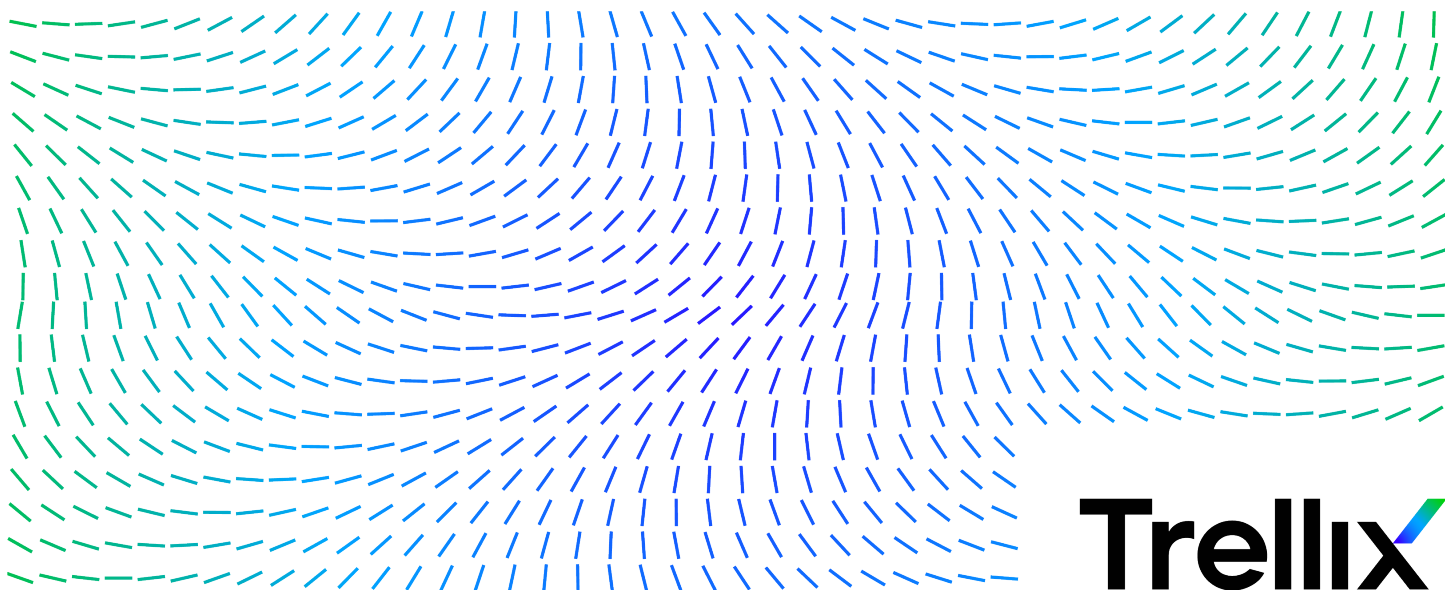


McAfee Data Loss Prevention Discover 11.6.x Installation Guide



Trellix

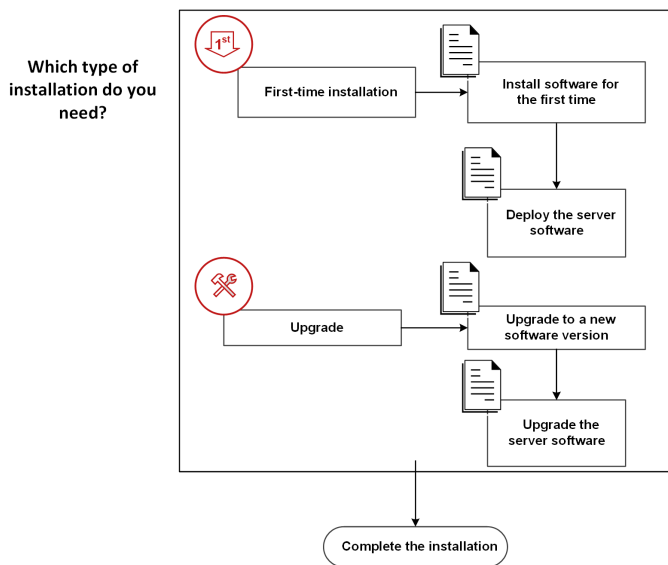
Contents

- Installation overview. 3**
 - Which type of installation do you need? 3
 - First-time installation workflow. 3
 - Upgrade installation workflow. 4
- Planning your installation. 6**
 - McAfee DLP Discover options. 6
- McAfee DLP Discover system requirements. 7**
- Pre-installation tasks. 9**
 - Download product extensions and installation files. 9
 - Prepare your network. 10
- Install software for the first time. 12**
 - Install the extension using Software Catalog (Software Manager). 12
 - Install the extension manually. 12
 - Check in the server software. 13
 - Deploy the server software. 13
- Upgrade to a new software version. 15**
 - Upgrade the server software. 15
- Post-installation tasks. 16**
 - Set up the Rights Management server. 16
 - License McAfee DLP. 16
 - Define a Rights Management server. 17
 - Configure HTTPS for DLP Server. 18
 - Back up and restore policies and settings. 19

Installation overview

Which type of installation do you need?

Install McAfee® Data Loss Prevention (McAfee DLP) software as a first-time installation or upgrade in McAfee® ePolicy Orchestrator® (McAfee® ePO™) on an on-premises, VDI, or AWS server. Deploy the McAfee® Data Loss Prevention Discover (McAfee DLP Discover) server software package to Windows Servers.



First-time installation workflow

Before you can install McAfee DLP Discover for the first time, you must install and set up McAfee ePO in the required configuration, and deploy McAfee Agent to the network endpoints.

1. Download the software from the McAfee DLP download site, or use the McAfee ePO Software Manager (Software Catalog in McAfee ePO 5.10) to view, download, and install the software.
2. Install the McAfee DLP extension in the McAfee ePO **Extensions** folder.
3. Check in the McAfee DLP Discover server package to the McAfee ePO Master Repository.

Note

If you are using the Registered Documents feature, check in the DLP Server package as well. If you are using the OCR feature, check in the OCR package. See *McAfee DLP Discover options* for more information.

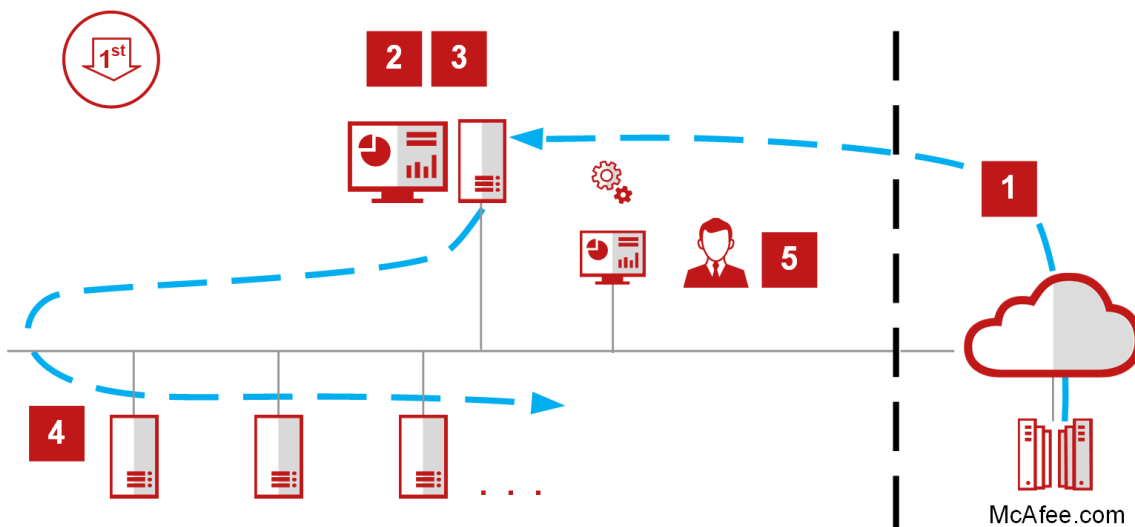
4. Deploy McAfee Agent to the McAfee DLP Discover servers.

6. Verify the installation in the DLP Operations console .



Note

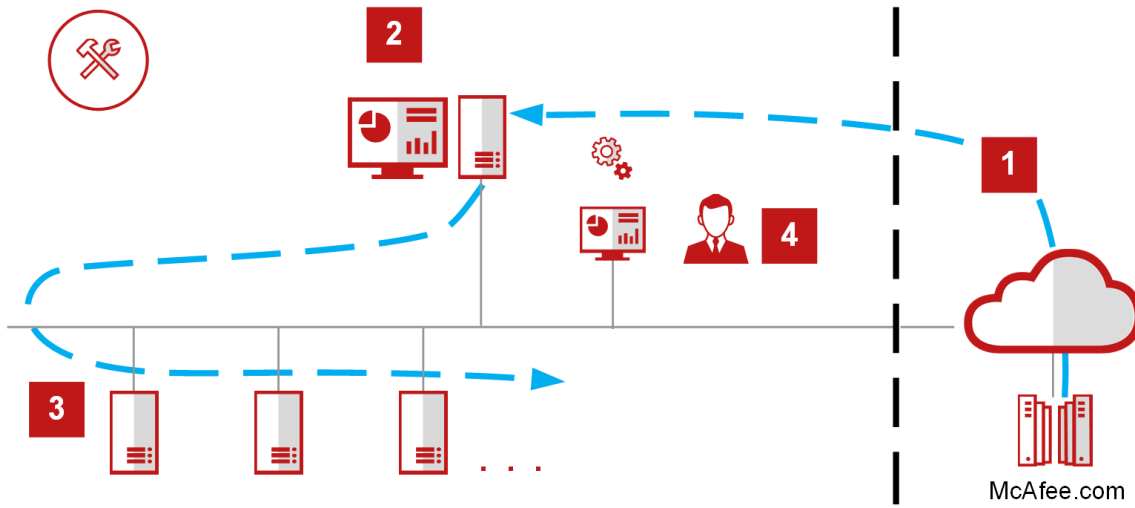
DLP Operations is a feature of the McAfee DLP extension in McAfee ePO. You must install at least one license on the **DLP Settings** page to use any of the McAfee DLP features.



Upgrade installation workflow

Upgrade installation requires only check-in and deployment of the McAfee DLP Discover server software.

1. Download the software from the McAfee DLP download site, or use the McAfee ePO Software Manager to view, download, and install the software.
2. Check in the McAfee DLP Discover server package update to the McAfee ePO Master Repository.
3. Deploy the McAfee DLP Discover server software to the servers from the McAfee ePO System Tree.
4. Verify the installation in the DLP Operations console.



Planning your installation

McAfee DLP Discover options

McAfee DLP Discover can run on physical or virtual servers. You can install one or multiple Discover servers on your network using McAfee ePO (recommended) or manually.

Large networks typically divide the workload by LAN or workgroup, and McAfee DLP can assign different policies to different groups. Reporting can be by group, or a rollout data server task can collect data from several servers to produce a single report.

Make sure that any servers you use for McAfee DLP Discover meet these requirements:

- The server has McAfee® Agent installed and running.
- The server is communicating with McAfee ePO.
- The server is added to the McAfee ePO **System Tree**.

Do not run other McAfee DLP server software on the same physical or virtual server.

McAfee DLP Discover software can be installed in one of two roles: McAfee DLP Discover server or DLP Server. The difference between a McAfee DLP Discover server (one that can run scans) and a DLP Server (a registered database server) is the server role. Setting the server role is done automatically when you install or upgrade from McAfee ePO. When installing DLP Server manually, use this command:

```
DiscoverServerInstallx64.exe ROLE=DLP
```

McAfee DLP Discover has an optional Optical Character Recognition (OCR) add-on package for extracting text from image files and scanned images saved as PDF. The add-on is installed separately in the McAfee ePO repository, and deployed to the server after deploying the McAfee DLP Discover server software. When updating, you must also update the OCR package, as it is automatically deleted when you update the server software.

DLP Servers use HTTPS as a secure communications channel with other McAfee servers, and therefore must have Microsoft Internet Information Services (IIS) installed. To use the registered documents feature, the DLP Server used to match Registered Documents content fingerprints must also be specified on the **Registered Documents** page of the server configuration in the Policy Catalog.


McAfee DLP Discover performs cryptographic operations in a way that is compliant with FIPS 140-2. Cryptographic libraries bundled with McAfee DLP Discover always have FIPS mode enabled without any option to disable it. To enable FIPS mode on Windows, refer to the published Security Policy Document for the applicable platform which can be found at the NIST Validated Modules web site. For additional information, refer to the Microsoft FIPS 140-2 Validation documentation.

For information about installing and running McAfee Agent, see the *McAfee Agent Installation Guide* and *McAfee Agent Product Guide*.

McAfee DLP Discover system requirements


Item	Requirement
McAfee ePO	<ul style="list-style-type: none">• 5.9.1• 5.10
McAfee Agent	<ul style="list-style-type: none">• 5.5.x and above• 5.6.x and above

McAfee DLP Discover Server requirements

Item	Requirement
Operating systems	<ul style="list-style-type: none">• Windows Server 2012 Standard, 64-bit• Windows Server 2012 R2 Standard, 64-bit• Windows Server 2016 Standard, 64-bit• Windows Server 2019 <div> Note: McAfee DLP Discover Server is not supported on Domain Controllers or Windows Workstations</div>
Hardware, minimum	<ul style="list-style-type: none">• CPU — Intel Core 2 64-bit, 2 CPUs minimum• RAM — 4 GB minimum• Hard Drive — 100 GB minimum
Hardware, recommended	<ul style="list-style-type: none">• CPU — Intel Core 2 64-bit, 12 CPUs• RAM — 32 GB• Hard Drive — 500 GB
Virtual servers	<ul style="list-style-type: none">• vSphere ESXi 5.0 Update 2 or 6.0• vCenter Server 5.0 Update 2 or 6.0

Item	Requirement
	<ul style="list-style-type: none"> • VMware vSphere 6.5 • VMware Server 6.5 • VMware vSphere 6.7 • VMware Server 6.7

McAfee DLP Server requirements

Item	Requirement
Operating systems	<ul style="list-style-type: none"> • Windows Server 2012 Std, 64-bit • Windows Server 2012 R2 Std, 64-bit • Windows Server 2016 R2 Std, 64-bit • Windows Server 2019 <div>  Note: McAfee DLP Server is not supported on Domain Controllers or Windows Workstations </div>
Web server	<ul style="list-style-type: none"> • Microsoft Internet Information Services (IIS) • .Net Framework 3.5
Hardware, minimum	<ul style="list-style-type: none"> • CPU — Intel Core 2 64-bit, 12 CPUs minimum • RAM — 32 GB minimum • Hard Drive — 500 GB minimum
Hardware, recommended	<ul style="list-style-type: none"> • CPU — Intel Core 2 64-bit, 24 CPUs • RAM — 64 GB • Hard Drive — 500 GB

Pre-installation tasks

Download product extensions and installation files

Before you can manually install the software, you must download the files for your installation. Alternatively, you can use **Software Catalog** to download and install.

Before you begin

Make sure that you have the grant number you received after purchasing the product.

All McAfee DLP products use the McAfee DLP extension for McAfee ePO. Install `DLP_Mgmt_version_Package.zip` as your starting point.

You can also use the McAfee ePO **Software Catalog** on McAfee ePO 5.10 (**Menu** → **Software** → **Software Catalog**) to view, download, and install the software.

In McAfee ePO 5.9 or earlier, select **Software Manager** (**Menu** → **Software** → **Software Manager**) to view, download, and install the software.

Task

1. In a web browser, go to <https://www.mcafee.com/us/downloads/downloads.aspx>.
2. Click **Download**. Enter your grant number, then select the product and version.
3. On the **Software Downloads** tab, select and save the appropriate file.

File description	File name
McAfee Data Loss Prevention extension	DLP_Mgmt_version_Package.zip
Server package for McAfee ePO	Discover_version.zip
Registered Documents server package for McAfee ePO	DLPServer_version.zip
Server StandAlone	DiscoverServerInstallx64.exe
OCR package	DLP_OCRAAddonPackage.zip
OCR StandAlone	DLP_OCRAAddon.msi

Prepare your network


Before installing McAfee DLP Discover software, you must configure the network, define administrators, and deploy the needed software.

Task

1. Configure any intermediary firewalls or policy-enforcing devices to allow the specified ports for network communication. All listed protocols use TCP only, unless noted otherwise. For information about ports that communicate with McAfee ePO, see [KB66797](#).

McAfee DLP Discover default ports

Port, protocol	Use
<ul style="list-style-type: none">• 137, 138, 139 — NetBIOS• 445 — SMB	CIFS scans
<ul style="list-style-type: none">• 80 — HTTP• 443 — SSL	Box and SharePoint scans SharePoint servers might be configured to use non-standard HTTP or SSL ports. If needed, configure firewalls to allow the non-standard ports.
53 — DNS (UDP)	DNS queries
<ul style="list-style-type: none">• 1801 — TCP• 135, 2101*, 2103*, 2105 — RPC• 1801, 3527 — UDP <p>* Indicates that the port numbers might be incremented by 11 depending on the available ports at initialization.</p> <p>For more information, see Microsoft KB article 178517.</p>	Microsoft Message Queuing (MSMQ)

Port, protocol	Use
 Note: MSMQ uses these ports only for internal communication. Nothing needs to be opened on the network firewall, but the local or host firewall needs to allow these communications.	
1433	Microsoft SQL
1521	Oracle
3306	MySQL
50000	DB2

2. Create users and groups for administrative assignments.
3. Deploy McAfee Agent to the servers.
4. Install Microsoft Internet Information Services (IIS) on the DLP Servers.

Install software for the first time

Install the extension using Software Catalog (Software Manager)

Using the **Software Catalog** (McAfee ePO version 5.10; **Software Manager** in McAfee ePO versions 5.9 or earlier) is the most convenient method of installation. As an added benefit, you can also use it to upgrade and remove extensions.

Before you begin

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

Task

1. In McAfee ePO 5.10, select **Menu** → **Software** → **Software Catalog**.
In McAfee ePO 5.9 or earlier, select **Menu** → **Software** → **Software Manager**.
2. In the left pane, expand the product categories and select **Data Loss Prevention**.
3. Select your McAfee DLP product extension you need to install.
In McAfee ePO 5.9 or earlier, the install package and extension details are displayed in the lower pane.
4. For all available software, click **Check In All**. To install a specific extension, click **Check In**.
5. Select the checkbox to accept the agreement, then click **Check In** in McAfee ePO 5.10. Click **OK** in McAfee ePO 5.9 or earlier.

Results

The extension is installed. Extensions that are checked in appear in the **Checked In Software** list. As new versions of the software are released, you can use the **Update** or **Update All** option to update the extensions.

Install the extension manually

Install the extension using the **Extensions** page.

Before you begin

Download the McAfee DLP extension from the McAfee download site.

Task

1. In McAfee ePO, select **Menu** → **Software** → **Extensions**, then click **Install Extension**.
2. Browse to the extension .zip file and click **OK**.
The installation dialog box displays the file parameters to verify that you are installing the correct extension.

3. Click **OK** to install the extension.

Check in the server software

You can add McAfee DLP Discover server software to the McAfee ePO Master Repository to prepare for deployment to enterprise servers. If you are using the Registered Documents feature, check in the DLP Server package and deploy it to the server required to act as the registration database. For Optical Character Recognition (OCR) feature, you must check in the OCR package.

Before you begin

Download the McAfee DLP Discover server software from [the McAfee download site](#) or use the Software Catalog.

For optimum performance, install McAfee DLP Discover server software on a clean server. Running other McAfee or third-party applications on the McAfee DLP Discover server can impact performance.

Task

1. In McAfee ePO, select **Menu** → **Software** → **Master Repository**.
2. In the Master Repository, click **Check In Package**.
3. Select package type **Product or Update (.ZIP)**, then click **Browse**.
 - McAfee DLP Discover server packages are named `Discover_[version number].zip`.
 - The DLP Server packages are named `DLPServer_[version number].zip`
 - The OCR package is named `DLP_OCRAaddonPackage[version number].zip`
4. Click **Next**.
5. Review the details on the **Check in Package** page, then click **Save**.

The package is added to the Master Repository.

Deploy the server software

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

Before you begin

Deploy McAfee Agent to the server and add the server to the McAfee ePO System Tree.

Task

1. In McAfee ePO, select **Menu** → **Product Deployment**.
2. Click **New Deployment**.
3. On the **Product Deployment** page, do the following:
 - a. Type the name of the deployment task: `Deploy DLP Discover Server`.

- b. Select the type: **Continuous** or **Fixed**.
- c. Select the package from the drop-down list: **McAfee DLP Discover Server [version_number]** or **DLPServer [version_number]**.

The OCR package is an add-on. Complete all steps on this page for the McAfee DLP Discover server software before deploying the OCR package.

- d. Click **Select Systems** and choose the system to deploy.
4. In the **System Tree**, select the system to deploy to and click **OK**.
 5. On the **Product Deployment** page, click **Save**.
 6. Track the progress of the deployment on the **Product Deployment** page.

Upgrade to a new software version

Upgrade the server software

Upgrade installation consists of checking in and deploying the McAfee DLP Discover server software and OCR software packages.

Before you begin

Download the McAfee DLP extension and McAfee DLP Discover server software from the [McAfee download site](#) or use the Software Catalog (with the **Download** option).

Upgrade the McAfee DLP extension in McAfee ePO before upgrading the McAfee DLP Discover server software.

Note

The McAfee DLP extension version must be the same or newer than the McAfee DLP Discover server version.

The OCR package is deleted when you upgrade the McAfee DLP Discover server software. After deploying the upgrade McAfee DLP Discover software, deploy the upgrade OCR package. The OCR package version must be the same as the McAfee DLP Discover server software.

Task

1. In McAfee ePO, select **Menu** → **Software** → **Master Repository**.
2. In the Master Repository, click **Check In Package**.
3. Select package type **Product or Update (.ZIP)**, then click **Browse**.
 - The McAfee DLP Discover server package is named `Discover_[version number].zip`.
 - The DLP Server package is named `DLPServer_[version number].zip`
 - The OCR package is named `DLP_OCRAaddonPackage.zip`
4. Click **Next**.
5. Review the details on the **Check in Package** page, then click **Save**.

The package is added to the Master Repository.
6. Deploy the server software with McAfee ePO.

Post-installation tasks

Set up the Rights Management server

If you are working with a Rights Management system, you must set up and register the rights management server. You must also install the needed version of the Active Directory Rights Management Services Client for McAfee DLP Discover to be able to apply Rights Management encryption to files.

Task

1. Set up the Rights Management server and register it with McAfee ePO.
2. For McAfee DLP Endpoint only, install Active Directory Rights Management Services Client 2.1 build 1.0.2004.0 on each endpoint using RM services.

License McAfee DLP

To access your McAfee DLP products, license details are required when accessing McAfee DLP for the first time and are entered in DLP Getting Started. Additional new licenses and edits to existing licenses are configured in **Data Protection → DLP Settings**.

Note

You can enter a license for either McAfee DLP Endpoint or Device Control in the McAfee DLP Endpoint field. Replacing one type of license with another changes the configuration.

You can enter keys for these products:

- McAfee DLP Endpoint or Device Control
- McAfee DLP Discover
- McAfee Legacy Network DLP (9.3.x)
- McAfee DLP Prevent (10.x or later)
- McAfee DLP Monitor (11.x or later)

The DLP Settings module has eight tabbed pages. Information about the **General** tab is required. You can use the default values or fields for most of the remaining settings if you don't have special requirements.

The **MVISION Cloud Server** tab is used to set up integration with McAfee® MVISION Cloud.

Task

1. In McAfee ePO select **Menu → Data Protection → DLP Settings**.
2. On the **General** tab in the **License Keys → Key** field, enter the license key for each license that you want to add, then click **Add**.

Installing the license activates the related McAfee ePO components and McAfee ePO Policy Catalog policies.

3. In the **Default Evidence Storage** field, enter the path.

The evidence storage path must be a network path, that is \\[server]\\[share]. This step is required to save the settings and activate the software.

4. Set the shared password.

5. Set the backward compatibility.

Choose from one of the five options ranging from **9.4.0.0** to **11.0.0** and later compatibility. This setting limits the possibility of using new features.

Two modes of compatibility are available: strict and non-strict. In strict mode, policies with backward compatibility errors cannot be applied. In non-strict mode, the policy owner, or a user with Administrator permissions, can choose to apply policies with backward compatibility errors.

**Note**

If you are using multiple client versions, set the compatibility to match the oldest client version in use.

6. Click **Save**.

7. To back up the configuration, select the **Back Up & Restore** tab, then click **Backup to file**.

Results

McAfee DLP modules appear in **Menu** → **Data Protection** according to the licenses entered.

Define a Rights Management server

McAfee DLP Endpoint and McAfee DLP Discover support two Rights Management (RM) systems: Microsoft Windows Rights Management Services (RMS) and Seclore FileSecure™. To use these systems, configure the server providing the RM policies in McAfee ePO.

Before you begin

- Set up the RM servers according to the Microsoft or Seclore instructions and create users and policies. Obtain the URL and password for all servers — policy template, certification, and licensing.
- If you are adding an Azure server for integration with Azure Information Protection, you need to first register a client application with Azure Active Directory. See [KB91833](#) for details about registering a client application with Microsoft Azure.
- For Seclore, you need the Hot Folder Cabinet ID and passphrase, and information about advanced licenses, if any.
- Verify that you have permission to view, create, and edit Microsoft RMS and Seclore servers. In McAfee ePO, select **Menu** → **User Management** → **Permission Sets**, and verify that you belong to a group that has the needed permissions in **Registered Servers**.
- Install Active Directory Rights Management Services Client 2.1 build 1.0.2004.0 on each endpoint using RM services. The **Apply RM** command doesn't work without this version of the RM client.

Task

1. In McAfee ePO, select **Menu → Registered Servers**.
2. Click **New Server**.
The **Registered Servers** description page opens.
3. From the **Server type** drop-down list, select the type of server you want to configure: **Microsoft RMS Server**, **Azure Server**, or **Seclore Server**.
4. Type a name for the server configuration, then click **Next**.
5. Enter the required details. When you have entered the required fields, click **Test Connectivity** to verify the data entered.
 - RMS settings also include a **DLP enforcement settings** section. The **Local path to RMS template** field is optional, but the URL fields for certification and licensing are needed unless you choose the AD auto-service discovery option.
 - Seclore requires **HotFolder Cabinet** information, but more license information is optional.
 - Azure Server settings require:
 - **Rights management owner** is the user that owns all the files that are protected with Azure RMS rule reaction.
 - **Application (Client) ID**, **Directory (Tenant) ID**, and **Client Secret** as defined in the Azure application registration details.
 - Azure Label IDs and Names as it appears in your Azure account. These labels can be selected for protection in rule reactions.
6. Click **Save** when you have completed the configuration.

Configure HTTPS for DLP Server

DLP Server uses HTTPS as a secure communications channel with other McAfee servers. After installing DLP Server, configure the server to enable HTTPS.

Before you begin

Obtain a certificate file from the certificate authority. You can use the certificate request tool (**Server Certificates → Actions → Create Certificate Request** in IIS) to obtain the certificate.

McAfee DLP Server software employs Microsoft Internet Information Services (IIS) as a web server, using HTTPS as a secure communications channel. HTTPS uses Secure Sockets Layer (SSL) to exchange information between the server and clients. To enable SSL/HTTPS in IIS you must configure the server with an SSL certificate file obtained from a certification authority.

Task

1. Obtain a certificate file.
 - a. In IIS, go to **Server Certificates → Actions → Create Certificate Request**.
 - b. Fill in the required fields on the first page and click **Next**.
 - c. Review the second page. In most cases, you can accept the defaults. Click **Next**, then **Finish**.
 - d. Send your request to the certificate authority to order your certificate.

2. Install the certificate file.
 - a. In IIS, go to **Server Certificates** → **Actions** → **Complete Certificate Request**.
 - b. Enter the name of the file you received from the certificate authority.
 - c. In the **Friendly name** field, enter the name you want to appear in the IIS certificates list.
 - d. Select **Personal** for the certificate store value, then click **OK**.

The certificate appears in the IIS certificates list.

3. Create a binding.

This step is required to make the web site available by HTTPS.

- a. In the **Connections** (left) panel in IIS, select **DlpServer**.
- b. Select **Actions** → **Bindings**.
- c. Select **https**, then click **Edit**.
- d. Select your certificate (by Friendly name) from the **SSL certificate** drop-down list. Click **OK**.

What to do next

We recommend configuring IIS to accept connections only from a list of specified McAfee DLP Discover, McAfee DLP Prevent, McAfee DLP Monitor, and other McAfee servers that need access to the DLP Servers. For information on restricting IIS to specific IPs, see Microsoft's [IP Security](#) documentation.

Back up and restore policies and settings

You can create a backup of your McAfee DLP policies and settings, and then restore them by loading it to another . This includes all your configurations in **Data Protection** → **DLP Settings**.

You can encrypt your backup file by setting up a password. Set up an encryption password so that your Shared Password isn't in readable format when recovering the backup file.

Task

1. Back up your McAfee DLP Endpoint policies and settings.
 - a. In , select **Data Protection** → **DLP Settings** → **Backup & Restore**.
 - b. Leave the default setting for **Encrypt the backup file** and enter an encryption password.
 - c. Click **Backup to file**. Options allow you to select the backup path, to open the file, and to save it.
 - d. (Optional) Select the checkbox to save the policy injection object (OPG) in the backup.
2. Restore your McAfee DLP Endpoint settings.
 - a. In another , select **Data Protection** → **DLP Settings** → **Backup & Restore**.
 - b. Select the checkbox **Password if the backup file is encrypted**.
 - c. Enter the password you set for encrypting the backup file.
 - d. Click **Restore from file** and select the file you saved.

Results

A restore report is generated for review.

COPYRIGHT

Copyright © 2022 Musarubra US LLC.

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others.