capture filter action.

   For example, you may drop all traffic containing the addresses from the Application or Transport layers, or you may store only the metadata defining the addresses.
6. Open the **Source/Destination** category.
7. Select **IP Address** and add a condition.

   For example, you may define all of the IP addresses, all but the defined addresses, or addresses moving in one direction only.
8. Type one or more IP addresses in the value field.
9. Click **Save**.

How content capture filters work

Content capture filters filter out or store specified types of data that are transmitted on the Application layer (also known as Flow A).

Standard content capture filters perform routine operations on network data to improve McAfee DLP performance and results.

Table 12-4 Standard content capture filters

Content capture filter	Purpose
Ignore binary	Exclude binary files from network traffic
Ignore BMP and GIF images	Exclude BMP and GIF images from network traffic
Ignore crypto	Exclude encrypted data from network traffic
Ignore HTTP GZip responses	Keep compressed files from being opened by the capture engine
Ignore HTTP headers	Keep HTTP header blocks from being captured
Ignore P2P	Keep Peer-to-Peer traffic from being captured
Ignore small JPG images	Excludes insignificant images (smaller than 4 MB) from network traffic
Ignore flow headers	Keeps flow headers from being recognized

How network capture filters work

Network capture filters included with McAfee DLP systems filter data streaming on the Transport Layer to improve performance and isolate significant traffic.

Network capture filters work by eliminating large portions of Transport (Layer 4) traffic. They operate in a cumulative sequence and always terminate in the BASE filter, which stores the configuration.

For example, most businesses are interested in monitoring traffic carried to or from external IP addresses. When the RFC (Request for Comments) 1918 filter is active, IP addresses set aside by IANA (Internet Assigned Numbers Authority) for internal use can be excluded from analysis by the capture engine.

Table 12-5 Standard network capture filters

Network capture filter	Purpose
Ignore RFC 1918	Excludes traffic routed to 10.0.0.0.-10.255.255.255, 172.16.0.0.-172.31.255.255 and 192.168.0.0-192.168.255.255
Ignore HTTP Responses	Excludes program output sent from a server after receiving and interpreting an HTTP Request
Ignore unknown	Excludes traffic using unknown protocols
Ignore SMB	Excludes Session Message Block and Microsoft Basic Input/Output System (NetBIOS) traffic
Ignore SSH	Excludes Secure Shell traffic
Ignore POP	Excludes Post Office Protocol 3 traffic
Ignore IMAP	Excludes Internet Message Access Protocol traffic
Ignore HTTPS	Excludes secure Hypertext Transport Protocol traffic
Ignore LDAP	Excludes Lightweight Directory Access Protocol traffic
Ignore NTLM	Excludes Microsoft New Technology Local Area Network Manager traffic
BASE	Base Configuration filter (opens the system for storage of incoming data)

Types of capture filters

Capture filter types are determined by the layer of the OSI (Open Systems Interconnection) model that is recognized and stored by the capture database.

There are two capture filter types.

- **Content capture filters** filter out specific content types, eliminating significant portions of Application layer data
- **Network capture filters** filter out or store network traffic on the Transport Layer, usually in a specific sequence.

Content capture filters are used to streamline data capture and improve performance. Network capture filters can be used to do more complex tasks, like finding spiders, robots, crawlers, types of webmail, browser versions, and operating systems in use.

Types of capture filter action

Capture filter actions exclude or store large amounts of captured data. The actions available differ, depending on whether the filter is designed to work on the Application or Transport layer.

There are two capture filter action types, and several sub-types that extend the functionality of content and network capture filters.

Content capture filters have three allow administrators to configure the capture engine to drop elements, sessions or store element only metadata.

> For example, if your network has a large cache of video files that you know are not a security threat because you have controlled them with configuration management software, you can set up a filter that drops those elements, saving time and resources for analysis of data at risk. Similarly, if your employees are authorized to send or receive any SMTP content that is processed by your company's mail server, you can drop those communications.

Network capture filters allow administrators to configure the capture engine to ignore or store traffic types.

> For example, if you want to know what kind of data is moving through the network data stream without storing its content, storing metadata allows you to keep incidental information (like the source and destination of the data, data types being transmitted, and protocols being used to transmit it).

Types of content capture filter action

Content capture filter actions drop elements or sessions from network traffic, or store only metadata.

There are three types of content capture filter action.

- **Drop element** keeps a particular type of content from being captured. For example, if your network has a large cache of video files that you know are not a security threat because you have controlled them with configuration management software, you can set up a filter that drops these secure files, saving time and resources for analysis of data at risk.
- **Drop Sessions** filters out sessions containing the defined elements from being captured. For example, if your employees are authorized to send or receive any SMTP content that is processed by your company's mail server, you can drop those communications.
- **Drop element; store metadata only** keeps all content from being captured, but retains all of the attributes that define the objects captured and stored in the database. For example, if you want to know what kind of data is moving through the network data stream without storing its content, storing metadata allows you to keep incidental information (like the source and destination of the data, data types being transmitted, and protocols being used to transmit it).

Types of network capture filter action

Network capture filter actions ignore or store network data, depending on port or protocol used.

There are two types of network capture filter action.

- **Ignore** keeps a particular type of traffic from being captured. For example, you can ignore all web traffic by using HTTP filters, or eliminate authorized email by ignoring traffic using port 25 (SMTP).
- **Store** stores a particular type of network traffic. For example, you can store chat traffic by creating a filter that identifies and keeps data transmitted using AOL_Chat, MSN_Chat, or Yahoo_Chat protocols.

Add content capture filters

Add content capture filters to identify types of Application Layer traffic that can be stored or ignored. After these blocks of data are identified, the capture engine will not capture or parse any of the traffic containing them.

Before you begin

Make a note of the types of Flow A traffic you want the capture engine to store or ignore.

Task

1. Select **System** | **System Administration** | **Capture Filters**.
2. Click **Create Content Filter**.
3. Enter a **Filter Name** and optional **Description**.
4. Select the boxes of the devices to which the capture filter is to be deployed.

   If you want to deploy a capture filter at a later time, select **None**.
5. Select a capture action.
6. Open each category and define parameters that describe the traffic that is to be stored or dropped.
7. Click **Save**.

   The new content capture filter will be saved to the list and returned to the main capture filters page.
8. Test the filter and modify it, if necessary.

Add network capture filters

Add network capture filters to identify types of Transport Layer traffic that can be stored or ignored. After these blocks of data are identified, the capture engine will not capture or parse any of the traffic containing them.

Open the **All** category in the **Network Filter** dialog box. This action either captures or cuts off all traffic, depending on the capture action you select, so that you can observe a limited pool of data before deciding what to filter.

> Designing network capture filters require experimentation because the order in which they are deployed is crucial, but taking the time to streamline the capture process can save a lot of processing time. When a network capture filter is applied to the network data stream, its position in the list indicates its priority. Because the BASE filter instructs the system to store all data that has not been dropped from the data stream, it must always run last.

Task

1. Make a note of the types of traffic you want the capture engine to store or ignore.
2. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
3. Click **Create Network Filter**.
4. Enter a **Filter Name** and optional **Filter Description**.
5. Select a capture action.
6. Select the boxes of the devices to which the capture filter is to be deployed.

   If you want to deploy a capture filter at a later time, select **None**.
7. Open each category and define parameters that describe the traffic that is to be stored or dropped.
8. Click **Save**.

   The new network capture filter will be saved to the list and returned to the main capture filters page.

9. On the capture filters page under **Network Filters**, use the **Priority** arrows to move the new capture filter into the correct position.

   When establishing a sequence for applying network capture filters to the network data stream, remember that changing the order of a single filter might skew your results.

10. Test the filter and modify it, if necessary.

Copy capture filters

If you have two or more McAfee DLP appliances of the same type registered to McAfee DLP Manager, you can copy the entire capture filter configuration of one to another.

Before you begin

Configure capture filters on one of the McAfee DLP appliances you plan to copy.

For example, you might copy capture filters from one McAfee DLP Discover to another, or from one McAfee DLP Monitor to another.

Both appliances must be registered to the same McAfee DLP Manager.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
2. On the list of capture filters, identify the device that you are copying the capture filter configuration to.
3. Click **Add Filter** and select a device from the pop-up.
4. Click **Apply**.

   The device information in the capture filter is updated.

Deploy capture filters

Deploy capture filters on McAfee DLP Monitor devices so that they can be applied to the network data stream. If undeployed, the **None** box will be checked, and the filter will be saved but not run.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
2. From the list of capture filters, select one that is undeployed.

   The default display shows filters by device. To view undeployed filters, change the **Views** to display either all content filters or all network filters.

3. From the **Devices** box, check the device on which you want to install the capture filter.
4. Click **Save**.

View deployed capture filters

View capture filters on the System dashboard to find out which ones are deployed on McAfee DLP Manager or a McAfee DLP Monitor.

If you are using a standalone McAfee DLP Monitor, you will see only the filters deployed on your own machine.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
2. On the list of capture filters, note the name of the system before each group of capture filters.

   Scroll down the page if McAfee DLP Manager is managing more than one McAfee DLP Monitor.

Remove deployed capture filters

Remove deployed capture filters to break their links to specific McAfee DLP devices.

> Capture filters may or may not be deployed when they are created.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
2. Open a capture filter deployed to a device.
3. Select the **None** check box under Devices.
4. Click **Save**.

Reprioritize capture filters

Reprioritize network capture filters to define specific positions on the list of filters. This is necessary because the order in which network capture filters are deployed has a cumulative affect on captured traffic.

Content capture filters do not require priority; they can be listed in any order.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
2. On the list of network capture filters by device, click up and down arrows until the proper order is established.

   Because the BASE filter instructs the system to store all data that has not been dropped from the data stream, it must always run last.
3. Click **Apply**.

Modify capture filters

Modify capture filters by editing their parameters.

The system might take some time to reflect modifications because this affects the action of the capture engine while it is in operation.

Task

1. On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.
2. From the list of capture filters, click the one that you want to modify.

   > To view undeployed capture filters, change the **Views**.
3. On the **Filter** page, edit the parameters of the filter to be modified.
4. Click **Save**.

13 Technical support

Before contacting McAfee technical support, create a tech support package.

Contact technical support

Contact technical support by phone, email, or online.

Table 13-1 Technical Support Options

Technical support option	How to contact
Telephone	(800) 937-2237; (408) 988-3832
Support portal	mysupport.mcafee.com
Email	support@mcafee.com

Create a technical support package

Create a technical support package to give your Technical Support engineer the information needed to troubleshoot your McAfee DLP appliances.

> **Before you begin**
>
> You can download a technical support package and send it to McAfee Technical Support.

When you create a technical support package, a compressed tar file will be saved to the McAfee DLP appliance you are troubleshooting.

Task

1. On your Linux-based appliance, select **System**.
2. Select a McAfee DLP Monitor or McAfee DLP Discover system and click **More**.

   If you cannot see the link, expand your dashboard.
3. Click **Create tech support package**.
4. After a minute or two, click **Check back**.
5. Click **Save** to download the file to your desktop.
6. Email the file to your McAfee support representative.

14 Typical scenarios

Use typical scenarios to address common problems or learn to use the McAfee DLP products.

Contents

Find significant network traffic

These use cases give you information on how to find significant content in network traffic.

Tasks

- *Find documents by file type* on page 252
  You might know that a confidential document you are looking for in your results was created by a Microsoft Office application.
- *Find email using non-standard ports* on page 253
  When non-standard ports are used to transmit email, a deliberate attempt to conceal illegal activity should be suspected.
- *Find encrypted traffic* on page 253
  Insiders attempting to conceal illegal activity or steal your intellectual property routinely use encryption.
- *Find evidence of foreign interference* on page 254
  Protecting intellectual property can be difficult when sensitive data is so easily transported beyond national borders.
- *Find evidence of frequent communications* on page 254
  You may suspect that a particular user is communicating with an off-site competitor. You might be able to identify the sources and destinations of frequent communications that will eventually reveal that leak.
- *Find high-risk incidents* on page 254
  When you have a high volume of violations to search through, it may be difficult to find the most significant ones.
- *Find leaked documents* on page 255
  Whether accidental or unintentional, confidential documents on corporate networks are often open to discovery by unauthorized users.
- *Find policies violated by a user* on page 255
  If you have a lot of incidents to sort through, it may be hard to find the ones that are related to a particular user.
- *Find postings to message boards* on page 256
  Employees sometimes spend company time posting to non-work-related internet sites.
- *Find unencrypted user data* on page 256
  You might assume that usernames and passwords are protected on your network as a matter of course, but that may not always be the case.
- *Find websites frequently visited* on page 256
  Find websites that are frequently visited by users who might be routinely allowed to use the Internet to complete their job duties, but have been told to curtail certain web sites that can compromise network security.

Find documents by file type

You might know that a confidential document you are looking for in your results was created by a Microsoft Office application.

This case helps you to find that document by filtering incidents to display only documents created by that program.

> If you know the name of the document, add another element to this procedure by using a **Filename | equals** filter, then type in its name.

Task

1 Select **Incidents | Incidents**.

2 From the **Filter by | Timestamp** menu, select a time frame.

3 Click the **plus** icon to add another parameter, then select **Content** | **equals** and type in the document extension.

Alternately, click **?** and select an office document type from the popup menu.

4 Click **Apply**.

The dashboard will reconfigure the results to display the document.

Find email using non-standard ports

When non-standard ports are used to transmit email, a deliberate attempt to conceal illegal activity should be suspected.

This case helps you to eliminate email that uses well-known ports, so that unknown or unsecured transmissions can be revealed.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

4 From the **Mail** menu, select one or more email formats.

5 Click **Apply**.

6 Open the **Protocol** category.

7 Select **Port** | **is none of** and type one or more standard email port numbers into the value field.

Ports 25 and 80 are commonly-used email and webmail ports.

8 Click **Search**.

Port information is displayed in the **Source** and **Destination** columns; add them to the dashboard if necessary.

Find encrypted traffic

Insiders attempting to conceal illegal activity or steal your intellectual property routinely use encryption.

This case helps you to identify the sources and destinations of encrypted traffic on your network to expose those activities.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Content Type** | **is any of** and click **?**.

4 From the **Protocol** menu, select **Crypto**.

5 Click **Apply**.

6 Click **Search**.

Find evidence of foreign interference

Protecting intellectual property can be difficult when sensitive data is so easily transported beyond national borders.

This case helps you to identify source and destination IP addresses that will tell where suspicious traffic is coming from and where it is going.

> Because dynamically-assigned IP addresses change regularly, hosts that are not local can be identified only if a DHCP server is installed on the network.

Task

1. On your Linux-based appliance, select **Capture** | **Basic Search**.
2. Select **Input Type** | **GeoIP Location** and click **?**.
3. Select one or more country names from the popup menu.
4. Click **Apply**, then **Search** and examine the incidents on your dashboard.

   If you do not see locations in your results, click **Columns** and add **Source**,**Destination**, **Sender** or **Recipient** columns to the dashboard.

Find evidence of frequent communications

You may suspect that a particular user is communicating with an off-site competitor. You might be able to identify the sources and destinations of frequent communications that will eventually reveal that leak.

This case helps you to find the other side of a session by searching for a **UserID** or email address.

> If the source and destination IP addresses are dynamically assigned, they will change over time. If you have added a DHCP server to McAfee DLP Manager, you can track the previous addresses of a host. Add another parameter to identify both sides of a conversation to find both sources and destinations of communications.

Task

1. Select **Incidents** | **Incidents**.
2. Select an incident.
3. From the **Filter by** | **Timestamp** menu, select a time frame.
4. Click the plus icon to add another parameter, then select **SourceIP** | **equals**.
5. Enter an IP address that you retrieved from the incident.
6. Click **Apply**.
7. Examine the incidents on your dashboard to find the **DestinationIP** that matches up to the **SourceIP**.

Find high-risk incidents

When you have a high volume of violations to search through, it may be difficult to find the most significant ones.

This case helps you to filter your results to display only the most significant incidents.

Task

1. Select **Incidents** | **Incidents**.
2. From the **Filter by** | **Timestamp** menu, select a time frame.

3 Click the plus icon to add another parameter, then select **Severity** | **equals** and type in a number from 1 to 5.

Alternatively, click **?** and select from the **Severity** popup menu.

4 Click **Apply**.

The incident list displays items of the selected severity.

Find leaked documents

Whether accidental or unintentional, confidential documents on corporate networks are often open to discovery by unauthorized users.

This case helps you to locate leaked documents, then analyze the incidents to find out how they were leaked.

Task

1 On your Linux-based appliance, select **Capture** | **Basic Search**.

2 Select **Input Type** | **Keywords**, then type in a word or phrase that might be found in a sensitive document, such as `Confidential`.

If you have additional information (such as content type or protocol), use an **Advanced Search** so you can add elements to include those values.

3 Select a time frame from the **Date/Time** menu.

4 Click **Search**.

Find policies violated by a user

If you have a lot of incidents to sort through, it may be hard to find the ones that are related to a particular user.

This case helps you to find policies that were violated by a user by keying on attributes that identify the user.

Task

1 Select **Incidents** | **Incidents**.

2 In the **Group by** menu select **Policy**, then click a policy the user might have violated.

If the policy did not generate incidents, it will not be listed.

3 From the **Filter by** menu, select a time from the **Timestamp** sub-menu.

4 Click plus to add a filter.

5 Select **UserID**, **UserName**, or **UserEmail** and **equals**, then type the user's ID, name, or email address in the value field.

> If you don't have exact information but want to guess at the identity of a sender or recipient, select the **Sender** or **Recipient** filter, add a **like** or **not like** condition, and type in a string that might match some characters in the user's ID, name or email address.

6 Click **Apply**.

Find postings to message boards

Employees sometimes spend company time posting to non-work-related internet sites.

This case helps you to identify that activity by targeting the protocol that is used to transmit such postings.

This filter identifies all posting traffic. If you know what web site is being posted to, add a **Content | equals** parameter and type in its name (for example, `webrats.com`).

Task

1. Select **Incidents | Incidents**.
2. From the **Filter by** menu, select a time from the **Timestamp** sub-menu.
3. Click the plus icon to add a filter and select **Protocol | equals**.
4. Click **?**, select a protocol from the pop-up list, then click **Apply**.
5. Click **Apply**.

Find unencrypted user data

You might assume that usernames and passwords are protected on your network as a matter of course, but that may not always be the case.

This case helps you to find out quickly if user account information is circulating in cleartext on your network by searching for account passwords.

Task

1. On your Linux-based appliance, select **Capture | Basic Search**.
2. Select **Input Type | Keywords**, and type the words `account password` into the value field.
3. Click **Search**.

   If there are any significant results, alert your IT department.

Find websites frequently visited

Find websites that are frequently visited by users who might be routinely allowed to use the Internet to complete their job duties, but have been told to curtail certain web sites that can compromise network security.

This case creates a content capture filter to store all traffic to and from inappropriate web sites to find out if your company policy is being violated.

Task

1. On your Linux-based appliance, select **Capture | Advanced Search**.
2. Open the **Source/Destination** category.
3. Select **URL | is any of** and type the URL of the website into the value field.

   For example, type in `www.webrats.com`.
4. Click **Search**.

   If no results are retrieved, check to see if the default `ignore_http_header` content capture filter is still active.

Filter traffic

These use cases give you information on how to use file types, keywords, and protocols to reveal significant traffic patterns.

Tasks

- *Filter out file types* on page 257
  Network data streams typically transport large numbers of images that that mask significant data.
- *Filter social networking traffic using blog postings* on page 258
  Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.
- *Filter social networking traffic using keywords* on page 258
  Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.
- *Filter social networking traffic using protocols* on page 258
  Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.

Filter out file types

Network data streams typically transport large numbers of images that that mask significant data.

This case helps you to filter out a large part of the data stream.

For example, if you wanted to eliminate multimedia content to improve performance of the capture engine, you might set up a filter to eliminate all configuration-controlled MPEG files.

Similarly, a pre-installed capture filter could automatically filter out images, like icons and thumbnails, that are too small to be significant.

Task

1. On your Linux-based appliance, select **System** | **System Administration**.
2. Select **Capture Filters** from the left pane options.

   Filters are displayed by device in the right panel.
3. Click **Create Content Filter.**
4. Type a name and optional description.
5. Select **Action** | **Drop Element**.
6. Select the devices for deployment.
   If you want to deploy a capture filter at a later time, select **None** in the **Devices** box.
7. In the **Content** category, select **Content Type** | **is any of**.
8. Click **?** and open the **Multi-Media Formats** popup menu.
9. Check the box of the contrrolled format (for example, MPEG).
10. Click **Apply**.
11. Click **Save**.

Filter social networking traffic using blog postings

Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.

This case helps you to find out how much social networking activity is occurring on your network by identifying all traffic to and from specific web sites.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Concept** | **is any of** and click **?**.

4 From the **Online** palette select BLOGPOST.

5 Click **Apply**.

6 Click **Search**.

You can customize the BLOGPOST concept to add more sites. Modify the **Content** definition on the **Policies** | **Concepts** page, then repeat the search.

Filter social networking traffic using keywords

Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.

This case helps you to find out how much social networking activity is occurring on your network by identifying all traffic to and from specific web sites.

Task

1 On your Linux-based appliance, select **Capture** | **Basic Search**.

2 Select **Input Type** | **Keywords**, and type site keywords into the value field (for example, `facebook` or `deadspin`).

3 Select a time frame from the **Date/Time** menu.

4 Click **Search**.

Filter social networking traffic using protocols

Employees who are accustomed to using social networking sites might not realize how much time they are spending on activities that reduce their productivity, or how much sensitive information might be leaked when they use such sites in the workplace.

This case helps you to find out how much social networking activity is occurring on your network by identifying all traffic to and from specific web sites.

Task

1 On your Linux-based appliance, select **Capture** | **Basic Search**.

2 Select **Input Type** | **Protocol** and click **?**.

3 Open the **Internet Protocols** palette and select **HTTP_Post** from the popup menu.

4 Click **Apply**.

5 Click **Search**.

Prevent data loss

These use cases give you information on how to prevent protected data from being compromised.

Tasks

- *Block data containing source code* on page 259
  Employees who are leaving the company might feel they have a right to the code they have written. You can protect your company's intellectual property by configuring your systems to block all source code leaving the network.
- *Block intellectual property residing on endpoints* on page 260
  If intellectual property is referenced in email or webmail communications and residing on an endpoint, it can be blocked from being sent to a competitor.
- *Block transmission of financial data* on page 261
  Even the most dedicated employees might not realize the implications of failing to protect financial documents, or they may not know how to encrypt them.
- *Keep intellectual property from being printed* on page 262
  If your employees are allowed to work remotely, they may be printing material that includes contains proprietary information in the course of performing legitimate tasks. If printed copies containing such information are lost or mishandled, your intellectual property could easily be lost to a competitor.
- *Keep IP address from being copied to a USB drive* on page 263
- *Prevent loss of project data from endpoints* on page 264
  Sensitive project data can easily be copied to laptops, USB drives, and other network endpoints.
- *Prevent release of privacy information* on page 265
  Billions of dollars have been lost by companies that have released privacy information by accident.

Block data containing source code

Employees who are leaving the company might feel they have a right to the code they have written. You can protect your company's intellectual property by configuring your systems to block all source code leaving the network.

When rules are configured to protect source code is run and incidents are found, action rules automatically keep it from leaving the network. This case helps you to customize the rule to a specific source code type, then make sure the responsible party receives email notification of the action.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Content** category and select **Content Type | is any of**, then click **?**.

3 Open the **Source Code** option from the popup menu and select one or more source code types.

If you don't know the source code type, select **Template | equals**, click **?** and select **Source Code**.

4 Click **Apply**, then click **Save as Rule**.

The **Add Rule** page opens.

5 Type a name for the rule and select a **Policy** to assign it to.

6 Select the **Action** tab.

7 Click the green + **Add Action** icon, then select the **Block and Notify Sender** action.

If more users should be notified, select **Policies** | **Action Rules** to edit the action rule.

8 Click **Save.**

Block intellectual property residing on endpoints

If intellectual property is referenced in email or webmail communications and residing on an endpoint, it can be blocked from being sent to a competitor.

Before you begin

Endpoint features require deployment of McAfee DLP Endpoint and an added evidence server.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Select **Actions** | **Add Policy**.

3 Give the policy a recognizable name, such as `Competitor Policy`.

4 From the **State** menu, select **Active**, then select the McAfee DLP devices to which you want to publish the policy.

5 Click **Save**.

6 On the **Policies** page, open the new policy.

7 Seclect **Add Rule** | **Actions**.

You can use an existing policy and add a rule to it, or clone an existing rule from another policy. You could also do a historical search, then save it as a rule when it returns the type of information you need.

8 Type a name for the rule.

9 Select a **Severity** and an inheritance state (**Enabled** rules run when the policy runs).

10 Define the intellectual property by selecting keywords, content type, or concepts from the Content menu. You can add values to one or more of the following categories:

a Enter **Keywords** that may be found in sensitive documents.

b Select **Content Type** from the menu, click **?** to launch the **Content Type** palette, and make one or more selections from it.

c Select **Concept** from the menu and click **?** to launch the definitions palette.

Inspect the Intellectual Property sub-menu to see if one or more of the default concepts will suit your purposes. If not, create a new concept and add your own parameters, then return to this page and add that new concept from the Concepts palette. \

11 The following selections are optional, depending on how much you know about what you are looking for:

12 Add a web protocol.

   a Open **Protocol** and select **Protocol | is any of**.

   b Click **?** and select from the **Internet Protocols** menu.

   For example, if you suspect intellectual property is being posted, select HTTP_Post and click **Apply**.

13 Add a user name.

   a Open **Source/Destination** and select **UserName | is any of** or **UserName | is none of.**

   b Click **?** and select from the remote **Directory Server List.**

   c Click **Find** and select a category of users, then click **Apply**. If you select **Everyone**, the rule will apply to all users on your directory servers.

14 Add an email address

   a Click plus to add another item under **Source/Destination**.

   b Select **Email Address | is all of** or another condition to focus the email address.

   c Type in an email address.

15 Select the **Action** tab.

16 Click **Add Action**, then select the **Block and Notify Sender** action.

   If more users should be notified, select **Policies | Action Rules** to edit the action rule.

17 After you have finished adding as much information as you have to the rule, click **Save** and let the policy and rule run. After you get results, tune as needed.

Block transmission of financial data

Even the most dedicated employees might not realize the implications of failing to protect financial documents, or they may not know how to encrypt them.

This case helps you to protect financial data by creating a concept that flags a variety of financial documents, then attaching an action rule to prevent them from leaving the network.

Task

1 On your Linux-based appliance, select **Capture | Advanced Search**.

2 Open the **Content** category and select **Concept | is any of**, then click **?**.

3 Check the **Select All** checkboxes on all groups of financial concepts. (For example, if you are in North America you might select `Banking and Financial Sector` and `Corporate Financial`).

   Concepts contain words and phrases that identify a broad range of content. Select **Policies | Concepts** and double-click on one of them to understand how they are constructed.

4 Click **Apply** then click **Save as Rule.**

   The **Add Rule** page opens.

5 Type a name for the rule and select a **Policy** to assign it to.

6 Select the **Action** tab.

7 Click the green + **Add Action** icon, then select the **Block and Notify Sender** action.

8 Click **Save**.

Keep intellectual property from being printed

If your employees are allowed to work remotely, they may be printing material that includes contains proprietary information in the course of performing legitimate tasks. If printed copies containing such information are lost or mishandled, your intellectual property could easily be lost to a competitor.

> **Before you begin**
>
> Endpoint features require deployment of McAfee DLP Endpoint and an added evidence server.

This case keeps intellectual property from being printed.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Select **Actions** | **Add Policy**.

3 Type in a recognizable name such as `Competitor Policy`. Select **State** | **Active**, then select the McAfee DLP devices to which you want to publish the policy.

4 Click **Save**.

5 On the **Policies** page, open the new policy.

6 Select **Actions** | **Add Rule**.

You can use an existing policy and add a rule to it, or clone an existing rule from another policy. You could also do a historical search, then save it as a rule when it returns the type of information you need.

7 Enter a name for the rule.

8 Select a **Severity** and an inheritance state (**Enabled** rules run when the policy runs).

9 Open the **Endpoint** category and select **Protect Local Printers** | **equals**.

10 Click **?**, check **Enable**, and click **Apply**.

11 Select the **Actions** tab and click the **Add Action** icon and select an action from the displayed list.

This definition, plus an action rule, constitutes a minimal printer policy. To refine the rule for specific content, add the following definitions.

12 Define content by selecting keywords, content type, or concepts from the Content menu. You can add values to one or more of the following categories:

a Enter **Keywords** that may be found in sensitive documents.

b Select **Content Type** from the menu, click **?** to launch the **Content Type** palette, and make one or more file types from it.

c Select **Concept** from the menu and click **?** to launch the definitions palette.

13 Inspect the sub-menus to see if one or more of the default concepts will suit your purposes. If not, create a new concept and add your own parameters, then return to this page and add that new concept from the palette.

14 Open **Source/Destination** and select **UserName** from the menu.

15 Select **is any of** or **is none of**. The latter selection will indicate an exception to the value provided.

16 Click **?** and select from the remote **Directory Server List**.

17 Click **Find** and select a category of users, then click **Apply**. If you select **Everyone** the rule will apply to all users on your directory servers.

The same action can be used on all three data types (**Data-in-Motion**, **Data-at-Rest**, **Data-in-Use**), but only one of each type to a single rule.

18 Scroll down to the **Data-in-Use** actions and select the **Printer Reaction** action rule.

Actions are defined and edited on the **Action Rules** page. All of the reactions listed in the **Actions** column will be applied.

19 Click **Save**.

Keep IP address from being copied to a USB drive

Before you begin

Endpoint features require deployment of McAfee DLP Endpoint and an added evidence server.

If your employees are allowed to work remotely, they might be duplicating material that includes contains proprietary information in the course of performing legitimate tasks. If USB drives containing such information are lost or mishandled, your intellectual property could easily be lost to a competitor.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Select **Actions** | **Add Policy**. Give the policy a recognizable name, such as `Competitor Policy`.

3 Select **State** | **Active**, then select the McAfee DLP devices to which you want to publish the policy.

4 Click **Save**.

5 On the **Policies** page, open the new policy.

You can use an existing policy and add a rule to it, or clone an existing rule from another policy. You could also do a historical search, then save it as a rule when it returns the type of information you need.

6 Select **Actions** | **Add Rule**.

7 Enter a name for the rule.

8 Select a **Severity** and an inheritance state (Enabled rules run when the policy runs).

9 Open the **Endpoint** category and select **Protect Removable Media** | **equals**.

10 Click **?** and select **Enable**, then click **Apply**.

This definition, plus an action rule, constitutes a minimal removable media policy. To refine the rule for specific content, add the following definitions. Define content by selecting keywords, content type, or concepts from the **Content** menu. You can add values to one or more of the following categories.

- Enter **Keywords** that may be found in sensitive documents.
- Select **Content Type** from the menu, click **?** to launch the **Content Type** palette, and make one or more file types from it.
- Select **Concept** from the menu and click **?** to launch the definitions palette.

Inspect the sub-menus to see if one or more of the default concepts will suit your purposes. If not, create a new concept and add your own parameters, then return to this page and add that new concept from the palette.

11 Open **Source/Destination** and select **UserName** from the menu.

The same action can be used on all three data vectors (**Data-in-Motion**, **Data-at-Rest**, **Data-in-Use**), but only one of each type to a single rule.

12 Select **is any of** or **is none of**. The latter selection will indicate an exception to the value provided.

13 Click **?** and select from the remote **Directory Server List**.

14 Click **Find** and select a category of users, then click **Apply**. If you select **Everyone**, the rule will apply to all users on your directory servers.

15 Select the Actions tab, then click **Add Action**.

The same action can be used on all three data vectors, but only one of each type to a single rule.

16 Scroll down to the **Data-in-Use** actions and select the **Removable Media Reaction** action rule.

Actions are defined and edited on the **Action Rules** page. All of the reactions listed in the **Actions** column will be applied.

17 Click **Save**.

Prevent loss of project data from endpoints

Sensitive project data can easily be copied to laptops, USB drives, and other network endpoints.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click **Actions** | **Add Policy**.

3 Enter a name and optional description for the policy. Select a **State**, **Region**, and **Devices**. Click **Save**.

4 On the **Policy** page, open the new policy.

5 Click **Actions** | **Add Rule**.

6 Enter a name and optional description for the rule.

7 Select a **Severity** and an inheritance state (**Enabled** rules run when the policy runs).

8 Define the project data by selecting keywords, content type, or concepts from the **Content** menu. You may add values to one or more of the following categories.

- • Type in **Keywords** that may be found in sensitive documents.
- Select **Content Type** from the menu, click **?** to launch the **Content Type** palette, and make one or more file types from it.
- Select **Concept** from the menu and click **?** to launch the definitions palette.

9 Inspect the sub-menus to see if one or more of the default concepts will suit your purposes. If not, create a new concept and add your own parameters, then return to the page and add that new concept from the palette.

10 If the user is known, open **Source/Destination** and type the username in the value field.

11 If you want to specify exclusions, go to the Exceptions tab and add project data that may be found, but is irrelevant. When you have finished, click **Save**.

12 In the Actions tab, click **Add Action** and select **Removable Media Reaction**.

The actions taken are listed in the **Actions** column.

13 Click **Save**.

Protection Rule Parameters

Rule category	Example
Content	Keywords | contains all of | Project X
Source/Destination	Email Address | contains all of | tjohnson
Endpoint	Protect Removable Media | equals | Enable
Actions	Removable Media Reaction

Prevent release of privacy information

Billions of dollars have been lost by companies that have released privacy information by accident.

This case prevents privacy violations by implementing existing policies to identify the information, then setting up automatic blocking to keep it from leaving the network.

Task

1 On your Linux-based appliance, select **Policies** | **Policies**.

2 Click a **Policy Name** that can be used to identify privacy information.

For example, you might select `HIPAA Compliance and Personal Health`, or `Payment Card Industry`.

3 Click the first rule listed under the policy, then select the **Actions** tab.

4 If no action is listed, or if the action listed does not block data, click **Add Action**.

5 From the popup menu, select an appropriate blocking action rule.

Actions are defined and edited on the **Action Rules** page. All of the reactions listed in the **Actions** column will be applied. If you do not see the one you need, create it under **Policies** | **Action Rules**, then return to this step.

6 Click **Save**.

Action rules act only on monitored or discovered data (**Data-in-Motion** or **Data-at-Rest**). Only one action type is allowed for each process.

7 Repeat this process for every rule under the policy.

8 When the policy runs, all privacy information defined in its rules will be blocked from leaving the network.

Monitor and manage user activity

These use cases give you information on how to monitor and manage user activity on local and remote networks.

Tasks

- *Exempt users from detection* on page 266
  Even network administrators may not be privileged to peruse certain information found in network data streams.
- *Identify disgruntled users* on page 267
  Unhappy insiders can do a lot of damage to your business operations if they are not found and stopped.
- *Monitor network activity after global close of business* on page 267
  Monitor network activity after global close of business to prevent confidential data from entering or leaving a company network during business hours (after 5 PM, movement of sensitive data may indicate a leak). Global operations make it difficult to define exactly when close of business occurs in local time zones, but McAfee DLP Manager and McAfee DLP Monitor automatically make those conversions.
- *Monitor user activity* on page 268
  Employees who have been warned to discontinue specific network activities should be monitored to prevent them from wasting company resources or sabotaging the system.
- *Use multiple capture filters to store traffic* on page 268
  Under some circumstances, you might want to block all encrypted traffic on the network, except for a particular type. You can do this by setting up multiple action filters that are applied to the data stream, gradually narrowing the filtering process by applying them one after another.

Exempt users from detection

Even network administrators may not be privileged to peruse certain information found in network data streams.

Before you begin

Endpoint features require deployment of McAfee DLP Endpoint and an added evidence server.

This case helps you to ensure absolute security for one or more endpoints that have access to top secret information by protecting them from detection by the capture engine.

Alternately, use this procedure with a user or group name, or an email address.

Task

1. On your Linux-based appliance, select **System** | **System Administration**.
2. Select **Capture Filters** from the left pane options.

   Filters are displayed by device in the right panel.
3. Click **Create Content Filter**.
4. Type a filter name and optional description.
5. Select **Action** | **Drop Element**.
6. Open the **Source/Destination** category.
7. Select **IP Address** | **is any of** and type an IP address into the value field.

   If the address is on a subnet, it is detectable only if the network and host portions of an IP address are standard classful IP (address fields are separated into four 8-bit groups). Separate multiple addresses by commas, and IP ranges by dashes.

8 Check the box of the device on which you want the filter deployed.

   To decide later, click **None**.

9 Click **Save**.

   A new capture filter is added to the existing list.

Identify disgruntled users

Unhappy insiders can do a lot of damage to your business operations if they are not found and stopped.

This case searches for instant messaging or email communications that contain clues to potential trouble by applying a concept that will identify those transmissions.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Content** category.

3 Select **Concept** | **is any of** and click **?**.

4 Open the **Acceptable Use** category from the popup menu and check the DISCONTENT box.

   This concept contains a collection of words and phrases that are often used by unhappy employees. Select **Policies** | **Concepts** and double-click on the concept to find out what the phrases are, and how the concept is constructed.

5 Click **Apply**.

6 Click **Search**.

   If no results are retrieved, check to see if the default `ignore_http_header` content capture filter is still active.

Monitor network activity after global close of business

Monitor network activity after global close of business to prevent confidential data from entering or leaving a company network during business hours (after 5 PM, movement of sensitive data may indicate a leak). Global operations make it difficult to define exactly when close of business occurs in local time zones, but McAfee DLP Manager and McAfee DLP Monitor automatically make those conversions.

This case creates a rule that tracks sensitive data between the hours of 5 and 6 PM in your Los Angeles, New York, London, and Tokyo offices.

> If you are managing several McAfee DLP Monitor appliances in different locations, this is how you can find activity at the same clock time in each of those locations. Monitoring data at the time most employees are leaving workplaces will help to prevent leaks.

Task

1 On your Linux-based appliance, select **Capture** | **Advanced Search**.

2 Open the **Date/Time** category.

3 Select **Exact Time** | **before**.

   Automatic Conversion to GMT selects the same moment globally; Local time selects the same clock time globally.

4 Click the **Calendar** icon to select a date.

5 Select the hour, minute and second from the thumbwheel menus.

6 Click **Search**.

Monitor user activity

Employees who have been warned to discontinue specific network activities should be monitored to prevent them from wasting company resources or sabotaging the system.

This case monitors all of a user's communications to determine if they are complying with your instructions.

> To monitor the user on a regular basis, save the search as a rule. In case of flagrant violations, incidents and events can be collected in a case and delegated to your legal team for use as evidence in court.

Task

1 On your Linux-based appliance, select **Capture** | **Basic Search**.

2 From the **Input Type** menu, select **UserID**, **Host Name**, **Host IP**, or **Email From Address**.

3 Type the identifying text into the value field.

The **User Name** corresponds to a field found on an LDAP server, so this option is not displayed unless a directory server has been added (in **System Administration** | **Directory Services**). Note that this parameter might not necessarily correspond to a user's email address, since a user could have more than one email address.

4 If the information is on a remote directory server:

a Click **?** and select the server.

b Type in a user name pattern and click **Find** to display a list of users and groups. Select a user or group then click **Apply**.

If you select **Everyone**, the rule will apply to all users on all of your directory servers.

5 Click **Search** or **Save as Rule**.

Use multiple capture filters to store traffic

Under some circumstances, you might want to block all encrypted traffic on the network, except for a particular type. You can do this by setting up multiple action filters that are applied to the data stream, gradually narrowing the filtering process by applying them one after another.

For example, isolating traffic using port 443, which commonly transports encrypted data, is one way of filtering out encrypted traffic. But that port is also used by AOL (America Online), and blocking that traffic too might eliminate traffic you need to monitor.

In such a case, you can set up the capture filters to retain the encrypted AIM (AOL Instant Messaging) traffic while dropping the broader category of encrypted traffic.

> You cannot save sessions or data that have already been eliminated, so pay attention to the filtering sequence.

Task

1 On your Linux-based appliance, select **System** | **System Administration** | **Capture Filters**.

2 Click **Create Network Filter**.

3 Type the file name `AOL_Chat` and a description (optional).

4 Select **Store** from the **Action** menu to retain AOL chat traffic.

5 Open the **Protocol** category.

6 Select **Protocol | is any of** and click **?**.

7 Select **Chat Protocols | AOL_Chat** from the **Protocol** popup menu.

8 Click **Apply** and **Save**.

9 Click **Create Netowork Filter** to create another filter.

10 Give the policy a recognizable name, such as SSH traffic, and a description (optional).

11 From the **Action** menu, select **Ignore**.

12 Open **Protocol** and select **Port | source is any of** and type `443` into the value field.

13 Click plus to add a parameter.

14 Repeat the process, but select **Port | destination is any of** and type `443` into the value field.

Traffic through ports and port ranges is bidirectional, so you must define source and destination transmissions separately.

15 Check the box of the device on which you want the filter deployed.

To decide later, click **None**.

16 Click **Save**.

A new **Ignore** filter is added to the existing list.

17 Use the **Priority** icons to change the order of the filters.

The **Store** filter must run first, because the Ignore filter will eliminate all of the rest of the port 443 traffic.

When a network capture filter is applied to the network data stream, its position in the list indicates its priority. Because the BASE filter instructs the system to store all data that has not been dropped from the data stream, it must always run last.

18 Let the system run. After some time, you can search for AIM traffic in the captured data on the **Incidents** page.

Index

McAfee®