Product Guide

McAfee Management of Native Encryption
4.0.0

For use with McAfee ePolicy Orchestrator
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>5</td>
</tr>
<tr>
<td>About this guide</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>Conventions</td>
<td>5</td>
</tr>
<tr>
<td>Find product documentation</td>
<td>6</td>
</tr>
<tr>
<td>1 Introduction</td>
<td>7</td>
</tr>
<tr>
<td>Product components</td>
<td>7</td>
</tr>
<tr>
<td>Features</td>
<td>8</td>
</tr>
<tr>
<td>2 Installing MNE</td>
<td>11</td>
</tr>
<tr>
<td>Overview of the installation process</td>
<td>11</td>
</tr>
<tr>
<td>Requirements</td>
<td>12</td>
</tr>
<tr>
<td>Supported McAfee ePO versions</td>
<td>13</td>
</tr>
<tr>
<td>Installing the product</td>
<td>14</td>
</tr>
<tr>
<td>Deploy McAfee Agent for Mac through SSH</td>
<td>14</td>
</tr>
<tr>
<td>Install the MNE and Help extensions</td>
<td>14</td>
</tr>
<tr>
<td>Check in the MNE software packages</td>
<td>15</td>
</tr>
<tr>
<td>Deploy MNE to client systems</td>
<td>15</td>
</tr>
<tr>
<td>Send an agent wake-up call</td>
<td>16</td>
</tr>
<tr>
<td>Turn on FileVault on a Mac client system</td>
<td>17</td>
</tr>
<tr>
<td>Turn on BitLocker on a Windows client system</td>
<td>18</td>
</tr>
<tr>
<td>Standalone installation</td>
<td>19</td>
</tr>
<tr>
<td>Upgrading the Mac client systems to MNE 4.0.0</td>
<td>19</td>
</tr>
<tr>
<td>Upgrading the Windows client systems to MNE 4.0.0</td>
<td>20</td>
</tr>
<tr>
<td>Uninstalling the product</td>
<td>20</td>
</tr>
<tr>
<td>Turn off FileVault</td>
<td>21</td>
</tr>
<tr>
<td>Remove MNE from the client using a McAfee ePO deployment task</td>
<td>21</td>
</tr>
<tr>
<td>Remove MNE and Help extensions</td>
<td>22</td>
</tr>
<tr>
<td>Remove the MNE software package</td>
<td>22</td>
</tr>
<tr>
<td>Manually uninstall MNE from the client system</td>
<td>23</td>
</tr>
<tr>
<td>Migrating from EEMac to MNE</td>
<td>23</td>
</tr>
<tr>
<td>Reporting FIPS status to client systems</td>
<td>24</td>
</tr>
<tr>
<td>Run in FIPS mode</td>
<td>24</td>
</tr>
<tr>
<td>3 Managing policies</td>
<td>25</td>
</tr>
<tr>
<td>Product policies</td>
<td>26</td>
</tr>
<tr>
<td>Enforce MNE policies on a system</td>
<td>31</td>
</tr>
<tr>
<td>Enforce policies to a group</td>
<td>32</td>
</tr>
<tr>
<td>4 Automatic network unlock</td>
<td>33</td>
</tr>
<tr>
<td>Automatic unlock of fixed volumes for client systems</td>
<td>33</td>
</tr>
<tr>
<td>5 Managing client systems</td>
<td>35</td>
</tr>
<tr>
<td>Add a system to an existing group</td>
<td>35</td>
</tr>
<tr>
<td>Contents</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Move systems between groups</td>
<td>36</td>
</tr>
<tr>
<td>System actions</td>
<td>36</td>
</tr>
<tr>
<td>How to run the MER tool on Mac systems</td>
<td>37</td>
</tr>
<tr>
<td>Maintenance mode on BitLocker systems</td>
<td>37</td>
</tr>
<tr>
<td>6 Managing MNE reports</td>
<td>39</td>
</tr>
<tr>
<td>Queries as dashboard monitors</td>
<td>39</td>
</tr>
<tr>
<td>View the standard MNE reports</td>
<td>40</td>
</tr>
<tr>
<td>Create MNE custom queries</td>
<td>41</td>
</tr>
<tr>
<td>View the standard MNE dashboard</td>
<td>42</td>
</tr>
<tr>
<td>View the &quot;Find MNE systems by user name&quot; dashboard</td>
<td>42</td>
</tr>
<tr>
<td>Create custom MNE dashboard</td>
<td>42</td>
</tr>
<tr>
<td>MNE client events</td>
<td>43</td>
</tr>
<tr>
<td>7 Recovering systems</td>
<td>47</td>
</tr>
<tr>
<td>Import the recovery key</td>
<td>48</td>
</tr>
<tr>
<td>Import the recovery key using System Tree</td>
<td>48</td>
</tr>
<tr>
<td>Import the recovery key using the Data Protection menu</td>
<td>48</td>
</tr>
<tr>
<td>Import the recovery key from a client system</td>
<td>49</td>
</tr>
<tr>
<td>Import the recovery key using the MNE command-line</td>
<td>49</td>
</tr>
<tr>
<td>Perform system recovery using McAfee ePO</td>
<td>50</td>
</tr>
<tr>
<td>Provide the recovery key to the user</td>
<td>50</td>
</tr>
<tr>
<td>MNE recovery key through scripting</td>
<td>50</td>
</tr>
<tr>
<td>Perform system recovery using the Data Protection Self Service Portal</td>
<td>51</td>
</tr>
<tr>
<td>Configure DPSSP server settings on McAfee ePO</td>
<td>52</td>
</tr>
<tr>
<td>Enable the DPSSP permission set for unblocking users or IP addresses</td>
<td>53</td>
</tr>
<tr>
<td>How to instantly unblock a user or IP address</td>
<td>53</td>
</tr>
<tr>
<td>Obtain a recovery key on the client system using DPSSP</td>
<td>53</td>
</tr>
<tr>
<td>View the Data Protection Self Service Portal (DPSSP) reports</td>
<td>54</td>
</tr>
<tr>
<td>Rotate recovery keys</td>
<td>55</td>
</tr>
</tbody>
</table>

**Index** 57
Preface

This guide provides the information you need to work with your McAfee product.

Contents

- About this guide
- Find product documentation

About this guide

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

Audience

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

The information in this guide is intended primarily for:

- **Administrators** — People who implement and enforce the company's security program.
- **Users** — People who use the computer where the software is running and can access some or all of its features.

Conventions

This guide uses these typographical conventions and icons.

- **Book title, term, emphasis**
  - Title of a book, chapter, or topic; a new term; emphasis.
- **Bold**
  - Text that is strongly emphasized.
- **User input, code, message**
  - Commands and other text that the user types; a code sample; a displayed message.
- **Interface text**
  - Words from the product interface like options, menus, buttons, and dialog boxes.
- **Hypertext blue**
  - A link to a topic or to an external website.
  - **Note:** Additional information, like an alternate method of accessing an option.
  - **Tip:** Suggestions and recommendations.
  - **Important/Caution:** Valuable advice to protect your computer system, software installation, network, business, or data.
  - **Warning:** Critical advice to prevent bodily harm when using a hardware product.
Find product documentation

On the ServicePortal, you can find information about a released product, including product documentation, technical articles, and more.

Task

1. Go to the ServicePortal at https://support.mcafee.com and click the Knowledge Center tab.

2. In the Knowledge Base pane under Content Source, click Product Documentation.

3. Select a product and version, then click Search to display a list of documents.
Introduction

McAfee® Management of Native Encryption (MNE) is a management product that allows McAfee® ePolicy Orchestrator® (McAfee ePO™) administrators to manage Apple FileVault and Microsoft BitLocker. These are products that provide full-disk encryption on Macintosh (Mac) and Windows systems.

McAfee Management of Native Encryption provides an easy-to-use administrative interface to perform these core functions:

- Manage FileVault and BitLocker
- Report encryption status
- Escrow, import, storage, and retrieval of recovery keys

You can also use the report only feature of MNE without having to actively manage FileVault or BitLocker.

We provide support only for MNE (the management solution) and not the underlying FileVault or BitLocker encryption technology. If you encounter any issues with FileVault or BitLocker technology (especially issues related to recovering systems), we recommend that you contact Apple or Microsoft Support respectively.

Contents

- Product components
- Features

Product components

MNE contains components and features that play a part in protecting your systems.

MNE

MNE integrates with the McAfee ePO server to enable or disable the FileVault or BitLocker volume encryption product on client systems, as well as reporting FileVault or BitLocker status and managing FileVault or BitLocker policies.

McAfee ePO server

The McAfee ePO server provides a scalable platform for centralized policy management and enforcement of your security products and systems where they reside. MNE is integrated with the McAfee ePO console, wherein you can manage FileVault or BitLocker encrypted client systems and deploy and manage the MNE product. The console provides comprehensive reporting and product deployment capabilities, all through a single point of control.
Product extensions and packages

The MNEAdmin extension that is installed on McAfee ePO allows managing and reporting of both FileVault and BitLocker on client systems by deploying policy to client systems. The Data Protection Self Service Portal (DPSSP) extension is a separate extension that integrates with MNEAdmin to provide self-recovery capabilities for client users. The MNEAdvancedFeatures extension is new in MNE 4.0.0, and when installed into McAfee ePO, will enable the new network-unlock capability within MNE on BitLocker systems.

The MNE software packages that are checked in to the master repository on the McAfee ePO server are the actual products that are installed on the client systems, and apply the policy received from the McAfee ePO server.

Privacy Notice

Data Protection Self-Service Portal (DPSSP) collects users’ login names, system names, IP addresses, and audit data. Access to this information is available in DPSSP reports within McAfee ePO. Make sure that access to these reports is authorized and appropriately managed. Please note that none of this information is transmitted externally to McAfee or other third parties.

Features

You can manage FileVault or BitLocker through MNE using the following features.

• Actively manage FileVault or BitLocker with a wide variety of policy options for each, or choose to manage elsewhere and simply report into McAfee ePO.

• Configure authentication policy appropriate to each:
  • Supports TPM, TPM and PIN, password, network-unlock for BitLocker
  • Supports password for FileVault

• Use a wide variety of useful reports to monitor the status and security posture of managed systems.

• Support FileVault and BitLocker recovery through the use of:
  • Administrative recovery through the McAfee ePO console
  • Self-service recovery through DPSSP
  • Administrative recovery through the web-api, allowing simple integration into your own helpdesk tools

• Rotate recovery keys periodically, or after a recovery workflow has occurred in McAfee ePO or DPSSP (Windows systems only) to improve security.

• On Windows systems, ensure that when taking over management of BitLocker, only MNE managed keys remain on the system to avoid older (insecure) keys remaining on the system.

• Configure network-unlock to permit remote-authentication of BitLocker Fixed Volumes on servers.

• FIPS mode.

• Use DEGO for a pre-flight check before activating FileVault (Mac systems only).
<table>
<thead>
<tr>
<th>Feature</th>
<th>Mac</th>
<th>Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management or reporting only</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Configuration of authentication policy</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Automated escrow of recovery keys</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Manual import of recovery keys (required for FileVault due to the way it's designed)</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>This is not required for BitLocker.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Multiple recovery keys for a system</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>This is not required for FileVault.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status reporting on EPM console</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Standalone installation</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Recovery key rotation (periodic)</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Recovery key rotation (following recovery workflow through console)</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Trusted Platform Module (TPM) support</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>Network unlock of fixed data volumes</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>FIPS support</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Installing MNE

You need to perform a set of tasks to complete the installation process on the required Mac or Windows client systems and manage them using McAfee ePO. Alternatively, Mac users have the option of installing MNE offline using the `MNE-4.0.0.xxx.dmg` package, which is provided by the administrator to client users along with the user credentials. Users can also configure the client systems remotely into the McAfee ePO server using the McAfee ePO Remote Provisioning Tool.

Windows users can install MNE offline using the msi package.

Contents

- Overview of the installation process
- Requirements
- Supported McAfee ePO versions
- Installing the product
- Standalone installation
- Upgrading the Mac client systems to MNE 4.0.0
- Upgrading the Windows client systems to MNE 4.0.0
- Uninstalling the product
- Migrating from EEMac to MNE
- Reporting FIPS status to client systems
- Run in FIPS mode

Overview of the installation process

The installation and deployment of MNE to the required client systems consist of the following tasks. Complete details are given in subsequent sections.

This assumes that the user has already installed McAfee ePO on the server system. For more information about installing McAfee ePO, see the product documentation for your version of McAfee ePO.

1. Deploy McAfee® Agent to the client system from McAfee ePO.

   A successful communication is required between the McAfee ePO server and McAfee Agent on the client system.

2. Install the `MNEADMIN_4.0.0.x.zip`, `help_MNE_400.zip`, and `dpssp.zip` extensions to the McAfee ePO server. If you wish to use the network unlock feature with Windows servers, also install the `mneadvancedfeatures.zip`.

3. If installing client software through McAfee ePO, check in the `MNE-OSX-4.0.0.x.zip` software package for Mac systems or `MNE-WIN-4.0.0.x.zip` software package for Windows systems to the McAfee ePO server.
4 Deploy the software package to the required client system.

5 Send an agent wake-up call.

6 Enable the Turn On (Enable) FileVault or Turn On (Enable) BitLocker policy in McAfee ePO and enforce on the Mac or Windows client systems respectively. You can also enable other policy options, as required. For more information, see the Product policies section.

The client system might prompt for a restart.

The exact behavior of the client system will depend on the underlying encryption product (FileVault or BitLocker), and policy settings defined.

Requirements

Make sure that your client systems meet these requirements before you install and deploy MNE.

For the latest information regarding supported environments, refer to the Supported Platforms, Environments, and Operating Systems for McAfee Management of Native Encryption KnowledgeBase article KB79375.

Table 2-1 System requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO server systems</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Client systems for MNE</td>
<td>• <strong>CPU</strong>: Works on all Intel-based systems</td>
</tr>
<tr>
<td></td>
<td>• <strong>RAM</strong>: 1 GB minimum</td>
</tr>
<tr>
<td></td>
<td>• <strong>Hard Disk</strong>: 1 GB minimum free disk space</td>
</tr>
</tbody>
</table>

Table 2-2 Software requirements

<table>
<thead>
<tr>
<th>Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO</td>
<td>McAfee ePO 5.1.0, 5.1.1, 5.1.2, 5.1.3, 5.3, and 5.3.1</td>
</tr>
<tr>
<td>MNE</td>
<td>• MNEADMIN-4.0.0.x.zip</td>
</tr>
<tr>
<td></td>
<td>• help_MNE_400.zip</td>
</tr>
<tr>
<td></td>
<td>• dpssp.zip</td>
</tr>
<tr>
<td>MNE software packages</td>
<td>• MNE-OSX-4.0.0.x.zip for Mac systems</td>
</tr>
<tr>
<td></td>
<td>• MNE-WIN-4.0.0.x.zip for Windows systems</td>
</tr>
<tr>
<td>McAfee Agent</td>
<td>McAfee Agent 4.8 Patch 3, 5.0.0, 5.0.1, or 5.0.2 for Windows and Mac systems</td>
</tr>
</tbody>
</table>

McAfee Agent 5.0.2 or later is recommended for use with Mac OS X for compatibility with Endpoint Security for Mac 10.1.0. Mac OS X 10.10.x (Yosemite) requires McAfee Agent 5.0.1 or later, and Mac OS X 10.11.x (El Capitan) requires McAfee Agent 5.0.2 HF1085179 or later.
Table 2-2  Software requirements (continued)

<table>
<thead>
<tr>
<th>Software</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows Installer 3.0 Redistributable package (for McAfee ePO)</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Microsoft .NET Framework 2.0 Redistributable package (for McAfee ePO)</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Microsoft MSXML 6 (for McAfee ePO)</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
</tbody>
</table>

Table 2-3  Operating system requirements

<table>
<thead>
<tr>
<th>Systems</th>
<th>Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO server systems</td>
<td>See the product documentation for your version of McAfee ePO.</td>
</tr>
<tr>
<td>Client systems for MNE</td>
<td>Mac client</td>
</tr>
<tr>
<td>- Mountain Lion: 10.8.2 or later (32- and 64-bit)</td>
<td></td>
</tr>
<tr>
<td>- Mavericks 10.9.0 or later (32- and 64-bit)</td>
<td></td>
</tr>
<tr>
<td>- Yosemite 10.10.0 or later (32- and 64-bit)</td>
<td></td>
</tr>
<tr>
<td>- El Capitan 10.11.0 or later (32- and 64-bit)</td>
<td></td>
</tr>
<tr>
<td>Windows client</td>
<td></td>
</tr>
<tr>
<td>- Windows 7 and SP1 (32- and 64-bit) - Enterprise and Ultimate</td>
<td></td>
</tr>
<tr>
<td>- Windows 8 and 8.1 (including updates) (32- and 64-bit) - Enterprise and Professional</td>
<td></td>
</tr>
<tr>
<td>- Windows 10 (32- and 64-bit)</td>
<td></td>
</tr>
<tr>
<td>- Windows To Go</td>
<td></td>
</tr>
<tr>
<td>- Windows Server 2012 and 2012 R2</td>
<td></td>
</tr>
</tbody>
</table>

Supported McAfee ePO versions

This release of McAfee Management of Native Encryption 4.0.0 is compatible with these McAfee ePO versions.

- McAfee ePO 5.1.0
- McAfee ePO 5.1.1
- McAfee ePO 5.1.2
- McAfee ePO 5.1.3
- McAfee ePO 5.3
- McAfee ePO 5.3.1

We don't guarantee that MNE 4.0.0 works with other versions of McAfee ePO.

For the latest information regarding supported environments, refer to the Supported Platforms, Environments, and Operating Systems for McAfee Management of Native Encryption KnowledgeBase article KB79375.
Installing the product

You need to install the MNE extensions and check in the software packages in to the master repository on the McAfee ePO server. A client deployment task is used to deploy the software package to client systems from the McAfee ePO server through McAfee ePO, allowing these client systems to be managed by McAfee ePO.

Once the packages are deployed, the Windows client system might require a restart to complete the installation. After the restart, the client communicates with the McAfee ePO server and manages BitLocker according to the policies configured. For the Mac client system, restart is not required after deployment and you can manage FileVault according to the policies configured.

Deploy McAfee Agent for Mac through SSH

You can deploy McAfee Agent for Mac to client systems through Secure Shell (SSH).

Before you begin

To deploy McAfee Agent for Mac to your system, you must enable SSH (remote login). SSH can be enabled on your Mac system by enabling the Remote Login option under System Preferences | Sharing | Remote Login.

Task

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click Menu | Systems | System Tree | Actions | New Systems.
3. Select the required option from How to add systems.
4. In the Systems to add field, type the NetBIOS name for each system, separated by commas, spaces, or line breaks. Alternatively, click Browse to select the systems.
5. Select Push agents and add systems to the current group (My Organization).
6. In the Target systems field, add the IP address of the system where you want to deploy the McAfee Agent.
7. In the Agent version field, select Non-Windows, then select McAfee Agent for Mac from the drop-down list.
8. In the Credentials for agent installation field, enter administrator credentials of the Mac.
9. Click OK to trigger the McAfee Agent deployment on the Mac system.

To view the deployment status, click Menu | Automation | Server Task Log.

Install the MNE and Help extensions

Install the product and Help extensions to the McAfee ePO server.

The MNE extension contains the policy settings and management features that are used to manage client system encryption products. The Help extension contains the Help content for the options in the user interface that appear when you click ? in the user interface.
**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Software | Extensions, then click Install Extension to open the Install Extension dialog box.
3. For each extension file, click Browse, select it, then click OK.
   You must install the extensions in this order:
   1. MNEADMIN-4.0.0.x.zip
   2. help_MNE_400.zip
   3. dpssp.zip
   
   **Info**
   Install the dpssp.zip extension to provide self recovery capabilities to users.

   4. mneadvancedfeatures.zip (only if you want to use the network unlock feature)
   5. EEGO.zip
   
   **Info**
   This extension is applicable only for Mac OS X systems.

The Install Extension page displays the extension name and version.

4. Click OK.

**Check in the MNE software packages**
The software package must be checked in to the master repository so that you can use McAfee ePO to deploy the software to your client systems.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Software | Master Repository, then click Actions | Check In Package.
3. From the Package type list, select Product or Update (.zip), then browse and select the MNE-OSX-4.0.0.x.zip software package for Mac systems or MNE-WIN-4.0.0.x.zip software package for Windows systems.

4. Click Next to open the Package Options page.
5. Click Save.

The new package appears in the Packages in Master Repository page under the respective branch in the repository.

**Deploy MNE to client systems**
Use this product deployment client task to deploy the product to your managed client systems.

For more information about performing this task, see the product documentation for your version of McAfee ePO. If you wish to deploy MNE without using McAfee ePO, please see a subsequent section on standalone installation.

For details about product features, usage, and best practices, click ? or Help.
**Task**

1. Log on to the McAfee ePO server as an administrator.

2. Click **Menu** | **Policy** | **Client Task Catalog**, select **McAfee Agent** | **Product Deployment** as **Client Task Types**, then click **Actions** | **New Task**.

3. Make sure that **Product Deployment** is selected, then click **OK**.

4. Type a name for the task and add any notes.

5. Next to **Target platforms**, select **Mac** or **Windows** for FileVault or BitLocker systems respectively.

6. Next to **Products and components** set the following:
   a. Select **McAfee Management of Native Encryption - FileVault 4.0.0.x.x.x** or **McAfee Management of Native Encryption - BitLocker 4.0.0.x.x.x** for FileVault or BitLocker systems respectively.
   b. Set the **Action** to **Install**, then select the **Language** of the package, and the **Branch**.
   c. Next to **Command line** type `ARPNOREMOVE=1` to allow administrators to prevent MNE uninstallation from Programs and Features under Control Panel. This option only greys out the **Uninstall** option in Control Panel. You can still uninstall the MNE product using the command line or third party tools.

7. Click **Menu** | **Systems** | **System Tree** | **Systems** tab, select the system where you want to deploy product, then click **Actions** | **Agent** | **Modify Tasks on a single system**.

8. Click **Actions** | **New Client Task Assignment** to open the **Client Task Assignment Builder** wizard.

9. On the **Select Task** page, select **Product** as **McAfee Agent** and **Task Type** as **Product Deployment**, then select **Management of Native Encryption - FileVault** for Mac systems or **Management of Native Encryption - BitLocker** for Windows systems.

10. Next to **Tags**, select the required platforms that you are deploying the packages to, then click **Next**:
   - **Send this task to all computers**
   - **Send this task to only computers that have the following criteria** — Use one of the edit links to configure the criteria.

11. On the **Schedule** page, select whether the schedule is enabled, specify the schedule details, then click **Next**.

12. On the **Summary** page, review the summary, then click **Save**.

**Send an agent wake-up call**

The client system gets the policy update whenever it connects to the McAfee ePO server during the agent-server communication. However, you can force an immediate update with an agent wake-up call.

**Task**

For details about product features, usage, and best practices, click **?** or **Help**.

1. Log on to the McAfee ePO server as an administrator.

2. Click **Menu** | **Systems** | **System Tree**, then select a system or a group of systems from the left pane.

3. Select the **System Name(s)** of that group.
4 Click Actions | Agent | Wake Up Agents.

5 Select a Wake-up call type and a Randomization period (0-60 minutes) to define the length of time when all systems must respond to the wake-up call.

6 Under Options, select Get full product properties.

7 Under Force policy update, select Force complete policy and task update.

8 Click OK.

To view the status of the agent wake-up call, navigate to Menu | Automation | Server Task Log.

**Turn on FileVault on a Mac client system**

You can turn on FileVault by enforcing the Turn On (Enable) FileVault policy on a Mac client system.

- The default MNE policy for FileVault enforces the Turn On (Enable) FileVault policy that enables FileVault on the Mac client system.

For Mac systems, once the MNE software package is deployed to the client system, the MNE client integrates with the user interface of McAfee Endpoint Protection for Mac 2.1.0 or McAfee Endpoint Protection for Mac 9.6.0, depending on what is already installed on that system. If neither product is available, the MNE deployment task installs the McAfee EPM 2.1.0 framework and MNE integrates into its user interface.

However, if the client system has McAfee EPM 2.0.0 or McAfee EPM 9.5.0 already installed, the user must upgrade it to McAfee EPM 2.1.0 or McAfee EPM 9.6.0 respectively, before installing MNE.

The user can see the status FileVault: Disabled on the user interface.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Policy | Policy Catalog, select Management of Native Encryption 4.0.0 from the Product drop-down list, then select FileVault Product Settings from the Category drop-down list.

3 Enable the Turn On (Enable) FileVault option.

You can also enable other policy options, as required. For more information, see the Product policies section.

4 Enable the Apply password content rules option, if required, to apply the password settings on to the client systems.

5 In the Display the following message, instead of the default, when enabling FileVault option, provide a message for the user to view on the client system when FileVault is enabled.

If you do not provide a message, the user will receive a pre-defined message on the client system.

6 Enable the Display the following login banner option, and provide a login banner for the user to view after authenticating into FileVault.

7 In the Display the following message when FileVault has been disabled by 3rd party application or user option, provide a message for the user to view on the client system when FileVault is disabled by anything other than MNE.

If you do not provide a message, the user will receive a pre-defined message on the client system.

8 Click Save.
Click Menu | Systems | System Tree | Systems tab, then select the group in the System Tree where the system belongs. The list of systems belonging to this group appears in the details pane.

Select a system, then click Actions | Agent | Modify Policies on a Single System.

Select McAfee Management of Native Encryption 4.0.0, then click Enforcing next to Enforcement status.

Select Break inheritance and assign the policy and settings below to change the enforcement status.

Next to Enforcement status, select Enforcing, then click Save.

Send an agent wake-up call.

The client system prompts for Restart now and Remind me later options. If the user clicks the Remind me later option, the notification will exit for the duration specified in the McAfee ePO policy and will re-appear again until the user restarts the system and enables FileVault by entering the password.

An Active Directory user cannot authenticate through the FileVault Pre-Boot Authentication screen if the password is changed. For more information, see the KnowledgeBase article KB81289.

FileVault is turned on, and the user can now see the status FileVault: Enabled on the user interface.

**Turn on BitLocker on a Windows client system**

You can turn on BitLocker by enforcing the Turn On (Enable) BitLocker policy on a Windows client system. For Windows systems, the BitLocker: Disabled status can be observed through the BitLocker option from Control Panel.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.

2. Click Menu | Policy | Policy Catalog, select Management of Native Encryption 4.0.0 from the Product drop-down list, then select BitLocker Product Settings from the Category drop-down list.

3. Enable the Manage BitLocker | Turn On (Enable) BitLocker option.

   You can also enable other policy options, as required. For more information, see the Product policies section.

4. Next to System authentication, enable the Use Trusted Platform Module (TPM) or Password (Windows 8 and above) option to protect the operating system volume for client systems accordingly.

5. Next to Authentication Settings, enter the minimum pin length and password length, if required.

6. Click Save.

7. Click Menu | Systems | System Tree | Systems tab, then select the group in the System Tree where the system belongs. The list of systems belonging to this group appears in the details pane.

8. Select a system, then click Actions | Agent | Modify Policies on a Single System.

9. Select McAfee Management of Native Encryption 4.0.0, then click Enforcing next to Enforcement status.

10. Select Break inheritance and assign the policy and settings below to change the enforcement status.
11 Next to Enforcement status, select Enforcing, then click Save.

The client system prompts for restart and remind later options. The user must restart the system and enter the password to authenticate.

12 Send an agent wake-up call.

BitLocker is turned on, and might request a password or PIN from the user depending on the policy selected.

### Standalone installation

Windows client users can simply install the .msi directly. Mac client users have an option of installing MNE on the client systems using the MNE-4.0.0.xxx.dmg package, which is provided by the administrator to client users along with user credentials. The standalone installer also installs or upgrades the older version of McAfee Agent to 4.8 Patch 2 HF972377 for Mac OS X on the system. Users can also configure client systems remotely into the McAfee ePO server using the McAfee ePO Remote Provisioning Tool. The McAfee ePO Remote Provisioning Tool works with McAfee Agent 4.8 Patch 2 HF972377, 4.8 Patch 3, or 5.0 for Mac OS X.

#### Before you begin

Make sure to note that this task must be performed by the user (who has admin rights) on a client system.

#### Task

For details about product features, usage, and best practices, click ? or Help.

1. Open the MNE-4.0.0.xxx.dmg package provided by the administrator.

   The MNE-4.0.0.xxx.pkg file opens.

2. Double-click the MNE-2.1.0.xxx.pkg file to open the Install McAfee Management of Native Encryption page.

3. Click Continue and Agree the License agreement.

4. Click Install, type the user's system password, and click Install Software.

   After the installation is complete, the McAfee ePO Remote Provisioning Tool app opens. The McAfee ePO Remote Provisioning Tool app is installed under Applications | Utilities directory. This app can be launched on demand to configure the Mac to the McAfee ePO server.

5. Type the ePO address, User name, and Password details provided by the administrator, then click Configure.

6. Type the user's system password on the prompt and click OK.

   The client system is successfully configured into the McAfee ePO server.

7. Click Close.

### Upgrading the Mac client systems to MNE 4.0.0

Use this high-level process to upgrade the Mac client systems from MNE 1.0.0, 2.0.0, 2.0.1, or 2.1.0 to MNE 4.0.0 using McAfee ePO.
Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Install or upgrade the required MNE 4.0.0 extensions to the McAfee ePO server. For more information, see the Install the MNE and Help extensions section.

3 Check in the MNE 4.0.0 FileVault package to the McAfee ePO server. For more information, see the Check in the MNE software packages section.

4 Create the Management of Native Encryption - FileVault product deployment task and apply it to the required client system that you want to upgrade. For more information, see the Deploy MNE to client systems section.

5 Send an agent-wake-up call to collect client's product properties to the McAfee ePO server.

Upgrading the Windows client systems to MNE 4.0.0

Use this high-level process to upgrade the Windows client systems from MNE 2.0.0, 2.0.1, 2.1.0, or 3.0.0 to MNE 4.0.0 using McAfee ePO.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the ePolicy Orchestrator server as an administrator.

2 Install or upgrade the required MNE 4.0.0 extensions to the McAfee ePO server. For more information, see the Install the MNE and Help extensions section.

3 Check in the MNE 4.0.0 BitLocker package to the McAfee ePO server. For more information, see the Check in the MNE software packages section.

4 Create the Management of Native Encryption - BitLocker product deployment task and apply it to the required client system that you want to upgrade. For more information, see the Deploy MNE to client systems section.

5 Send an agent-wake-up call to collect client's product properties to the McAfee ePO server.

Uninstalling the product

To uninstall MNE, you must perform the following tasks.

- Turn off FileVault (turning off BitLocker is not required prior to uninstallation)
- Remove MNE from the client using a McAfee ePO deployment task, or by uninstalling locally
- Remove MNE extensions and package

Note that recovery keys are not deleted when the MNE extension is removed.
Turn off FileVault

On the McAfee ePO console, you must modify the product setting policy to turn off FileVault. Make sure to note that you can turn off FileVault only if the client system is managed by McAfee ePO through MNE.

Task

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Systems | System Tree | Systems, then select a group under System Tree. All systems within this group (but not its subgroups) appear in the details pane.

3 Select a system, then click Actions | Agent | Modify Policies on a Single System to open the Policy Assignment page for that system.

4 From the Product drop-down list, select McAfee Management of Native Encryption 4.0.0. The policy Categories under MNE are listed with the system’s assigned policy.

5 Select the Product Setting policy category, then click Edit Assignments.

6 If the policy is inherited, select Break inheritance and assign the policy and settings below next to Inherit from.

7 From the Assigned policy drop-down list, select a product setting policy. From this location, you can edit the selected policy, or create a new policy.

8 Select whether to lock policy inheritance. Any system that inherit this policy can’t have another one assigned in its place.

9 Enable Manage FileVault | Turn Off (Disable) FileVault for FileVault users.

10 Click Save on the Policy Settings page, then click Save on the Product Settings page.

11 Send an agent wake-up call.

On turning off the FileVault policy, all the encrypted drives get decrypted, and the status become FileVault: Disabled. This can take a few hours depending on the number and size of the encrypted drives.

Remove MNE from the client using a McAfee ePO deployment task

Use this product deployment client task to remove the software package from the client system using McAfee ePO.

For more information about performing this task, see the product documentation for your version of McAfee ePO.

Task

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Policy | Client Task Catalog, select McAfee Agent | Product Deployment as Client Task Types, then click Actions | New Task.

3 Make sure that Product Deployment is selected, then click OK.

4 Type a name for the task and add any notes.
5 Next to Target platforms, select Mac or Windows as appropriate.

6 Next to Products and components set the following:
   a Select McAfee Management of Native Encryption 4.0.0.x.x.x to specify the version of the MNE package to be removed.
   b Set the Action to Remove.

7 Click Menu | Systems | System Tree | Systems tab, select the system where you want to remove the product, then click Actions | Agent | Modify Tasks on a single system.

8 Click Actions | New Client Task Assignment.

9 On the Select Task page, select Product as McAfee Agent and Task Type as Product Deployment, then select the task you created.

10 Next to Tags, select the desired platforms that you are removing the packages from, then click Next:
   • Send this task to all computers
   • Send this task to only computers that have the following criteria — Use one of the edit links to configure the criteria.

11 On the Schedule page, select whether the schedule is enabled, specify the schedule details, then click Next.

12 On the Summary page, review the summary, then click Save.

**Remove MNE and Help extensions**

You must remove MNE and the Help extensions from the McAfee ePO server to uninstall them from McAfee ePO.

You must remove the MNEADMIN_4.0.0.x.zip, help_MNE_400.zip, dpssp.zip, mneadvancedfeatures.zip, and EEAGO.zip extensions by following this procedure.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Software | Extensions, then select McAfee Management of Native Encryption 4.0.0. The Extension page appears with the extension name and version details.

3 Click Remove on the required extension. The Remove extension confirmation page appears.

4 Click OK to remove the extension.

The MNE tables are not dropped from the database when MNEAdmin is uninstalled. This is to prevent recovery keys from being accidentally deleted.

**Remove the MNE software package**

Remove the MNE software package using the following process.

**Before you begin**

Make sure that you turn off FileVault before removing the MNE software package on the Mac system from McAfee ePO. This step is not mandatory for BitLocker clients.

You need to remove the MNE-OSX-4.0.0.x.zip or MNE-WIN-4.0.0.x.zip software package as follows.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.

2. Click Menu | Software | Master Repository. The Packages in Master Repository page appears with the list of software packages and their details.

3. Click Delete next to the MNE software package.

4. Click OK to confirm.

Manually uninstall MNE from the client system
You can manually uninstall MNE from the client system, although McAfee ePO has all the required features for removing the product from the client system.

Before you begin
- You must have administrative privileges to perform this task.
- For Mac systems, make sure that you turn off the FileVault policy in McAfee ePO before uninstalling MNE manually.

Task
- a. For Mac systems, type this command sudo /usr/local/McAfee/uninstall MNE from the command-line. This removes the MNE software package from the client system.

- b. For Windows systems, click Windows | Control Panel | Uninstall a product to uninstall MNE.

You need not disable BitLocker to uninstall MNE.

Migrating from EEMac to MNE
You can migrate from EEMac to MNE on Mac client systems by following these steps.

1. Check that the minimum version of McAfee Agent for Mac is 4.8 or above on the client system. If not, deploy McAfee Agent for Mac 4.8 or above. For more information, see the Deploy McAfee Agent for Mac through SSH topic.

2. Deploy MNE to the client system with the appropriate policy setting. For more information, see the Deploy MNE to client systems topic.

3. Deactivate and uninstall EEMac. For more information, see McAfee Endpoint Encryption 7.0 Product Guide.

4. Monitor the progress of EEMac in the dashboard to confirm that it is uninstalled. After EEMac is uninstalled, MNE will automatically enable FileVault at the next policy enforcement. For more information, see the Enable FileVault on the client system topic.

MNE will not enable FileVault on the Mac client system if EEMac is installed and active.
Reporting FIPS status to client systems

The 140 series of Federal Information Processing Standards (FIPS) is a U.S. government computer security standard that specifies requirements for cryptography modules.

MNE checks the client systems for FIPS certification and reports whether the client systems are running in FIPS mode or not. For this to happen, the user must perform these tasks.

1. Make sure that the OS is running in FIPS mode. For Mac systems, install the FIPS Administration tools (http://support.apple.com/kb/HT5396). For Windows systems, refer the relevant Microsoft documentation.

2. Send an agent wake-up call.

MNE will automatically report the FIPS status back to McAfee ePO.

For Mountain Lion 10.8.4 or above Mac systems, the FIPS status is reported automatically to McAfee ePO by MNE, and the user does not have to install the FIPS Administration tools.

Run in FIPS mode

To run the client systems in FIPS mode, refer to the FileVault or BitLocker FIPS Security Policy for Mac and Windows client systems respectively.

**BitLocker systems**

For FIPS mode to be reported as active on a BitLocker-managed system, the client must be encrypted and managed by MNE with FIPS GPO set. If the client is already encrypted when MNE was installed (even if it was encrypted with FIPS mode), then MNE will report that the client system does not meet the FIPS requirements. This is because BitLocker FIPS Security policy states that:

- BitLocker can only be initialized by a Crypto Officer.
- BitLocker will only allow a Crypto Officer to perform key management operations.

In this case, the client has to be disabled, decrypted, and re-enabled using MNE under the control of the Crypto Officer for the system to be reported as FIPS compliant.

This Security Policy places restrictions on the use of BitLocker in FIPS mode. In particular, when running in FIPS mode, make sure to note that:

- only Cryptographic Officers are permitted to perform administrative BitLocker functions (such as recovery).
- on windows 7 systems, only 256-bit binary recovery keys are permitted; 48-digit numeric recovery keys are not permitted.

McAfee recommends that only Cryptographic Officers are given permission to perform MNE recoveries in McAfee ePO using the relevant MNE permission sets. When the Cryptographic Officer performs the recovery, a .bek file that contains the binary key must be requested from the MNE recovery page. This file must be securely transported to the required client system on a USB stick, before the Cryptographic Officer performs the recovery, as per BitLocker FIPS Security Policy. The self-service portal will not serve up the 256-bit binary recovery keys used in FIPS mode.
Managing policies

You can manage the MNE client systems from McAfee ePO through a combination of product policies. You assign policies to the required client systems to make sure that systems are managed and function as specified.

What is a policy?
A policy is a collection of settings that you create in McAfee ePO and assign it to the required MNE clients to make sure that client systems are configured and perform accordingly.

Are you configuring policies for the first time?
When configuring policies for the first time:

1. Plan product policies for different segments of your System Tree.
2. Create and assign policies to groups and systems.

To create, edit, and assign policies to systems or groups, refer to the product documentation for your version of McAfee ePO.

Contents
- Product policies
- Enforce MNE policies on a system
- Enforce policies to a group
Product policies

On the Policy Catalog page, the policies for Management of Native Encryption 4.0.0 appear under the FileVault Product Settings, BitLocker Product Settings, and Security Posture Report Settings categories.

Table 3-1  FileVault Product Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FileVault Management</td>
<td>Manage FileVault — Allows you to manage FileVault and receive reports from the client system.</td>
</tr>
<tr>
<td>• Turn On (Enable) FileVault</td>
<td>When enforced, will turn on FileVault on client systems if not already enabled and then manage accordingly. The client systems also report the status to McAfee ePO.</td>
</tr>
<tr>
<td>• Destroy FileVault key in standby mode</td>
<td>The FileVault recovery key will be removed from memory when a system goes into a standby mode. This defends against memory related attacks during various sleep states. Resuming from the sleep mode will force a user authentication to bring the key back into memory.</td>
</tr>
<tr>
<td>• Generate a new FileVault key in days __ (1-360)</td>
<td>Enable this option and specify how frequently the recovery key is to be rotated. This improves security by reducing the validity period of each individual recovery key.</td>
</tr>
<tr>
<td>• Allows users to import recovery key on client</td>
<td>Enable this option to allow users to import the recovery key on client systems. This is useful if end users use theFileVault application to generate new recovery keys.</td>
</tr>
<tr>
<td>• Prompt user to create a new recovery key on already enabled systems</td>
<td>If FileVault is already enabled by the user when MNE policy is enforced, the client system will prompt the user to authenticate using their FileVault password. Once authenticated, the recovery key of the client system can be queried from FileVault and will be escrowed to the McAfee ePO database.</td>
</tr>
<tr>
<td>• Only enable FileVault if DEGO tests pass</td>
<td>If the user has installed the Drive Encryption GO (DEGO) - OSX 2.1.0.xxx on the Mac client system, then FileVault will be enabled only if DEGO tests pass.</td>
</tr>
<tr>
<td>• Restart timeout period in minutes __ (1-60)</td>
<td>Defines the length of the restart timeout period.</td>
</tr>
<tr>
<td>• Turn Off (Disable) FileVault</td>
<td>When enforced, will turn off FileVault on client systems. Client systems status will continue to be reported in McAfee ePO.</td>
</tr>
<tr>
<td>• Do not manage FileVault</td>
<td>When enforced, MNE will not manage FileVault.</td>
</tr>
<tr>
<td>• Report client system status</td>
<td>When enforced, MNE will not manage FileVault, but will report FileVault status and security posture data to McAfee ePO allowing you to manage FileVault with a third party management tool, yet report status within McAfee ePO database.</td>
</tr>
</tbody>
</table>
Table 3-1  FileVault Product Settings (continued)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>McAfee ePO. This can be useful to report on BYOD (Bring Your Own Device) or contractor laptops to monitor compliance to company encryption policies. If FileVault is managed by MNE, or if report-only mode is selected, the client system reports the following information to McAfee ePO:</td>
<td></td>
</tr>
<tr>
<td>• FileVault status</td>
<td>System encryption status</td>
</tr>
<tr>
<td>• FileVault mode</td>
<td>FIPS status</td>
</tr>
<tr>
<td>• System information</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Password Settings</th>
<th>Apply password content rules — Allows you to set password settings on to OS X, which will enforce these password settings on the client system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Minimum length __ (4-40)</td>
<td>The user must create a password of the specified minimum length.</td>
</tr>
<tr>
<td>• Maximum length __ (4-255)</td>
<td>The user must create a password of the specified maximum length.</td>
</tr>
<tr>
<td>• Require at least one alphabetic character in password</td>
<td>The user must include at least one alphabetic character in creating the password.</td>
</tr>
<tr>
<td>• Require at least one numeric character in password</td>
<td>The user must include at least one numeric character in creating the password.</td>
</tr>
<tr>
<td>• Require password change after days __ (1-180)</td>
<td>The user must change the password after the specified number of days.</td>
</tr>
<tr>
<td>• Do not apply password content rules to these users (separate users with a semi-colon, for example, user1; user2)</td>
<td>Type the username (in short name) of users to make sure the password settings do not apply to the specified users.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client Messaging</th>
<th>Display the following message, instead of the default, when enabling FileVault — The user receives this message when FileVault is enabled. If left empty, a default message will be provided.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display the following login banner</td>
<td>Enable this option and provide a login banner for the user to receive this login banner after authenticating into FileVault.</td>
</tr>
<tr>
<td>Display the following message, instead of the default, when FileVault has been disabled by 3rd party application or user</td>
<td>The user receives this message if FileVault is disabled by anything other than MNE. If left empty, a default message will be provided.</td>
</tr>
<tr>
<td>Settings</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Show/Hide Advanced</td>
<td>Clicking this will show or hide advanced settings within the policy page. All policy options have suitable defaults for those that do not wish to define advanced settings.</td>
</tr>
<tr>
<td>BitLocker management</td>
<td>• <strong>Manage BitLocker</strong> — Allows you to manage BitLocker and receive reports from the client system.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Turn On (Enable) BitLocker</strong> — When enforced, will turn on BitLocker on client systems and manage accordingly. The client systems also report the status to McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AES-128</strong> — Configures BitLocker on client systems to use AES-128 algorithm for encryption.</td>
</tr>
<tr>
<td></td>
<td>• <strong>AES-256</strong> — Configures BitLocker on client systems to use AES-256 algorithm for encryption.</td>
</tr>
<tr>
<td></td>
<td>Make sure to note that the encryption strength cannot be changed on a previously encrypted client. To change the encryption strength, BitLocker needs to be decrypted, disabled, and then re-enabled by MNE.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Rotate recovery keys after a specified number of days __ (1-360)</strong> — Enable this option and specify how frequently the recovery key is to be rotated. This improves security by reducing the validity period of each individual recovery key.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Remove keys not added by Management of Native Encryption</strong> — Enable this option to remove any pre-existing keys for better security when MNE takes over management. This is useful for BYOD (Bring your Own Device) systems to make sure that any pre-existing non-MNE recovery keys are removed.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Turn Off (Disable) BitLocker</strong> — When enforced, will turn off BitLocker and decrypt client systems. However, the client systems report the status to McAfee ePO.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Do not manage BitLocker</strong> — When enforced, MNE will not manage BitLocker and receive BitLocker.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Report client system status</strong> — When enforced, MNE will not manage BitLocker, but will report BitLocker status and security posture data to McAfee ePO allowing you to manage BitLocker with a third party management tool, yet report status within McAfee ePO. This can be useful to report on BYOD (Bring Your Own Device) or contractor laptops to monitor compliance to company encryption policies.</td>
</tr>
<tr>
<td>If BitLocker is managed by MNE, or report-only mode is enabled, the client system reports the following information to McAfee ePO:</td>
<td>• BitLocker status</td>
</tr>
<tr>
<td></td>
<td>• BitLocker protection status</td>
</tr>
<tr>
<td></td>
<td>• BitLocker mode</td>
</tr>
<tr>
<td></td>
<td>• System information</td>
</tr>
<tr>
<td></td>
<td>• System encryption status</td>
</tr>
<tr>
<td></td>
<td>• FIPS status</td>
</tr>
</tbody>
</table>
Table 3-2  BitLocker Product Settings (continued)

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System authentication</td>
<td>• System authentication (V4) — This is applicable for systems installed with MNE 4.0 only.</td>
</tr>
<tr>
<td></td>
<td>• Use Trusted Platform Module (TPM) — Allows you to use the TPM authentication method to protect the operating system volume for TPM supported client systems.</td>
</tr>
<tr>
<td></td>
<td>• Also use PIN — Allows you to use a PIN number as an additional security for TPM supported client systems.</td>
</tr>
<tr>
<td></td>
<td>• Fall back to Password if no TPM is available (Windows 8 and above) — Allows you to use password authentication for client systems that do not support TPM.</td>
</tr>
<tr>
<td></td>
<td>If the Use Trusted Platform Module (TPM), Also use PIN, and Fall back to Password if no TPM is available (Windows 8 and above) options are all enabled and the current protector is the passphrase protector, then the client system is compliant to the policy.</td>
</tr>
<tr>
<td></td>
<td>• Password (Windows 8 and above) — Allows you to use password authentication to protect the operating system volume for client systems that are installed with Windows 8 or above.</td>
</tr>
<tr>
<td></td>
<td>If you enable this option, Windows 7 systems will automatically fall back to using TPM with PIN, as password is not supported for Windows 7 systems.</td>
</tr>
<tr>
<td></td>
<td>• Automatic (Network) — Data volumes will be encrypted and protected; they will automatically unlock when mounted if the server provides a key to do so. Access rules need to be defined in Server Settings in conjunction with this policy.</td>
</tr>
<tr>
<td></td>
<td>• Also encrypt OS volume with protection disabled — Allows you to encrypt the client system's operating system volume, although the protection mechanism is disabled. If this is left unchecked, the OS volume is not encrypted.</td>
</tr>
<tr>
<td></td>
<td>• System authentication (pre-V4) — This is applicable for systems installed with MNE 3.0 or below.</td>
</tr>
<tr>
<td></td>
<td>• Use Trusted Platform Module (TPM) — Allows you to use the TPM authentication method to protect the operating system volume for TPM supported client systems.</td>
</tr>
<tr>
<td></td>
<td>• Also use PIN — Allows you to use a PIN number as an additional security for TPM supported client systems.</td>
</tr>
<tr>
<td></td>
<td>• Fall back to Password if no TPM is available (Windows 8 and above) — Allows you to use password authentication for client systems that do not support TPM.</td>
</tr>
<tr>
<td></td>
<td>If the Use Trusted Platform Module (TPM), Also use PIN, and Fall back to Password if no TPM is available (Windows 8 and above) options are all enabled and the current protector is the passphrase protector, then the client system is compliant to the policy.</td>
</tr>
<tr>
<td></td>
<td>• Password (Windows 8 and above) — Allows you to use password authentication to protect the operating system volume for client systems that are installed with Windows 8 or above.</td>
</tr>
<tr>
<td></td>
<td>If you enable this option, Windows 7 systems will automatically fall back to using TPM with PIN, as password is not supported for Windows 7 systems.</td>
</tr>
<tr>
<td></td>
<td>The fixed volumes are encrypted and automatically unlocked when the operating system volume is unlocked.</td>
</tr>
<tr>
<td>Authentication</td>
<td>Minimum pin length __ (4-20) — Enter the minimum PIN length from 4 to 20 that you would like to set for the PIN number.</td>
</tr>
<tr>
<td>Settings</td>
<td>Minimum password length __ (8-99) — Enter the minimum password length from 8 to 99 that you would like to set for the password.</td>
</tr>
</tbody>
</table>
Table 3-2 BitLocker Product Settings (continued)

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>End user messaging</strong></td>
<td>Provide a custom URL for the BitLocker recovery screen in preboot (Windows 10 and above) — Enable this option to enter a custom URL that will appear in the pre-boot BitLocker recovery screen on Windows 10 systems. The user needs to copy this URL on a web page of another system for information about retrieving the recovery key.</td>
</tr>
<tr>
<td>Recovery URL</td>
<td>Enter the URL that will appear in the pre-boot BitLocker recovery screen.</td>
</tr>
<tr>
<td><strong>BitLocker advanced settings</strong></td>
<td>You can choose to enable, disable, or not manage the following options:</td>
</tr>
<tr>
<td>• Enable hardware test</td>
<td>Enable this option to perform hardware test for the required client systems before BitLocker starts protecting the system. The system will not start encrypting until a successful hardware test is completed. This makes sure that systems that do not support BitLocker because of hardware compatibility issues can be easily recovered after they fail to boot.</td>
</tr>
<tr>
<td>• Activate on platforms</td>
<td>Enable this option to allow activation on tablets, even when the slate/tablet reports that a keyboard is not available in pre-boot.</td>
</tr>
<tr>
<td>• Only encrypt used space</td>
<td>Allows you to encrypt only the used space of the volumes for client systems, significantly speeding up initial encryption. This is applicable for systems installed with Windows 8 or above. Sensitive data that was previously deleted from the file system may not be protected, as not all sectors are protected.</td>
</tr>
<tr>
<td>• Reduce restart delays</td>
<td>Improves restart performance by skipping key-zeroization during the restart process. This leaves systems more vulnerable to very sophisticated memory attacks.</td>
</tr>
<tr>
<td>• Re-measure TPM validation</td>
<td>After a BitLocker recovery, the system boot is re-measured using the TPM to ensure that it is current, therefore reducing the risk of reoccurrence of a recovery scenario caused by a boot measurement change.</td>
</tr>
<tr>
<td>• Deny write access</td>
<td>Enable this option to deny right access to fixed volumes for client systems that are not protected by BitLocker. This will prevent users from writing data to unprotected volumes until they are fully protected, thus improving data security.</td>
</tr>
<tr>
<td>• Require hardware-based</td>
<td>Enable this option to ensure that BitLocker will only activate with self-encrypting drives.</td>
</tr>
<tr>
<td>• Fallback to software-based</td>
<td>Enable this option to allow BitLocker to use software encryption if a self-encrypting drive is not available. Used in combination with the parent option, this allows a preference to be stated for self-encrypting drives.</td>
</tr>
</tbody>
</table>

Security posture reporting allows you to report the endpoints that meet your required security posture settings for your organization, and those that do not.

The security posture report settings allow you to define the criteria for securing endpoints. This policy has no effect on the management of the endpoint; it simply defines the tests that the endpoints should run to assure its security posture with respect to data protection.
Each specific posture test will pass unless there is a specific reason for failing. For example, a system without data volumes will pass all data volume tests, since there are no data volumes to fail. In other words, this reporting is primarily designed to report failures against specific criteria.

Table 3-3  Security Posture Report Settings

<table>
<thead>
<tr>
<th>Settings</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security posture reports apply to:</td>
<td>• OS Volume — Enable this option to test the OS volume against the selected criteria.</td>
</tr>
<tr>
<td></td>
<td>• Data Volume(s) — Enable this option to test data volumes against the selected criteria.</td>
</tr>
<tr>
<td></td>
<td>If the system doesn't have data volumes, the data volume tests will pass each of the posture tests.</td>
</tr>
<tr>
<td>Security posture reporting:</td>
<td>• Used space on selected volumes(s) should be fully encrypted (recommended) — Enable this option to report that the system is secure only if the used space on the selected volume types are fully encrypted.</td>
</tr>
<tr>
<td></td>
<td>• Selected volumes(s) require user, automatic (network), or TPM authentication (recommended) — Enable this option to report that the system is secure only if the selected volume types require user authentication, network unlock, or TPM authentication.</td>
</tr>
<tr>
<td></td>
<td>• Selected volume(s) should use a minimum encryption strength of: — Enable this option to report that the system is secure only if the selected volume types use at least:</td>
</tr>
<tr>
<td></td>
<td>• AES-128 — Can use AES-128 or AES-256.</td>
</tr>
<tr>
<td></td>
<td>Systems that are activated with higher strength Algorithm AES-256 and Security Posture set to Algorithm AES-128 displays as pass. Note that XTS mode encryption, introduced in Windows 10 November 2015 update, is currently not supported and will show as a failure against security posture.</td>
</tr>
<tr>
<td></td>
<td>• AES-256 — Must use AES-256.</td>
</tr>
<tr>
<td></td>
<td>• Selected volume(s) should be FIPS compliant — Enable this option to report that the system is secure only if the selected volume types are FIPS compliant.</td>
</tr>
<tr>
<td></td>
<td>(Note: Systems that were activated prior to being managed by MNE cannot be verified as FIPS compliant)</td>
</tr>
</tbody>
</table>

Enforce MNE policies on a system

Enable or disable policy enforcement on a client system. Policy enforcement is enabled by default, and is inherited in the System Tree.

For more information about performing this task, see the product documentation for your version of McAfee ePO.

Task

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Systems | System Tree | Systems tab, then under System Tree, select the group where the system belongs. The list of systems belonging to this group appears in the details pane.

3 Select a system, then click Actions | Agent | Modify Policies on a Single System.
Managing policies
Enforce policies to a group

4 Select McAfee Management of Native Encryption 4.0.0, then click Enforcing next to Enforcement status.

5 Select Break inheritance and assign the policy and settings below to change the enforcement status.

6 Next to Enforcement status, select Enforcing, then click Save.

After restarting, the client system communicates with the McAfee ePO server and pulls down the assigned MNE policies and encrypts the system according to the defined policies. The assigned user can be initialized through the Pre-Boot screen after the subsequent restart.

Enforce policies to a group

Enable or disable policy enforcement for a product on a System Tree group. Policy enforcement is enabled by default, and is inherited in the System Tree.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Systems | System Tree | Assigned Policies, then select a group in the System Tree.

3 From the Product drop-down list, select McAfee Management of Native Encryption 4.0.0, then click Enforcing next to Enforcement Status.

4 To change the enforcement status, select Break inheritance and assign the policy and settings below.

5 Next to Enforcement status, select Enforcing.

6 Select whether to lock policy inheritance so that groups and systems that inherit this policy can't break enforcement, then click Save.
Automatic network unlock

Automatic network unlock is a feature ideally suited for protecting servers. It can be used to automatically unlock fixed data volumes whilst they are on the corporate network and whilst server rules permit, and prevent unlock when not on the corporate network or when server rules deny access.

To enable network unlock, it's necessary to assign a suitable BitLocker product policy to the system (as described earlier in this guide), and also define access rules as discussed below.

When a Fixed volume is mounted, the MNE client software requests the unlock key from McAfee ePO. If a suitable access control rule has been provided, then McAfee ePO will release the unlock key to the client, which will unlock the Fixed volume. If no suitable rule can be found, or the rule denies access, then no key will be released by McAfee ePO and the Fixed volume will remain locked.

In this release, network unlock is available on Fixed volumes only. In order to avoid the need for any user authentication when the system is booted, OS volumes may be left unencrypted, or may be encrypted but with protection disabled.

Access rules can be defined on the Server Settings page. For more information, refer to the Automatic unlock of fixed volumes for client systems topic. This feature is applicable for endpoints installed with MNE 4.0 only.

For more information on setting network unlock polices, refer to the Product policies section.

Automatic unlock of fixed volumes for client systems

The administrator can define a selection of access control rules in the Server Settings page.

**Before you begin**

Make sure that you have installed the mneadvancedfeatures.zip extension into McAfee ePO. Installing this extension unlocks the network unlock feature.

Each separate rule applies to a system tree branch and all its children (via inheritance). Where a rule is explicitly defined for a system tree branch and its children, it supersedes any rule inherited by that branch, allowing complete flexibility in access rule specification.

By default, no systems in the entire system tree have network unlock granted. This is expressed by the path \My Organisation having a DENY rule applied. This is inherited by the entire tree.

Since it is preferable to GRANT network unlock permission only where necessary, ensure that your system tree is organized so that systems that require network unlock are separated into a separate branch.
Task
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Configuration | Server Settings.
3. On the left pane, select McAfee Management of Native Encryption, and click Edit to open the Edit McAfee Management of Native Encryption page.
4. Next to Automatic (network) unlock of volumes for system under, click Edit network rule, select whether you wish to grant or deny access for systems in this branch by selecting GRANTED or DENIED respectively, then click Apply.
5. Browse through the System Tree View, select the required system or group, and click OK.
6. Click Add rule, then click Save.
Managing client systems

System management allows you to import system information into McAfee ePO. This is useful in the process of installing MNE and viewing the list of FileVault or BitLocker users.

Client systems are managed by McAfee ePO through a combination of product policies. You can identify systems that require the same policy settings, and place them in a system group. This grouping allows you to update the policy settings to all systems in that group at the same time.

Contents
- Add a system to an existing group
- Move systems between groups
- System actions
- How to run the MER tool on Mac systems
- Maintenance mode on BitLocker systems

Add a system to an existing group

You can import systems from your neighborhood network to groups through McAfee ePO. You can also import a network domain or Active Directory container.

The client systems are automatically added to the System Tree in McAfee ePO on successful installation of the McAfee Agent for Mac.

For more information about performing this task, see the product documentation for your version of McAfee ePO.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the ePolicy Orchestrator server as an administrator.
2 Click Menu | Systems | System Tree, then click Actions | New Systems.
3 From How to add systems, select the required option.
4 In the Systems to add field, type the NetBIOS name for each system, separated by commas, spaces, or line breaks. Alternatively, click Browse to select the systems.
5 Select Push agents and add systems to the current group to enable automatic System Tree sorting. Do this to apply the sorting criteria to these systems.

Complete the following options:
<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent version</td>
<td>Select the agent version to deploy.</td>
</tr>
<tr>
<td>Installation path</td>
<td>Type the agent installation path or accept the default.</td>
</tr>
<tr>
<td>Credentials for agent installation</td>
<td>Type valid credentials to install the agent:</td>
</tr>
<tr>
<td></td>
<td>• Domain — Type the domain of the system.</td>
</tr>
<tr>
<td></td>
<td>• User name — Type the user name.</td>
</tr>
<tr>
<td></td>
<td>• Password — Type the password.</td>
</tr>
<tr>
<td>Number of attempts</td>
<td>Type an integer for the specified number of attempts, or use zero for continuous attempts.</td>
</tr>
<tr>
<td>Retry interval</td>
<td>Type the interval in number of seconds between two attempts.</td>
</tr>
<tr>
<td>Abort After</td>
<td>Type the number of minutes before stopping the connection.</td>
</tr>
<tr>
<td>Connect using (McAfee ePO 4.6) or Push Agent using (McAfee ePO 4.6)</td>
<td>Select the connection used for the deployment:</td>
</tr>
<tr>
<td></td>
<td>• Selected Agent Handler — Select the server from the list.</td>
</tr>
<tr>
<td></td>
<td>• All Agent Handlers</td>
</tr>
</tbody>
</table>

6. Click OK.

---

**Move systems between groups**

You can move systems from one group to another in the System Tree. You can also move systems from any page that displays a table of systems, including the results of a query.

In addition to the steps below, you can also drag-and-drop systems from the Systems table to any group in the System Tree.

Even if you have a perfectly organized System Tree that mirrors your network hierarchy and uses automated tasks and tools to regularly synchronize your System Tree, you might need to move systems manually between groups. For instance, you might need to periodically move systems from the Lost&Found group.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the ePolicy Orchestrator server as an administrator.
2. Click **Menu** | **Systems** | **System Tree** | **Systems**, then browse and select the systems.
3. Click **Actions** | **Directory Management** | **Move Systems**.
4. Select whether to enable or disable, or to not change the System Tree sorting on the selected systems when they are moved.
5. Select the group where you want to place the systems, then click **OK**.

---

**System actions**

Use system actions to perform actions like recovering MNE and importing the recovery key.

You can perform these tasks by navigating through **Menu** | **Systems** | **System Tree**, select the required system, then click **Actions** | **Management of Native Encryption**.
Table 5-1 System actions

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance report</td>
<td>You can view the report, system, and native encryption properties for the selected system.</td>
</tr>
<tr>
<td>Import FileVault recovery key</td>
<td>You can manually import the recovery key of the Mac systems to the McAfee ePO database using the Import FileVault recovery key by Machine Node page. For more information, see the Recovering systems section.</td>
</tr>
<tr>
<td>Management of Native Encryption Recovery</td>
<td>You can recover a system, if a user reports accessibility issues to that system. To recover a system, select the required system in the System Tree, then click Actions</td>
</tr>
</tbody>
</table>

How to run the MER tool on Mac systems

The Minimum Escalation Requirements (MER) tool is used to collect diagnostic data for MNE and operating system details of the client system. You can run the MER tool in two ways.

For Windows systems, we recommend that you refer the standard McAfeee MER tool.

How to run the MER tool on the Terminal application

You must run the MER tool on the Terminal application using the sudo privileges. After you authenticate, a diagnostic report log (McAfeeMERTool_xxx.zip) is created and located in your home directory.

`sudo /usr/local/McAfee/MSCMertool -s McAfeeMERTool`

How to run the MER tool using the McAfee EPM 2.1 interface

1. Open the McAfee Endpoint Protection for Mac 2.1 interface.
2. Navigate to Help | Run MER Tool to open the Terminal window.
3. Type the administrator password.

You see that a diagnostic report log (McAfeeMERTool_xxx.zip) is created under the user’s home directory.

Maintenance mode on BitLocker systems

This feature allows you to temporarily disable pre-boot authentication on BitLocker systems, in order to roll out Windows or software updates that may require a system reboot. To use this feature, the maintainancemode-x.x.x.x.exe file must be copied to the system, and executed with command-line parameters within the roll out scripts.

Maintenance mode will disable BitLocker protection on the system and all subsequent enforcement of MNE policy, until the specified number of reboots have occurred, or maintenance mode is explicitly cleared. Once cleared, BitLocker protection will be restored to its original state upon next local policy enforcement.
An API version is used to check whether the maintenance mode executable is compatible with the installed version of MNE. To test for compatibility, run the command `maintenancemode-x.x.x.x.exe --version` and check the output.

To restore BitLocker protection immediately, you can trigger a local policy enforcement from the McAfee Agent by calling `CmdAgent.exe`, within your script(s). For more information about using command line switches with `CmdAgent`, see the KnowledgeBase article KB52707.

The maintenance mode executable requires Administrator privileges to run.

**Examples**

For command-line options, run `maintenancemode-x.x.x.x.exe --help`.

- Enter maintenance mode, allowing for 3 reboots before maintenance mode is cleared: `maintenancemode-x.x.x.x.exe --number-of-reboots 3`
- Clear the maintenance mode: `maintenancemode-x.x.x.x.exe --clear`
- Obtain the version of the maintenance mode executable, and API versions: `maintenancemode-x.x.x.x.exe --version`
Managing MNE reports

MNE queries are configurable objects that retrieve and display data from the database. These queries can be displayed in charts and tables.

Any query results can be exported to a variety of formats, any of which can be downloaded or sent as an attachment to an email message. Most queries can be used as dashboard monitor.

Privacy and Data Protection Self-Service Portal (DPSSP) reports

Ensure that access to these reports is authorized and appropriately managed. DPSSP reports within ePO contain users’ login names, system names, IP addresses, and audit data. Please note that none of this information is transmitted externally to McAfee or other third-parties.

Contents

- Queries as dashboard monitors
- View the standard MNE reports
- Create MNE custom queries
- View the standard MNE dashboard
- Create custom MNE dashboard
- MNE client events

Queries as dashboard monitors

Most queries can be used as a dashboard monitor (except those using a table to display the initial results). Dashboard monitors are refreshed automatically on a user-configured interval (five minutes by default).

Exported results

MNE query results can be exported to four different formats. Exported results are historical data and are not refreshed like other monitors when used as dashboard monitors. Like query results and query-based monitors displayed in the console, you can drill down into the HTML exports for more detailed information.

Reports are available in several formats:

- CSV — Use the data in a spreadsheet application (for example, Microsoft Excel).
- XML — Transform the data for other purposes.
- HTML — View the exported results as a web page.
- PDF — Print the results.
You can run and view the standard MNE reports from the **Queries & Reports** page.

**Task**
For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click **Menu | Reporting | Queries & Reports**.
3. On the **Groups** pane, under the **McAfee Groups** category, select **Management of Native Encryption**.

You can view these standard reports:

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report data protection security posture</td>
<td>Displays the results of the data protection security posture check on MNE systems. This report can be used to identify and report those systems that do not meet the definition of a secure system.</td>
</tr>
<tr>
<td>Report native encryption Status</td>
<td>Displays the MNE status of the client systems.</td>
</tr>
<tr>
<td>Report overall encryption status</td>
<td>Displays the encryption status of the client systems.</td>
</tr>
<tr>
<td>Report policy compliance</td>
<td>Reports the level of policy compliance of MNE systems. This report can be used to identify systems that cannot or have not enforced the McAfee ePO policy correctly. For example, a system previously encrypted with AES-128 with an AES-256 policy cannot transition to AES-256, so will be out of compliance with the McAfee ePO policy.</td>
</tr>
<tr>
<td>Report policy compliance (rollup)</td>
<td>Reports the level of policy compliance of MNE systems (rollup).</td>
</tr>
<tr>
<td>Report product events</td>
<td>Displays the product related events for managing FileVault or BitLocker.</td>
</tr>
<tr>
<td>Report recovery keys</td>
<td>Displays the list of client systems with recovery information.</td>
</tr>
<tr>
<td>Reports users per machine</td>
<td>Displays the list of users assigned to a Mac client system, or who have logged on to Windows systems.</td>
</tr>
<tr>
<td>Report systems in maintenance mode</td>
<td>Displays the systems currently in maintenance mode, where BitLocker protection has been disabled.</td>
</tr>
<tr>
<td>Report systems pending key rotation</td>
<td>Displays the systems where key rotation is pending after a recovery has been performed on the system through MNE recovery pages or DPSSP (Data Protection Self-Service Portal).</td>
</tr>
<tr>
<td>Processed requests for automatic network unlock of volumes</td>
<td>Displays a list of all the unlock requests from systems that have network unlock enabled, and the state of the request.</td>
</tr>
</tbody>
</table>

4. From the **Queries** list, select the required query.
5. Click **Actions | Run**. The query results appear.

You can also edit or duplicate the query, and view the details.

6. Click **Options | Export Data**, make the required selections, then click **Export** to export the query data.
7 Click on the .xml link to open the query data or right-click and save the .xml file to the required location.

8 Click Close.

---

## Create MNE custom queries

You can create queries that retrieve and display the details like disk status, users, and product client events for MNE. With this wizard you can configure which data is retrieved and displayed, and how it is displayed.

### Task

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the MNE server as an administrator.

2 Click Menu | Reporting | Queries & Reports, then click Actions | New.

3 On the Feature Group pane, select Management of Native Encryption.

4 On the Result Types page, select the required query type, then click Next.

5 On the Chart page, from the Display Result As pane, select the type of chart or table to display the primary results of the query, then click Next.

   If you select Boolean Pie Chart, you must configure the criteria to include in the query.

6 On the Columns page, from the Available Columns pane, select the columns to be included in the query, then click Next.

   If you had selected Table on the Chart page, the columns you select here are the columns of that table. Otherwise, these are the columns that make up the query details table.

7 On the Filter page, from the Available Properties pane, select the required properties to narrow the search results, then click Run. The Unsaved Query page displays the results of the query, which is actionable, so you can take any available actions on items in any tables or drill-down tables.

   Selected properties appear in the content pane with operators that can specify criteria used to narrow the data that is returned for that property.

   - If the query didn’t appear to return the expected results, click Edit Query to go back to the Query Builder and edit the details of this query.

   - If you don’t need to save the query, click Close.

   - If this is a query you want to use again, click Save and continue to the next step.

8 On the Save Query page, type a name for the query, add any notes, and select one of the following:

   - **New Group** — Type the new group name and select either:
     - **Private (Private Groups)**
     - **Public (Shared Groups)**
   
   - **Existing Group** — Select the group from the list of Shared Groups.

9 Click Save.
View the standard MNE dashboard
You can view the standard MNE reports from the Dashboards page.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 From the Dashboard drop-down list, select MNE Dashboard.
   You can view the dashboard.

Tasks
• View the "Find MNE systems by user name" dashboard on page 42
  You can view the Find MNE systems by user name dashboard on the Dashboards page.

View the "Find MNE systems by user name" dashboard
You can view the Find MNE systems by user name dashboard on the Dashboards page.
The Find MNE systems by user name dashboard allows the administrator to enter a user name that will report all systems associated with that user.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 From the Dashboard drop-down list, select MNE Dashboard.

3 Type the name of the user and click GO.
   The administrator can now view all the systems associated with that user.

Create custom MNE dashboard
Dashboards are collections of user-selected and configured monitors that provide current data about your environment. You can create your own dashboards from query results or use McAfee ePO default dashboards.

Task
For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 From the Dashboard Actions drop-down list, select New.

3 Next to Dashboard Name, type a name for the dashboard.

4 Next to Dashboard Visibility, select one of these options, as required:
  • Private — To make the dashboard visible to a specific set of users.
  • Public — To make the dashboard visible to all the users.
  • Shared with the following permission set(s) — To make the dashboard visible to the specified permission set(s).
6 Click **Add Monitor**, select the **MNE query**, and drag and drop to the **MNE dashboard**.

---

**MNE client events**

While implementing and enforcing the MNE policies that control how sensitive data is encrypted, you can monitor real-time client events and generate reports using the MNE client events query.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>Event Description</th>
<th>Event Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>35203</td>
<td>This event is reported in McAfee ePO when the FileVault activation is failed with an error message <strong>OS X recovery partition is not found.</strong></td>
<td>Critical</td>
</tr>
<tr>
<td>35204</td>
<td>This event is reported in McAfee ePO when an incompatible product is found like McAfee Drive Encryption.</td>
<td>Informational</td>
</tr>
<tr>
<td>35205</td>
<td>This event is reported in McAfee ePO when FileVault or BitLocker activation is successful.</td>
<td>Informational</td>
</tr>
<tr>
<td>35206</td>
<td>This event is reported in McAfee ePO when the restart prompt appears on the client system.</td>
<td>Informational</td>
</tr>
<tr>
<td>35207</td>
<td>This event is reported in McAfee ePO when the FileVault or BitLocker activation is failed with an error message <strong>Unsupported operating system found.</strong></td>
<td>Critical</td>
</tr>
<tr>
<td>35208</td>
<td>This event is reported in McAfee ePO when FileVault activation is failed with an error message <strong>EEMac is active.</strong></td>
<td>Informational</td>
</tr>
<tr>
<td>35209</td>
<td>This event is reported in McAfee ePO when FileVault or BitLocker is already turned on in the client system.</td>
<td>Informational</td>
</tr>
<tr>
<td>35210</td>
<td>This event is reported in McAfee ePO when FileVault activation is failed with an error message <strong>Unable to retrieve the recovery key from FileVault.</strong></td>
<td>Error</td>
</tr>
<tr>
<td>35211</td>
<td>This event is reported in McAfee ePO when FileVault or BitLocker activation is failed with an error message <strong>Unknown exception occurred.</strong></td>
<td>Error</td>
</tr>
<tr>
<td>35212</td>
<td>This event is reported in McAfee ePO when the recovery key is sent to the McAfee ePO database successfully.</td>
<td>Informational</td>
</tr>
<tr>
<td>35213</td>
<td>This event is reported in McAfee ePO when the user is waiting for system to restart.</td>
<td>Informational</td>
</tr>
<tr>
<td>35214</td>
<td>This event is reported in McAfee ePO when MNE is running in Report and Manage mode.</td>
<td>Informational</td>
</tr>
<tr>
<td>35215</td>
<td>This event is reported in McAfee ePO when MNE is running in Report only mode.</td>
<td>Informational</td>
</tr>
<tr>
<td>35216</td>
<td>This event is reported in McAfee ePO when MNE is disabled.</td>
<td>High</td>
</tr>
<tr>
<td>35217</td>
<td>This event is reported in McAfee ePO when OS X login banner is applied.</td>
<td>Informational</td>
</tr>
<tr>
<td>35218</td>
<td>This event is reported in McAfee ePO when OS X login banner is removed.</td>
<td>Informational</td>
</tr>
<tr>
<td>35219</td>
<td>This event is reported in McAfee ePO when OS X password settings are applied.</td>
<td>Informational</td>
</tr>
<tr>
<td>35220</td>
<td>This event is reported in McAfee ePO when OS X password settings are disabled.</td>
<td>Critical</td>
</tr>
<tr>
<td>35221</td>
<td>This event is reported in McAfee ePO when disabling FileVault is failed as the recovery key is invalid, and the user must manually disable FileVault.</td>
<td>Error</td>
</tr>
<tr>
<td>35222</td>
<td>This event is reported in McAfee ePO when disabling FileVault is failed as the recovery key is unavailable, and the user must manually disable FileVault.</td>
<td>Error</td>
</tr>
<tr>
<td>Event ID</td>
<td>Event Description</td>
<td>Event Type</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
<td>------------</td>
</tr>
<tr>
<td>35223</td>
<td>This event is reported in McAfee ePO when the Mac serial number is not found.</td>
<td>Error</td>
</tr>
<tr>
<td>35224</td>
<td>This event is reported in McAfee ePO when the volume information is not available.</td>
<td>Error</td>
</tr>
<tr>
<td>35225</td>
<td>This event is reported in McAfee ePO when FileVault user information is sent.</td>
<td>Informational</td>
</tr>
<tr>
<td>35226</td>
<td>This event is reported in McAfee ePO when FileVault is disabled by third party application or user.</td>
<td>Critical</td>
</tr>
<tr>
<td>35227</td>
<td>This event is reported in McAfee ePO when the encryption is started.</td>
<td>Informational</td>
</tr>
<tr>
<td>35228</td>
<td>This event is reported in McAfee ePO when the encryption is completed.</td>
<td>Informational</td>
</tr>
<tr>
<td>35229</td>
<td>This event is reported in McAfee ePO when the decryption is started.</td>
<td>Informational</td>
</tr>
<tr>
<td>35230</td>
<td>This event is reported in McAfee ePO when the decryption is completed, and FileVault or BitLocker is disabled.</td>
<td>Informational</td>
</tr>
<tr>
<td>35231</td>
<td>This event is reported in McAfee ePO when the restart prompt fails to appear.</td>
<td>Error</td>
</tr>
<tr>
<td>35232</td>
<td>This event is reported in McAfee ePO when disabling FileVault or BitLocker fails.</td>
<td>Error</td>
</tr>
<tr>
<td>35233</td>
<td>This event is reported in McAfee ePO when a user is removed from FileVault.</td>
<td>Informational</td>
</tr>
<tr>
<td>35234</td>
<td>This event is reported in McAfee ePO when a user is failed to be removed from FileVault.</td>
<td>Error</td>
</tr>
<tr>
<td>35235</td>
<td>This event is reported in McAfee ePO when the user imports a FileVault recovery key.</td>
<td>Informational</td>
</tr>
<tr>
<td>35236</td>
<td>This event is reported in McAfee ePO when the user fails to import a FileVault recovery key since the key is invalid.</td>
<td>Informational</td>
</tr>
<tr>
<td>35238</td>
<td>This event is reported in McAfee ePO when the system is not compliant to MNE policy as the local policy changes have been made.</td>
<td>Critical</td>
</tr>
<tr>
<td>35239</td>
<td>This event is reported in McAfee ePO when the BitLocker GPO policy is overriding the MNE policy.</td>
<td>Critical</td>
</tr>
<tr>
<td>35240</td>
<td>This event is reported in McAfee ePO when BitLocker fails to activate as TPM is not available, or when changing from password to TPM policy, if TPM is not available, leaving the system in an unprotected state.</td>
<td>Error</td>
</tr>
<tr>
<td>35241</td>
<td>This event is reported in McAfee ePO when BitLocker fails to activate as TPM is not available and fails to fall back to password authentication on Windows 7 systems that do not support the password encryption method.</td>
<td>Error</td>
</tr>
<tr>
<td>35242</td>
<td>This event is reported in McAfee ePO when BitLocker fails to activate as the password policy is not supported on Windows 7 systems.</td>
<td>Error</td>
</tr>
<tr>
<td>35243</td>
<td>This event is reported in McAfee ePO when BitLocker fails to activate as TPMs PIN policy is not supported on Windows 7 systems.</td>
<td>Error</td>
</tr>
<tr>
<td>35244</td>
<td>This event is reported in McAfee ePO when the encryption algorithm strength used to encrypt the disk is weaker than the strength specified in the policy.</td>
<td>Warning</td>
</tr>
<tr>
<td>35245</td>
<td>This event is reported in McAfee ePO when the encryption algorithm strength used to encrypt the disk is stronger than the strength specified in the policy.</td>
<td>Warning</td>
</tr>
<tr>
<td>35246</td>
<td>This event is reported in McAfee ePO when TPM is not available and the client system has fallen back to password encryption method for authentication.</td>
<td>Informational</td>
</tr>
<tr>
<td>Event ID</td>
<td>Event Description</td>
<td>Event Type</td>
</tr>
<tr>
<td>----------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>35247</td>
<td>This event is reported in McAfee ePO when the client system has more than one user on the system while activating FileVault.</td>
<td>Informational</td>
</tr>
<tr>
<td>35248</td>
<td>This event is reported in McAfee ePO when the FileVault users have been successfully excluded from inheriting the password policy.</td>
<td>Informational</td>
</tr>
<tr>
<td>35249</td>
<td>This event is reported in McAfee ePO when excluding FileVault users fails from inheriting the password policy.</td>
<td>Error</td>
</tr>
<tr>
<td>35250</td>
<td>This event is reported in McAfee ePO when the recovery key is successfully regenerated on the client system.</td>
<td>Informational</td>
</tr>
<tr>
<td>35251</td>
<td>This event is reported in McAfee ePO when the recovery key fails to regenerate on the client system.</td>
<td>Critical</td>
</tr>
<tr>
<td>35252</td>
<td>This event is reported in McAfee ePO when BitLocker activation fails as SafeBoot or McAfee Drive Encryption is installed.</td>
<td>Critical</td>
</tr>
<tr>
<td>35253</td>
<td>This event is reported in McAfee ePO when FIPS mode activations fails on Windows 8 systems.</td>
<td>Critical</td>
</tr>
<tr>
<td>35254</td>
<td>This event is reported in McAfee ePO when password authentication is not supported on Windows 7 systems and falls back to TPM and PIN authentication method.</td>
<td>Informational</td>
</tr>
<tr>
<td>35255</td>
<td>This event is reported in McAfee ePO when MNE activation is refused due to failed hardware test.</td>
<td>Critical</td>
</tr>
<tr>
<td>35256</td>
<td>This event is reported in McAfee ePO when the hardware test is ignored as FIPS is enabled.</td>
<td>Critical</td>
</tr>
<tr>
<td>35257</td>
<td>This event is reported in McAfee ePO when the key rotation is successful.</td>
<td>Informational</td>
</tr>
<tr>
<td>35258</td>
<td>This event is reported in McAfee ePO when key rotation is failed as one or more key(s) failed to rotate.</td>
<td>Major</td>
</tr>
<tr>
<td>35259</td>
<td>This event is reported in McAfee ePO when the calculation of compliance to policy is failed. For more information, refer the client logs.</td>
<td>Critical</td>
</tr>
<tr>
<td>35260</td>
<td>This event is reported in McAfee ePO when there are no supported BitLocker volumes. For more information, see KB83141.</td>
<td>Major</td>
</tr>
<tr>
<td>35261</td>
<td>This event is reported in McAfee ePO when a keyboard is not detected for use in pre-boot environment for tablets/slates and the activation is failed.</td>
<td>Major</td>
</tr>
<tr>
<td>35262</td>
<td>This event is reported in McAfee ePO when the non-MNE recovery keys have been removed.</td>
<td>Informational</td>
</tr>
<tr>
<td>35263</td>
<td>This event is reported in McAfee ePO when the system fails to remove the non-MNE recovery keys.</td>
<td>Major</td>
</tr>
<tr>
<td>35264</td>
<td>This event is reported in McAfee ePO when key rotation is requested by McAfee ePO from the client system.</td>
<td>Informational</td>
</tr>
<tr>
<td>35265</td>
<td>This event is reported in McAfee ePO when the maintenance mode has been disabled successfully.</td>
<td>Informational</td>
</tr>
<tr>
<td>35266</td>
<td>This event is reported in McAfee ePO when the maintenance mode is currently active.</td>
<td>Informational</td>
</tr>
<tr>
<td>35267</td>
<td>This event is reported in McAfee ePO when the maintenance mode is failed to activate.</td>
<td>Major</td>
</tr>
<tr>
<td>35268</td>
<td>This event is reported in McAfee ePO when the maintenance mode has ended after the specified number of reboots.</td>
<td>Informational</td>
</tr>
<tr>
<td>35269</td>
<td>This event is reported in McAfee ePO when key rotation was only partially successful (some keys failed to rotate).</td>
<td>Informational</td>
</tr>
<tr>
<td>35270</td>
<td>This event is reported in McAfee ePO when a fixed volume was successfully unlocked using network unlock.</td>
<td>Informational</td>
</tr>
<tr>
<td>Event ID</td>
<td>Event Description</td>
<td>Event Type</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------</td>
<td>------------</td>
</tr>
<tr>
<td>35271</td>
<td>This event is reported in McAfee ePO when a fixed volume failed to successfully unlock using network unlock.</td>
<td>Major</td>
</tr>
<tr>
<td>35272</td>
<td>This event is reported in McAfee ePO when a network unlock key request failed to be queued.</td>
<td>Major</td>
</tr>
<tr>
<td>35273</td>
<td>This event is reported in McAfee ePO when a network unlock key request timed out.</td>
<td>Major</td>
</tr>
<tr>
<td>35274</td>
<td>This event is reported in McAfee ePO when a user successfully changed their password through the MNE user interface.</td>
<td>Informational</td>
</tr>
<tr>
<td>35275</td>
<td>This event is reported in McAfee ePO when a user successfully changed their PIN through the MNE user interface.</td>
<td>Informational</td>
</tr>
</tbody>
</table>
Recovering systems

System recovery is a process of recovering a user's system from system crashes, system malfunctions, accessibility issues, and more. If a user reports any such problems, you must provide the recovery key of the system to the user for the user to recover the system using FileVault recovery tools provided by Apple or BitLocker recovery tools provided by Microsoft.

We don't provide support for FileVault or BitLocker recovery tools. If you encounter any problems with this recovery process, we recommend that you contact Apple or Microsoft Support as appropriate.

How is the key escrowed in the McAfee ePO database?

The recovery key can be escrowed in two ways:

- When enabling FileVault or BitLocker on a client system using MNE, MNE obtains the recovery key of the system automatically and sends it to the McAfee ePO database.

- If FileVault has been previously enabled by the user at the point when MNE is installed on the client system, then either:
  - the system user must enter their FileVault password when prompted in order to grant MNE the right to the recovery key, or
  - the system user must import their FileVault recovery key on the system, or
  - the administrator must import the recovery key of the system manually into the McAfee ePO database in order for the recovery feature to be available for that system.

If none of these actions are taken, recovery will not be possible.

You can obtain the recovery key of a client system only if FileVault or BitLocker is managed by MNE.

How to obtain the serial number of a Mac system?

The serial number of the Mac system can be obtained in two ways:

- At the back/side/bottom of your Mac hardware, the serial number of the system is displayed.
- When you click the About this Mac option, the serial number of the system is displayed.
Import the recovery key

You might need to manually import the recovery key of a Mac client system to the McAfee ePO database using the System Tree or Data Protection menu. The client user can also import the recovery key to the McAfee ePO database from the client system.

These tasks must be performed only if FileVault has been previously enabled by the user.

This is not required for BitLocker systems.

**Import the recovery key using System Tree**

You must manually import the recovery key of the client system to the McAfee ePO database using the Import FileVault recovery key by Machine Node page.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Systems | System Tree | Systems tab, select the required system, then click Actions | Management of Native Encryption | Import FileVault recovery key to open the Import FileVault recovery key by Machine Node page.
3. In the Enter recovery key field, type the recovery key of the system that you obtained.
4. Click Ok.

**Import the recovery key using the Data Protection menu**

You must manually import the recovery key of the client system to the McAfee ePO database using the Import FileVault recovery key by serial number page.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Data Protection | Import FileVault recovery key to open the Import FileVault recovery key by serial number page.
3. In the Enter serial number field, type the serial number of the system that you received from the user.
4. In the Enter recovery key field, type the recovery key of the system that you obtained.
5. Click Ok.
**Import the recovery key from a client system**

Client users now have an option of importing the recovery key directly from the client system, installed with Mavericks operating system, to the McAfee ePO database.

**Before you begin**

- Make sure to note that this task must be performed by the client user on the client system.
- Make sure that the administrator has enabled the FileVault policy for the client system.
- Make sure that the administrator has enabled and enforced the **Allows users to import recovery key on client** policy on to the client system.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Open the MNE client interface on the client system.
2. On the left pane, click **Encryption**.
3. Enter the new recovery key below the **Recovery Key**.
4. Click **Apply**.

After the recovery key is escrowed to the McAfee ePO database, the last key import time is displayed on the **Encryption** pane.

The recovery key is successfully escrowed to the McAfee ePO database.

---

**Import the recovery key using the MNE command-line**

Client users now have an option of importing the recovery key directly from the client system, installed with Mavericks operating system or above, to the McAfee ePO database using the MNE CLI (Command-Line Interface) tool.

**Before you begin**

- Make sure to note that this task must be performed by the client user who has 'sudo' or 'root' privileges on the client system.
- Make sure that the administrator has enabled the FileVault policy for the client system.
- Make sure that the administrator has enabled and enforced the **Allows users to import recovery key on client** policy on to the client system.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Open the **Terminal.app** on the Mac client system.
2. Run the command: `sudo /usr/local/McAfee/MNE/bin/MNEMacTool -i xxxx-xxxx-xxxx-xxxx-xxxx`.

The recovery key is successfully escrowed to the McAfee ePO database.
Perform system recovery using McAfee ePO

If a user reports the system to be recovered, you must provide the recovery key of the system to the user for the user to recover the system using the Apple FileVault or Microsoft BitLocker recovery tools.

Note that FileVault provides a single recovery key per system. BitLocker provides one or more recovery keys per volume. If multiple recovery keys are available for a single volume (which may happen when MNE is installed on a previously encrypted system), then any of the recovery keys can be used to recover the volume.

Provide the recovery key to the user

You must provide the recovery key of the client system that is managed by McAfee ePO to the user for the user to recover the system using the Apple FileVault or Microsoft BitLocker recovery tools.

Task

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Data Protection | Management of Native Encryption recovery.

You can also access Management of Native Encryption recovery by navigating through Menu | Systems | System Tree | Systems tab, select the required system, then click Actions | Management of Native Encryption recovery.

3 On the Enter serial number (FileVault) or recovery key ID (BitLocker) page, type the serial number for FileVault systems or recovery key ID for BitLocker systems that you received from the user, then click Next.

This step is not applicable if you access Management of Native Encryption recovery through the System Tree menu, because the serial number or recovery key ID of the system is automatically populated. In this case, multiple keys might be displayed.

The recovery key(s) of the system appears on the Recovery key from serial number/ recovery key ID page.

4 Provide the recovery key to the user so that the user can recover the system.

For FileVault, the recovery key is always a string. For BitLocker in non-FIPS mode, the recovery key is always a string. For BitLocker in FIPS mode, the recovery key is always a file that must be downloaded and managed by Cryptographic Officers.

Once the user has received the recovery key, we recommend the user to contact Apple or Microsoft Support for assistance in recovering the client system.

MNE recovery key through scripting

MNE recovery keys can be retrieved from McAfee ePO using the McAfee ePO web API by passing the serial number, recovery key ID, or McAfee ePO leaf node.

How does scripting work?

Scripts using the Web API can be run from any computer that can connect to the ePolicy Orchestrator server. For security reasons, they should not be run on the same computer as the ePolicy Orchestrator server itself.

The Web API is used primarily for two purposes:

- Scripting sequences of tasks
- Performing simple tasks without using the user interface
MNE key recovery by serial number or recovery key ID

FileVault or BitLocker recovery keys can be retrieved from McAfee ePO using the `mc.mne.recoverMachine` command by passing the serial number of the system for FileVault systems or recovery key ID for BitLocker systems.

Note that this API is not available for systems running in FIPS mode. It will only display numeric keys, not binary file keys as are used in FIPS mode.

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mc.mne.recoverMachine</td>
<td><code>mc.mne.recoverMachine(serialNumber='&lt;&gt;', recoveryKeyID='&lt;&gt;')</code></td>
<td>Pass the serial number of the client system to retrieve the FileVault recovery key and recovery key ID to retrieve the BitLocker recovery key.</td>
</tr>
<tr>
<td></td>
<td>For example,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mc.mne.recoverMachine(serialNumber='12345')</code></td>
<td></td>
</tr>
</tbody>
</table>

MNE key recovery by McAfee ePO leaf node

FileVault or BitLocker recovery key can be retrieved from McAfee ePO using `mc.mne.recoverMachine` command by passing the McAfee ePO leaf node id number.

<table>
<thead>
<tr>
<th>Command</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mc.mne.recoverMachine</td>
<td><code>mc.mne.recoverMachine(epoLeafNodeId='&lt;&gt;')</code></td>
<td>Pass the McAfee ePO leaf node id to retrieve the FileVault or BitLocker recovery key for the client system.</td>
</tr>
<tr>
<td></td>
<td>For example,</td>
<td></td>
</tr>
<tr>
<td></td>
<td><code>mc.mne.recoverMachine(epoLeafNodeId='10')</code></td>
<td></td>
</tr>
</tbody>
</table>

Perform system recovery using the Data Protection Self Service Portal

The client user can obtain the recovery key for a client system using the Data Protection Self Service Portal (DPSSP), and perform system recovery using the Apple FileVault or Microsoft BitLocker recovery tools.

The administrator must first install the dpssp.zip extension in McAfee ePO, make the required DPSSP server settings. An authorized client user can open the DPSSP portal on a system, enter the serial number or recovery key ID for the FileVault or BitLocker system respectively, and obtain the recovery key.

The full DPSSP URL in displayed in Menu \ Configuration \ Server Settings \ DPSSP Settings.

The DPSSP URL will be of the general form `https://ePO_IP_address:Port_Number/dpssp/selfRecovery`.

- The DPSSP URL is displayed on the DPSSP policy page and can be copied into an email or other notification provided to users to identify the URL that can be used for recovery.
- If you have previously provided the URL to users based on port 8443, this URL will still work after upgrading to the latest version. However, it is recommended that users are provided with the revised URL using port 8444, as port 8443 is used by other McAfee ePO services. This is especially important in environments where there are significant number of client systems that could undertake recovery in response to some common problem affecting multiple systems.
Configure DPSSP server settings on McAfee ePO

The administrator must configure DPSSP server settings on the client system and enforce the settings on to the required client system to allow the user to obtain the recovery key on the client system using DPSSP.

**Before you begin**

Make sure that you have installed the dpssp.zip extension on the McAfee ePO server before performing this task.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.
2. Click Menu | Configuration | Server Settings.
3. On the left pane, select DPSSP Settings and click Edit to open the Edit DPSSP Settings page.
4. Enable the Self Service Portal option.
5. Next to ePO user, type the McAfee ePO user name.
   
   Make sure that the McAfee ePO user name that you enter has the permission to perform recovery operations in MNE. We recommend creating a specific McAfee ePO user for DPSSP recoveries, and limiting the permission set privileges to MNE recovery only.

   Next to Authentication, AD is selected by default as the Active Directory sever.
   
   Make sure to note that the administrator has selected the registered AD in McAfee ePO.

   Next to Logging, enable the Log authentication attempts and Log user activity options.

8. Next to Blocking, enable the Enable IP address blocking option, and perform the following operations:
   a. Block IP address after (failed logins) — Type the numeric value to block the IP address after the specified number of unsuccessful logon attempts.
   b. Unblock after (minutes) — Type the numeric value in minutes to unblock the respective IP address after the specified number of minutes.

9. Next to Blocking, enable the Enable user blocking option, and perform the following operations:
   a. Block user after (failed logins) — Type the numeric value to block the user after the specified number of unsuccessful logon attempts.
   b. Unblock after (minutes) — Type the numeric value in minutes to unblock the respective user after the specified number of minutes.

   If you either install the dpssp.zip extension or restart the McAfee ePO system, you cannot block or unblock users for 10 minutes.

   To instantly unblock a user, refer to the How to instantly unblock a user or IP address section.

Recovering systems

Perform system recovery using the Data Protection Self Service Portal
10 Next to Session, type the numeric value in minutes to log off the user’s session after the specified number of minutes.

11 Click Save.

**Enable the DPSSP permission set for unblocking users or IP addresses**

Enabling the DPSSP permission set allows you to remove users or IP addresses from the blocked list in the event of multiple failed logons (in the DPSSP portal) by users or IP addresses leading to being blocked.

To enable the DPSSP permission set for unblocking users or IP addresses, follow these steps:

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Click Menu | User Management | Permission Sets.

2 Next to the Data Protection Self Service Portal permission set, click Edit.

3 Next to the Data Protection Self Service Portal option, select Unblock users or IP addresses.

4 Click Save.

**How to instantly unblock a user or IP address**

To instantly unblock a user or IP address after the specified number of unsuccessful logon attempts, follow these steps:

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Log on to the McAfee ePO server as an administrator.

2 Click Menu | Reporting | Queries & Reports.

3 On the Groups pane, under McAfee Groups category, select Data Protection Self Service Portal.

4 Select the Blocked users or Blocked IP addresses query, click Actions | Run.

5 Select the required user or IP address, click Actions | Unblock users or IP addresses.

6 Click Yes when the system prompts Are you sure? to unblock the selected user or IP address.

**Obtain a recovery key on the client system using DPSSP**

When DPSSP is used for recovery with systems managed with MNE, the user must open the DPSSP portal, enter the serial number or recovery key ID for the FileVault or BitLocker system respectively, and obtain the recovery key.

**Before you begin**

Make sure to note that this task must be performed by the client user on the system.

The Data Protection Self-Service Portal (DPSSP) can now be used with both MNE 2.0.0 and later, and McAfee Drive Encryption 7.1 Patch 2 and later. In the event that both MNE and Drive Encryption are installed within the customer environment, the user is required to choose the product for which recovery is being requested.
**Task**

For details about product features, usage, and best practices, click ? or Help.

1. In the address bar of a web browser, enter the URL `https://<ePO IP address>:8444/dpssp/selfRecovery`, then press Enter to open the Data Protection Self Service Portal (DPSSP) page.

2. Select the required Language, type the domain user name prefixed with domain name, type the password, then click Login.

   - If you exceed the specified number of unsuccessful logon attempts as set in McAfee ePO, your user account will be blocked and you will see the message "Login failed." In that case, you must wait for the specified number of minutes as set in McAfee ePO to get your account unlocked.

   - Upon a successful login to DPSSP, if MNE and Drive Encryption are both installed in the environment managed by McAfee ePO, the user will need to select the appropriate product for which recovery information is required.

3. Type the serial number or recovery key ID of the FileVault or BitLocker system respectively, then click Get key.

4. Obtain the Recovery code to recover the system using the Apple FileVault or Microsoft BitLocker recovery tools.

   If the entered serial number or recovery key ID is not recognized, the user should check the value entered was correct and then contact the help desk. The help desk can then check the McAfee ePO User Audit log for more detailed information.

5. Click Logout.

**View the Data Protection Self Service Portal (DPSSP) reports**

You can run and view the standard DPSSP reports from the Queries & Reports page.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1. Log on to the McAfee ePO server as an administrator.

2. Click Menu | Reporting | Queries & Reports.
3 On the Groups pane, under the McAfee Groups category, select Data Protection Self Service Portal.

You can view these standard reports:

<table>
<thead>
<tr>
<th>Query</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Blocked IP addresses</td>
<td>Displays the IP addresses of client systems that are blocked.</td>
</tr>
<tr>
<td>Blocked users</td>
<td>Displays the list of users who are blocked.</td>
</tr>
<tr>
<td>Number of recoveries per point product in the last 24 hours</td>
<td>Displays the number of recoveries per point product in the last 24 hours.</td>
</tr>
<tr>
<td>Number of recoveries per point product in the last 30 days</td>
<td>Displays the number of recoveries per point product in the last 30 days.</td>
</tr>
<tr>
<td>Number of recoveries per user in the last 24 hours</td>
<td>Displays the number of recoveries per user in the last 24 hours.</td>
</tr>
<tr>
<td>Number of recoveries per user in the last 30 days</td>
<td>Displays the number of recoveries per user in the last 30 days.</td>
</tr>
</tbody>
</table>

4 From the Queries list, select the required query.

5 Click Actions | Run. The query results appear.

   You can also edit or duplicate the query, and view the details.

6 Click Options | Export Data, make the required selections, then click Export to export the query data.

7 Click on the .xml link to open the query data or right-click and save the .xml file to the required location.

8 Click Close.

---

Rotate recovery keys

You can enable rotating the recovery keys when the system recovery is performed through MNE recovery pages and DPSSP. Please note that there may be a delay of up to an hour before the server requests that the client rotates the keys.

**Task**

For details about product features, usage, and best practices, click ? or Help.

1 Click Menu | Configuration | Server Settings.

2 In the Setting Categories pane, click Management of Native Encryption, then click Edit to open the Edit Management of Native Encryption page.

3 Enable the options as follows:
   a Recovery is performed through MNE recovery pages — Enable this option to rotate the recovery keys when the recovery is performed through MNE recovery pages.
   b Recovery is performed through DPSSP — Enable this option to rotate the recovery keys when the recovery is performed through DPSSP.

   Note: Key rotation following recovery is not available on OS X systems.

4 Click Save.
Recovering systems

Rotate recovery keys
Index

A
about this guide 5
agent wake-up call, sending 16

C
client events, viewing 40
client systems
  actions 36
  adding and importing 35
  managing 35
  moving 36
  recovering 47, 50
client, MNE
  deactivating 21
  installing 11, 14
  migrating 23
  uninstalling 23
conventions and icons used in this guide 5

D
dashboards, MNE
  creating 42
  viewing 42
disk status
  reporting 40
documentation
  audience for this guide 5
  product-specific, finding 6
  typographical conventions and icons 5

E
extensions, MNE
  installing 14
  removing 22
  uninstalling 20

F
features
  FileVault recovery 8
  management of FileVault or BitLocker 8
  password policy enforcement 8
  reporting 8

I
installation
  MNE extensions 14

M
managed platform, supported versions 13
McAfee Agent for Mac, downloading and deploying 14
McAfee ServicePortal, accessing 6
MER tool, using 37
MNE
  removing 20

P
packages, installing
  MNE 15
policies
  categories 26
  disabling 20
  enforcing 31, 32
  managing 25
product components
  client system 7
  extensions 7
  McAfee ePO 7
  policies 7
  software packages 7
product setting policy
  disabling 21
product version, reporting 40

Q
queries, MNE
  creating 41
  dashboard monitor 39
  running 40

R
reports, MNE
  exporting results 39
  managing 39
  viewing 40
requirements, MNE 12
Index

S
ServicePortal, finding product documentation 6
software package, MNE
    removing 20–22
software packages, MNE
    checking in 15
    deploying 15
    supported management platform versions 13

T
technical support, finding product information 6

U
users
    reporting 40

V
volume status, reporting 40