Revision A

McAfee Data Loss Prevention Monitor 11.0.300 Installation Guide

(McAfee ePolicy Orchestrator)
COPYRIGHT
Copyright © 2018 McAfee, LLC

TRADEMARK ATTRIBUTIONS
McAfee and the McAfee logo, McAfee Active Protection, ePolicy Orchestrator, McAfee ePO, McAfee EMM, Foundstone, McAfee LiveSafe, McAfee QuickClean, Safe Eyes, McAfee SECURE, SecureOS, McAfee Shredder, SiteAdvisor, McAfee Stinger, True Key, TrustedSource, VirusScan 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.

LICENSE INFORMATION
License Agreement
NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANY YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEBSITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.
## Contents

1 **Planning your deployment** ............................................................... 5
   McAfee DLP implementation .................................................................. 6
   McAfee DLP Monitor deployment options ........................................... 7
   Requirements ....................................................................................... 8
   Deployment scenarios ........................................................................... 9
   Deploying McAfee DLP appliances in clusters ...................................... 9
   Deploying a virtual appliance .............................................................. 11
   Deployment checklist .......................................................................... 13

2 **Installing the software** ................................................................. 15
   Download product extensions and installation files ............................... 15
   Virtual appliance installation download package .................................. 16
   Install and license the McAfee DLP extension ..................................... 16
   Install the extension using the Software Manager .............................. 16
   Install the extension manually ............................................................ 17
   License McAfee DLP .......................................................................... 17
   Set advanced configuration options .................................................... 18
   Set classification settings ................................................................... 18
   Install your McAfee DLP Monitor appliance ..................................... 18
   Install the extensions in McAfee ePO .................................................. 19
   Configure network information in McAfee ePO .................................. 19
   Install the appliance software on a virtual appliance ....................... 20
   Install the appliance software on a hardware appliance ..................... 20
   Connect Capture port 1 to your network .......................................... 22
   Configuring the appliance ................................................................. 23
   Configuring IP addresses ................................................................... 23
   Run the Setup Wizard and register the appliance with McAfee ePO ..... 23
   Post-installation tasks ........................................................................ 24

3 **Upgrading the software** ................................................................. 25
   Upgrading options ............................................................................. 25
   Apply a patch, hotfix, or new version using the internal installation image . 26
   Alternate upgrade options for a hardware appliance ............................ 26
   Re-image an appliance using RMM virtual media ............................... 26
   Re-image an appliance using a USB CD drive .................................... 27
   Make the USB device bootable ........................................................... 28
   Re-image an appliance using a USB drive .......................................... 28
   Re-image model 4400 using a DVD .................................................... 29
   Upgrade a virtual appliance by binding an ISO image ...................... 29

4 **Maintenance and troubleshooting** .................................................. 31
   Managing with the McAfee DLP appliance console ............................ 31
   Accessing the appliance console ........................................................ 32
   Change original network settings ....................................................... 32
   Modify speed and duplex settings for hardware appliances ............... 33
Planning your deployment

Contents
- McAfee DLP implementation
- McAfee DLP Monitor deployment options
- Deployment scenarios
- Deployment checklist
McAfee DLP implementation

The recommended installation for a simple McAfee® Data Loss Prevention (McAfee DLP) implementation is on a single McAfee® ePolicy Orchestrator® (McAfee® ePO®) server.

McAfee DLP extension is installed on the McAfee ePO server. It manages the policies and data analysis for all McAfee DLP applications. It is the starting point for all deployments.

Figure 1-1  Basic McAfee DLP deployment with options

1  McAfee ePO server — Hosts the embedded McAfee DLP software and the DLP Classification, Incident Manager, Operations, and Case Management modules.
1a  Administrator workstation — Accesses McAfee ePO and the McAfee DLP module consoles in a browser.
1b  McAfee ePO database

For recommendations on using a separate server for the McAfee ePO database in more complex installations, see the McAfee ePolicy Orchestrator Hardware Sizing and Bandwidth Usage Guide.

1c  Evidence storage — stores an encrypted copy of the content that was blocked or monitored
2 Managed endpoints — Apply the security policies using the McAfee® Data Loss Prevention Endpoint (McAfee DLP Endpoint) client software.

3 McAfee® Data Loss Prevention Discover (McAfee DLP Discover) servers (physical or virtual) — Scan network repositories and databases, classify data, and apply security policies (remediation).

3a McAfee DLP Discover local or cloud repositories

4 McAfee® Data Loss Prevention Prevent (McAfee DLP Prevent) appliance (physical or virtual) — Analyzes email and web traffic and applies security policies.

4a Email gateway and web gateway

5 McAfee® Data Loss Prevention Monitor (McAfee DLP Monitor) appliance (physical or virtual) — Acquires network packets through a network tap, monitors network traffic and applies security policies.

6 McAfee® Data Loss Prevention Prevent for Mobile Email (McAfee DLP Prevent for Mobile Email) server — Receives email from a MobileIron Sentry server (6a). It analyzes the email and attachments and creates incidents, or saves evidence, based on mobile protection rules.

6a MobileIron Sentry server

---

**McAfee DLP Monitor deployment options**

McAfee DLP Monitor passively assesses your network without blocking traffic and can run on physical or virtual hardware. You can set it up as a standalone appliance or as a member of a cluster. Deploying the appliance in a cluster enables you to load balance the analysis of the network traffic.

- Virtual appliances can run on your own VMware ESX or VMware ESXi.
- You can install McAfee DLP Monitor on 4400, 5500, or 6600 appliance models.
- You can install a VMware ESX or VMware ESXi on 5500 or 6600 appliance models.

**High-level steps for implementation**

1 Connect the appliance to your network.

2 Install McAfee DLP Monitor.

3 Configure the McAfee DLP Monitor appliance as a standalone device or as a member of a cluster.

   After the appliance is configured, register it with McAfee ePO to be managed.

4 Integrate the appliance into your network using, for example, a SPAN port or network tap.

5 Enable relevant predefined policies and rules.

6 Create additional rules and policies.

7 Review incidents generated by McAfee DLP Monitor.

8 Tune rules as needed to reduce false positives.

To use McAfee DLP Monitor and McAfee DLP Prevent on the same network, install McAfee DLP Monitor first to analyze how traffic flows through your network.

---

**Network placement**

The placement of McAfee DLP Monitor determines what data is analyzed. McAfee DLP Monitor can connect to any switch in your network using, for example, a SPAN port or network tap. Typically, it connects to the LAN switch before the WAN router. This placement makes sure that McAfee DLP Monitor analyzes all connections entering or leaving the network.
McAfee DLP Monitor Capture port 1 must be connected to a network port that transmits all packets you want it to analyze.

**Cluster setup**

A cluster of McAfee DLP Monitor appliances consists of a packet acquisition device and two or more dedicated scanning appliances. You can configure the cluster role from the Setup Wizard during the installation of an appliance.

Once the cluster role is applied to an appliance, the system reboots automatically. Later, to change the cluster role, you must reset the appliance to factory defaults and apply the cluster role you want.

All nodes in a cluster must be connected to the same physical network. One of the scanning nodes listens on the configured virtual IP address for the incoming scanning requests and distributes them to the remaining cluster members.

The scanning appliances support failover, that is, if the appliance listening on the virtual IP address fails, another scanner member takes over its responsibilities.

To manage the appliances, provide the cluster ID and virtual IP address from the McAfee ePO console.

The cluster ID and virtual IP address must be unique and different from that of the McAfee DLP Prevent cluster ID and virtual IP address.

**Best practices for setting up a cluster**

Use these guidelines when setting up a McAfee DLP Monitor cluster.

- Run McAfee DLP Monitor appliances as part of a cluster to load balance the analysis of network traffic.
- Deploy two or more scanners to achieve maximum scanning capacity.
- Connect all scanners to a private scanning network and not to a public network.

**Requirements**

To ensure that your deployment is successful, your environment must meet the minimum requirements.

For performance optimization, make sure that all appliances in a cluster are of the same model, and all virtual appliances have the same specifications.

**System requirements for setting up a virtual appliance**

Your host computer must adhere to the system requirements. For VMware virtual environment, see the VMware Knowledge Base article 1003661 available at [https://www.vmware.com](https://www.vmware.com) to get the minimum system requirements for VMware ESX or VMware ESXi.

The processor in your virtual environment must support the SSE (Streaming SIMD Extensions) 4.2 instruction set.

You need a computer that has a 64-bit x86 CPU.

Ensure that the virtual machine that you run meets these minimum system requirements:
System requirements for setting up a hardware appliance
You can install your appliance on 4400, 5500, or 6600 models, which are Intel Server systems.

Table 1-3  Model specifications

<table>
<thead>
<tr>
<th>Model</th>
<th>Number of hard drives</th>
<th>Capture database capacity*</th>
<th>RAM**</th>
<th>Remote Management Module (RMM)</th>
<th>Rack height</th>
</tr>
</thead>
<tbody>
<tr>
<td>4400</td>
<td>12</td>
<td>7.2 TB</td>
<td>24 GB</td>
<td>Yes</td>
<td>2U</td>
</tr>
<tr>
<td>5500</td>
<td>8</td>
<td>9 TB</td>
<td>32 GB</td>
<td>Yes</td>
<td>2U</td>
</tr>
<tr>
<td>6600</td>
<td>2</td>
<td>N/A</td>
<td>32 GB</td>
<td>Yes</td>
<td>1U</td>
</tr>
</tbody>
</table>

* McAfee DLP Monitor 11.x appliances do not use a capture database.
** McAfee does not support adding more memory to McAfee DLP Monitor appliances.

Deployment scenarios

Contents
- Deploying McAfee DLP appliances in clusters
- Deploying a virtual appliance

Deploying McAfee DLP appliances in clusters
You can deploy a McAfee DLP Monitor cluster or a McAfee DLP Prevent cluster or both clusters based on your environment.

Deploy a McAfee DLP Monitor cluster when the network traffic monitoring and scanning capacity you want exceeds that of a standalone McAfee DLP Monitor appliance. In this scenario, a single deployment of McAfee DLP Monitor cluster monitors and scans a busy network.

Deploy a McAfee DLP Prevent cluster to load balance the incoming email and web traffic, and accomplish high availability if a cluster node fails. In this scenario, a single deployment of McAfee DLP Prevent cluster analyzes and load balances the email and web traffic.

The cluster ID and the virtual IP address must be different from that of a McAfee DLP Prevent cluster ID and virtual IP address. You must not share the cluster scanners between two clusters.

Using a McAfee DLP Monitor cluster has the following requirements:
- A dedicated McAfee DLP Monitor packet acquisition device.
- Two or more dedicated McAfee DLP Monitor scanners.
Using a McAfee DLP Prevent cluster has the following requirements:

- A McAfee DLP Prevent primary node (the master). The master is responsible for distributing email and web traffic for analysis between itself and the cluster scanners. If the master fails, any of the cluster scanners take over the primary role.

- One or more McAfee DLP Prevent scanners.

**How McAfee DLP appliances in clusters work**

![Deployment diagram]

**Figure 1-2 Deployment of McAfee DLP appliances as clusters**

Three networks are connected to three routers:

- R1 is connected to general network traffic.

- R2 is connected to a management network with the McAfee ePO server connected to it. All McAfee DLP Monitor and McAfee DLP Prevent systems have their management interfaces connected to R2.

- R3 is connected to a private scanning network of the McAfee DLP Monitor cluster. All McAfee DLP Monitor systems have their LAN1 interfaces connected to R3.

Mail Transfer Agent (MTA) is the mail server for the R1 network, while McAfee® Web Gateway is used as the web proxy. Other systems are also connected to this network and R1 is the route out.

P1 and P2 are two McAfee DLP Prevent servers in a cluster. Their LAN1 interfaces are connected to R1. They receive email traffic from MTA and web traffic from the web gateway (MWG). The responses go back to MTA and MWG, while the events are sent to the McAfee ePO server.
A network tap mirrors all network traffic going through R1 to the capture interface on the packet acquisition device, MON PAD. The appliances, MON SCAN 1 and MON SCAN 2 are dedicated load balancing scanners and receive scanning requests from MON PAD. The scan results are sent to McAfee ePO for monitoring and tracking the incidents.

**Deploying a virtual appliance**

You can install and deploy appliances in virtual environments with different server configurations.

**Running the virtual appliance as the only virtual machine on the host**

This is a possible single-server deployment of the virtual appliance on your chosen virtual environment. VMware ESX or VMware ESXi are dedicated servers to the virtual appliance. Their hardware specification must exceed the minimum hardware requirements.

![Figure 1-3 Single server deployment](image)

**Running the virtual appliance with other virtual machines**

This is a possible deployment of the virtual appliance on your chosen virtual environment alongside other virtual machines.
In this example, one virtual machine host is responsible for the virtual appliance and other virtual machines, all of which run on the same hardware. The resource pool must also have the minimum levels of CPU and memory allocated to it.

Figure 1-4 Multiple server deployment
Deployment checklist

Before installing a McAfee DLP product, verify that you have all information needed for a successful deployment.

Table 1-4  McAfee DLP Monitor considerations

<table>
<thead>
<tr>
<th>Determine</th>
<th>Consideration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>• Use out-of-band management on a network that McAfee ePO can access to isolate management and network traffic.</td>
</tr>
<tr>
<td></td>
<td>• When clustering is enabled, LAN1 traffic must not be accessible from outside your organization. You do not have to connect LAN1 if you are not using clustering.</td>
</tr>
<tr>
<td></td>
<td>• Connect any baseboard management controller (BMC) interface to a dedicated secure management network.</td>
</tr>
<tr>
<td></td>
<td>• Control who can access the physical or virtual appliance console.</td>
</tr>
<tr>
<td>Network information</td>
<td>• Determine the most appropriate place in your network to attach the McAfee DLP Monitor appliance Capture port 1. For example, consider using a SPAN port or a network tap.</td>
</tr>
<tr>
<td></td>
<td>• Network interfaces — Verify that these are statically assigned IP addresses, rather than dynamically assigned IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• Logon account — The appliance has a local administrator account for logging on to the virtual machine shell. To make the account secure, change the default password.</td>
</tr>
<tr>
<td></td>
<td>• In a cluster environment, the virtual IP address must be in the same subnet as the appliance LAN1 IP addresses.</td>
</tr>
<tr>
<td></td>
<td>• The cluster ID and the virtual IP address must be different from that of a McAfee DLP Prevent cluster ID and virtual IP address.</td>
</tr>
<tr>
<td>Remote Management Module (RMM)</td>
<td>(Hardware appliances only) If you intend to use the RMM for appliance management, use a secure or closed network to connect to the RMM.</td>
</tr>
</tbody>
</table>
Installing the software

Contents
- Download product extensions and installation files
- Install and license the McAfee DLP extension
- Install your McAfee DLP Monitor appliance
- Configuring the appliance
- Post-installation tasks

Download product extensions and installation files

Download the files for your installation.

Before you begin
Locate 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 Manager (Menu | Software | Software Manager) to view, download, and install the software.

Task
2 Enter your grant number, then select the product and version.
3 On the Software Downloads tab, select, and save the appropriate file.

<table>
<thead>
<tr>
<th>File description</th>
<th>File name</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee Data Loss Prevention</td>
<td>DLP_Mgmt_version_Package.zip</td>
</tr>
<tr>
<td>extension</td>
<td></td>
</tr>
<tr>
<td>McAfee DLP Appliance Management</td>
<td>dlp-appliance-management-package-version-extensions.zip</td>
</tr>
<tr>
<td>extension</td>
<td></td>
</tr>
<tr>
<td>AME extension</td>
<td>appliance-management-package-version-extensions.zip</td>
</tr>
<tr>
<td>Common UI extension</td>
<td>commonui-core-package-version-extensions.zip</td>
</tr>
<tr>
<td>Installation image</td>
<td>• For VMware vSphere virtual appliance — McAfee-MS-version.ms.hw8.hdd.ova</td>
</tr>
<tr>
<td></td>
<td>• Hardware appliance — McAfee-MS-version.iso</td>
</tr>
</tbody>
</table>
Tasks

• Virtual appliance installation download package on page 16
  The McAfee DLP Monitor virtual appliance for installation on VMware vSphere is supplied as an .ova file that contains the software installation files.

Virtual appliance installation download package
The McAfee DLP Monitor virtual appliance for installation on VMware vSphere is supplied as an .ova file that contains the software installation files.

The download package does not contain VMware vSphere product installation files.

If you don't have your virtual software set up, go to the product website. To purchase VMware vSphere (ESX) or VMware vSphere Hypervisor (ESXi), go to https://www.vmware.com.

Install and license the McAfee DLP extension

Contents

• Install the extension using the Software Manager
• Install the extension manually
• License McAfee DLP
• Set advanced configuration options
• Set classification settings

Install the extension using the Software Manager
You can use the Software Manager to install, 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, select Menu | Software | Software Manager.
2 In the left pane, expand Software (by Label) and select Data Loss Prevention.
3 Select your McAfee DLP product.
   Select the entry for McAfee DLP Appliance Management, which installs all of the necessary extensions:
   • McAfee DLP
   • Common UI
   • Appliance Management Extension
   • McAfee DLP Appliance Management
4 For all available software, click Check In.
5 Select the checkbox to accept the agreement, then click OK.
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** 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.

**License McAfee DLP**
Provide the license to access the McAfee DLP consoles.
You must enter at least one license key — more if you have multiple McAfee DLP products. The licenses you enter determine which configuration options in McAfee ePO are available to you. 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)

**Task**

1. Install licenses and components in **DLP Settings** to customize the installation.
   - The **DLP Settings** module has seven tabbed pages. Information about the **General** tab is required. You can use the default values or fields for the remaining settings if you don't have special requirements.
   
   a. Select **Menu | Data Protection | DLP Settings**.
   
   b. For each license that you want to add: in the **License Keys | Key** field, enter the license, then click **Add**.
      - Installing the license activates the related McAfee ePO components and McAfee ePO Policy Catalog policies.
   
   c. 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.
      - Installing the license activates the related McAfee ePO components and McAfee ePO Policy Catalog policies.
   
   d. Set the shared password.
2 Click Save.

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

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

**Set advanced configuration options**
Changing settings on the Advanced tab is optional.

**Task**

1 Set System Tree permissions to filter information for incidents, events, queries, and dashboards.

2 Set the Customized Event Timezone to order events according to their local time zone.
   The setting is the offset from UTC time.

3 Set the DLP Policy Manager defaults for rule states and rule reactions.

4 Enable or disable REST API calls.

**Set classification settings**
Set classification settings if you are using McAfee DLP Monitor with the registered documents feature.

**Before you begin**
Install the registration document server software.

**Task**

1 Go to Menu | Data Protection | DLP Settings, then select the Classification tab.

2 Enter the host name or IP Address of the registration document server.
   The default server port is 6379, and can't be changed.

3 (Optional) Set the maximum number of signatures to store in the master registration server.
   Signatures can have a large RAM impact. When calculating the maximum database size, use the approximation that 100 million signatures take about 5 GB of RAM.

4 Click Save.

**Install your McAfee DLP Monitor appliance**
You can install the software on both physical and virtual appliances.
You can enable your McAfee DLP Monitor appliance to perform cryptographic operations in a way that is compliant with FIPS 140-2. To do so, go to the General category in the DLP Appliance Management product in the Policy Catalog.

To analyze traffic on a 10 Gigabit Ethernet link using a cluster of McAfee DLP Monitor appliances, all members of the cluster must have 10 Gigabit Ethernet card.

Only 6600 appliances and virtual installations (where the virtualization host supports 10G networking) support 10 Gigabit Ethernet link. The 4400 and the 5500 appliances do not support 10G networking.
Tasks

- **Install the extensions in McAfee ePO on page 19**
  If you have manually installed the McAfee DLP extension instead of using the Software Manager, you must also install the extensions necessary for McAfee DLP Monitor.

- **Configure network information in McAfee ePO on page 19**
  Connect the appliance to the network.

- **Install the appliance software on a hardware appliance on page 20**
  You can install McAfee DLP Monitor on 4400, 5500, or 6600 appliance models based on your usage of the product.

- **Connect Capture port 1 to your network on page 22**
  Integrate McAfee DLP Monitor into your network using, for example, a SPAN port or network tap.

### Install the extensions in McAfee ePO

If you have manually installed the McAfee DLP extension instead of using the Software Manager, you must also install the extensions necessary for McAfee DLP Monitor.

**Before you begin**
- Download the extensions.
- Install the McAfee DLP extension.

**Task**

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

2. Follow these steps for each of the extensions. Install the extensions in this order:
   - Common UI package
   - Appliance Management Extension
   - McAfee DLP Appliance Management
     a. Browse to the extension .zip file.
     b. Click **OK** twice.

### Configure network information in McAfee ePO

Connect the appliance to the network.

To connect to the network, configure the DNS server and NTP server for your appliances from McAfee ePO.

**Task**

1. In McAfee ePO, select **Menu | Policy | Policy Catalog**.

2. From the **Product** drop-down list, select **Common Appliance Management**.

3. Select the **My Default** policy.

4. Add the DNS server and the NTP server, then click **Save**.
Install the appliance software on a virtual appliance

Install the appliance software in VMware virtual environment
Set up your virtual environment and install the McAfee DLP Monitor virtual appliance. Install the appliance from the .ova file you have downloaded.

For performance optimization, make sure that all virtual appliances in a cluster have the same specifications.

Task
1. Start the VMware vSphere client and log on to the VMware vCenter Server.
2. Select File | Deploy OVF Template. The Deploy OVF Template dialog box appears.
   a. In the Source page, click Browse to search the OVA file you downloaded from the McAfee download site. Click Open to select the file and click Next.
   b. In the OVF Template Details page, validate the package details and click Next.
   c. In the Name and Location page, enter a name for your appliance. Specify the data center and folder to deploy to and click Next.
   d. Select the cluster and an optional resource pool.
   e. Select a datastore for the appliance from the Disk Format page.
   f. For Network Mapping, map the networks used in the OVF template (source networks — LAN_1, OOB, and Capture_1) with the virtual networks (destination networks). Configure the default IP addresses and click Next.
   g. Review the summary in the Ready to Complete page and click Finish.
      To turn on the virtual machine, select the Power on after deployment checkbox.
3. The deployment task starts and displays a message after the deployment is successful, click Close.
   Use the information in Recent Tasks to check if the virtual machine is created.
4. Right-click the deployed virtual machine and click Open Console.
   The virtual appliance console opens and you can continue with the configuration of the appliance.

See also
Configuring IP addresses on page 23

Install the appliance software on a hardware appliance
You can install McAfee DLP Monitor on 4400, 5500, or 6600 appliance models based on your usage of the product.

For performance optimization, make sure that all appliances in a cluster are of the same model.
**Tasks**

- **Connect your appliance on page 21**
  When you connect your appliance to the network device, you can configure the appliance IP address and other parameters for integration in your network.

- **Install a new image on hardware appliance on page 21**
  Install McAfee DLP Monitor on the appliance.

**Connect your appliance**

When you connect your appliance to the network device, you can configure the appliance IP address and other parameters for integration in your network.

Configure each appliance with the required static IP addresses. If no IP addresses are specified, the appliance is configured with the default static IP addresses. The default gateway for the appliance uses the LAN1 network. Configure any routing required on the OOB interface using static routes.

The hardware appliance has a Remote Management Module (RMM), which provides *Lights Out Management* functionality, such as remote KVM access and access to the appliance BIOS.

**Task**

1. Connect a monitor, keyboard, and mouse to the appliance.
2. Connect the LAN1 interface of the appliance to your network.
3. (Optional) Connect the OOB interface to a different network.
4. (Optional) Connect the RMM interface to a management network.

   💡 Use a closed or secure network for the RMM.

**See also**

*Configuring IP addresses on page 23*
*Port assignments on page 4*

**Serial console settings**

You can use the serial console to install the McAfee DLP appliance software only.

You must use another method, such as the RMM, to configure network settings and register with McAfee ePO. You can enable the RMM through the serial console.

💡 Installation progress does not appear when using the serial console.

**Table 2-1  Serial connection parameters**

<table>
<thead>
<tr>
<th>Port setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud rate</td>
<td>115200</td>
</tr>
<tr>
<td>Data bits</td>
<td>8</td>
</tr>
<tr>
<td>Stop bits</td>
<td>1</td>
</tr>
<tr>
<td>Parity</td>
<td>None</td>
</tr>
<tr>
<td>Flow control</td>
<td>None</td>
</tr>
</tbody>
</table>

**Install a new image on hardware appliance**

Install McAfee DLP Monitor on the appliance.

You can perform the initial installation using these methods:
• USB drive

Use image writing software, such as Launchpad Image Writer, to write the image to the USB drive. For more information, see KB87321.

• USB CD drive
• Virtual CD drive using the RMM

Task

1 Using the installation ISO file, create or set up the external imaging media.
2 Insert or connect the media to the appliance.
3 Turn on or restart the appliance.
4 Before the operating system starts, press \textbf{F6} for the boot menu and select the external media.
5 Follow the on-screen prompts.
6 Read the End-User License Agreement, then press \textbf{Y} to accept it.
7 At the installation menu, press \textbf{A} for a full installation, then press \textbf{Y} to continue.

When the installation sequence is complete, the appliance restarts.

\textbf{Warning:} If the installation fails, call technical support. Do not perform the installation again.

\section*{Connect Capture port 1 to your network}

Integrate McAfee DLP Monitor into your network using, for example, a SPAN port or network tap. Configure a portgroup or virtual switch for promiscuous mode.

The capture port is set to \textit{promiscuous mode}. You must enable promiscuous mode on a portgroup or virtual switch to allow the appliance to passively inspect copies of all network packets that pass through the network.

On physical appliance, the capture port can be connected to a SPAN port or a network tap.

On a virtual appliance, the capture port is connected to a standard virtual switch or a portgroup on a distributed switch with promiscuous mode enabled.

\section*{Tasks}

- \textit{Connect Capture port 1 to your network in VMware virtual environment on page 22}

On a VMware virtual appliance, the capture port is connected to a standard virtual switch or a portgroup on a distributed switch with promiscuous mode enabled.

\section*{See also}

\textit{Port assignments on page 4}

\section*{Connect Capture port 1 to your network in VMware virtual environment}

On a VMware virtual appliance, the capture port is connected to a standard virtual switch or a portgroup on a distributed switch with promiscuous mode enabled.

See \url{https://kb.vmware.com/s/article/1004099} for more information.

Task

1 Log on to the VMware ESXi or VMware ESX host, or on to vCenter Server using the vSphere Client.
2 Select the VMware ESXi or ESX host in the inventory list.
3 Click the **Configuration** tab.

4 In the **Hardware** section, click **Networking**.

5 Select the **Properties** of the virtual switch that you want to enable promiscuous mode on.

6 Select the virtual switch or portgroup you want to modify and click **Edit**.

7 Click the **Security** tab.

8 From the **Promiscuous Mode** menu, click **Accept**.

---

### Configuring the appliance

**Contents**
- **Configuring IP addresses**
- **Run the Setup Wizard and register the appliance with McAfee ePO**

#### Configuring IP addresses

Configure each appliance with the default IP addresses after installation. Map the network interfaces with the default static IP addresses, rather than dynamically assigning IP addresses.

Use these default IP addresses to configure the appliances:

- **LAN_1** — 10.1.1.108/24
  
  You can use LAN_1 for management traffic.

- **OOB** — 10.1.3.108/24
  
  (Optional) Use the Out-of-band (OOB) network for management traffic including McAfee ePO communication.

- **Capture_1** — Use the Capture_1 port as a packet capture interface. Capture port 1 does not require an IP address. It must be connected to your network to acquire packets for analysis. Typically, it is connected to a SPAN port or network tap.

  If your network uses DHCP, the first IP address that the DHCP server assigns to the appliance is used instead. You can manually configure the IP address with the Setup Wizard. The appliance doesn't support using a continuous DHCP configuration.

The default gateway for the appliance uses the LAN1 network. Configure any routing required on the OOB interface using static routes.

#### Run the Setup Wizard and register the appliance with McAfee ePO

After the appliance installs and restarts, the Setup Wizard starts automatically. Use the Setup Wizard to configure network settings and register the appliance with McAfee ePO.

If you installed the software using the serial console on a hardware appliance, use another method, such as the RMM, to complete the Setup Wizard.

**Task**

1 Choose the language for the Setup Wizard, then configure the basic network settings.
The wizard contains information to help you configure the settings.

a  On the Welcome page, select Basic Network Setup and click Next.

b  Complete the options on the Basic Settings page.
Configure the McAfee DLP Monitor appliance as a standalone device or as a member of a cluster. For the appliance to be a member of a cluster, set it as a packet acquisition device or as a dedicated scanner.

Setting a cluster role causes a reboot when the changes are applied. Later, to change the cluster role, reset the appliance to factory defaults and apply the cluster role you want.

Change the default password the first time you run the Setup Wizard and click Next.

The new password must have at least eight characters. The default password is password.

c  Complete the options on the Network Services page, then click Next.

d  Review the information about the Summary page and make any corrections.

e  Click Finish.

The initial network settings are applied. The first time you complete the Setup Wizard, or if you need to register with a new McAfee ePO, the wizard restarts after the network settings are applied.

2  Register with McAfee ePO.

a  Select ePO Registration and click Next.

b  Complete the options on the ePO Registration page using valid McAfee ePO user credentials.
You can choose any McAfee ePO user to do the registration. McAfee ePO administrator privileges are not required. The user name and password are not stored on the appliance after the registration is complete.

c  Click Finish.

3  Log on to McAfee ePO.

The product appears in the System Tree. If needed, move the entry to the correct location in the hierarchy.

---

**Post-installation tasks**

After installation, configure settings and policies for your products.
Tasks include:

- Create and configure evidence folders.
- Create classifications, definitions, and rules.
- Assign the configurations and policies in the System Tree.
- Check the DLP Incident Manager.
Upgrading the software

Contents
- Upgrading options
- Apply a patch, hotfix, or new version using the internal installation image
- Alternate upgrade options for a hardware appliance
- Upgrade a virtual appliance by binding an ISO image

Upgrading options

Upgrade the appliance software to the latest version.

Patches, hotfixes, and new versions of the software are distributed as .iso files. To apply a patch, hotfix, or new version, you must boot from the .iso file. You can write this to a CD or USB and boot from it, or copy the image over the appliance's internal installation image and boot from that. If you are installing a version earlier than what is currently installed, a warning is displayed that you can only perform a reinstallation. Downgrading to an earlier version does not retain any configuration or McAfee ePO registration.

Copy the .iso file to the appliance, then boot from the internal installation image. This option is available from the appliance console when you log on as admin from the console menu or SSH. You can also update the appliance installation image from a CD, USB (Exfat filesystem is not supported), or virtual CD (RMM or VMware).

Installation options

- **Full** — Retains all configuration, including evidence files and hit highlighting waiting to be copied to the evidence storage share
- **Config** — Retains all configuration but does not retain evidence files or hit highlighting waiting to be copied
- **Basic** — Retains only network configuration and McAfee ePO registration
- **Reinstall** — Reinstalls without retaining any configuration; you must use the Setup Wizard to register with McAfee ePO

We recommend that you upgrade the appliance via the internal installation image path using the **Full** installation option for all deployments.
Apply a patch, hotfix, or new version using the internal installation image

McAfee DLP Monitor appliances contain a partition with an internal installation image, which you can use to upgrade or reinstall the appliance.

Task
1. Update the installation image using a utility such as WinSCP or a command line session to copy the .iso file to /home/admin/upload/iso/.
2. Using a command line session, log on to the appliance as administrator.
3. From the appliance console menu, select Upgrade.
4. Select Show the internal install image details to confirm the version.
   The current installation image version should be the one you copied earlier.
5. Select Boot from the internal install image.
6. Select the Full option, then select Yes.
   The appliance restarts and installs, preserving all data.
7. Return to the menu, and click Show the internal install image details to confirm the new version has been installed.

Alternate upgrade options for a hardware appliance

Contents
- Re-image an appliance using RMM virtual media
- Re-image an appliance using a USB CD drive
- Make the USB device bootable
- Re-image an appliance using a USB drive
- Re-image model 4400 using a DVD

Re-image an appliance using RMM virtual media
Re-image an appliance to the latest version using the Remote Management Module virtual media.

Before you begin
- Make sure the RMM virtual media is connected to your network.
- Decide the IP address, subnet mask, and gateway IP address to use when configuring the RMM port.
- Make sure Java is installed on the computer that connects to the RMM virtual media.
- Locate the grant number you received after purchasing the product.
Task
1. Download the McAfee DLP Monitor .iso image file to the computer that connects to the RMM virtual media.
   b. Enter your grant number, then select the appropriate product and version.
   c. In the Software Downloads tab, select and save the appropriate *.iso file.

2. Log on to the appliance as administrator.

3. From the appliance console menu, select Reboot to restart the system.

4. On the computer that connects to the RMM virtual media, open a web browser and enter:
   \[https://<RMM IP address>\]
   Use the administrator account credentials.

5. Select the .iso file and follow these instructions to re-image.
      The appliance is re-imaged using the .iso file. Wait for the installation to complete.
   d. On the Device tab, disable Redirect ISO.

   **Warning:** If you don't disable the Redirect ISO setting, the appliance is re-imaged after the next reboot, removing your current installation and returning the appliance to factory default.

Re-image an appliance using a USB CD drive
Re-image an appliance to the latest version using a USB CD drive. Only model 4400 includes a built-in USB CD drive.

**Before you begin**
Make sure that the USB device is made bootable.

Use image writing software to write the ISO image (bootable image) to a USB CD drive.

**Task**
1. Connect the USB CD drive with the bootable image to one of the USB ports on the appliance.
2. Log on to the appliance as administrator.
3. From the appliance console menu, select Reboot to restart the system.
4. Press F6 to enter the boot menu.
5. From the boot menu options, select the USB CD device where the appliance upgrades from.
   The installation image starts loading. Wait until the install image gets unpacked and displays the Installation menu.
6. Select the full installation mode, which is the default and the recommended option.
Follow the on-screen instructions to re-image the appliance.

When the re-imaging is complete, remove the USB CD drive.

If you don't remove the USB CD drive, the appliance is re-imaged from the USB CD drive after the next reboot, removing your current installation and returning the appliance to factory default settings.

See also

Make the USB device bootable on page 28

Make the USB device bootable
Make sure that you allow all USB mass storage devices as a bootable devices.

Task
1  Log on to the appliance as administrator.
2  From the appliance console menu, select Reboot to restart the system.
3  Press F2 to enter the Setup menu.
4  Navigate to the Advanced settings page and select USB Configuration.
5  Select the option to allow all USB mass storage devices as bootable devices.
6  Press F10 to save and exit the USB configuration page.

Re-image an appliance using a USB drive
Re-image an appliance to the latest version.

Before you begin
Make sure that the USB device is made bootable.

Task
1  Create a USB drive with the installation image.

   Use image writing software, such as Launchpad Image Writer, to write the image to the USB drive. For more information, see KB87321.

2  Insert the USB drive into the appliance.
3  Log on to the appliance as administrator.
4  From the appliance console menu, select Reboot to restart the system.
5  Press F6 to enter the boot menu.
6  From the boot menu options, select the USB drive where the appliance re-images from.
   The installation image starts loading. Wait until the image gets unpacked and displays the Installation menu.
7  Select the full installation mode, which is the default and the recommended option.
8 Follow the on-screen instructions to re-image the appliance.
9 When the re-imaging is complete, remove the USB drive.

⚠️ If you don't remove the USB drive, the appliance is re-imaged from the USB drive after the next reboot, removing your current installation and returning the appliance to factory default settings.

See also
Make the USB device bootable on page 28

Re-image model 4400 using a DVD
Re-image an appliance to the latest version. Use an image writing software to write the ISO image (bootable image) to a DVD. Only model 4400 includes a built-in DVD drive.

Task
1 Insert the DVD into the appliance.
2 Using the command-line session, log on to the appliance as administrator.
3 From the appliance console menu, select Reboot to restart the system.
4 Press F6 to enter the boot menu.
   The boot menu options are displayed and boot from DVD is the default option.
5 Select to boot from DVD.
   The installation image starts loading. Wait until the install image gets unpacked and displays the Installation menu.
6 Select the full installation mode, which is the default and the recommended option.
7 Follow the on-screen instructions to re-image the appliance.
8 When the re-imaging is complete, remove the DVD.

⚠️ If you do not remove the DVD, the appliance is re-imaged from the DVD after the next reboot, removing your current installation and returning the appliance to factory default settings.

Upgrade a virtual appliance by binding an ISO image
Alternative upgrade option for an appliance in the VMware virtual environment includes binding the downloaded .iso image.

Task
1 From the inventory, right-click the virtual appliance that you want to upgrade and select Edit Settings to open Virtual Machine Properties.
2 From the Hardware tab, select CD/DVD drive 1 | Datastore ISO.
3 Browse to the .iso file.
4 (Optional) Select Connect At Power On to connect the device when the virtual machine turns on.
5 Click OK.
Upgrading the software
Upgrade a virtual appliance by binding an ISO image
4

Maintenance and troubleshooting

Contents
- Managing with the McAfee DLP appliance console
- Accessing the appliance console
- Change original network settings
- Modify speed and duplex settings for hardware appliances
- Managing hardware appliances with the RMM
- Restart the appliance
- Reset the appliance to its factory defaults
- Log off the appliance

Managing with the McAfee DLP appliance console

Use administrator credentials to open the appliance console to edit the network settings that you entered in the Setup Wizard, and to perform other maintenance and troubleshooting tasks.

You can add your own text to appear on the top of the appliance console or SSH logon screen using the Custom Logon Banner option in McAfee ePO (Menu | Policy Catalog | DLP Appliance Management | General).

SSH is primarily controlled from McAfee ePO. Whenever a policy is pushed, the McAfee ePO settings take priority, overriding any SSH setting enabled through the local console.

Table 4-1 Appliance console menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Graphical configuration wizard</td>
<td>Open the graphical configuration wizard.</td>
</tr>
<tr>
<td></td>
<td>◼️ If you log on using SSH, the graphical configuration wizard option is not available.</td>
</tr>
<tr>
<td>Shell</td>
<td>Open the appliance Shell.</td>
</tr>
<tr>
<td>Enable/Disable SSH</td>
<td>Enable or disable SSH as a method of connecting to the appliance.</td>
</tr>
<tr>
<td>MER and Diagnostic tests</td>
<td>Create a Minimum Escalation Report (MER) to send to McAfee Support to diagnose problems with the appliance or run diagnostic tests:</td>
</tr>
<tr>
<td></td>
<td>◼️ Basic LDAP Tests</td>
</tr>
<tr>
<td></td>
<td>◼️ LDAP NetBIOS Tests</td>
</tr>
<tr>
<td></td>
<td>◼️ Evidence Share Tests</td>
</tr>
<tr>
<td>Power down</td>
<td>Shut down the appliance.</td>
</tr>
<tr>
<td>Reboot</td>
<td>Restart the appliance.</td>
</tr>
</tbody>
</table>
Table 4-1 Appliance console menu options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade</td>
<td>You can perform one of these actions:</td>
</tr>
<tr>
<td></td>
<td>• Upgrade to the latest version of the appliance using the internal install image.</td>
</tr>
<tr>
<td></td>
<td>• Update the internal install image from external devices like a CD or USB.</td>
</tr>
<tr>
<td></td>
<td>• Copy the internal install image to a USB flash device.</td>
</tr>
<tr>
<td></td>
<td>• Check the current version of the internal install image.</td>
</tr>
<tr>
<td>Reset to factory defaults</td>
<td>Reset the appliance to its factory default settings.</td>
</tr>
<tr>
<td>Change password</td>
<td>Change the administrator account password.</td>
</tr>
<tr>
<td>Logout</td>
<td>Log off the appliance.</td>
</tr>
</tbody>
</table>

Accessing the appliance console

The appliance console allows you to perform various maintenance tasks. There are different ways to access the console depending on the type of appliance you have.

Table 4-2 Methods for accessing the console

<table>
<thead>
<tr>
<th>Method</th>
<th>Virtual appliance</th>
<th>Hardware appliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>vSphere Client</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Local KVM (keyboard, monitor, mouse)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>RMM</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Serial port</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Change original network settings

You can use the graphical configuration wizard to change network settings that you entered during the installation process.

Task

1. Log on to the appliance with administrator credentials.

   - If you log on using SSH, the graphical configuration wizard option is not available.

2. Open the graphical configuration wizard.

3. Edit the **Basic Network Setup** settings that you want to change.

4. Click Finish.
Modify speed and duplex settings for hardware appliances

By default, the network interfaces are configured for auto-negotiation. Use the command line to change the speed and duplex settings.

**Task**

1. Using a command line session, log on to the appliance.
2. From the options menu, select the **Shell** option.
3. View the help on forming the command.
   ```
   $ /opt/NETAwss/mgmt/nic_options -?
   
   • Use `lan1` for the client interface and `mgmt` for the management interface.
   • `--(no)autoneg` turns auto-negotiation on or off. The default is on.
   • `--duplex` specifies the duplex — half or full. The default is full.
   • `--speed` specifies the network speed in Mb/s — 0, 100, or 1000. The default is 1000.
   • `--mtu` specifies the Maximum Transmission Unit (MTU) size in bytes — a value between 576–1500. The default is 1500.
   
4. Enter the command to change the setting. **Examples:**
   • To disable auto-negotiation and set a network speed of 100 Mb/s on the client interface:
     ```
     $ sudo /opt/NETAwss/mgmt/nic_options --noautoneg --speed 100 lan1
     ```
   • To restore the default behavior to the management port:
     ```
     $ sudo /opt/NETAwss/mgmt/nic_options mgmt
     ```

Managing hardware appliances with the RMM

Use the RMM — also called the Baseboard Management Controller (BMC) — to manage a hardware appliance remotely. The RMM is not available on virtual appliances.

The RMM must be configured with its own IP address and cabled separately. Log on with the administrator account with the user name as `admin` and administrator password. Use the appliance console to enable and configure basic settings for the RMM. After configuring the RMM network settings, you can also access the appliance console using the integrated web server. From the web interface, you can check the hardware status, perform additional configuration, and remotely manage the appliance. Go to:

https://<RMM IP address>

Use the appliance administrator credentials to access the user interface. You can configure the RMM to use LDAP for authentication instead of the admin account.

By default, all protocols used to access the RMM are enabled:
- HTTP/HTTPS
- SSH
Configure the RMM from BIOS

Configure network settings used by the RMM.

**Before you begin**

Make sure the server board has the latest firmware.

You can enable or configure RMM from the text menu system, appliance console, serial console, or SSH session.

In an uninstalled appliance, you can configure the RMM settings from BIOS using the root account. In an installed appliance, you can configure the RMM settings from the appliance console without entering the BIOS.

**Task**

1. Log on to the appliance as administrator.
2. From the appliance console menu, select Reboot to restart the system.
3. Before the operating system boots, press F2 to enter the BIOS.
4. Select the LAN configuration for your appliance model:
   - 5500 and 6600 — Select Server Management | BMC LAN Configuration.
   - 4400 — Select Server Management | Baseboard LAN Configuration.
5. Configure IP source, IP address, Subnet mask, and Gateway IP for your appliance model:
   - 5500 and 6600 — Configure Intel® RMM4 IPv4 LAN Configuration.
   - 4400 — Configure Intel® RMM3 LAN Configuration.
6. Select User Configuration, then configure these settings:
   - User ID — Select root
   - User status — Select Enabled
   - User name — Enter root
   - User password — Enter the password. You must enter this password twice
7. Confirm the network and user information, and press F10 to save and exit the BIOS.
   The appliance boots with the new settings.
8. On the computer that connects to the RMM, open a web browser and enter:
   https://RMM IP address
   Use the credentials root/password you entered in the earlier step.
   The appliance boots with the new settings.

For more information about Intel® RMM4, go to https://www.intel.in/content/www/in/en/support/articles/000006023/server-products.html.

Configure the RMM from appliance console
Configure network settings and protocols used by the RMM.

Task
1. Log on to the appliance as administrator.
2. From the appliance console menu, select Configure the BMC.
3. Configure the network information:
   a. Select Configure the address.
   b. Type the IP address, the network mask, and the optional gateway. Use the up and down arrows to navigate between options.
   c. Press Enter or select OK to save the changes.
4. Configure the allowed protocols:
   a. Select Configure remote protocols.
   b. Press the space bar to enable or disable an option.
   c. Press Enter or select OK to save the changes.

Use the administrator account and password to log on to the appliance using the RMM.

Run the Setup Wizard using the remote KVM service
If you do not have local access to the keyboard, monitor, and mouse to run the Setup Wizard, you can do so using the RMM web interface.

Task
1. Using a web browser, log on to https://<RMM IP address>.
2. Click the Remote Control tab.
3. Click Launch Console.
4. For some browsers, you might need to download the remote console application. In this case, download and open the jviewer.jnlp file.
5. From admin shell, select Graphical configuration wizard.

Best practice: Securing the RMM
Secure your RMM environment to prevent unauthorized users from accessing the appliance.
- Make sure the RMM firmware is up-to-date.
- Connect the RMM port to a secure, dedicated physical network or VLAN.
- Disable unused protocols. Only HTTP/HTTPS and the remote KVM service are required to remotely configure the appliance.
If your appliance uses RMM4, make sure the appliance is configured to force the use of HTTPS.

The appliance console and the web-based interface display which RMM type the appliance uses — RMM3 or RMM4.

From the web-based interface, click the **Configuration tab**, select **Security Settings**, then select the **Force HTTPS** option.

- Periodically change the administrator password.

---

**Restart the appliance**

Shut down and restart the appliance.

**Task**

1. Log on to the appliance as administrator.
2. From the appliance console menu, select **Reboot** to restart the system.

---

**Reset the appliance to its factory defaults**

Return the appliance to its original settings.

You will have to reconfigure network configuration settings.

**Task**

1. Log on to the appliance with administrator credentials.
   
   The general console menu opens.

2. From the general console menu, press the **Reset to factory defaults** option.

---

**Log off the appliance**

Close the logon session and return to a logon prompt.

**Task**

1. Log on to the appliance with administrator credentials.
   
   The general console menu opens.

2. From the general console menu, press the **Logout** option.
   
   Either the SSH session closes, or the console returns to the logon prompt.
Port assignments

McAfee DLP Monitor appliances have multiple ports. Identify the hardware components on the back panel and network port assignments before setting up the appliance. Use the numbered callouts in the figures to locate these ports on your appliance.

Contents

- Model 4400
- Model 5500
- Model 6600

Model 4400

Back panel hardware components and port assignments
Be familiar with the hardware components on the back panel and network port assignments before setting up the 4400 appliance.

Figure A-1  4400 back panel
Table A-1 Port assignments

<table>
<thead>
<tr>
<th>Usage</th>
<th>4400 (Copper)</th>
<th>4400 (Fiber)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common ports</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial —</td>
<td>callout 1</td>
<td>callout 1</td>
</tr>
<tr>
<td>Use these connection settings:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Baud rate</strong> — 115200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Parity</strong> — None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Data bits</strong> — 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Flow control</strong> — None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Stop bits</strong> — 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VGA</td>
<td>callout 2</td>
<td>callout 2</td>
</tr>
<tr>
<td>USB</td>
<td>callout 3</td>
<td>callout 3</td>
</tr>
<tr>
<td>Remote Management Module (RMM)</td>
<td>callout 6</td>
<td>callout 6</td>
</tr>
<tr>
<td>Power supplies</td>
<td>callout 9</td>
<td>callout 9</td>
</tr>
<tr>
<td><strong>Network port assignments in McAfee DLP Monitor 11.x and later</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OOB — Out-of-band management traffic such as McAfee® ePolicy Orchestrator® (McAfee® ePO™) management</td>
<td>callout 4</td>
<td>callout 4</td>
</tr>
<tr>
<td><strong>LAN1</strong> —</td>
<td>callout 5</td>
<td>callout 5</td>
</tr>
<tr>
<td>• Load balancing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IP traffic - management and scanning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Capture port 1 — Packet acquisition</td>
<td>callout 8</td>
<td>callout 8</td>
</tr>
<tr>
<td><strong>Network port assignments in McAfee DLP Monitor 9.x</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management traffic</td>
<td>callout 5</td>
<td>callout 5</td>
</tr>
<tr>
<td>Capture port 0</td>
<td>callout 8</td>
<td>callout 8</td>
</tr>
<tr>
<td>Capture port 1</td>
<td>callout 7</td>
<td>callout 7</td>
</tr>
</tbody>
</table>

Callouts that are not referenced in the table are unused ports.
Model 5500

Back panel hardware components and port assignments

Be familiar with the hardware components on the back panel and network port assignments before setting up the 5500 appliance.

**Figure A-2  5500 back panel**

**Table A-2 Port assignments**

<table>
<thead>
<tr>
<th>Usage</th>
<th>5500 (Copper)</th>
<th>5500 (Fiber)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Common ports</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Serial —</td>
<td>callout 7</td>
<td>callout 7</td>
</tr>
<tr>
<td>Use these connection settings:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Baud rate</strong> — 115200</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Data bits</strong> — 8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Stop bits</strong> — 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Parity</strong> — None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• <strong>Flow control</strong> — None</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VGA</td>
<td>callout 6</td>
<td>callout 6</td>
</tr>
<tr>
<td>USB</td>
<td>callout 8</td>
<td>callout 8</td>
</tr>
<tr>
<td>Remote Management Module (RMM)</td>
<td>callout 9</td>
<td>callout 9</td>
</tr>
<tr>
<td>This port is labeled <strong>RMM</strong> on the appliance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power supplies</td>
<td>callout 3</td>
<td>callout 3</td>
</tr>
<tr>
<td><strong>Network port assignments in McAfee DLP Monitor 11.x and later</strong></td>
<td>callout 4</td>
<td>callout 4</td>
</tr>
<tr>
<td>OOB port — Out-of-band management traffic such as McAfee® ePolicy Orchestration® (McAfee® ePO®) management.</td>
<td>callout 4</td>
<td>callout 4</td>
</tr>
<tr>
<td>This port is labeled <strong>N/A</strong> on the appliance.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN1 —</td>
<td>callout 5</td>
<td>callout 5</td>
</tr>
<tr>
<td>• Load balancing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• IP traffic - management and scanning</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Model 6600

Back panel hardware components and port assignments

Be familiar with the hardware components on the back panel and network port assignments before setting up the 6600 appliance.

![Figure A-3 6600 back panel](image)

Table A-3 Port assignments

<table>
<thead>
<tr>
<th>Usage</th>
<th>6600</th>
</tr>
</thead>
<tbody>
<tr>
<td>Common ports</td>
<td></td>
</tr>
<tr>
<td>Serial — Use these connection settings:</td>
<td>callout 6</td>
</tr>
<tr>
<td>• <strong>Baud rate</strong> — 115200</td>
<td>• <strong>Parity</strong> — None</td>
</tr>
<tr>
<td>• <strong>Data bits</strong> — 8</td>
<td>• <strong>Flow control</strong> — None</td>
</tr>
<tr>
<td>• <strong>Stop bits</strong> — 1</td>
<td></td>
</tr>
<tr>
<td>VGA</td>
<td>callout 5</td>
</tr>
<tr>
<td>USB</td>
<td>callout 7</td>
</tr>
<tr>
<td>Remote Management Module (RMM)</td>
<td>callout 8</td>
</tr>
<tr>
<td>Power supplies</td>
<td>callout 1</td>
</tr>
</tbody>
</table>

Network port assignments in McAfee DLP Monitor 11.x and later

<table>
<thead>
<tr>
<th>Usage</th>
<th>6600</th>
</tr>
</thead>
<tbody>
<tr>
<td>OOB port — Out-of-band management traffic such as McAfee® ePolicy Orchestrator® (McAfee® ePO®) management</td>
<td>callout 4</td>
</tr>
</tbody>
</table>

Callouts that are not referenced in the table are unused ports.
Table A-3 Port assignments *(continued)*

<table>
<thead>
<tr>
<th>Usage</th>
<th>6600</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN1 port — (10 GBase-T)</td>
<td>callout 2</td>
</tr>
<tr>
<td>• Load balancing</td>
<td></td>
</tr>
<tr>
<td>• IP traffic - management and scanning</td>
<td></td>
</tr>
<tr>
<td>Capture port 1 — (10 GBase-T)</td>
<td>callout 3</td>
</tr>
</tbody>
</table>

Callouts that are not referenced in the table are unused ports.
Port assignments
Model 6600
Index

H
hotfix 26

I
installation
  patch or hotfix 26
  internal install image 26

M
management port, connecting 21
McAfee DLP appliance
  installation 18
  serial console 21
McAfee DLP Monitor
  cluster setup 7
  network requirements 7
  promiscuous mode 22
McAfee DLP Prevent
  Setup Wizard 23, 35

N
network tap 7

P
patch
  upgrade 26
  promiscuous mode 22

R
registered documents
  classification settings for 18
RMM 33-35

S
SPAN port 7