McAfee Data Loss Prevention

version 1.7
## Contents

### Preface
- Using this guide
- Audience
- Conventions
- Contact information

### Introducing Data Loss Prevention
- Overview
- What is Data Loss Prevention?
- How does McAfee Data Loss Prevention work?
- Key scenarios for data loss

### Creating Policies with the Management Console
- The DLP Management Console
- Creating definitions
- Working with the Enterprise Applications List
- Defining application groups
- Classifying data with secured text patterns
- Network address ranges
- Using the Whitelist for text segments
- File extensions
- File servers
- Printers
- Web servers
- Email destinations
- Classifying content with tags
- Using tags to classify content
- Manually tagging content
- Tagging rules
- Creating tagging rules
- Reaction rules
- Creating a reaction rule
- Controlling devices
- Device definitions
- Built-in device protection rules
- Device protection rules
- Ignored devices
- Deployment groups
- Policy analyzer

### Using the Product
- Policy deployment
- Installed agents
- Monitor
- Filtering event data
- Labels
- Administrative maintenance
- Maintaining the DLP agent
- Database administration
- Database statistics

### Database statistics
- Database administration
- Maintaining the DLP agent
- Database administration
- Database statistics
Agent override key generator ................................................................. 61
Configure the agent update server .......................................................... 61

**Advanced Configuration** .................................................................. 62

Configuring the agent ........................................................................... 62
  - Events tab .......................................................................................... 63
  - Notification Service tab ....................................................................... 64
  - Security tab ........................................................................................ 65
  - Whitelist tab ....................................................................................... 65
  - File Tracking tab ................................................................................ 66
  - Outlook Probe tab ............................................................................... 67
  - Advanced Configuration tab ............................................................... 68
  - Modules ............................................................................................. 69
  - Managing agent configuration ............................................................ 70
System tools ............................................................................................ 71
  - System log .......................................................................................... 71
  - Options .............................................................................................. 71
Preface

Using this guide

This guide is intended to help security officers and network administrators use McAfee® Data Loss Prevention™ (DLP) software through the day-to-day tasks involved in managing the system. It contains an overview of the product technology, concepts and architecture, as well as a detailed description of the Management Console and Data Loss Prevention components.

The guide includes these topics:

- Introduction and system components
- A tour of the McAfee DLP Management Console
- Creating Policies with the Management Console
- Using the Product
- Advanced Configuration

Audience

This information in this guide is intended primarily for two audiences:

- Security officers who are responsible for determining sensitive and confidential data, and for defining the corporate policy on how the company’s intellectual property is to be protected.
- Network administrators who are responsible for implementing and enforcing the corporate policy on protecting the company’s intellectual property.

Conventions

This guide uses the following conventions:

**Bold Condensed**
All words from the interface, including options, menus, buttons, and dialog box names.

**Courier**
The path of a folder or program; text that represents something the user types exactly (for example, a command at the system prompt).

**Italic**
Emphasis or introduction of a new term; names of product manuals.

**Blue**
A web address (URL); a live link.

**Note**
Supplemental information; for example, an alternate method of executing the same command.

**Caution**
Important advice to protect your computer system, enterprise, software installation, or data.

**Warning**
Important advice to protect a person from bodily harm when using a hardware product.
Contact information

**Threat Center: McAfee Avert® Labs** http://www.mcafee.com/us/threat_center/default.asp
Avert Labs Threat Library
http://vil.nai.com

**Avert Labs WebImmune & Submit a Sample** *(Logon credentials required)*
https://www.webimmune.net/default.asp

**Avert Labs DAT Notification Service**
http://vil.nai.com/vil/signup_DAT_notification.aspx

**Download Site** http://www.mcafee.com/us/downloads/
**Product Upgrades** *(Valid grant number required)*

**Security Updates (DATs, engine)**

**HotFix and Patch Releases**
- **For Security Vulnerabilities** *(Available to the public)*
- **For Products** *(ServicePortal account and valid grant number required)*

**Product Evaluation**

**McAfee Beta Program**

**KnowledgeBase Search**
http://knowledge.mcafee.com/

**McAfee Technical Support ServicePortal** *(Logon credentials required)*
https://mysupport.mcafee.com/eservice_enu/start.swe

**Customer Service**
**Web**
http://www.mcafee.com/us/about/contact/index.html

**Phone** — US, Canada, and Latin America toll-free:
**+1-888-VIRUS NO** or **+1-888-847-8766** Monday – Friday, 8 a.m. – 8 p.m., Central Time

**Professional Services**

**Small and Medium Business** http://www.mcafee.com/us/smb/services/index.html
Introducing Data Loss Prevention

Overview

McAfee® Data Loss Prevention™ (DLP) software protects enterprises from the risk associated with unauthorized transfer of data from within or outside the organization. Data loss is defined as confidential or private information leaving the enterprise as a result of unauthorized communication via channels such as applications, physical devices, and network protocols.

What is Data Loss Prevention?

The program is a content-based agent solution that inspects corporate users’ actions concerning sensitive content, in their own work environment, their computers.

McAfee Data Loss Prevention provides:

- **Universal protection** – protects against data loss through the broadest set of data-loss channels.
- **Content-aware data protection** – protects against data loss regardless of the format in which data is stored or manipulated; enforces data loss prevention without disrupting legitimate user activities.
- **Protection on-the-go** – prevents transmission of sensitive data from desktops and laptops, whether or not they are connected to the enterprise’s network.

How does McAfee Data Loss Prevention work?

Data Loss Prevention software safeguards sensitive corporate information through tagging rules, reaction rules, policy deployment, and forensics (monitoring, reporting, and storing content as evidence).

Tagging rules

Tagging rules are based on corporate requirements and are created to identify confidential information and its sources. Data can be classified by:

- **Location** – When files are copied or accessed by local processes, tags are applied based on the location of the source file. For example, a file being copied locally from a share on a network server.
- **Content** – When data is being transmitted or replicated, tags are applied based on parsing the content and matching it against predefined patterns or keywords. For example, parsing the text of an email and matching the content against known strings such as “Company Confidential” or multiple Social Security Number patterns.
- **File type, extension, or application** – Tagging rules can apply tags when a known application creates a file or generically based on the file type or extension.
Reaction rules
Reaction rules prevent unauthorized distribution of tagged data. When tagged data is being distributed, the reaction rules determine whether the distribution should be allowed, monitored, or blocked.

Classified data can be monitored, prevented from being distributed, or prevented from being replicated via:

- Microsoft Outlook.
- Internet Explorer web postings.
- Network connections.
- Printing.
- Physical devices such as floppy drives, CD-ROM drives, USB drives.

Deployment groups
Deployment groups are used to apply specific reaction rules to different groups, users and computers in the enterprise.

Policies and policy deployment
A policy is the combination of tagging rules, reaction rules, definitions, and deployment groups. Policy deployment uses the corporate Active Directory infrastructure to distribute policies to the enterprise’s managed computers (computers with a DLP agent installed).

Monitoring and reporting
- Event monitoring – The McAfee DLP Monitor allows administrators to view agent events as they are received.
- Executive reports – Executive-level reports allow high-level users to view overall statistics and summaries about the operation of McAfee Data Loss Prevention.
- Event reporting – Event-level reports allow administrators to inspect the information and identify trends in event and user behavior.
- Evidence collection – If reaction rules are defined to collect evidence, a copy of the tagged data is linked to the specific event. This information can be used to determine the severity or exposure of the event.
Key scenarios for data loss

Data loss can occur by copying data to removable media, through network connections, and by printing. McAfee Data Loss Prevention provides the tools to monitor and optionally block these methods of transmitting sensitive or confidential data.

Email protection

Action: An employee copies information from an internal memo, pastes it into an email message, and sends it to someone outside the company.

Reaction: The email is blocked by McAfee Data Loss Prevention, and a customized popup message is displayed on the employee's computer. An event is generated and stored on the Event Collector server for review.

Malicious document printing

Action: A disgruntled salesperson is planning to leave the company and to work for a competitor. Before quitting, the employee tries to print all of the contact information for customers in that region.

Reaction: The printing activity is blocked by McAfee Data Loss Prevention. An event is generated and stored on the Event Collector server for review.

External storage device

Action: A visitor or temporary employee tries to copy financial data from a server onto a USB storage device, such as a thumb drive.

Reaction: The file copy to the USB device is monitored by McAfee Data Loss Prevention. An event is generated and stored on the Event Collector server for review.

Malicious webmail

Action: A roaming laptop user sends a webmail containing private customer data (for example, an attachment with credit card numbers).

Reaction: The message is blocked by McAfee Data Loss Prevention. An event is generated and stored on the Event Collector server for review.
McAfee Data Loss Prevention components

McAfee Data Loss Prevention software includes these components:

- Management Console
- DLP agent
- Event Collector server
- Monitor
- Reports

Management Console

The McAfee DLP Management Console is the interface where the administrator defines and enforces the corporate information security policy. It is used to create the information security policy and administer the Data Loss Prevention components.

The Management Console’s policy deployment mechanism uses existing corporate domains and groups (available in the corporate Active Directory) for flexible rule distribution.

DLP agent

The McAfee DLP agent resides on corporate computers, referred to as managed computers, and enforces corporate policy as defined by the security officer or network administrators. The agent audits user activities to monitor, control, and prevent unauthorized users from copying or transferring sensitive data.

Event Collector server

When events are generated by an agent, they are sent to the Event Collector. The events are stored in the database for further analysis and use by other system components.

Monitor

After events are sent to the Event Collector, they are displayed in the McAfee DLP Monitor. All events can be filtered and sorted based on criteria such as reaction rules, severity, date, time, user, computer name, or policy version.

Reports

The reporting interface of Data Loss Prevention provides time-based reports that can be used to summarize information security events. These summaries can be used for executive-level reports, or can provide insight into trends in user behavior.
Creating Policies with the Management Console

To use McAfee Data Loss Prevention, you must determine your enterprise’s security needs, define the corporate policies, configure the software to deploy and enforce policies, then monitor the activity and tune the software as necessary.

The security policy prevents information loss with a set of rules and definitions that:

- Classify information.
- Control the way information is protected.
- Monitor the flow of information.
- Determine information backup, recovery, and updating.
The DLP Management Console

The Management Console is the interface for Data Loss Prevention. You use this interface to create and enforce policies that protect your corporation’s sensitive information. This is where you create, edit and control system rules and objects, maintaining the corporate policy to prevent information loss.

The console is divided into three areas:

1 **Navigation panel** – Where the system administrator selects a rule or definition. The main panel displays information about the selected object.
   - **Rules** – Access Tagging Rules which classify content, and Reaction Rules which enforce the company policy.
   - **Definitions** – Create new objects for system rules.
   - **Devices** – Monitor and control the use of physical devices.
   - **Deployment** – Create and maintain new groups for deploying policies, and manually tag files and folders.
   - **Agent Installation** – View the listed managed computers, and allow operations such as agent installation, uninstallation, viewing system status, agent shutdown and troubleshooting tools activation.
   - **Monitoring** – Link to the Event Monitor and reports.
   - **DB Administration** – Monitor and maintain the system’s database.

2 **Main panel** – Where the system administrator edits and reviews rules or definitions, depending on which object is currently selected in the navigation panel.

3 **Details panel** – Displays a detailed description of a single object selected in the main panel.
Creating definitions

Definitions let you customize the system to enforce your corporate security policy and any other corporate requirements, such as compliance issues and privacy laws.

Customizing these definitions with corporate-relevant information creates an efficient method of maintaining company policies. Definitions can be assigned to any new or existing rule. All changes take effect immediately by redeploying the system policy to all agents.

Available definitions include:

- **Enterprise Applications List** – Import a customized list of applications. This allows you to customize application groups that can later be used with application-related rules.

- **Application groups** – Group applications that appear in the Enterprise Applications List. This allows you to customize rules about specific applications and apply the rules efficiently.

- **Secured text patterns** – Set static or regular expressions, which are used in content-based classification (tagging) rules.

- **Network address ranges** – Set a specific network address range or a single address, which can be used in network connections rules to monitor and control incoming or outgoing traffic.

- **Whitelist** – Store specific content that can be safely ignored by the system. Content is stored as files in the Whitelist folder.

- **File extensions** – Edit the existing list or create new file extension entries, which are used as filter criteria in reaction rules.

- **File servers** – Create a list of file servers available within the corporate network, using network scan and LDAP queries.

- **Printers** – Create a list of network printers, using LDAP queries.

- **Web servers** – Create web server entries, which are used with web posts rules.

- **Email destinations** – Create entries for email domains and specific email addresses, which can be used with email protection rules.
Working with the Enterprise Applications List

The Enterprise Applications List contains the applications whose data you want to control. For example, if you want to control the data in Excel files, you can add Excel to the Enterprise Applications List, then create a rule that defines whether Excel files or their contents can be printed or copied.

Application-based tagging rules and some reaction rules reference application definitions. For the references to work, these applications must be defined in the Enterprise Applications List.

To add applications to the Enterprise Application List:

1. Open the McAfee DLP Management Console.
2. Under Definitions, select Enterprise Applications List.
   On the right-hand side you’ll find the available applications list.
3. Add new applications using one of these options.

   **Manual import**
   - Click or right-click on the Enterprise Applications List window and select Add Executable.
     The Edit Application window appears.
   - Click and select the application EXE file.
   - Click Open.
     The application details appear.

   **Drag & drop**
   - Select the needed application EXE file.
   - Drag & drop the selected EXE file into the Enterprise Applications List window.
     The application details appear.

   **Scan for new applications**
   - Click or right-click on the Enterprise Applications List window and select Scan Applications.
     The Scan for Applications window appears.
   - Click the start button and select the drives and/or folder to scan for applications.
     All available applications appear.
   - Select the needed action from the list:
     - Clear discards the current list.
     - Merge adds the applications into the system applications list.
     - Export exports the applications list to a file.
   - Close the Scan for Applications window.
     The merged applications appear in the Enterprise Applications List.
4 On the **strategy** column, select the system observation strategy according to the type of application:

- **Archiver** – an archive application such as WinZip or WinRAR.
- **Editor** (default) – an application that modifies file content; for example, Microsoft Word.
- **Explorer** – an application that copies or moves the file without modifying it; for example, Windows Explorer.
- **Trusted** – an application that doesn’t need to be inspected by the system; for example, McAfee VirusScan.

**Caution:** Because the strategy type affects the system’s observation level, use the strategy selection wisely to improved system performance. Changing the strategy affects all application versions (all available executables MD5).

---

**To remove applications from the list:**

1. Open the McAfee DLP Management Console.
2. Under **Definitions**, select **Enterprise Applications List**.
   - *On the right-hand side you’ll find the available Applications list.*
3. Select the needed application to be removed, then click **Remove**, or right-click on the Enterprise Applications List window and select **Remove**.
   - *The confirmation window appears.*
4. Click **YES** to confirm the deletion.

---

**To save the applications list:**

1. Open the McAfee DLP Management Console.
2. In the **File** menu, select **Save Enterprise Applications List**.
   - *The Save as window appears.*
3. Select the needed location and file name.
4. Click **Save**.
   - *The application list is saved to a file and can be used as an applications resource on a different system environment.*

---

**To import the applications list:**

1. Open the McAfee DLP Management Console.
2. In the **File** menu, select **Load Enterprise Applications List**.
   - *The Open window appears.*
3. Select the needed application list file.
4. Click **Open**.

**Note:** The application list is included and saved in the policy. The list can be loaded and saved manually, external to the policy. This is meant for archival or backup purposes.
Defining application groups

Once applications are included in the Enterprise Applications List, you can create application groups. Tagging and reaction rules can reference a single entity, an application group, rather than a list of applications. For example, if multiple versions of a product exist, they need to be defined and grouped as an application group.

To create a new application group:

1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Application Groups.
   On the right-hand side you’ll find the available application groups.
3. Click or right-click on the Application Groups Window and select Application Group.
   The New Application Group icon appears.
4. Name the new application group and double-click the icon.
   The Edit Application Group window appears.
5. Select the needed applications for the group. Groups can be based on the manufacturer, product family, a single application, or a single version.
   When adding new applications to the group, selecting the specific file (with a unique file identifier) makes only this version available for the group. To add all versions of a specific application, select other executables.
6. Click OK.

To create a new application group from the Enterprise Applications List:

1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Enterprise Applications List.
   On the right-hand side you’ll find the available applications list.
3. Select the needed application (using the Ctrl or Shift functions) and click Create Application Group, or right-click on the Enterprise Applications List window and select Create Application Group.
   The Edit Application Group window appears.
4. Name the new application group.
5. Click OK.

Note: To locate where a specific application group is in use, right-click the group and select Go To.

To delete an application group:

1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Application Groups.
   On the right-hand side you’ll find the available applications groups.
3. Select the application group to be removed and click , or right-click on the Application Group window and select Delete.
   The confirmation window appears.
4. Click YES to confirm the deletion.
5. Click OK.

Note: Application groups that are currently in use can be deleted only after the relevant rules containing the specific groups have been deleted.
Classifying data with secured text patterns

Content-based tags use text patterns to classify data according to specific words or patterns. They can identify known strings, such as *Company Classified* or *Internal Use Only*, or regular expressions, which allow complex pattern matching such as in social security numbers or credit card numbers.

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

**To create a new text pattern:**

1. Open the McAfee DLP Management Console.
2. In the navigation panel under *Definitions*, select *Secured Text Patterns*.
   
   On the right-hand side you’ll find the available secured text patterns.
3. Click or right-click on the Secured Text Patterns window and select *Secured Text Patterns*.
   
   The Secured Text Patterns icon appears.
4. Name the new text pattern and double-click the icon.
   
   The Secured Text Pattern editor window appears.

   ![Secured Text Pattern editor window](image)

5. Add a description to the text pattern (optional).
6. Under *Included Patterns*, select the pattern recognition method (All or Any patterns).
7. Click to define the new pattern.
8. Type the text string.
9. Select *Is Regex* if the string is a regular expression.
10. Under *Threshold*, type the number of times the pattern must be found in the data for it to be considered a match. For example, finding one credit card in an email may be acceptable, but adding a threshold of 5 requires five or more matches of the credit card pattern.
11. Under *Excluded Patterns*, select the pattern recognition method (All or Any patterns).
Creating definitions

12 Click \textbf{Add} to add an exclusion pattern.
13 Type the text strings that, when found, are ignored by the system.
14 Select Is Regex if the string is a regular expression.
15 Under Threshold, add the number of times the pattern must be found to be considered a match.
16 Use \textbf{Remove} to delete specific patterns from the table.
17 Click \textbf{OK}.

To create a new text pattern group:
1 Open the McAfee DLP Management Console.
2 In the navigation panel under Definitions, select Secured Text Pattern.
   \textit{On the right-hand side you’ll find the available secured text patterns groups.}
3 Click \textbf{Add} or right-click on the Secured Text Patterns window, and select Secured Text Pattern Group.
   \textit{The New Secured Text Pattern Group icon appears.}
4 Double-click the icon.
   \textit{The Text Pattern Group editor window appears.}
5 Name the new text pattern group.
6 Add a description to the text pattern group (optional).
7 Select the needed text patterns from the available list.
8 Click \textbf{OK}.

To delete a secured text pattern or text pattern group:
1 Open the McAfee DLP Management Console.
2 In the navigation panel under Definitions, select Secured Text Patterns.
   \textit{On the right-hand side you’ll find the available secured text patterns and groups.}
3 Select the text pattern or pattern group to be removed and click \textbf{x}, or right-click on the Secured Text Patterns window and select Delete.
   \textit{The confirmation window appears.}
4 Click \textbf{YES} to confirm the deletion.
5 Click \textbf{OK}.

To save text patterns:
1 Open the McAfee DLP Management Console.
2 In the File menu, select Save Secured Text Patterns.
   \textit{A progress bar window appears.}
\textbf{Note:} All text patterns are saved to C:\Program Files\McAfee\DLP\Management Tools\Text Patterns.
Network address ranges

Network address ranges serve as filter criteria in network-related reaction rules. The **Outgoing Network Address Group** option allows you to use network ranges as a group for network-related rules.

The **Incoming Network Address Range** monitors network connections between an external source and a managed computer (the external source initiates the connection). The **Outgoing Network Address Range** is used to monitor network connections between the managed computer and the external destination (the managed computer initiates the connection).

**To create a new network address range:**

1. Open the McAfee DLP Management Console.
2. In the navigation panel under **Definitions**, select **Network Address Ranges**.
   On the right-hand side you’ll find the available incoming/outgoing network addresses ranges.
3. Click ![Add New](add_new.png) or right-click on the Network Address Ranges window, and select **Incoming Network Address Range** or **Outgoing Network Address Range**.
   The *New Network Address Range* icon appears.
4. Double-click the icon.
   The *Network Address Range Entry* window appears.

![Network Address Range Entry window](network_address_range_entry.png)

5. Add the name of the incoming/outgoing network address range.
6. Add a description for this network (optional).
7. Add the IP range as needed.
8. If the definition is related to specific protocols or ports, select **Include all of the selected ranges** or **Include all ranges except any of the selected ranges**.
9. Add the protocol type and the port ranges you want to include or exclude from the range. If you want all protocols and ports, leave the selection on **Include all of the selected ranges**, and don’t add any protocol or port ranges.
10. Click **OK**.
To create a new outgoing network address group:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Network Address Ranges.
   *On the right-hand side you’ll find the available network address groups.*
3. Click or right-click on the Network Address Ranges window and select Outgoing Network Address Group.
   *The New Network Address Group icon appears.*
4. Double-click the icon.
   *The Network Address Group window appears.*
5. Add the name of the network address group.
6. Add a description for this group (optional).
7. Select the needed outgoing network address ranges from the available list.
8. Click OK.

To delete a network address range or network address range group:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Network address Ranges.
   *On the right-hand side you’ll find the available network addresses and groups.*
3. Select the network address or network address group to be removed, click or right-click on the Network Address Ranges window, then select Delete.
   *The confirmation window appears.*
4. Click YES to confirm the deletion.
5. Click OK.
Using the Whitelist for text segments

The Whitelist allows you to define text that will be ignored by the system’s tracking mechanism. Doing this allows users to distribute known files that would otherwise be tagged and restricted by the system.

The Whitelist is a file share that contains the names of files, which agents reference when tagging data. If the data being examined exists in the whitelist, it is not tagged. To use the Whitelist, a file share must be created with read-only access by the Windows group domain computers. A typical use for the Whitelist is to include text paragraphs that are often added to documents, such as a disclaimer, license and trademark attributions, and copyright notes.

To add new whitelist content:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Whitelist.
   
   On the right-hand side you’ll find the available whitelist.
3. To use the Whitelist, a file share must be defined in the Agent Configuration options (see Configuring the agent).
4. Copy files to be whitelisted to the specified share.

To delete whitelist content:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Whitelist.
   
   On the right-hand side you’ll find the available Whitelist.
3. Select the file to be removed from the Whitelist and click or right-click on the Whitelist window, then select Delete.
   
   The confirmation window appears.
4. Click YES to confirm the deletion.
5. Click OK.

Notes: Each file available in the Whitelist folder should contain at least 400 characters for it to be ignored by the system.

If a file contains both tagged data and whitelisted data, it is not ignored by the system. However, all relevant tags associated with the content remain in effect.
File extensions

File extensions restrict tagging rules and reaction rules to particular file types. A list of default file extensions is available with in the software, and you can manually add file extensions as needed for your environment.

To create a new file extension entry:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select File Extensions. On the right-hand side you’ll find the available file extensions.
3. Click or right-click on the File Extensions window and select File Extension. The New File Extension icon appears.
4. Name the new file extension entry and double-click the icon. The File Extension Editor window appears.
5. Type the extension.
6. Type a description for the file extension (optional).
7. Click OK.

To delete a file extension:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select File Extensions. On the right-hand side you’ll find the available file extensions.
3. Select the file extension to be removed, click or right-click on the File Extensions window, and select Delete. The confirmation window appears.
4. Click YES to confirm the deletion.
5. Click OK.

Note: File extensions that are currently in use can’t be deleted; you must first delete the relevant rules containing the specific extensions.
File servers

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

To create a server list:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select File Servers.
   On the right-hand side you’ll find the available file servers.
3. Right-click on the File Servers window and select Scan for these scan options:
   - All Network Servers - By Organizational Units – select the needed organizational unit to be searched for file servers and click OK.
   - All Network Servers - By Net View – use this option to find all available file servers on the local network by using network scan.
   - Network Servers By LDAP Selection – select the needed file servers and click OK.

To add a single server:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Servers.
   On the right-hand side you’ll find the available file servers.
3. Click and select Server or right-click on the File Servers window and select Add New - Server.
   The New Server icon appears.
4. Type the server name.

Printers

The printers list is created by an LDAP query or network scan. Network printers can be defined as All Printers or can be referenced individually. If you require different printing protection rules for specific printers, define them in this list.

To create the printers list:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Printers.
   On the right-hand side you’ll find the available printers.
3. Right-click on the Printers window and select Scan for these scan options:
   - Network Printers By Organizational Units – select the needed organizational unit and click OK.
   - Network Printers By LDAP Selection – select the needed printers and click OK.
   - Scan Shared Printers – select the relevant computer, type the user name and password, select the shared printer, and click OK.
Web servers

Web Servers objects are predefined web addresses that can be referenced in web post protection rules. You can use web server definitions to block tagged data from being posted to defined web servers, or use them to prevent tagged data from being posted to websites that are not defined. Typically the web servers section defines any internal websites as well as external websites where posting tagged data is allowed.

If you have defined numerous web servers, you can create web server groups so that reaction rules can reference a single entity. A typical use of this feature is to create a web server group for all internal web sites.

To create a new web server:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Web Servers.
   On the right-hand side you’ll find the available web servers.
3. Click or right-click on the Web Servers window, and select Web Server.
   A new Web Server icon appears.
4. Double-click the icon.
   The Web Server window appears.
5. Add the web server address.
6. Add a description for this web server.
7. Click OK.

To create new web servers group:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Web Servers.
   On the right-hand side you’ll find the available web servers groups.
3. Click or right-click on the Web Servers window and select Web Server Group.
   A new Web Server Group icon appears.
4. Double-click the icon.
   The Web Server Group window appears.
5. Add the name of the web server group.
6. Add a description for this group (optional).
7. Select the needed web servers from the available list.
8. Click OK.

To delete a web server or web server group:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Web Servers.
   On the right-hand side you’ll find the available web servers and groups.
3. Select the web server or web server group to be removed and click , or right-click on the web server window and select Delete.
   The confirmation window appears.
4. Click YES to confirm the deletion.
5. Click OK.
Email destinations

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

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

To create a new email destination:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Email Destinations. On the right-hand side you’ll find the available email destinations.
3. Click or right-click on the Email Destinations window, and select Email Destination. A new Email Destination icon appears.
4. Double-click the icon.

![Figure 4: Email Destination window](image)

5. Add the email destination name.
6. Type the domain name in the Email address field and click .
   - To create an email destination of external domains, add a domain entry for every internal domain, then deselect all domains and select Other email domains.
   - To add a specific email address from this domain, right-click the domain name and select Email User, then add the needed user name.
   - To exclude a particular email address from the domain, add the user to the domain, deselect the user, then select Other email users.
7. Click OK.
To create new email group:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Email Destinations.
   On the right-hand side you’ll find the available email groups.
3. Click Add Email or right-click on the Web Servers window and select Email Group.
   A new Email Group icon appears.
4. Double-click the icon.
   The Email Destination Group window appears.
5. Add the name of the email group.
6. Add a description for this group (optional).
7. Select the needed email destinations from the available list.
8. Click OK.

To delete an email destination or email group:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Email Destinations.
   On the right-hand side you’ll find the available email destinations and groups.
3. Select the email destination or email group to be removed, click Delete or right-click on the Email Destinations window and select Delete.
   The confirmation window appears.
4. Click YES to confirm the deletion.
5. Click OK.
Classifying content with tags

To protect data, follow this high-level process.

1. Identify the types of information that need to be protected.
2. Create tags for each classification of data that needs to be protected.
3. Create tagging rules that associate data to be protected with the appropriate tag.

Each part of this process is described in this section.

Using tags to classify content

A tag is the method for maintaining the classification of content. The tag stays with the content throughout its life cycle. Two types of tags are available:

- **Standard tags** – used for location- and application-based tagging rules (see Tagging rules).
- **Content tags** – used for content-based tagging rules, which match a file’s content against predefined patterns or keywords.

To create a new tag:

1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Tags.
   
   On the right-hand side you’ll find the available tags.
3. Click [Add New] or right-click on the Tags window, then select Tag or Content based Tag.
   
   The New Tag icon appears.
4. Name the new tag and double-click the icon.
   
   The Tag Entry window appears.
5. Add a description to the tag (optional).
6. Click OK.

   **Note:** To create new tags, click the add new button in the Tagging Rule wizard. See Tagging rules for details.

To create a new tag group:

1. Open the McAfee DLP Management Console.
2. In the navigation panel under Definitions, select Tags.
   
   On the right-hand side you’ll find the available tag groups.
3. Click [Add New] or right-click on the Tags window and select Tag Group.
   
   The New Tag Group icon appears.
4. Name the new tag group and double-click the icon.
   
   The Tag group Entry window appears.
5. Add a description to the tag group (optional).
6. Select Include all of the selected tags to group these tags, or Include all tags except any of the selected tags to group all other available tags.
7. Select the needed tags for the group.
8. Click OK.

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

**To delete a tag or tag group:**
1. Open the McAfee DLP Management Console.
2. In the navigation panel under **Definitions**, select **Tags**.
   
   *On the right-hand side you’ll find the available tags and tag groups.*
3. Select the tag or tag group to be removed, click **Delete** or right-click on the Tags window, then select **Delete**.
   
   *The confirmation window appears.*
4. Click **YES** to confirm the deletion.
5. Click **OK**.

**Note:** Tags that are currently in use can be deleted only after all rules containing the specific tags are deleted.
Manually tagging content

The Manual Tagging option allows authorized users to add to or remove tags from files or folders. This option is accessed from the Management Console or, after you install the manual tagging utility on any computer, from Windows Explorer.

Tags that are applied to files immediately affect the transmission options of this content, based on the relevant rules.

In order to use manual tagging, the user must be authorized. Permission for manual tagging is defined in the Management Console under Tools | Options | Access Control tab. If a user does not have permission, the Manual Tagging option is grayed out.

Using the Management Console for manual tagging

To add a new tag manually from the Management Console:

1. Open the McAfee DLP Management Console.
2. In the navigation panel under Deployment, select Manual Tagging.

On the right-hand side you’ll find a list of the computer’s folders and files.

3. Highlight and right-click the file, then select Manual Tagging | Set Tags.
4. To add a specific tag to multiple files, highlight and right-click the files, then select Manual Tagging | Add Tags.

The Manual Tags Editor window with all the available tags appears.

5. Select the tags that are appropriate for the selected file or folder.
6. Click OK.
To remove a tag from multiple files or a folder using the Management Console:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Deployment, select Manual Tagging.
3. Highlight and right-click the needed files, then select Manual Tagging | Remove Tags.
   The Manual Tags Editor window with all the available tags appears.
4. Select the tags that need to be removed from these files.
5. Click OK.

Installing and using the manual tagging utility

To install the manual tagging utility:
1. Run the manual tagging utility Setup file.
2. Click Next to start the installation.
3. Type the full path of the installation folder and click Next.
4. Click Install to start the installation.
5. Click Finish.

To add a new tag from Windows Explorer:
1. Open Windows Explorer.
2. Highlight and right-click the file, then select Manual Tagging | Set Tags.
3. To add a specific tag to multiple files, highlight and right-click the files, then select Manual Tagging | Add Tags.
   The Manual Tags Editor window with all the available tags appears.
4. Select the tags that are appropriate for the file(s).
5. Click OK.

To remove a tag from multiple files or a folder using Windows Explorer:
1. Open Windows Explorer.
2. Highlight and right-click the needed files, then select Manual Tagging | Remove Tags.
   The Manual Tags Editor window with all the available tags appears.
3. Select the tags that need to be removed from these files.
4. Click OK.
Tagging rules

McAfee Data Loss Prevention uses *tags* to mark, track and control sensitive information. *Tagging rules* are used to associate files and data with the appropriate tags.

Creating tagging rules

Follow this procedure to create a tagging rule. Information for each tagging rule type is described under [Tagging rule wizards](#).

To create tagging rules:

1. Open the McAfee DLP Management Console.
2. Under **Rules**, select **Tagging Rules**. On the right-hand side you’ll find the available tagging rules.
3. Click ![Add file](#) or right-click on the Tagging Rules window and select one of the tagging rule types:
   - **Application Based Tagging Rule** – Files can be tagged automatically based on the application that created it. For example, all files created by Excel could automatically inherit a tag such as *Financial Data*.
   - **Location Based Tagging Rule** – Content can be tagged automatically based on the location of the file when it was accessed or copied. For example, if a file is copied from a specific file share on the network and that file share had been specified in a location-based tagging rule, the file is associated with the tag specified in the tagging rule.
   - **Content Based Tagging Rule** – Before data is transmitted, it is matched against known patterns or keywords defined in the content-based tagging rules. If a match is found, the data will be associated to the tag.

   *The New Tagging Rule icon appears.*

4. Name the new tagging rule and double-click the icon. *Based on the tagging rule type selection, the rule editor window appears.* *The new rule is disabled by default.*
5. Click ![Enable](#) to activate the rule.
Tagging rule wizards
Follow the instructions for the specific tagging rule you selected in Step 3 of Creating tagging rules.

**Application Based Tagging Rule wizard:**

1. Select the needed application from the available application groups.
2. To restrict the tag, follow one of these actions:
   - To restrict the tag to a particular file type(s), choose select from list, then select the file type from the available list.
     File types are predefined in the system and cannot be modified by the administrator. Using a specific file type in this tagging rule generates tags only on files created by a specific application and with the selected file type. This restriction is valid only for the initial tagging, based on this rule. The content related to this rule can be copied to a different file type and the new file inherits the relevant tag.
   - To restrict the tag to a particular file extension(s), choose select from list, then select the file extension from the available list.
     File extensions are predefined in the system and new extensions can be modified by the administrator (see File extensions). Using a specific file extension in this tagging rule generates tags only on files created by a specific application and with the selected file extension. This restriction is valid only for the initial tagging, based on this rule. The content related to this rule can be copied to a different file extension and the new file inherits the relevant tag.
   - To restrict the tag to files that contain a particular pattern match(es) (see Secured text patterns), choose select from list, then select the text pattern from the available list.
     Using the pattern matching restriction in this tagging rule generates tags only on files created by a specific application and files containing the specific pattern. This restriction is valid only for the initial tagging, based on this rule.
3. Select the tag for this rule or create a new one by clicking Add New... (see Classifying content with tags).
4. Click Finish to complete the rule.
Location Based Tagging Rule wizard:

1. Select the file location from the available options.
   - Network File Servers – Select Network File Servers, then in the Summary tab, click choose to open the Configure Selection window. Select the file server and specific shares.
     To add a new server or share, type its network path or click Browse, then click Add to include it in the selection list. To tag file shares or servers not in the list, select Other Shares or Other Servers, respectively.

   ![Figure 6: File servers window](image)

   - CDROM and DVD Devices – Tag files that were copied or referenced from a CD or DVD.
   - Mass Storage Devices and Floppy Disks – Tag files that were copied or referenced from flash drives, floppy disks, etc.

2. To restrict the tag, follow one of these actions:
   - If the tag should be restricted to a particular file type(s), choose select from list, then select the file type(s) from the available list.
     File types are predefined in the system and cannot be modified by the administrator. Using a specific file type in this tagging rule generates tags only on files in a specific location, as defined, and with the selected file type. This restriction is valid only for the initial tagging, based on this rule. The content related to this rule can be copied to a different file type and the new file inherits the relevant tag.

   - If the tag should be restricted to a particular file extension(s), choose select from list, then select the file extension(s) from the available list.
     File extensions are predefined in the system and new extensions can be modified by the administrator (see File extensions). Using a specific file extension in this tagging rule generates tags only on files in a specific location, as defined, and with the selected file extension. This restriction is valid only for the initial tagging, based on this rule. The content related to this rule can be copied to a different file extension and the new file inherits the relevant tag.

   - If the tag should be restricted to a particular text pattern(s), choose select from list, then select the text pattern(s) from the available list.
     Using the text pattern restriction in this tagging rule generates tags only on files in a specific location, as defined, and files containing the specific pattern. This restriction is valid only for the initial tagging, based on this rule.
3. Select the tag for this rule, or create a new one by clicking [Add Now...](see Classifying content with tags).

4. Click Finish to complete the rule.

**Content Based Tagging Rule wizard:**

1. Select the needed secured text pattern or group from the available list, or create a new pattern by clicking [Add Pattern...](see Secured text patterns).

2. Select the content-based tag for this rule, or create a new one by clicking [Add...](see Classifying content with tags).

3. Click Finish to complete the rule.

**Note:** A specific tag can be generated by more than one tagging rule. For example, an application-based tagging rule can generate a tag called "tag1," while a location-based tagging rule can generate the same "tag1" tag.

---

**Reaction rules**

Reaction rules define the action taken when an attempt is made to transfer or transmit tagged data. The reaction rule specifies the transfer method, named tag(s), and how the system should react to the event. Each event is given a severity level, and options on how to respond to the event. In some cases, reaction rules will merely log the event. In other cases, the reaction rules may prevent the transfer of data and notify the user of the violation. Reaction rules are applied to deployment groups, so a rule can be applied to all entities on the network, or potentially a predefined subset such as a particular user group.

Available reaction rule types are:

- **Application File Access Rule** – monitors the file system and determines what applications are accessing tagged data.

- **Clipboard Blocking Rule** – blocks tagged content from being copied via the clipboard.

- **Email Protection Rule** – monitors/blocks Microsoft Outlook emails containing tagged content.

- **File System Protection Rule** – monitors tagged content being copied to removable media or a network file servers.

- **Outgoing Network Connections Rule** – monitors/blocks network traffic, which is initiated by the managed computer, to an external destination using network applications such as FTP client and instant messaging (IM) client. This rule can be used to monitor and prevent:
  - Any attempt to establish a network connection using a specific application.
  - Any attempt to transmit sensitive information using a specific network application. The agent blocks the network connection as soon as it detects the tagged data transition.

- **Incoming Network Connections Rule** – monitors/blocks network traffic, which is initiated by an external source, to the managed computer. This rule can be used to monitor and prevent:
  - Any attempt to establish a network connection using a specific application.
  - Any attempt to transmit sensitive information using a specific network application. The agent blocks the network connection as soon as it detects the tagged data transition.

- **Printing Protection Rule** – monitors/blocks tagged content from being printed.
Creating Policies with the Management Console

Reaction rules

- **Screen Capture Prevention** – blocks the user from capturing the screen when tagged content is displayed.

- **Web Post Protection Rule** – monitors/blocks tagged content from being posted to web servers. This rule can prevent uploading sensitive content to web-based email servers as attachments, and can block attempts to copy content to web sites such as forums, webmails, news groups, etc.

Creating a reaction rule

Follow this procedure to create a reaction rule. Information for each reaction rule type is described under [Reaction rule wizards](#).

**To create a reaction rule:**

1. Open the McAfee DLP Management Console.
2. Under **Rules**, select **Reaction Rules**.
   
   *On the right-hand side you’ll find the available reaction rules.*
3. Click ![Add Reaction Rule](add.png) or right-click on the Reaction Rules window and select one of the reaction rule types:
   
   - **Application File Access Rule** – monitors the application file system access to tagged content.
   - **Clipboard Blocking Rule** – prevents information being copied from specific applications through the clipboard.
   - **Email Protection Rule** – monitors/blocks Microsoft Outlook emails containing tagged content.
   - **File System Protection Rule** – monitors content copied to removable media or a network file server.
   - **Network Connections Rule** – monitors/blocks applications from connecting to network resources.
   - **Printing Protection Rule** – monitors/blocks tagged content from being printed.
   - **Screen Capture Prevention** – blocks the user from copying the screens of specific applications.
   - **Web Post Protection Rule** – monitors/blocks tagged content from being posted to web servers. This rule can prevent uploading sensitive content to web-based email servers as attachments, and can block any attempt to copy content to web sites such as forums, webmails, news groups, etc.

   *The New Reaction Rule icon appears.*

4. Name the new reaction rule and double-click the icon.
   
   *Based on the reaction rule type selection, the Rule Editor window appears.*
5. Follow the instructions in the wizard for the reaction rule you selected (see [Reaction rule wizards](#) for details).
   
   *The new rule is disabled by default.*
6. Click ![Enable](enable.png) to activate the rule.
Reaction rule wizards

Follow the instructions for the specific reaction rule you selected in Step 3 of Creating a reaction rule.

Application File Access Rule wizard:
1. If the rule is related to specific application groups, select the application groups from the available application groups list.
2. If the rule is related to specific tags, choose select from list, then select the tags from the available list.
3. If the rule is related to specific file extensions, choose select from list, then select file extensions from the available list.
4. Set the Monitor level of severity.
5. Select the deployment group to apply this rule to, or define a new group by clicking Add.
6. Click Finish to complete the rule.

Clipboard Blocking Rule wizard:
1. If the rule is related to specific applications, select the applications from the available application groups list.
2. If the rule is related to a specific application window title, add the string in the Write the Window's title here field and click Add.
3. If the rule is related to specific tags, choose select from list, then select tags from the available list.
4. Select the deployment group to apply this rule to, or define a new group by clicking Add.
5. Click Finish to complete the rule.

Note: Clipboard blocking has no severity or reaction options. The events are blocked at the agent, but are not reported to the Event Collector. The user does see a popup message, but the clipboard content contains a string telling the user that the clipboard has been blocked.
Email Protection Rule wizard:
1. Select the email destination or email group from the available list.
2. If the rule is related to specific tags, choose select from list, then select tags from the available list.
3. If the rule is related to specific file types, choose select from list, then select file types from the available list.
4. If the rule is related to specific file extensions, choose select from list, then select file extensions from the available list.
5. Select actions from the available list as needed:
   - **Block** – Prevents sending tagged content via email.
   - **Monitor** – Sends events to the event collector server (with the level of severity).
   - **Notify User** – A message is displayed to the user regarding the policy violation (see Configuring the agent to customize messages).
   - **Store Evidence** – The agent creates a copy of the tagged content and saves it in the file share specified by the agent’s policy.

6. Select the deployment group to apply this rule to, or define a new group by clicking Add.

7. Click Finish to complete the rule.
File System Protection Rule wizard:
1 Select the target location from the available options:
   - **Network File servers** – If the file server and or share is already defined, you can add additional shares or directories by right clicking on the item. If the file server is not defined, you can type the share’s path in the Network Path text box and click **Add**.
   - **Other Removable Media** – select this option for mass storage devices or floppy drives.
2 If the rule is related to specific applications, select applications from the available application groups list.
3 If the rule is related to specific tags, choose **select from list**, then select the tags from the available list.
4 If the rule is related to specific file types, select **select from list**, then select file types from the available list.
5 If the rule is related to specific file extensions, choose **select from list**, then select file extensions from the available list.
6 Select actions from the available list as needed:
   - **Monitor** – sends events to the event collector server (with the level of severity).
   - **Store Evidence** – The agent creates a copy of the tagged content and saves it in the file share specified by the agent’s policy.
7 Select the deployment group to apply this rule to, or define a new group by clicking **Add** (see **Deployment groups**).
8 Click **Finish** to complete the rule.

Outgoing Network Connections Rule wizard:
1 Select the host/network to protect or define a new host/network by clicking **Add** (see **Network address ranges**).
2 If the rule is related to specific applications, choose **select from list**, then select the applications from the available application groups list.
3 If the rule is related to specific tags, choose **select from list**, then select the tags from the available list.
4 Select actions from the available list as needed:
   - **Block** – disables the connection to the selected network. To restore the network connection, the application must be closed and restarted.
   - **Monitor** – sends events to the event collector server (with the level of severity).
   - **Notify User** – sends the user a message regarding the policy violation (see **Configuring the agent** to customize messages).
5 Select the deployment group to apply this rule to, or define a new group by clicking **Add** (see **Deployment groups**).
6 Click **Finish** to complete the rule.

Incoming Network Connections Rule wizard:
1 Select the source host/network to protect connections from or define a new host/network by clicking **Add** (see **Network address ranges**).
2 If the rule is related to specific applications, choose **select from list**, then select the applications from the available application groups list.
3 If the rule is related to specific tags, choose **select from list**, then select the tags from the available list.
4 Select actions from the available list as needed:
   - **Block** – disables the connection to selected network. In order to restore the network connection, the application must be closed and restarted.
   - **Monitor** – sends events to the event collector server (with the level of severity).
   - **Notify User** – sends the user a message regarding the policy violation (see Configuring the agent to customize messages).

5 Select the deployment group to apply this rule to, or define a new group by clicking (see Deployment groups).

6 Click **Finish** to complete the rule.

**Note:** McAfee recommends applying the network connections rule for both incoming and outgoing connections, in order to eliminate any configuration oversights and to fully cover all connection options.

**Printing Protection Rule wizard:**

1 If the rule is related to specific network printers, choose **select from list** and select the needed printers. If the rule is related to all printers except a specific one, select **Other network printers**.

2 If the rule is related to restricting local printers, choose **select from list** and select **Local Printers**.

3 If the rule is related to specific applications, select the applications from the available application groups list.

4 If the rule is related to specific tags, choose **select from list**, then select tags from the available list.

5 Select actions from the available list as needed:
   - **Block** – prevents printing of tagged content.
   - **Monitor** – sends events to the event collector server (with the level of severity).
   - **Notify User** – sends the user a message regarding the policy violation (see Configuring the agent to customize messages).
   - **Store Evidence** – The agent will create a copy of the tagged content and save it in the file share specified by the agent policy.

6 Select the deployment group to apply this rule, or define a new group by clicking (see Deployment groups).

7 Click **Finish** to complete the rule.

**Screen Capture Prevention wizard:**

1 If the rule is related to specific applications, choose **select from list**, then select the applications from the available application groups list.

2 If the rule is related to specific tags, choose **select from list**, then select the tags from the available list.

3 Select the deployment group to apply this rule to, or define a new group by clicking (see Deployment groups).

4 Click **Finish** to complete the rule.

**Note:** Screen capture prevention has no severity or reaction options. The events are blocked at the agent, but are not reported to the Event Collector. The user does not see a popup message, and the screen capture fails.
Web Post Protection Rule wizard:

1. Select the web server or web server group from the available list. To select any other unlisted web servers, select **Other web servers**.

![Figure 8: Web Post Protection Rule – Step 1](image)

2. If the rule is related to specific tags, choose **select from list**, then select the tags from the available list.

3. If the rule is related to specific file types, choose **select from list**, then select the file types from the available list.

4. If the rule is related to specific file extensions, choose **select from list**, then select file extensions from the available list.

5. Select actions from the available list as needed:
   - **Block** – prevents tagged content from being posted.
   - **Monitor** – sends events to the Event Collector server (with the level of severity).
   - **Notify User** – sends the user a message regarding the policy violation (see **Configuring the agent** to customize messages).
   - **Store Evidence** – The agent will create a copy of the tagged content and save it in the file share specified by the agent’s policy.

6. Select the deployment group to apply this rule to, or define a new group by clicking **Add**.

7. Click **Finish** to complete the rule.
Controlling devices

Hardware and mass storage devices can be defined so that they can be included in device protection rules and mass storage device rules, respectively.

- **Device protection rules** – monitor hardware devices such as Bluetooth adapters and modems, and prevent the devices from being loaded by the system.
- **Mass storage device rules** – monitor hardware devices and prevent them from being loaded by the system. Additionally, mass storage device rules can restrict a device to read-only mode, preventing data from being written to the device.

Device definitions

The device list is a tool for managing and controlling available devices. New classes of devices can be added to the list for use in device protection rules. If multiple devices with similar functionality or permission issues are defined, you can create device groups to simplify how the devices are referenced in device protection rules.

**To create a new device class:**

1. Open the McAfee DLP Management Console.
2. In the navigation panel under Devices, select Device Definitions. On the right-hand side you’ll find the available devices.
3. Click or right-click on the Devices window and select Device Class. The New Device Class icon appears.
4. Name the new device class and double-click the icon. The Device Class editor window appears.
5. Add a description to the device class (optional).
6. Type the Device Internal Name. The Device Internal Name can be obtained from the registry’s device entry at: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class.
7. Type the Device GUID.
8. Click OK.
To create a new device group:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Devices, select Device Definitions.
   On the right-hand side you’ll find the available device groups.
3. Click or right-click on the Devices window and select Device Classes Group.
   The New Device Classes Group icon appears.
4. Name the new device group and double-click the icon.
   The Device Classes Group editor window appears.

![Figure 9: Device Classes Group window](image)

5. Add a description to the device class (optional).
6. Select the needed device classes.
7. Click to exclude specific device types from the device class. If a particular hardware device needs to be excluded from a device group, you can specifically exclude it here.

![Figure 10: Device Exclusion List window](image)

8. Type the Vendor ID and/or Product ID for the specific device.
9. Click OK.

**Note:** Vendor ID and Product ID can be obtained from the device entry located in the device manager.
To move a device to the ignored device list:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Devices, select Device Definitions.
   On the right-hand side you’ll find the available devices.
3. Right-click on the relevant device and select Move to Ignored devices list.
   The selected device is available on the Ignored devices list.

Built-in device protection rules
The built-in device protection rules are predefined rules that monitor and control the use of physical devices.

To edit a built-in device protection rule:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Devices, select Built In Device Protection Rules.
   On the right-hand side you’ll find the available built-in device protection rules.
3. Right-click on the rule and select Edit.
4. Follow the wizard.
   - **Step 1:** Select the deployment group to apply this rule to, or define a new group by clicking (see Deployment groups).
   - Click Finish to complete the rule.
   - The rule is disabled by default.
5. Click to activate the rule.

Device protection rules
Device protection rules monitor and potentially block the system from loading physical devices such as mass storage devices, Bluetooth, Wi-Fi, and other plug-and-play devices. Mass storage device rules offer additional functionality to set the device as read-only, to prevent saving data to the device.

To create a device protection rule:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Devices, select Device Protection Rules.
   On the right-hand side you’ll find the available device protection rules.
3. Click or right-click on the Device Protection Rules window and select one of the device protection rule types:
   - **Device Protection Rule** – monitors and/or blocks connections of physical devices.
   - **Mass Storage device rule** – monitors and/or blocks connections of all external mass storage devices.

Note: You can use the Device Protection Rule to block USB devices, but McAfee recommends using the Mass Storage Device Rule instead. Using the Device Protection Rule can result in blocking the entire USB Hub/Controller. The Mass Storage Device Rule allows the device to initialize and register with Windows, but prevents file-write operations to the device (if so configured).
4 Name the new Reaction Rule and double-click the icon.
For the Device Protection Rule, follow the wizard.

- **Step 1:** Select the needed device from the available device list. A specific device brand or product can be excluded from the list by creating a device group with the specific vendor ID and/or product ID (see Device definitions – device group).

  On the device protection rule type selection, the rule editor window appears.

![Figure 11: Device Protection Rule wizard – Step 1](image)

- **Step 2:** Select actions from the available list as needed:
  - **Block** – disables the selected devices.
  - **Monitor** – sends events to the event collector server (with the level of severity).
  - **Notify User** – sends the user a message regarding the policy violation (see Configuring the agent to customize messages).

- **Step 3:** select the deployment group to apply this rule to or define a new group by clicking ![Add...](image) (see Deployment groups).

- Click **Finish** to complete the rule.
For the Mass Storage Device Rule, follow the wizard.

- **Step 1:** Select actions from the available list as needed:
  - **Block** – disables the selected devices.
  - **Monitor** – sends events to the Event Collector server (with the level of severity).
  - **Notify User** – sends the user a message regarding the policy violation (see Configuring the agent to customize messages).
  - **Read Only** – enables read-only permissions to the mass storage device.

![Mass Storage Device Rule wizard – Step 1](image)

**Figure 12: Mass Storage Device Rule wizard – Step 1**

- **Step 2:** select the deployment group to apply this rule to or define a new group by clicking [Add...](image) (see Deployment groups).
- Click **Finish** to complete the rule.

*The new rule is disabled by default. Check the content of the rule before activation.*

- **Step 3:** Click [Enable](image) to activate the rule.
Ignored devices

The Ignored Devices option can be used to define device classes such as keyboard, mouse or other devices that can’t transfer or store data, and therefore can be ignored by the system. If a device protection rule repeatedly warns of known attached devices, you can add the devices to the ignored list to prevent further warnings.

To create a new ignored device:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Devices, select Ignored Device Definitions.
   On the right-hand side you’ll find the available devices.
3. Click Add device or right-click on the Ignored Device Definitions window and select Device Class.
   The New Device Class icon appears.
4. Name the new device class and double-click the icon.
   The Device Class Editor window appears.
5. Add a description to the Device Class (optional).
6. Type the Device Internal Name.
   The Device Internal name can be obtained from the registry’s device entry at:
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class.
7. Type the Device GUID.
8. Click OK.
   Note: The Ignored Device setting overrides what is configured in the Device Blocking Rule for this class.

To move an ignored device to the device list:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Devices, select Ignored Device Definitions.
   On the right-hand side you’ll find the available devices.
3. Right-click on the relevant ignored device and select Move to device list.
   The selected device is available on the device list.
Deployment groups

Definitions and reaction rules are applied equally to every computer and user receiving a policy. Reaction rules can be applied to particular users, groups, Active Directory organizational units, or computers. This functionality gives security officers or administrators flexibility in applying rules that are appropriate for a user’s job function. Individuals or computers that should not be accessing sensitive data can have very restrictive rule sets, while a CEO or CFO’s rule set could be much less restrictive. When reaction rules are created, they must be applied to a deployment group.

To create a deployment group:
1 Open the McAfee DLP Management Console.
2 In the navigation panel under Deployment, select Deployment Groups. On the right-hand side you’ll find the available deployment groups.
3 Click or right-click on the Deployment Groups window and select Deployment Group. The New Deployment Group icon appears.
4 Name the new Deployment Group entry and double-click the icon. The Deployment Group editor window appears with the Deployment tab displayed.

![Deployment Groups Editor window](image)

Figure 13: Deployment Groups Editor window

5 Select the needed objects for this group (domains, organizational units, groups, users and computers).
6 Click OK.
To assign specific rules to deployment groups:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Deployment, select Deployment Groups. On the right-hand side you’ll find the available deployment groups.
3. Double-click the relevant deployment group to assign the rule to. The Deployment Group editor window appears.
4. Click the Reaction Rules tab. The available reaction rules list appears.
5. Select the needed reaction rules to be deployed on this deployment group, the rule can be deployed differently when logging-in as a local user or as a domain user.

Note: The deployment group can also be created or modified from the Reaction Rule wizard (see Reaction rules).

Policy analyzer

The policy analyzer can be used to check and maintain the set of rules and system definitions. It generates errors and warnings based on the way you have configured the necessary checks.

To run the policy analyzer:
1. Open the McAfee DLP Management Console.
2. In the Tools menu, select Run Policy analyzer (or press F6).

The bottom of the management window displays policy analysis errors and warning entries.

Figure 14: Policy analyzer window
Using the Product

After creating the rules and definitions required for your enterprise, you can enforce them by deploying the policy to your managed computers. Once the policy is in place, you can use the DLP Monitor to audit the state of your enterprise’s sensitive information.

Using the Data Loss prevention software involves:

- **Deploying the policy** – distribute the DLP policy to managed computers.
- **Maintaining installed agents** – obtain status of the DLP agents, and install and uninstall agents as needed.
- **Monitoring events** – use the DLP Monitor to view, filter, and sort events in your corporate network.
- **Performing administrative maintenance** – keep the DLP agents up-to-date, maintain the DLP database, generate an agent override key, and configure the agent update server.

**Policy deployment**

The DLP policy contains definitions, tagging rules, reaction rules, deployment groups and agent configuration. A policy is first deployed to the Active Directory, then distributed to the agents.

Before deploying a policy, verify that:

- All settings are configured correctly.
- Deployment groups are assigned to each rule and enabled (see Deployment groups).
- The logged-on user has access to save the policy in the Active Directory.
- The logged-on user has adequate permissions defined in the Enterprise Policy Deployment Authorization List in the Tools | Options menu of the Management Console.

**To deploy the system policy:**

1. Open the McAfee DLP Management Console.
2. In the File menu, select Deployment | Deploy policy or click Deploy on the toolbar to enforce the system rules.
   
   The Deploying Rules window appears.
3. Click Browse to select the group policy object to deploy the system policy to, or Create to create a new policy object.
4. Click Deploy to distribute and enforce the rules.
5. Click Close.

**Note:** The system always deploys the most recently modified policy file. This prevents ambiguity when multiple Management Consoles are used.
To import a system policy from the Active Directory:
1. Open the McAfee DLP Management Console.
2. In the File menu, select Import Global Policy from Active Directory.
   The Import Policy window appears.
3. Select a policy:
   - For the current policy, select Import Policy from Current Global McAfee DLP GPO.
   - For a different policy, select Import Policy by Selected GPO.
   The Group Policy Object List window appears.
4. Select the needed group policy objects from the available list.
5. Click OK.

To restore the previous system policy (last policy that was deployed):
1. Open the McAfee DLP Management Console.
2. In the File menu, select Restore Previous Policy.
   The previous policy is available on the Management Console.
3. Select the previous policy.

To edit a policy description:
1. Open the McAfee DLP Management Console.
2. In the File menu, select Edit Policy Description.
   The policy description editor window appears.
3. Edit the policy name and/or description.
4. Click OK.
Installed agents

The McAfee DLP Management Console allows you to centrally control all installed agents within the company network. You can obtain agent status and install or uninstall agents from the selected computers. The installed agents list can be saved and loaded on a different Management Console to prevent unnecessary network scans or LDAP queries.

To allow agent installation and updates, you must first configure the Agent Installation tab on the Options menu (see Agent Installation tab).

To scan for available managed computers:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Agent Installation, select Installed agents.
   - On the right-hand side you’ll find the list of computers that were previously scanned or loaded from a saved file.
3. Right-click on the Installed Agents window and select Scan for these scan options:
   - **Hosts By Organizational Units** – managed computers can be listed by selecting an Active Directory organizational unit. This is useful for viewing managed computers from a particular department or subset of the organization.
   - **Hosts By LDAP Selection** – managed computers can be searched individually by name or as a group using LDAP queries.
4. To scan hosts by organizational units, select Hosts By Organizational Units, select the needed organizational unit in the Organizational Unit window, then click OK.
5. To scan hosts by LDAP selection, select Hosts By LDAP Selection, select the needed computers in the LDAP Query window, then click OK.
   - To search for a specific computer, type the computer name and click Search.
   - To list all available computers, leave the text blank and click Search.
   - Based on the scan, all relevant managed computers appear. If no computers are found, the list remains blank.

To refresh the agent installation status:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Agent Installation, select Installed agent.
3. Right-click on the relevant computers and select Refresh Agent Installation status to retrieve the agent status.
   - The remote machine authentication window appears.
4. Enter the user name and password of an account which has Administrative rights on the target computer.
   - The agent status is displayed.
To install the McAfee DLP agent on managed computers:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Agent Installation, select Installed agents.
3. Right-click on the relevant computers and select Install McAfee DLP Agent to install the agent on selected systems.
   The remote machine authentication window appears.
4. Type the user name and password of an account that has administrative rights on the target computer.
5. The agent installation will be executed on the target computer(s) using the authentication provided.

To uninstall the McAfee DLP agent:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Agent Installation, select Installed agents.
3. Right-click on the relevant managed computer and select one:
   - Uninstall McAfee DLP Agent With Reboot
   - Uninstall McAfee DLP Agent Without Reboot
4. Click YES to uninstall the agent from the selected computer.
   Note: Uninstalling the agent is not complete until the computer is rebooted. If reboot is selected, the computer is rebooted immediately, and the user receives no warning.

To save the installed agent list:
1. Open the McAfee DLP Management Console.
2. In the File menu, select Save Installed Agent List.
   The Save as window appears.
3. Select the needed location and file name.
4. Click Save.

To load an existing installed agent list:
1. Open the McAfee DLP Management Console.
2. In the File menu, select Load Installed Agent List.
   The Open window appears.
3. Select the needed installed agent list file.
4. Click Open.
   The installed agent list appears.
   Note: If a personal firewall is activated on the managed computer, some of the installed agent operations listed above might not work properly or might not work at all.
To open the tuning tool connection:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Agent Installation, select Installed agent.
3. Right-click on the relevant computer and select Open Tuning Tool Connection to gather agent status and other information.
4. Follow instructions provided by technical support.
   Caution: The tuning tool should only be used when instructed to do so by technical support.

To shut down a specific agent:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Agent Installation, select Installed agent.
3. Right-click on the relevant computers and select Shutdown Agent to stop the specific agent.
   The challenge/response window appears.
4. Open the tuning tool authenticator.
5. Type the challenge key and the security password (see Security tab) and click Generate Key to retrieve a response key.
6. Type the response key in the challenge/response window and click OK.

To create an agent memory dump:
1. Open the McAfee DLP Management Console.
2. In the navigation panel under Agent Installation, select Installed agent.
3. Right-click on the relevant computers and select Agent Memory Dump to generate an agent log file, which is used to troubleshoot a system malfunction.
   The challenge/response window appears.
4. Open the tuning tool authenticator.
5. Type the challenge key and the security password (see Security tab) and click Generate Key to retrieve a response key.
6. Type the response key in the challenge/response window and click OK.
7. Follow instructions provided by technical support.
   Caution: The agent memory dump should only be used when instructed to do so by technical support.
Monitoring events

When an agent determines a policy violation has occurred, it generates an event and sends it to the Event Collector. These events can be viewed, filtered, and sorted in the DLP Monitor, allowing security officers or administrators to view events and respond quickly. If applicable, suspicious content is attached as evidence to the event.

The DLP Monitor can be installed on multiple systems, and specific monitoring permissions are defined during the installation of the Event Collector.

As McAfee Data Loss Prevention takes a major role in a corporation’s effort to comply with all regulation and privacy laws, the DLP Monitor presents the sensitive information transmission in the most accurate and flexible way. Auditors, signing officers, privacy officials and other key workers can use the DLP Monitor to observe suspicious or unauthorized activities and act in accordance with corporate privacy policy, relevant regulations or other laws. The system administrator or the security officer can follow administrative events regarding agents and policy distribution status.

To monitor system events and alerts:

1. Open the McAfee DLP Event Monitor.

2. Under All Events, sort the list by clicking any column. Events can be sorted by severity, time of day, user, etc.

3. From the list, select a single event to display its full details. The event information appears at the right side of the window under Details.

4. If any Evidence is available, double-click the attached file to view its content. When the Monitor window is minimized to the taskbar, new event notifications are displayed via the popup tray.
To navigate through the complete event list:
1. Open the McAfee DLP Event Monitor.
2. On the toolbar, click \( \text{Previous} \) or \( \text{Next} \) to page through the full event list.

Filtering event data

When viewing events, you might need to reduce the amount of information shown to see relevant details at a glance. You can apply a filter to define specific criteria in order to reduce the list of events to only relevant data.

Typically when monitoring events, you might want to narrow the list to include only:

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

To define filters:
1. Open the McAfee DLP Management Console.
   By default, the filters window is hidden.
2. Click Show filter on the toolbar.
   On the left-hand side you’ll find the filters window.
3. Add a new filter by clicking Add Filter on the toolbar.
   The filter configuration window appears.

![Figure 17: Filter configuration window](image)

4. Select the needed filter conditions and properties.
5. Click OK.

The event list with the filter definition appears. To edit the filter, click. 

---

55
To filter the Events Monitor list:
1. Open the McAfee DLP Event Monitor.
2. Click to display the available filter list window.
3. Select the needed predefined filter from the filters section.
   *The event list with the filter definition appears.*
4. Select more than one filter to display them all at the same time.

   **Note:** As default, all administrative events such as agent state (up or down), policy changed etc. are displayed in the event list with all other system events. To exclude all administrative events from the list, click *Hide administrative events*.

To configure the Event Monitor settings:
1. Open the McAfee DLP Event Monitor.
2. In the *Tools* menu, select *Options*.
   *The Options window appears.*
3. Set the *Web server path* (if different than the default on the managed computer).
4. Select the data refresh interval.
5. Select the number of results per page to be displayed on the monitor event list.
6. Select *Show popup tray* to enable popup messages about new events, even when the monitor window is minimized to the taskbar.
7. Select *Focus on new event* to mark the newest event on arrival.
8. Select *Reload filter on automatic refresh* to update the filter selection tables from the reporting database automatically.
9. Click *OK*.

Export events to an Excel file for further analysis:
In some cases, when certain events should be used for further analysis (by importing these events to analysis application or unified auditing tool) or as part of an external report, you can export these events to an external Excel file.

1. Open the McAfee DLP Event Monitor.
2. In the *File* menu, select *Export*.
3. Select *Export Events to Excel* to export the complete event list, or *Export Selected Event to Excel* to choose a specific event to export from the list.
   *The Export to window appears.*
4. Type a file name and click *Save*.

To print events:
1. Open the McAfee DLP Event Monitor.
2. In the *File* menu, select *Print*.
3. Select *Print Event Table* to print the complete event list, or *Print Selected Events* to choose specific events to print.
   *The Preview window appears.*
4. Click *Print*.
To print details of a specific event:
1. Open the McAfee DLP Event Monitor.
2. Select a specific event.
3. In the File menu, select Print.
4. Select Print Details to print the event details.
   *The Preview window appears.*
5. Click Print.

To search specific content:
1. Open the McAfee DLP Event Monitor.
2. Type the needed string into the search field located in the toolbar.
3. Click to start the search.
   *The search result is marked.*

   **Note:** The search option is available only for events on the current page.

To send specific events by email:
1. Open the McAfee DLP Event Monitor.
2. Select specific events.
3. Right-click on the event and select Send email report.
   *An email message with the selected event details appears.*
4. Add recipient and click Send.

Labels

Customized labels allow you to mark events with a unique tag. The events can then be easily sorted and filtered by these customized labels.

To define labels:
1. Open the McAfee DLP Event Monitor.
2. Select a specific event.
3. Right-click on the specific event and select Set labels.
   *The Label Editor window appears.*
4. Select an available label or create a new label.
5. Click OK.
Performing administrative maintenance

For reliable system operation, Data Loss Prevention software provides administrative and maintenance tools.

- **DLP agent icon** – if applicable, the DLP agent icon is available on a managed computer, allowing the user basic operations such as updating the policy and making an override key request.

- **Database administration** – perform basic operations on the system’s database and view database statistics.

- **Agent override key generator** – allow a specific agent to bypass the system policy enforcement for a limited period of time.

- **Agent update server** – configure the location of the agent update server to retrieve updates and hotfixes automatically.

Maintaining the DLP agent

The DLP agent can be installed and maintained silently without any user interaction. The company policy arrives at the agents via the Active Directory infrastructure and can be updated as needed. Depending on the policy configuration, an agent icon can be available in the system tray to allow the user to manually update the policy and to request an override key for temporary bypass of the system policy.

![Figure 18: McAfee DLP agent menu](image)

Refreshing the DLP agent policy

Since the system policy deployment relies on the corporate Active Directory; the policy refresh on the managed computer is performed in accordance with the Active Directory settings (as a default every 90 minutes). To allow immediate policy refresh, the user must follow this procedure.

**To refresh the DLP agent policy:**

1. Right-click the DLP icon on the system tray of the managed computer.
2. Select **Refresh Policy** from the menu.
   
   *The system policy is immediately updated with the latest available policy (equivalent to the `gpupdate` command).*

**Note:** Policies are updated on a scheduled basis by Active Directory. Users of managed computers do not refresh policies manually, unless specifically instructed to do so.
Temporarily allowing an agent override
Agent override allows you to temporarily suspend blocking by the agent. When in override mode, the agent still collects and sends event information to the Event Collection server. Events are marked with the override flag. The user does not receive visual notification of events while in override mode.

To request an override key:
1. Right-click the DLP icon on the system tray of the managed computer.
2. Select Request Agent Bypass from the menu.
   The Request Agent Bypass window appears.

3. Type the Release Code that was generated using the agent override key generator (see Configuring the agent) based on the Identification Code.

   Note: The system administrator sets the length of time for the override in the system key generator. Information about the bypass period is displayed in the system tray popup message.
Database administration

Database administration provides you with a set of database-related actions for maintaining the DLP database. These actions allow you to delete events from the database. This feature is useful if the database size is too large; a new policy is created and old events are no longer considered relevant.

To administer the database:
1. Open the McAfee DLP Management Console.
2. Under DB Administration, select DB Administration.
   On the right-hand side you’ll find the administrative actions.
3. Select an action from the available list:
   - Reset Database – clears all database entries, allowing the agent to resend all locally stored events to the system central database. This can be used to resolve any current database issues, while still allowing agents to report currently cached events.
   - Delete all events – removes all database entries without the agent being able to resend these events. Deleting all events from the system can potentially allow violations to be deleted without having been seen by security officers or administrators.
   - Delete events by number of days – deletes events older than the specified number of days.
   - Delete events by date – deletes from the database events older than the specified date.
   
   The confirmation window appears.
4. Click YES to proceed with the operation.
   The operation progress bar window appears.

Note: Any time events are deleted from the database, make sure that the events being deleted have been properly reported and analyzed. Creating a database backup prior to deleting events is advised.

Database statistics

The DB Statistics interface provides you with general information about the state of the Data Loss Prevention database.

To view database statistics:
1. Open the McAfee DLP Management Console.
2. Under DB Administration, select DB Statistics.
   On the right-hand side you’ll find the list of available statistical values.
3. Select any value from the available list to view details:
   - Database Uptime – displays the time (in days and hours) since the system’s database was last started.
   - Free Disk Space – displays the free disk space available on the database machine physical disk.
   - Number of Events – displays the total number of events available on the system’s database
   - Number of Events in last day – display the number of events added to the system database within the last day
   - Number of Events in last hour – displays the number of events added to the system database within the last hour
   - Space Usage – displays the total use of disk space by system events.
Agent override key generator

In some cases, when a temporary system bypass is needed, the user can access and transfer sensitive information for a limited period of time. The agent override key generator temporarily permits a specific user – the security officer, privacy official or any identity set by the corporation – to bypass the system rules in order to deal with sensitive information. While the policy bypass is activated, the agent will only monitor the sensitive data transmission according to the applied rules but will not enforce any of the rules for the bypass time period set by the system administrator. Both the user and the system administrator receive messages about the bypass status when it’s enabled and disabled (the user via popup message and the administrator via an event entry in the DLP Event Monitor).

To generate an override key:

1. Open the McAfee DLP Management Console.
2. In the Tools menu, select Generate Agent Override Key.
3. Type the agent override request code.
4. Select the length of time to override the system rules.
5. Type the agent override key password.
6. Click to create the override code for the user.

Configure the agent update server

To allow future agent updates and patches, you must set a dedicated location on a web server, which is available to all managed computers. All future updates, patches or hotfixes released by McAfee should be stored in this location, along with a special configuration file (update.ini). This .ini file points the specific agent version to the specific update file needed in environments that support multiple versions. The address of the update web server must be added to the Update Service URL, located on the Installed Agent tab under the Options menu.
Advanced Configuration

The advanced configuration allows you to adjust the system, in order to safeguard the corporate sensitive information. System components can be customized to best fit the needs of your corporation. You can configure and fine-tune these options and components:

- **Agent configuration** – sends the agents all relevant information about event storage locations, customized user notifications, whitelisted content limitations and locations, file tracing parameters, Outlook login settings, and system module selections.

- **System options** – allows you to set access control, server location, agent installation parameters, policy analyzer settings, system logging options, and system report printing options.

### Configuring the agent

The DLP agent resides on corporate computers and executes the defined corporate policy. The agent also monitors user activities involving sensitive content. To define the behavior of the agent and other system components, use the Configuration menu in the Management Console. Agent configuration is stored in the policy, which is deployed to Active Directory. If the agent configuration is updated, the policy needs to be redeployed.

To edit the agent configuration, open the McAfee DLP Management Console. In the **Configuration** menu, select **Configure DLP Agents**.

The Agent Configuration window includes these tabs:

- Events
- Notification Service
- Security
- Whitelist
- File Tracking
- Outlook Probe
- Advanced Configuration
- Modules
Events tab

Use the Events tab to set the location of the system Event Collector and define the settings for storing evidence.

To configure the Events settings:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Configure DLP Agents.
3. The Agent Configuration window appears.
4. Click the Events tab.

![Agent Configuration - Events tab](image)

Figure 21: Agent Configuration – Events tab

4. Under Events Collector Service, define the following items:
   - **Server address and port** – name or IP address of the Event Collector and port number.
   - **Agent reconnect retry interval** – the length of time the agent waits before trying to reconnect to the Event Collector after a failed connection.
   - **Minimum backlog time** – the number of hours the agent saves events locally after sending them to the server.
5. Under Evidence Storage, type the UNC path for the location on the server where evidence should be saved.
6. Under Agent Evidence Settings, define the following items:
   - **Maximum storage limit** – the maximum space (in megabytes) allocated for storage on the managed computer.
   - **Storage limit relative to free space** – the maximum used space (in %) on the managed computer, including the space for evidence storage.
   - **Required free space on disk** – the minimum free space (in megabytes) needed on the managed computer including the evidence storage space.
   - **Evidence reconnect retry interval** – the length of time (in seconds) for the agent to try to connect to the server, in order to copy the evidence while the managed computer is disconnected from the server.
   - **Single evidence size limit** – the maximum size of one evidence file.
### Configuring the agent

#### Evidence transmission bandwidth
- the network bandwidth available between the managed computer and the server.

#### Maximum evidence age
- the maximum number of days that evidence remains on the managed computer before it is deleted.

Click **OK**.

### Notification Service tab

Use the agent notification service to send notifications to users whenever they violate the corporate policy for information protection. Using these notifications can be part of the company’s general employee training program or in accordance with government regulations. In addition, when the system bypass feature is needed, the challenge messages can be customized.

#### To configure the agent notification service:

1. Open the McAfee DLP Management Console.
2. In the **Configuration** menu, select **Configure DLP Agents**.
   The **Agent Configuration** window appears.
3. Click the **Notification Service** tab.

#### Figure 22: Agent Configuration – Notification Service tab

4. Select **Show notification** to enable the popup service.
5. Set the popup duration time (in seconds).
6. Select **Show icon** to enable the McAfee DLP icon on the managed computer system tray.
7. Type the relevant message for each of the customized agent bypass challenge messages.
8. Under **Reaction rules messages** section, type the relevant message for each reaction rule.
9. Click **OK**.
Security tab

Use the Security tab to set a password for the agent override key generator (see Override key generator) and the tuning tool authenticator.

To set the agent override key password:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Configure DLP Agents.
   The Agent Configuration window appears.
3. Click the Security tab.
4. Type a password, then retype it for confirmation.
5. Click OK.

Whitelist tab

Use the Whitelist tab to set the location of the Whitelist folder and to set the files and the folder size limits.

To configure Whitelist options:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Configure DLP Agents.
   The Agent Configuration window appears.
3. Click the Whitelist tab.
4. Under Whitelist Content, type the path to the Whitelist folder.
5. Under Size Limits, type the minimum and maximum size for the document to be whitelisted and the maximum total size of the Whitelist folder.
6. Click OK.
**File Tracking tab**

The file tracking mechanism is a fundamental component of the agent. Configuring the different content tracking related parameters, allows you to fine-tune the way that the system tracks sensitive information for a precise and efficient operation. Usually, sensitive information will be classified with appropriate tags by using NTFS extended attributes. In case of a different file system, tags can be stored by using the alternate data stream or the network share options.

To configure file tracking:

1. Open the McAfee DLP Management Console.
2. In the **Configuration** menu, select **Configure DLP Agents**.
   
The **Agent Configuration** window appears.
3. Click the **File Tracking** tab.
4. Under **General**, select **Use alternate data stream** to enable tags to be written when the extended attributes are unavailable.
5. Under **Text Extractor**, define the following items:
   - **Number of concurrent threads** – the maximum number of threads to be handled simultaneously by the system’s text extractor.
   - **Maximum input file size** – the maximum file size to be handled by the text extractor.
   - **Maximum output file size** – the maximum file size to be generated by the text extractor to be used by the agent.
6. Under **Data Service Configuration**, define the **Consecutive chunks for match** by setting the number of chunks needed to determine text matching.

When content is tracked, it is stored as chunks in the fingerprinting database. To identify similarity between portions of files, a certain amount of consecutive chunks (as defined) must be identical.

7. The **Network Shares** section should be configured when using a non-NTFS file system. If needed, define the following items:
   - **Network Tagging Strategy** – from the drop-down menu, select **File per folder** to store all tags related to a specific folder in a single file, or **File per File** to store specific file tags in a single file.
   - **Net Share Directory Name** – the network share of the specific folder where the system stores the tags information file.
8. Click **OK**.

**Caution:** Changing the Network Tagging Strategy method removes all existing file tags.
Outlook Probe tab

Use the Outlook Probe tab to configure the settings of the Microsoft Outlook plug-in. The Outlook plug-in allows the system to monitor and control the transmission of sensitive information via email messages using Microsoft Outlook.

To configure the Outlook probing options:

1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Configure DLP Agents. The Agent Configuration window appears.
3. Click the Outlook Probe tab.
4. Under Outlook Probe Cache, define the following items:
   - Enable caching – allows temporary storage of email messages for inspection.
   - Maximum cache size – the maximum size (in megabytes) allocated for caching email messages.
   - Minimum required free space – the minimum free space (in megabytes) needed on the local disk to allow caching.
   - Minimum free space – the minimum free space (in percentage) needed on the local disk to allow caching.
5. Under Outlook Progress bar, define the following items:
   - Show progress bar – enables the progress message while the system inspects outgoing email.
   - Processing time before showing progress bar – the minimum time (in seconds) the system processes the email before the progress bar appears.
   - Progress window title – the title of the progress bar window.
   - Progress window message – a customized message for the progress bar window.
6. Click OK.
Advanced Configuration tab

Use the Advanced Configuration tab to set all relevant system-related registry keys on the McAfee DLP managed computers. With this option, you can remotely define a specific set of registry keys for a specific computer. Using these registry keys allows you to remotely change various system log size values, and update service and additional system settings.

To set Advanced Configuration:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Configure DLP Agents.
   - The Agent Configuration window appears.
3. Click the Advanced Configuration tab.
4. Under Advanced Configuration, select the needed registry keys to be distributed from the available list:
   - Agent logic log size – the size (in bytes) of the agent logic log file.
   - Agent service log size – the size (in bytes) of the agent service log file.
   - Enable all reaction rules – in policy injection mode, 1 enables all reaction rules on all agents.
   - Enable Winlogon log file – the log file for agent status on the managed computer.
   - Internet Explorer probe log size – the size (in bytes) of the Internet Explorer probe log file.
   - Launch agent upon startup – 1 disables the agent at system startup.
   - Logging mask – the audit levels. Set one of the available combinations:
     - Information + warning + error + critical – type 1A8
     - Warning + error + critical – type 1A0
     - Error + critical – type 180
     - Critical – type 100
   - Outlook probe log size – the size (in bytes) of the Microsoft Outlook probe log file.
   - Relaxed login interval – the time (in seconds) before the agent starts running after user login.
   - Shell extension probe log size – the size (in bytes) of the shell extension probe log file.
   - Text extractor log size – the size (in bytes) of the text extractor log file.
   - Update service interval – the length of time (in seconds) for the agent to check for system updates.
5. In the applied on column, select all computers to apply on all available managed computer, or Choose to select a specific computer (using LDAP query).
6. Click OK.
Modules

The agent modules allow you to activate and deactivate agent components. For performance reasons, McAfee recommends that you enable only the components that will be used by the policy.

To activate/deactivate agent modules:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Configure DLP Agents.
   The Agent Configuration window appears.
3. Select any of the following available modules as needed:
   - **Agent Popup Service** – enables the popup service from the agent’s system tray icon.
   - **Clipboard Handler** – enables clipboard operations related rules ( Clipboard Blocking Rule) enforcement.
   - **HTTP Handler** – enables enforcement of Internet Explorer related rules ( Web Post Protection Rule).
   - **Network Handler** – enables enforcement of IP address/network related rules ( Network Connections Rule).
   - **Outlook Handler** – enables enforcement of Microsoft Outlook violation prevention related rules ( Email Protection Rule).
   - **Printer Handler** – enables enforcement of printing related rules ( Printing Protection Rule).
   - **Replication Service** – enables the evidence collector. This module allows the system to copy the sensitive content triggered a reaction rule and save it centrally for further forensics analysis.
   - **Reporting Service** – enable the connection to the system event collector server. This module allows the agent to transmit system events to the central event collector server.
4. Type the interval (in seconds) for the agent online status check. This indicates if a specific event occurred while the agent was offline or online.
5. Click OK.
Managing agent configuration

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

To restore the agent configuration defaults:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Restore Default Agent Configuration Settings.
   The confirmation window appears.
3. Click YES to restore default settings.

To save the agent configuration to a file:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Save Agent Configuration to File.
   The Save as window appears.
3. Select the file destination and click Save.

To load agent configuration from a file:
1. Open the McAfee DLP Management Console.
2. In the Configuration menu, select Load Agent Configuration from File.
   The Open window appears.
3. Select the needed configuration file and click Open.
System tools

Data Loss Prevention includes various tools to help you keep track of system health alerts, and to configure advanced features.

System log

Use the system log to observe and receive alerts about the system health and related events. The system log is crucial for troubleshooting.

To view the log:

1. Open the McAfee DLP Management Console.
2. In the Tools menu, select View Log (or press F7).

   The bottom of the management window displays the system log entries.

Options

System options allow you to configure some of the system’s advanced functions.

To edit the Options:

1. Open the McAfee DLP Management Console.
2. In the Tools menu, select Options.

The Options window includes these tabs:

- Access Control – configure permissions for policy deployment and manual tagging.
- Servers – configure the path to system services.
- Agent Installation – configure agent installation settings.
- Messages Boxes – hide or display specific warnings.
- Policy Analyzer – configure tests that the policy analyzer performs.
- Logging – configure logging options.
- Printing – configure printing preferences.
Access Control tab
The Access Control tab lets you allow specific users or groups (based on the Active Directory users and groups) to deploy the policy and add manual tags.

To set access control:
1. Open the McAfee DLP Management Console.
2. In the Tools menu, select Options.
   The Options window opens, displaying the Access Control tab.
3. Type the names of users or groups (based on the Active Directory) authorized to deploy the system's policy.
4. Type the names of users or groups (based on the Active Directory) authorized to set tags manually.
5. Click Validate Entries to confirm the users and groups.
6. Click OK.
Servers tab
Use the Servers tab to configure the system’s remote server paths.

To configure the server locations:
1. Open the McAfee DLP Management Console.
2. In the Tools menu, select Options.
   The Options window appears.
3. Click the Servers tab.

   ![Figure 24: Options window – Servers tab](image)

4. If the management console is not installed on the same system as the Event Collector, replace localhost with the machine name where the Event Collector is installed.
5. Click OK.

Agent Installation tab
The Agent Installation tab allows you to configure the installation properties and set additional parameters.

To configure the agent installation settings:
1. Open the McAfee DLP Management Console.
2. In the Tools menu, select Options.
   The Options window appears.
3. Click the Agent Installation tab.

   ![Figure 25: Options window – Agent Installation tab](image)
4 Select an option for reboot after installation: **Force reboot** or **Do not reboot**.

   Note: Installation of the agents is not complete until a reboot has been completed. The force reboot option does not notify the user of the reboot, and reboots immediately upon completion of the agent installation.

5 Type the following information:
   - **Installation file path** – the full UNC path for the agent installation file location.
   - **Product name**
   - **Destination folder** – the location in the managed computer of the temporary installation folder (default is ADMIN$\TEMP).
   - **Additional Parameters** – any MSI parameters to add options to the installation process (for example, `MsiLogging` to log installation).


6 Click **OK**.

**Message Boxes tab**

With the Message Boxes tab you can enable or disable common system messages.

**To select the message boxes:**

1 Open the McAfee DLP Management Console.
2 In the **Tools** menu, select **Options**.
   - The **Options window appears**.
3 Click the **Message Boxes** tab.
4 Select message types to be discarded when specific events occur:
   - **Overwrite Existing Exe** – discards the overwrite warning when replacing an EXE file in the Enterprise Applications List.
   - **Notify only 1000 items** – discards the information message about display limitations when querying LDAP objects.
   - **Load with local permission** – discards the initial message while running the management console with local permission.
   - **Load with unchecked permission** – discards the initial message while running the management console with unchecked permission (typically while the computer running the management console is disconnected from the network).
5 Click **OK**.
Policy Analyzer tab
The Policy Analyzer tab allows you to configure the needed system checks before deploying any policy or settings.

To select the checks used by the Analyzer to validate the policy:
1 Open the McAfee DLP Management Console.
2 In the Tools menu, select Options.  
   The Options window appears.
3 Click the Policy Analyzer tab.
4 Select the needed options for the errors and warnings analysis.
5 Click OK.

Logging tab
The Logging tab allows you to configure the needed audit level and log types.

To configure the logging options:
1 Open the McAfee DLP Management Console.
2 In the Tools menu, select Options.  
   The Options window appears.
3 Click the Logging tab.
4 Select options for the audit levels, log destination and log types.
5 Click OK.

Printing tab
The Printing tab allows you to select the needed rules and definitions that will be available in the system report using Export policy to HTML menu.

To configure the printing options:
1 Open the McAfee DLP Management Console.
2 In the Tools menu, select Options.  
   The Options window appears.
3 Click the Printing tab.
4 Select the needed definitions and rules to be displayed in the policy report.
5 Click OK.